СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ В ВИРТУАЛЬНЫХ ИНФРАСТРУКТУРАХ

DALLAS LOCK

СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ **В ВИРТУАЛЬНЫХ ИНФРАСТРУКТУРАХ**

ЛАБОРАТОРНЫЙ ПРАКТИКУМ

КОНФИДЕНТ®
ЦЕНТР ЗАЩИТЫ ИНФОРМАЦИИ

ФИЛАТОВ Н. В.

САНКТ – ПЕТЕРБУРГ, 2023

СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ В ВИРТУАЛЬНЫХ ИНФРАСТРУКТУРАХ

DALLAS LOCK

ОГЛАВЛЕНИЕ

Термины и сокращения 1
Введение 1
1. Назначение и возможности системы защиты 2
1.1 Общее описание 2
1.2 Структура и составные модули 2
1.3 Возможности СЗИ ВИ Dallas Lock 3
2. Лабораторный практикум 5
2.1 Лабораторная работа №1 5
2.2 Лабораторная работа № 2 13
2.3 Лабораторная работа № 3 16
3. Литература 19

ТЕРМИНЫ И СОКРАЩЕНИЯ

АРМ - автоматизированное рабочее место
ВИ - виртуальная инфраструктура
ВМ - виртуальная машина
Гипервизор - программа или аппаратная схема, обеспечивающая или позволяющая одновременное, параллельное выполнение нескольких или даже многих операционных систем на одном и том же хост-компьютере
КЦ - контроль целостности
ОС - операционная система
KVM - Kernel-based Virtual Machine, программное решение, обеспечивающее виртуализацию в среде Linux на платформе x86, которая поддерживает виртуализацию на базе Intel VT (Virtualization Technology) либо AMD SVM (Secure Virtual Machine)

ВВЕДЕНИЕ

Данное пособие предназначено для рассмотрения теоретических вопросов и при-обретения практических навыков использования сертифицированного ФСТЭК России решения – программного продукта «Система защиты информации в виртуальных инфраструктурах «Dallas Lock».

Документ включает в себя 3 лабораторных работы, в которых рассматривается назначение и возможности системы защиты информации в виртуальных инфраструктурах Dallas Lock.

Пособие может использоваться в учебных учреждениях для обучения студентов по направлению УГСНП «Информационная безопасность», в целях рассмотрения теоретических аспектов и приобретения практических навыков настройки и эксплуатации СЗИ ВИ Dallas Lock.

Для выполнения заданий потребуется следующее программное обеспечение:

1. Демонстрационная или коммерческая версия СЗИ ВИ Dallas Lock редакций «Стандартная» или «Расширенная».
2. Пакет офисных программ Open Office или MS Office.
3. Программа для поиска остаточной информации, в данном примере будет использоваться комплекс Сканер-ВС Инспектор.

Для выполнения лабораторных работ потребуется 3 АРМ/ВМ:

- 1 АРМ/ВМ для установки СЗИ ВИ «Dallas Lock» (АРМ1).
- 1 или 2 АРМ/ВМ для системы управления виртуализацией на базе oVirt (zVirt, РЕД Виртуализация, HOSTVM) в соответствии с эксплуатационной документацией и методом развертывания СВ (АРМ2).
  - 3 ВМ внутри инфраструктуры oVirt (test1, test2, test3).
- 1 АРМ/ВМ для проверки работы СЗИ ВИ «Dallas Lock» (АРМ3).

1. НАЗНАЧЕНИЕ И ВОЗМОЖНОСТИ СИСТЕМЫ ЗАЩИТЫ

1.1 ОБЩЕЕ ОПИСАНИЕ

СЗИ ВИ Dallas Lock — система защиты информации в виртуальных инфраструктурах, которая предназначена для защиты среды виртуализации на базе технологий VMware vSphere (vCenter for Windows 5.5, 6.0, 6.5, 6.7 и vCSA 6.5, 6.7, 7.0 совместно с ESXi[1] аналогичной версии), Windows Server (Hyper-V) (версий 2012, 2012 R2, 2016, 2019, 2022), oVirt 4.4, zVirt 3.0, HOSTVM, РЕД Виртуализация 7.3 и KVM (использующей библиотеки libvirt (версии не ниже 4.5.0) в качестве инструмента управления гипервизором) от несанкционированного доступа при работе в многопользовательских автоматизированных системах (АС), государственных информационных системах (ГИС), в автоматизированных системах управления (АСУ), информационных системах персональных данных (ИСПДн) и при защите значимых объектов критической информационной инфраструктуры (КИИ).

1.2 СТРУКТУРА И СОСТАВНЫЕ МОДУЛИ

СЗИ ВИ Dallas Lock состоит из следующих основных компонентов:

1) Ядро СЗИ ВИ.
2) Подсистема управления пользователями.
3) Подсистема управления доступом.
4) Подсистема гарантированной очистки памяти.
5) Подсистема контроля целостности.
6) Подсистема администрирования.
7) Подсистема восстановления после сбоев.
8) Подсистема фильтрации трафика.
9) Подсистема аудита.
10) Подсистема развертывания (установочные модули).

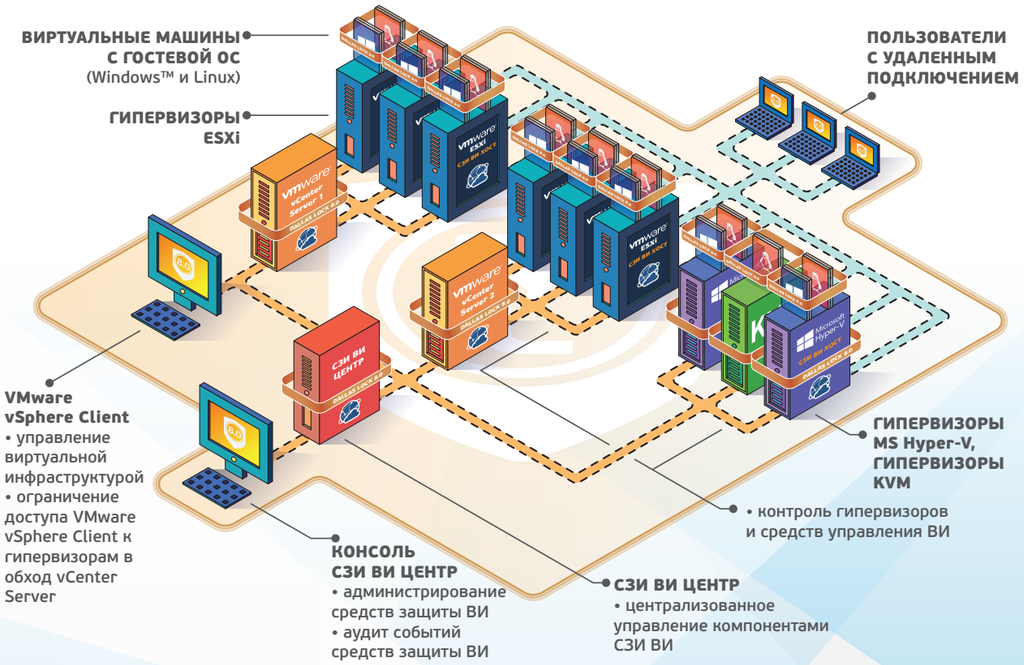

Рисунок 1. Компоненты СЗИ ВИ

1. Для защиты среды виртуализации на базе гипервизора ESXi 5.5 необходимо применять сертифицированную версию изделия СЗИ ВИ Dallas Lock 376.3. С назначением, возможностями и требованиями к данной версии можно ознакомиться в документе «Руководство по эксплуатации» ИК1.

1. Ядро системы защиты информации в виртуальных инфраструктурах.
Обеспечивает централизованное управление объектами виртуальной инфраструктуры. Взаимодействует с защитными подсистемами ниже.
2. Подсистема управления пользователями.
Обеспечивает идентификацию и аутентификацию локальных, доменных, терми-нальных и удаленных пользователей на этапе входа в операционную систему. А также осуществляет работу с различными типами аппаратных идентификаторов.
3. Подсистема управления доступом.
Обеспечивает управление доступом к файловой системе, реестру, устройствам, в том числе дискреционное разграничение доступа.
4. Подсистема гарантированной очистки памяти.
Подсистема осуществляет очистку остаточной информации для гарантии предотвращения восстановления удаленных данных.
5. Подсистема контроля целостности.
Обеспечивает возможность контролировать целостность программно-аппаратной среды компьютера, целостность объектов файловой системы и реестра, а также восстанавливать файлы и ветки реестры в случае обнаружения нарушенной целостности.
6. Подсистема администрирования.
Обеспечивает возможности по управлению ОО, аудиту и настройке параметров, просмотру, фильтрации и очистке журналов. Также в подсистему администрирования входит управление конфигурацией СЗИ и режимами работы.
7. Подсистема восстановления после сбоев.
Обеспечивает аварийное восстановление системы в целом и подсистем.
8. Подсистема фильтрации трафика.
Обеспечивает защиту рабочих станций и серверов от несанкционированного доступа посредством осуществления контроля и фильтрации, проходящих через сетевые интерфейсы ПК сетевых пакетов в соответствии с заданными правилами.
9. Подсистема аудита.
Обеспечивает ведение аудита и хранение информации о событиях в журналах.
10.Подсистема развертывания.
Обеспечивает установку агентов и консоли управления СЗИ ВИ.

1.3 ВОЗМОЖНОСТИ СЗИ ВИ DALLAS LOCK

1. СЗИ ВИ обеспечивает идентификацию и аутентификацию администраторов и пользователей в виртуальной среде по идентификатору и паролю условно-постоянного действия – на ЦУ СЗИ ВИ, серверах виртуализации vCenter, vCSA, oVirt, zVirt, HOSTVM, РЕД Вирт и гипервизорах Hyper V, KVM, oVirt, zVirt, HOSTVM и РЕД Вирт.
2. СЗИ ВИ обеспечивает контроль и аудит входа в среду VMware vSphere через механизм SSO.
3. СЗИ ВИ позволяет использовать в качестве средства опознавания пользователей ОС Windows следующие электронные идентификаторы:
- USB-Flash накопители;
- электронные ключи Touch Memory (iButton);
- HID Proximity-карты;
- USB-ключи Aladdin eToken Pro/Java;
- смарт-карты Aladdin eToken Pro/SC;
- USB-ключи и смарт-карты Рутокен (Rutoken) и Рутокен ЭЦП;
- USB-ключи и смарт-карты JaCarta;
- USB-ключи и смарт-карты ESMART;
- NFC-метки и смарт-карты семейства MIFARE.

4. В соответствии со своим назначением СЗИ ВИ запрещает доступ к защищаемым ресурсам не идентифицированных пользователей и пользователей, подлинность идентификации которых при аутентификации не подтвердилась.

5. СЗИ ВИ обеспечивает управление средствами аутентификации, в том числе хранение, выдача и инициализация всех компонент защищаемой виртуальной инфраструктуры. Также осуществляется блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации для ЦУ СЗИ ВИ, СВ vCenter, СВ oVirt, СВ zVirt, СВ HOSTVM, СВ РЕД Вирт и гипервизоров Hyper V, KVM, oVirt, zVirt, HOSTVM и РЕД Вирт.
6. Для решения проблемы «простых паролей» СЗИ ВИ имеет гибкие настройки сложности паролей. Можно задать минимальную длину пароля, необходимость обязательного наличия в пароле цифр, специальных символов, строчных и прописных букв, степень отличия нового пароля от старого и срок действия.
7. В СЗИ ВИ реализована система контроля целостности параметров ТС. Для контроля целостности используются контрольные суммы, вычисленные по одному из алгоритмов на выбор: CRC32, MD5. Кроме того, СЗИ ВИ выполняет периодический контроль целостности ВМ.
8. СЗИ ВИ позволяет производить настройку правил фильтрации сетевого трафика гипервизора ESXi.
9. СЗИ ВИ в рамках поддержки требований безопасности для финансовых организаций в соответствии с ГОСТ Р 57580.1-2017 обеспечивает выполнение следующих требований[2]:
- Создание сегмента безопасности в полуавтоматическом режиме с доступом только для одного пользователя к выбранной ВМ.
- Контроль сессий пользователей ВМ при работе с консолей осуществляется централизовано из Консоли ЦУ СЗИ ВИ.
- Разделение виртуальной инфраструктуры vSphere и Hyper-V на сегменты безопасности, состоящие из ВМ и учетных записей/групп учетных записей, ограничивая сетевое взаимодействие между сегментами посредством технологии VLAN.
- Проверка целостности настроек параметров безопасности ВМ при ее запуске.

10. В СЗИ ВИ реализовано разграничение доступа к компонентам виртуальной инфраструктуры – к ЦУ СЗИ ВИ, СВ vCenter, СВ oVirt, СВ zVirt, СВ HOSTVM, СВ РЕД Вирт и гипервизорам Hyper V, KVM, oVirt, zVirt, HOSTVM и РЕД Вирт. Разграничение доступа к гипервизорам ESXi и файлам виртуальных машин реализуется в пределах ролевой модели разграничения доступа VMware vSphere 6.0/6.5/6.7/7.0. Разграничение доступа к гипервизорам Hyper V и файлам виртуальных машин реализуется в пределах ролевой модели разграничения доступа Hyper V. Разграничение доступа к гипервизорам KVM и файлам виртуальных машин реализуется в пределах ролевой модели разграничения доступа KVM. Разграничение доступа к СВ oVirt, zVirt, HOSTVM, РЕД Вирт и гипервизорам oVirt, zVirt, HOSTVM, РЕД Вирт и файлам виртуальных машин реализуется в пределах ролевой модели разграничения доступа oVirt, zVirt, HOSTVM, РЕД Вирт соответственно.
11. Средствами СЗИ ВИ обеспечивается контроль доступа к операциям, выполняемым с помощью средств управления виртуальными машинами, в том числе к операциям создания, запуска, остановки, создания копий, удаления виртуальных машин, которые должны быть разрешены только назначенным пользователям.
12. СЗИ ВИ обеспечивает разграничение доступа по дискреционному принципу к объектам файловой системы и устройствам в виртуальной среде – на ЦУ СЗИ ВИ, СВ vCenter и гипервизорах Hyper V. Разграничение доступа к гипервизорам ESXi и файлам виртуальных машин реализуется в пределах ролевой модели разграничения доступа vSphere 6.0/6.5/6.7/7.0. Разграничение доступа к гипервизорам KVM и файлам виртуальных машин реализуется в пределах ролевой модели разграничения доступа KVM. Разграничение доступа к СВ oVirt, zVirt, HOSTVM, РЕД Вирт и гипервизорам oVirt, zVirt, HOSTVM, РЕД Вирт и файлам виртуальных машин реализуется в пределах ролевой модели разграничения доступа oVirt, zVirt, HOSTVM, РЕД Вирт соответственно.
13. При первоначальном назначении или при перераспределении внешней памяти СЗИ ВИ Dallas Lock предотвращает доступ субъекту к остаточной информации. Осуществляется очистка освобождаемых областей оперативной памяти ТС, освобождаемых областей памяти внешних накопителей. Очистка осуществляется однократной произвольной записью в освобождаемую область памяти, ранее использованную для хранения защищаемых данных (файлов). На гипервизорах ESXi, oVirt, zVirt, HOSTVM и РЕД Вирт осуществляется очистка остаточной информации по отношению к дискам виртуальных машин.
14. СЗИ ВИ позволяет создавать снапшоты как в ручном режиме, так и в автоматическом (по расписанию и/или с заданным интервалом) на платформах виртуализации vSphere и Hyper-V.
15. В СЗИ ВИ реализовано ведение журналов:
- Журнал ЦУ СЗИ ВИ. В журнал заносятся события, связанные непосредственно с работой ЦУ СЗИ ВИ.
- Журнал событий ВИ vSphere. Журнал событий ВИ содержит информацию об операциях над контролируемыми объектами на СВ, поступающую от агентов DL vCenter for Windows, DL vCSA.
- Журнал событий ВИ Hyper V. Журнал событий ВИ содержит информацию об операциях над контролируемыми объектами на СВ, поступающую от агента DL Hyper V.
- Журнал событий ВИ KVM/oVirt/zVirt/HOSTVM/РЕД Вирт. Журнал событий ВИ содержит информацию об операциях над контролируемыми объектами на СВ, поступающую от агента DL KVM и DL Engine.
- Журнал сервера виртуализации vCenter. Журнал содержит информацию об изменениях состояния управляемых объектов на СВ vCenter. События включают в себя действия системы и пользователей, которые происходят на объектах ВИ.
- Журнал сервера виртуализации Hyper V. Журнал содержит информацию об изменениях состояния управляемых объектов на СВ Hyper V. События включают в себя действия системы и пользователей, которые происходят на объектах ВИ.
- Журнал сервера виртуализации KVM. Журнал содержит информацию об изменениях состояния

2. Данные требования реализованы для среды виртуализации vSphere и Hyper-V.

управляемых объектов на СВ KVM. События включают в себя действия системы и пользователей, которые происходят на объектах ВИ.

- Системный журнал сервера виртуализации KVM. Журнал содержит информацию о работе операционной системы.
- Журнал сервера виртуализации oVirt/zVirt/HOSTVM/РЕД Вирт. Журнал содержит информацию об изменениях состояния управляемых объектов на СВ oVirt/zVirt/HOSTVM/РЕД Вирт. События включают в себя действия системы и пользователей, которые происходят на объектах ВИ.
- Системный журнал сервера виртуализации oVirt/zVirt/HOSTVM/РЕД Вирт. Журнал содержит информацию о работе операционной системы.
- Системный журнал гипервизора oVirt/zVirt/HOSTVM/РЕД Вирт. Журнал содержит информацию о работе операционной системы.
- Журнал гипервизора ESXi. В журнале регистрируются события безопасности гипервизора ESXi, на котором установлен агент DL. Журнал включает в себя системные события и действия агента DL на гипервизоре ESXi.
- Журнал Сервера УД. Данный журнал содержит информацию о событиях, происходящих на подключенных клиентах.
- Журналы, которые ведутся отдельно на каждом АУД ОС Windows: журнал входов, журнал управления учетными записями, журнал ресурсов, журнал управления политиками, журнал процессов, журнал пакетов МЭ.

16. Для облегчения работы с журналами есть возможность фильтрации записей по определенному признаку и экспортирования журналов в различные форматы. При переполнении журнала, а также по команде администратора, его содержимое архивируется и помещается в специальную папку, доступ к которой есть, в том числе и через средства удаленного администрирования. Этим обеспечивается непрерывность ведения журналов.

17. В СЗИ ВИ возможно использование предустановленных шаблонов типовых политик безопасности на основе требований следующих документов:

- Руководящий документ. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации (утвержден решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.) (АС).
- ГОСТ Р 56938-2016. Защита информации. Защита информации при использовании технологий виртуализации. Общие положения.
- Приказ ФСТЭК России от 18 февраля 2013 г. № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» (ИСПДн).
- Методический документ. Меры защиты информации в государственных информационных системах (утвержден ФСТЭК России 11 февраля 2014 г.) (ГИС).
- Стандарт безопасности данных индустрии платежных карт (PCI DSS).
- Стандарт Банка России по обеспечению информационной безопасности организаций банковской системы Российской Федерации (СТО БР ИББС).

2. ЛАБОРАТОРНЫЙ ПРАКТИКУМ

2.1 ЛАБОРАТОРНАЯ РАБОТА №1

Цель работы
Ознакомление с функциональными возможностями и особенностями работы системы защиты информации в виртуальных инфраструктурах на примере разграничения прав доступа.

Исходные данные
Для ознакомления с функциональными возможностями и особенностями конфигурирования СЗИ ВИ Dallas Lock потребуется несколько ПК или ВМ (далее по тексту АРМ): АРМ1 с установленным Центром Управления СЗИ ВИ, АРМ2 с развернутой системой управления виртуализацией на базе oVirt (в данном случае Ред Виртуализация, далее СВ oVirt), введенной в домен безопасности СЗИ ВИ, 3 ВМ развернутые в инфраструктуре oVirt (test1, test2, test3), АРМ3 с которого будет осуществляться подключение и проверка выполненных настроек.
Также, для получения доступа к управлению СВ oVirt необходимо добавить в доверенные клиенты АРМ3, с которого будет осуществляться подключение к порталу администрирования СВ oVirt.

Порядок выполнения работ
1. Настройка доступа в ЦУ СЗИ ВИ

1) Включить АРМ1 и авторизоваться.

2) Запустить «Консоль ЦУ СЗИ ВИ» и авторизоваться под учетной записью администратора.

3) На вкладке «Агенты ВИ» выбрать ветку группы «KVM».

4) Во вкладке «Состояние» выбрать категорию «Клиенты управления СВ», в блоке «Действия с клиентом» нажать кнопку «Добавить клиента».

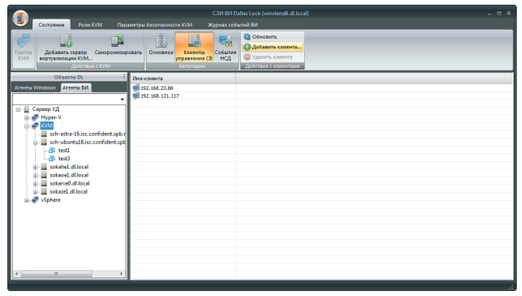

Рисунок 2. Клиенты управления СВ СЗИ ВИ

5) В открывшемся окне «Добавить клиента управления» ввести ip-адрес АРМ3 и нажать кнопку «ОК».

6) Вызвать контекстное меню в дереве на объекте группы «KVM» и выбрать пункт «Синхронизировать».

2. Создание пользователей

1) В консоли ЦУ СЗИ ВИ на во вкладке «Агенты ВИ» в дереве объектов выбрать уровень СВ oVirt.

2) Во вкладке «Учетные записи oVirt» выбрать категорию «Учетные записи».

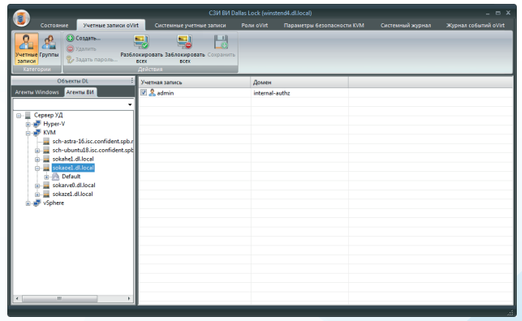

Рисунок 3. Учетные записи

3) В блоке «Действия» нажать кнопку «Создать» и в открывшемся окне «Создание нового пользователя» ввести имя «user1».

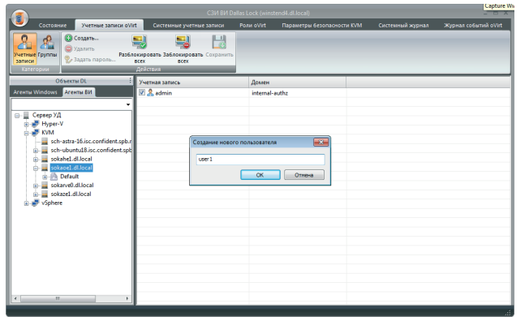

Рисунок 4. Новый пользователь

4) Нажать кнопку «ОК» и в появившемся окне «Пароль пользователя ‘user1’», ввести пароль и подтвердить его кнопкой «ОК».

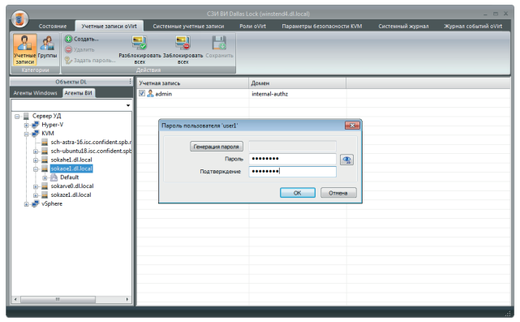

Рисунок 5. Пароль учетной записи

5) Повторить действия п.3 и п.4 и создать учетные записи «user2» и «user3».

6) В блоке «Действия» нажать кнопку «Сохранить».

7) На объекте СВ oVirt вызвать контекстное меню и выбрать пункт «Синхронизировать».

3. Создание и настройка прав пользователей

1) На объекте СВ oVirt на вкладку «Параметры безопасности KVM» и в блоке «Категории» нажать кнопку «Права пользователей», затем в блоке «Действия» нажать кнопку «Добавить».

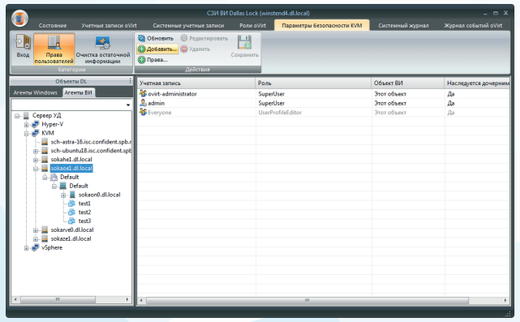

Рисунок 6. Параметры безопасности

2) В появившемся окне «Выбор пользователей и групп» нажать на кнопку «Пользователи» и дождаться открытия окна «Выбор учетной записи». В открывшемся окне в поле «Размещение» из выпадающего списка выбрать имя СВ oVirt, а в окне «Имя (Логин)» выбрать «user1».

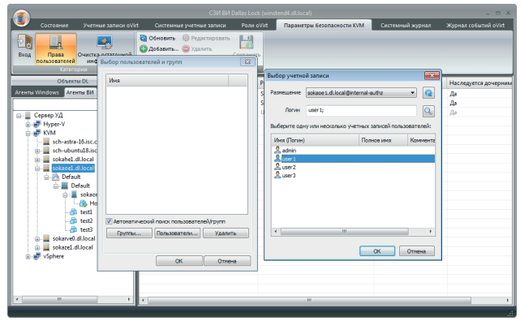

Рисунок 7. Выбор учетной записи

3) Нажать на кнопку «ОК», затем подтвердить, нажав на кнопку «ОК».

4) В отрывшемся окне «Выбор роли доступа» из выпадающего списка выбрать «SuperUser» и нажать на кнопку «ОК».

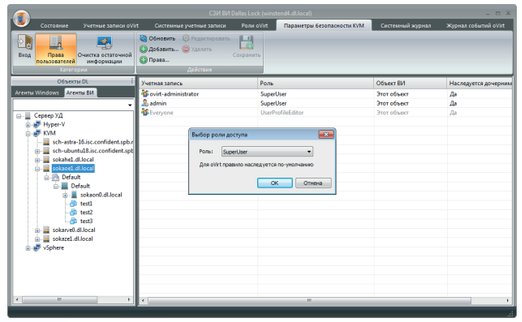

Рисунок 8. Выбор роли доступа

5) Для учетной записи user2 роль не назначать, что приравнивается к отсутствию доступа к порталу администрирования и порталу виртуальных машин.

6) Для учетной записи user3 выбрать роль «ReadOnlyAdmin».

7) В блоке «Действия» нажать кнопку «Сохранить».

4. Разграничение прав доступа к ВМ

1) Во вкладке «Агенты ВИ» в дереве «Сервер УД» перейти на ветку ВМ «test1» СВ oVirt.

2) Во вкладке «Параметры безопасности KVM», где в блоке «Категории» нажать кнопку «Права пользователя», затем в блоке «Действия» нажать кнопку «Добавить».

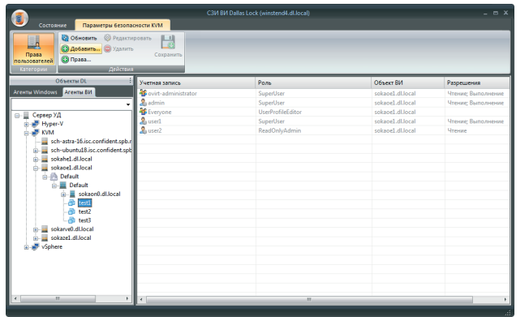

Рисунок 9. Параметры безопасности

3) В открывшемся окне «Выбор пользователей и групп» нажать на кнопку «Пользователи» и дождаться открытия окна «Выбор учетной записи». В открывшемся окне в поле «Размещение» из выпадающего списка выбрать имя СВ oVirt, а в окне «Имя (Логин)» выбрать «user3».

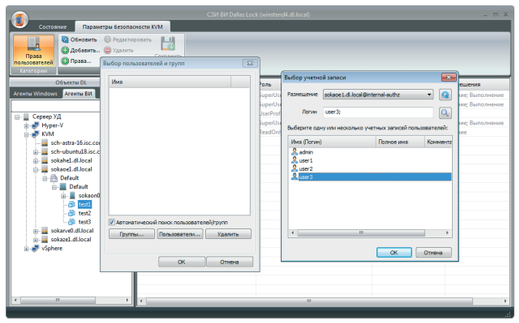

Рисунок 10. Выбор учетной записи

4) Нажать на кнопку «ОК», затем подтвердить, нажав на кнопку «ОК».

5) В отрывшемся окне «Выбор роли доступа» из выпадающего списка выбрать «UserVmManager» и нажать на кнопку «ОК».

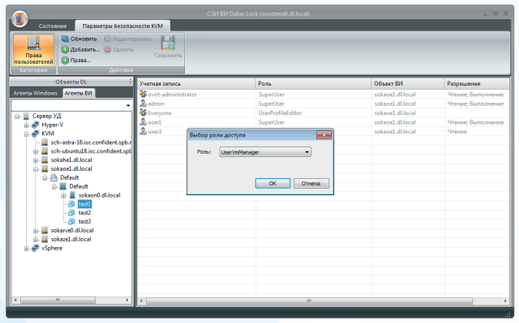

Рисунок 11. Выбор роли доступа

6) В блоке «Действия» нажать кнопку «Сохранить».

7) Во вкладке «Агенты ВИ» в дереве «Сервер УД» на ветке ВМ «test2» СВ oVirt пользователю user3 не назначать права, что приравнивается к отсутствию доступа.

8) В блоке «Действия» нажать кнопку «Сохранить».

9) Для пользователя user3 назначить роль «TemplateCreator» на ВМ «test3».

10) В блоке «Действия» нажать кнопку «Сохранить».

11) На ветке СВ oVirt вызвать контекстное меню и выбрать пункт «Синхронизировать».

5. Проверка дискреционного принципа контроля доступа к ВМ

1) Матрица доступа представлена в таблице 1.

Таблица 1. Матрица доступа

	user1	**user2**	**User3**
СВ oVirt	Администратор/SuperUser	Без доступа	ReadOnlyAdmin (доступ к Administration Portal)
гипервизор oVirt	Администратор/SuperUser	Без доступа	ReadOnlyAdmin (доступ к Administration Portal)
ВМ (test1)	Администратор/SuperUser	Без доступа	Привилегированный пользователь ВМ/UserVmManager (запуск/остановка и управление параметрами виртуальной машины)
ВМ (test2)	Администратор/SuperUser	Без доступа	Без доступа
ВМ (test3)	Администратор/SuperUser	Без доступа	Управление шаблонами ВМ/TemplateCreator (разрешение на создание и работу с шаблонами ВМ)

2) На АРМ3 запустить браузер и осуществить подключение к Administration Portal СВ oVirt (указать полное доменное имя) под пользователем user1.

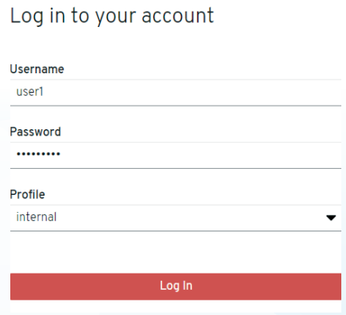

Рисунок 12. Окно авторизации

Проверка доступа к управлению системой виртуализации.

3) В окне «Administration» → «Configure» → «Roles» → «New» создать новую роль, например «TestRole». Убедиться, что роль создана.

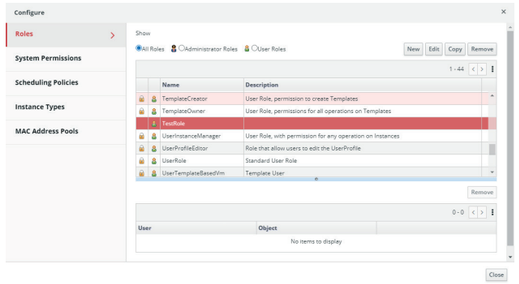

Рисунок 13. Роли Ред Виртуализации

Проверка доступа к параметрам хоста.

4) В окне «Compute» → «Hosts» выбрать любой хост и нажать кнопку «Edit».

5) Убедиться, что в окне «Edit Host» поля доступны для редактирования.

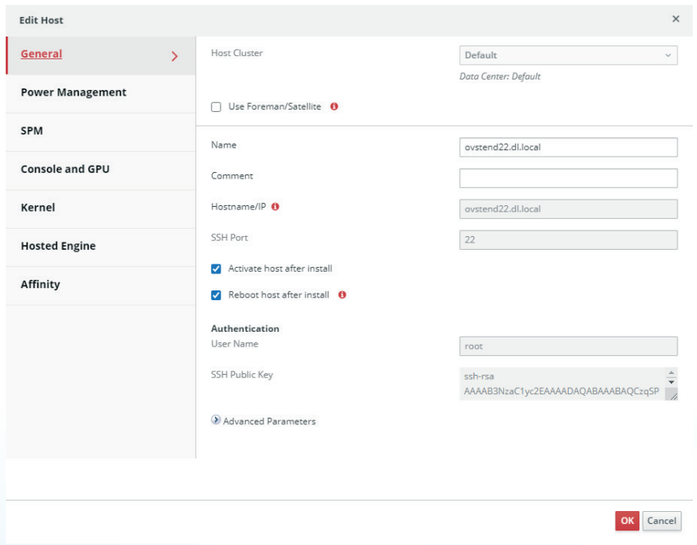

Рисунок 14. Параметры хоста

Проверка доступа к управлению ВМ.

6) Перейти в раздел «Compute» → «Virtual Machines».

7) Выбрать ВМ «test1», нажать кнопку «Edit».

8) В открывшемся окне убедиться, что можно вносить изменения в конфигурацию ВМ.

9) Выйти из «Administration Portal» и авторизоваться в «VM Portal» под пользователем user1.

10) Убедиться, что доступны все ВМ и все возможности по управлению.

11) Осуществить подключение к Administration Portal под учетной записью user3.

12) В окне выбрать вкладку «Compute» → «Virtual Machines».

13) Из списка выбрать ВМ «test1» и нажать кнопку «Run».

14) Убедиться, что ВМ запущена.

15) Из списка выбрать ВМ «test2» и нажать кнопку «Run».

16) Убедиться, что операция заблокирована.

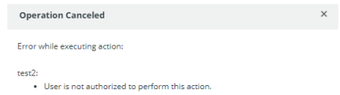

Рисунок 15. Сообщение о блокировке операции

17) Из списка выбрать ВМ «test3» и нажать кнопку «Run».

18) Убедиться, что операция заблокирована.

19) Открыть окно ВМ «test3», вызвать дополнительное меню и выбрать пункт «Make Template».

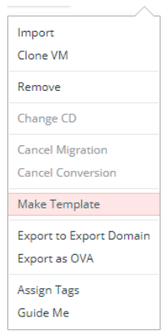

Рисунок 16. Создание шаблона

20) В появившемся окне в поле «Name» ввести «Test», в поле «Description» ввести «Test». Нажать кнопку «ОК».

21) На вкладке «Templates» убедиться, что шаблон создан.

Рисунок 17. Список шаблонов

22) Во вкладке «Administration» → «Configure» → «Roles» → «New» создать новую роль.

23) Убедиться, что операция заблокирована.

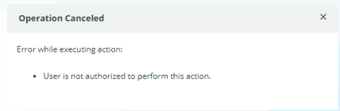

Рисунок 18. Сообщение о блокировке операции

Проверка доступа к порталу администрирования и порталу виртуальных машин

24) Осуществить подключение к Administration Portal под учетной записью user2.

25) Убедиться, что доступ к порталу администрирования ограничен.

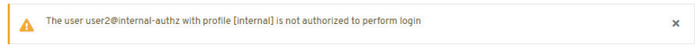

Рисунок 19. Сообщение о блокировке доступа

26) Осуществить подключение к VM Portal под учетной записью user2.

27) Убедиться, что доступ к порталу администрирования ограничен.

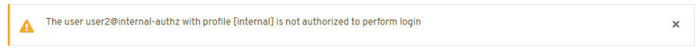

Рисунок 20. Сообщение о блокировке доступа

Содержание отчета
Отчет о выполненной работе должен содержать:
1. Оглавление.
2. Краткие теоретические сведения.
3. Результаты выполнения работы. В главу должно быть включено детализированное описание выполненных настроек и результатов проверок работоспособности по следующим параметрам:
- идентификация и аутентификация пользователей (путем создания учетных записей и назначения им паролей);
- разграничение доступа, реализация дискреционной модели.

4. Ответы на контрольные вопросы.

Контрольные вопросы
1. Какие возможности по разграничению доступа реализует СЗИ ВИ Dallas Lock для объектов ВИ?
2. Охарактеризуйте подсистему централизованного управления.
3. Укажите категории средств обеспечения информационной безопасности, которые, помимо СЗИ ВИ Dallas Lock, должны функционировать в комплексе средств защиты информации.

2.2 ЛАБОРАТОРНАЯ РАБОТА № 2.

Цель работы
Ознакомление с функциональными возможностями и особенностями работы системы защиты информации в виртуальных инфраструктурах на примере контроля целостности объектов ВИ.

Исходные данные
Для ознакомления с функциональными возможностями и особенностями конфигурирования СЗИ ВИ Dallas Lock потребуется несколько ПК или ВМ (далее по тексту АРМ): АРМ1 с установленным Центром Управления СЗИ ВИ, АРМ2 с развернутой системой управления виртуализацией на базе oVirt (в данном случае Ред Виртуализация, далее СВ oVirt), введенной в домен безопасности СЗИ ВИ, 3 ВМ развернутые в инфраструктуре oVirt (test1, test2, test3), АРМ3 с которого будет осуществляться подключение и проверка выполненных настроек.
Также, для получения доступа к управлению СВ oVirt необходимо добавить в доверенные клиенты АРМ3, с которого будет осуществляться подключение к порталу администрирования СВ oVirt.

Порядок выполнения работ
1. Настройка контроля целостности в ЦУ СЗИ ВИ
1) Включить АРМ1 и авторизоваться.
2) Запустить «Консоль ЦУ СЗИ ВИ» и авторизоваться под учетной записью администратора.

Настроить периодический контроль целостности.
3) В дополнительном меню выбрать пункт «Параметры сервера УД» и дождаться открытия окна «Параметры сервера УД», где в поле «Частота проверки КЦ системных файлов» установить значение равным 5 минут.

Поставить объекты под контроль целостности
4) На вкладке «Агенты ВИ» выбрать гипервизор oVirt (хост) в ветке СВ oVirt.
5) Во вкладке «Состояние» в блоке «Категории» нажать на кнопку «Контроль целостности» и убедиться, что в списке файлов под контролем присутствует файл agentd.ic.

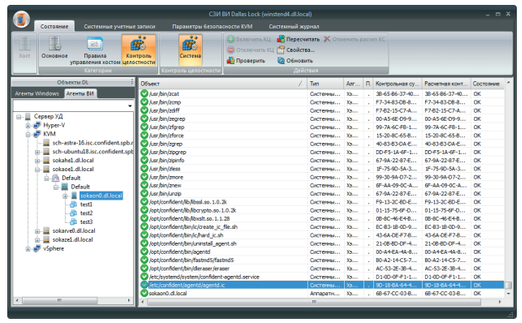

Рисунок 21. Список системных файлов под КЦ

6) В ветке СВ oVirt выбрать ВМ «test1».
7) Во вкладке «Состояние» в блоке «Категории» нажать кнопку «Контроль целостности», в блоке «Контроль целостности» нажать «Конфигурации ВМ» и выбрать ВМ (test1), нажать на кнопку «Включить КЦ» и подтвердить алгоритм расчета в появившемся окне. Убедиться, что в списке под контролем присутствует ВМ (test1).

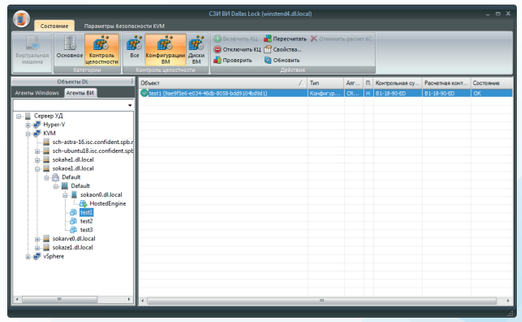

Рисунок 22. КЦ конфигурации ВМ

2. Проверка работы контроля целостности

8) Подключиться локально к гипервизору oVirt или по SSH, например, с помощью PuTTy.

9) Изменить файл «agentd.ic» командой «echo “test123” >> /etc/confident/agentd/agentd.ic».

10) Осуществить вход на АРМ1. Убедиться, что появилось сообщение о нарушение целостности файла «agentd.ic».

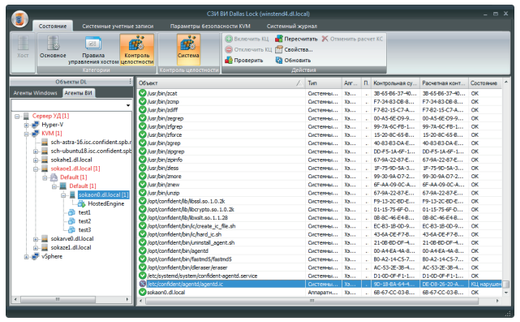

Рисунок 23. Нарушение целостности файла

11) Подключиться к СВ oVirt и авторизоваться в «Administration Portal» под администратором.

12) Перейти «Compute» → «Virtual Machines», в окне выбрать ВМ test1, нажать кнопку «Edit» и изменить какие-либо параметры, например, «Total Virtual CPUs» и подтвердить изменения.

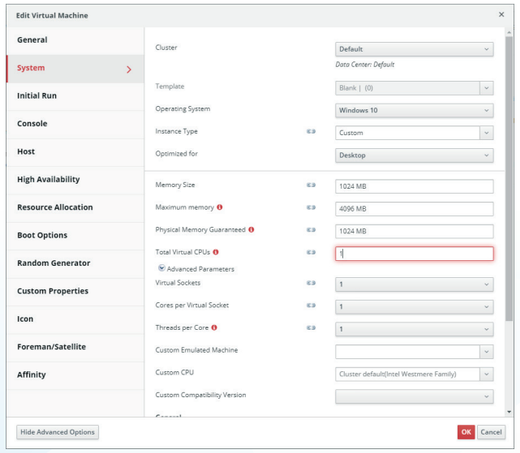

Рисунок 24. Параметры ВМ

13) Осуществить вход в «АРМ1». Убедиться, что появилось сообщение о нарушении целостности ВМ «test1».

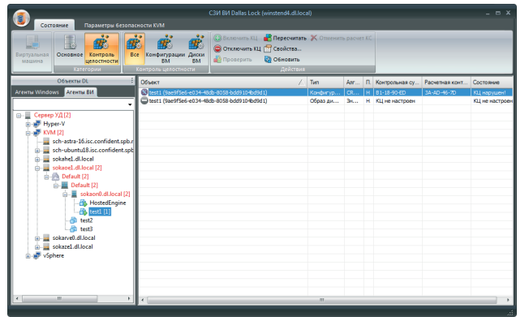

Рисунок 25. Нарушение целостности конфигурации ВМ

Содержание отчета

Отчет о выполненной работе должен содержать:

1. Оглавление.

2. Краткие теоретические сведения.

3. Результаты выполнения работы. В главу должно быть включено детализированное описание выполненных настроек и результатов проверок работоспособности по следующим параметрам:

- контроль целостности системных файлов гипервизора;
- контроль целостности конфигурации ВМ.

4. Ответы на контрольные вопросы.

Контрольные вопросы

1. Что такое контроль целостности?

2. Какие возможности по обеспечению контроля целостности реализует СЗИ ВИ Dallas Lock для объектов ВИ?

3. Охарактеризуйте подсистему контроля целостности.

4. Укажите какие алгоритмы для расчета контрольных сумм используются в СЗИ ВИ Dallas Lock.

2.3 ЛАБОРАТОРНАЯ РАБОТА № 3.

Цель работы

Ознакомление с функциональными возможностями и особенностями работы системы защиты информации в виртуальных инфраструктурах на примере зачистки остаточной информации объектов ВИ.

Исходные данные

Для ознакомления с функциональными возможностями и особенностями конфигурирования СЗИ ВИ Dallas Lock потребуется несколько ПК или ВМ (далее по тексту АРМ): АРМ1 с установленным Центром Управления СЗИ ВИ, АРМ2 с развернутой системой управления виртуализацией на базе oVirt (в данном случае Ред Виртуализация, далее СВ oVirt), введенной в домен безопасности СЗИ ВИ, 3 ВМ развернутые в инфраструктуре oVirt (test1, test2, test3), АРМ3 с которого будет осуществляться подключение и проверка выполненных настроек.

Также, для получения доступа к управлению СВ oVirt необходимо добавить в доверенные клиенты АРМ3, с которого будет осуществляться подключение к порталу администрирования СВ oVirt.
Для проверки результатов требуется программа для поиска остаточной информации, в данном примере будет использоваться комплекс Сканер-ВС Инспектор.

Порядок выполнения работ

1. Подготовка ВМ для выполнения проверки

1) Подключиться к СВ oVirt и авторизоваться в «Administration Portal» под администратором.

2) Перейти «Compute» → «Virtual Machines» в окне выбрать ВМ test1 и нажать кнопку «Run».

3) Дождаться загрузки ВМ и открыть консоль нажав кнопку «Console».

4) В открывшемся окне ВМ на рабочем столе гостевой ОС создать текстовый файл «test».

5) Открыть файл «test» в текстовом редакторе и написать какую-либо фразу, например, «ghjcnjghjdthrf1209».

6) Сохранить изменения в файле, закрыть, удалить файл и выключить ВМ «test1», выключить АРМ2.

7) Подключить к СВ oVirt (АРМ2) диск с программой «Сканер-ВС» и выполнить загрузку с него.

8) Нажать кнопку «Пуск» → «Форензика» → «Поиск остаточной информации».

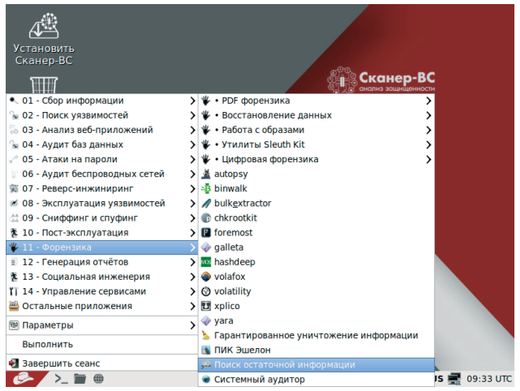

Рисунок 26. ПО для поиска остаточной информации

9) В открывшемся окне выбрать диск с ВМ «test1».

10) Установить флаг напротив пункта «Поиск фразы», ввести контрольную фразу «ghjcnjghjdthrf1209» и нажать кнопку «Начать поиск».

11) Дождаться окончания поиска и убедиться, что ключевая фраза найдена.

12) Выключить СВ oVirt (АРМ2), размонтировать диск с программой «Сканер-ВС» и запустить основную ОС.

2. Выполнение зачистки остаточной информации

В СЗИ ВИ затирание производится записью маскирующей последовательности поверх освобождаемого пространства.

13) Авторизоваться на АРМ1 и запустить Консоль ЦУ СЗИ ВИ.

14) Перейти на вкладку «Агенты ВИ», в ветке с СВ oVirt на ВМ «test1» вызвать контекстное меню.

15) В контекстном меню выбрать «Удалить и зачистить» и подтвердить удаление.

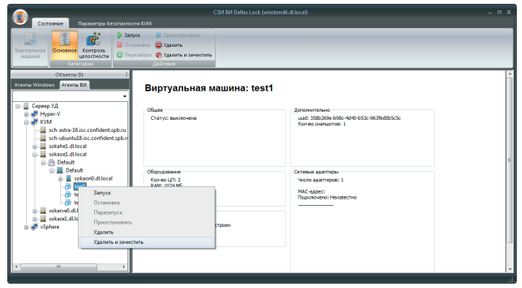

Рисунок 27. Удаление и зачистка ВМ

16) Убедиться, что ВМ «test1» удалена и не отображается в дереве вкладки «Агенты ВИ».

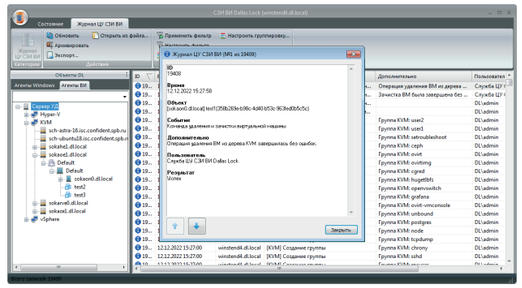

Рисунок 28. Сообщение в журнале о завершении зачистки

Проверка результатов зачистки остаточной информации.

17) Подключить к СВ oVirt (АРМ2) диск с программой «Сканер-ВС» и выполнить загрузку с него.

18) Повторить поиск контрольной фразы «ghjcnjghjdthrf1209».

19) Дождаться окончания поиска и убедиться, что ключевая фраза не найдена.

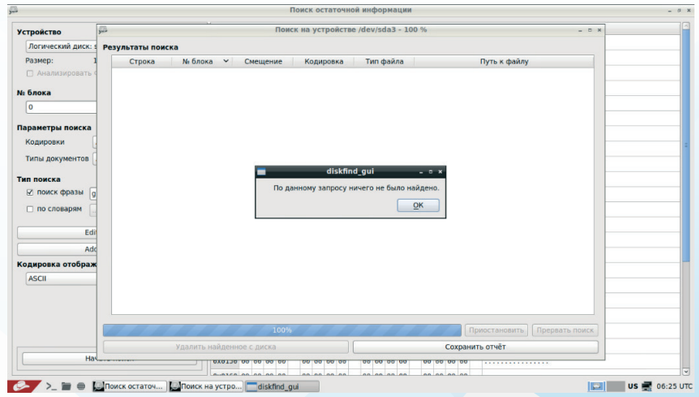

Рисунок 29. Результат поиска ключевой фразы

Содержание отчета

Отчет о выполненной работе должен содержать:

1. Оглавление.
2. Краткие теоретические сведения.
3. Результаты выполнения работы. В главу должно быть включено детализированное описание выполненных настроек и результатов проверок работоспособности по следующим параметрам:
- зачистка остаточной информации.

4. Ответы на контрольные вопросы.

Контрольные вопросы

1. Что такое остаточная информация?
2. Какие возможности по обеспечению зачистки остаточной информации реализует СЗИ ВИ Dallas Lock для объектов ВИ?
3. Охарактеризуйте подсистему зачистки остаточной информации.
4. Укажите какие методы и средства используются для уничтожения остаточной информации.

3. ЛИТЕРАТУРА

1. Описание применения СЗИ ВИ Dallas Lock [Электронный ресурс]. – URL: https://dallaslock.ru/products/szi-vi-dallas-lock/#tabs-2.
2. Руководство оператора СЗИ ВИ Dallas Lock [Электронный ресурс]. – URL: https://dallaslock.ru/products/szi-vi-dallas-lock/#tabs-2.
3. Руководство по эксплуатации СЗИ ВИ Dallas Lock [Электронный ресурс]. – URL: https://dallaslock.ru/products/szi-vi-dallas-lock/#tabs-2.

КОНФИДЕНТ®
ЦЕНТР ЗАЩИТЫ ИНФОРМАЦИИ

192029, г. Санкт-Петербург
пр. Обуховской Обороны, д. 51, лит. К
телефон/факс: (812) **325-1037**

https://www.**confident**.ru/
https://www.**dallaslock**.ru/
e-mail:
distribution@confident.ru - коммерческие вопросы
helpdesk@confident.ru - техническая поддержка

Схема проезда: