УТВЕРЖДЕН
ПФНА.501410.001 31-ЛУ

СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ В ВИРТУАЛЬНЫХ ИНФРАСТРУКТУРАХ

Dallas Lock

(версия 5.87.1695.0)

Описание применения

ПФНА.501410.001 31

Листов 15

АННОТАЦИЯ

Данный документ выполнен в соответствии с ГОСТ 19.502-78 и распространяется на изделие **Система защиты информации в виртуальных инфраструктурах Dallas Lock** ПФНА.501410.001 (далее по тексту — изделие или **СЗИ ВИ Dallas Lock**).

В настоящем документе содержатся общие сведения о назначении изделия, условиях применения, описание задачи, перечень входных и выходных данных.

Содержание

ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ

Сокращение	Полная формулировка
ESXi	гипервизор ESXi. Средство виртуализации VMware vSphere
HOSTVM Engine	средство мониторинга и управления вычислительными узлами, хранилищами, сетями и виртуальными машинами. Далее по тексту — сервер виртуализации HOSTVM (СВ HOSTVM)
HOSTVM Host	вычислительный узел (гипервизор), на котором выполняются ВМ, а также могут быть размещены локальные хранилища. Далее по тексту — гипервизор HOSTVM
FQDN	Fully Qualified Domain Name. Доменное имя, которое не имеет неоднозначностей в определении. FQDN включает в себя доменные имена родительских доменов иерархии DNS
KVM	Kernel-based Virtual Machine. Программное решение, обеспечивающее виртуализацию в среде Linux
oVirt Engine	средство мониторинга и управления вычислительными узлами, хранилищами, сетями и виртуальными машинами. Далее по тексту — сервер виртуализации oVirt (СВ oVirt)
oVirt Host	вычислительный узел (гипервизор), на котором выполняются ВМ, а также могут быть размещены локальные хранилища. Далее по тексту — гипервизор oVirt
RedVirt Engine	средство мониторинга и управления вычислительными узлами, хранилищами, сетями и виртуальными машинами. Далее по тексту — сервер виртуализации RedVirt (СВ RedVirt)
RedVirt Host	вычислительный узел (гипервизор), на котором выполняются ВМ, а также могут быть размещены локальные хранилища. Далее по тексту — гипервизор RedVirt
vCSA	VMware vCenter Server Appliance. Сервер управления средством виртуализации ESXi (vCenter на виртуальной машине на базе ОС Photon)
VMware vSphere	платформа (среда) виртуализации серверов/рабочих станций с возможностями согласованного управления виртуальными центрами обработки данных
zVirt Engine	средство мониторинга и управления вычислительными узлами, хранилищами, сетями и виртуальными машинами. Далее по тексту — сервер виртуализации zVirt (СВ zVirt)
zVirt Host	вычислительный узел (гипервизор), управляющий физическими хостами виртуализации, доменами данных, кластерами, виртуальными машинами и предоставляющая администратору интерфейс управления. Далее по тексту – гипервизор zVirt
Агент DL HOSTVM Engine	компонент защиты сервера виртуализации HOSTVM
Агент DL HOSTVM Host	компонент защиты гипервизора HOSTVM
Агент DL KVM	компонент защиты гипервизора KVM
Агент DL oVirt Engine	компонент защиты сервера виртуализации oVirt
Агент DL oVirt Host	компонент защиты гипервизора oVirt
Агент DL RedVirt	компонент защиты сервера виртуализации RedVirt

Engine	
Агент DL RedVirt Host	компонент защиты гипервизора RedVirt
Агент DL zVirt Engine	компонент защиты сервера виртуализации zVirt
Агент DL zVirt Host	компонент защиты гипервизора zVirt
ВИ	виртуальная инфраструктура **Dallas Lock**
Веб-сервер ЦУ СЗИ ВИ	позволяет подключаться через веб-интерфейс из любого браузера с любого АРМ к Ядру **ЦУ СЗИ ВИ** для выполнения функций аудита **СЗИ ВИ**. Реализован в виде службы
ВМ	Виртуальная машина
Гипервизор	программа или аппаратная схема, обеспечивающая или позволяющая одновременное, параллельное выполнение нескольких ОС на одном ТС
ДБ	организация единой политики безопасности совокупностью **ЦУ СЗИ ВИ** и агентов **DL**, работающих под управлением **ЦУ СЗИ ВИ**
Консоль	Консоль Центра управления **СЗИ ВИ Dallas Lock**. Программное обеспечение для управления Центром управления **СЗИ ВИ Dallas Lock**
Объект ВИ	объекты виртуальной инфраструктуры **Dallas Lock**, такие как: СВ vCSA, СВ на базе oVirt (zVirt, RedVirt, HOSTVM), гипервизор ESXi, гипервизор KVM, гипервизор на базе oVirt (zVirt, RedVirt, HOSTVM), виртуальная машина
ОС	операционная система
ОЗУ	оперативное запоминающее устройство
ПЗУ	постоянное запоминающее устройство
ПК	персональный компьютер
СВ	сервер виртуализации
СЗИ ВИ	система защиты информации в виртуальных инфраструктурах
ТС	техническое средство
ТУ	технические условия
ЦУ СЗИ ВИ	Центр управления **СЗИ ВИ**. Совокупность агентов **DL** и ядра **СЗИ ВИ**, управляемая с помощью веб-консоли
Ядро СЗИ ВИ	компонент Центра управления **СЗИ ВИ Dallas Lock**, обеспечивающий централизованное управление объектами виртуальной инфраструктуры и включающий в себя веб-сервер. Реализовано в виде службы

1. НАЗНАЧЕНИЯ

Система защиты информации в виртуальных инфраструктурах **Dallas Lock** предназначена для защиты среды виртуализации на базе технологий vSphere (vCenter for Windows 5.5, 6.0, 6.5, 6.7 и vCSA 6.5, 6.7, 7.0, 8.0 совместно с ESXi[1] аналогичной версии), Windows Server (Hyper-V) (версий 2012, 2012 R2, 2016, 2019)[2], KVM, использующей библиотеки libvirt (версии не ниже 4.5.0) в качестве инструмента управления гипервизором, oVirt (версия 4.4.x) и Виртуализация zVirt (версий 3.0, 3.1, 3.3, 4.0[3], 4.1, 4.2[4]), РЕД Виртуализация 7.3 и HOSTVM от несанкционированного доступа при работе в многопользовательских автоматизированных системах (АС), государственных информационных системах, в автоматизированных системах управления, информационных системах персональных данных и при защите значимых объектов критической информационной инфраструктуры.

Изделие предназначено для использования на различных технических средствах (ТС), в том числе: персональных компьютерах (ПК), серверах и узлах виртуальной инфраструктуры в составе локальной вычислительной сети.

[1] Для защиты среды виртуализации на базе гипервизора ESXi 5.5 необходимо применять сертифицированную версию изделия **СЗИ ВИ Dallas Lock 376.3**. Для защиты среды виртуализации на базе гипервизора ESXi 6.0, 6.5, 6.7 совместно с СВ vCenter for Windows 6.0, 6.5, 6.7 необходимо применять сертифицированную версию изделия **СЗИ ВИ Dallas Lock 4.68**.

[2] Для защиты среды виртуализации на базе гипервизора Windows Server (Hyper-V) (версий 2012, 2012 R2, 2016, 2019) необходимо применять сертифицированную версию изделия **СЗИ ВИ Dallas Lock 4.68**.

[3] Для защиты среды виртуализации zVirt версий 3.0, 3.1, 3.3, 4.0 необходимо применять сертифицированную версию изделия **СЗИ ВИ Dallas Lock 4.68**.

[4] При работе с платформой виртуализации zVirt 4.2 поддерживается только конфигурации с использованием провайдера по умолчанию - AAA-JDBC.

2. УСЛОВИЯ ПРИМЕНЕНИЯ

2.1. Изделие **СЗИ ВИ Dallas Lock** включает в себя следующие компоненты:

- ядро системы защиты информации в виртуальных инфраструктурах;
- агент DL KVM для гипервизора KVM;
- агент DL oVirt Engine для СВ oVirt;
- агент DL oVirt Host для гипервизора oVirt;
- агент DL zVirt Engine для СВ zVirt;
- агент DL zVirt Host для гипервизора zVirt;
- агент DL RedVirt Engine для СВ РЕД Виртуализация;
- агент DL RedVirt Host для гипервизора РЕД Виртуализация;
- агент DL HOSTVM Engine для СВ HOSTVM;
- агент DL HOSTVM Host для гипервизора HOSTVM.

2.2. Изделие предназначено для защиты виртуальной инфраструктуры с программным и техническим обеспечением, состав и характеристики которого приведены ниже.

Для установки компонентов **СЗИ ВИ** необходимо минимум 1 Гб свободного дискового пространства на системном разделе жесткого диска. ТС с установленным **ЦУ СЗИ ВИ** должно иметь следующий состав и характеристики программно-технического обеспечения:

1. Поддерживаемые ОС:
    - Debian 11;
    - Ubuntu 22.04.4 LTS, 24.04 LTS;
    - РЕД ОС 7.3, 8.0;
    - Astra Linux Special Edition 1.7 (SE) (Воронеж) (Server/Desktop);
    - Альт 8 СП релиз 10 (Рабочая станция, Сервер);
    - Альт Рабочая станция 10.1, К;
    - Альт Сервер 10;
    - РОСА «КОБАЛЬТ» 7.9 Рабочая станция/Сервер;
    - РОСА «ХРОМ» 12.4 Рабочая станция/Сервер.
2. Минимальная конфигурация ТС:
    - процессор: Intel или AMD с 2 логическими ядрами по 2 ГГц каждое;
    - ОЗУ — минимум 2 Гб;
    - ПЗУ — минимум 20 Гб;
    - видеоадаптер: поддержка режима SVGA800x600;
    - сетевая карта.

Для ввода в домен безопасности и корректной работы со средой виртуализации ТС с установленным гипервизором VMware ESXi 6.5/6.7/7.0/8.0 должно иметь следующий состав и характеристики программно-технического обеспечения:

- процессор: Intel или AMD с 2 логическими ядрами по 2 ГГц каждое, только x64;
- ОЗУ — минимум 8 Гб;
- ПЗУ — минимум 60 Гб;
- сетевая карта.

Для ввода в домен безопасности и корректной работы со средой виртуализации ТС с установленным VMware vCSA 6.5/6.7/7.0/8.0 должно иметь следующий состав и характеристики программно-технического обеспечения:

- процессор: Intel или AMD с 2 логическими ядрами по 2 ГГц каждое, только x64;
- ОЗУ — минимум 12 Гб;
- ПЗУ — более 350 Гб;
- сетевая карта.

Для установки агента DL KVM ТС с установленным гипервизором KVM, использующим библиотеки libvirt версии не ниже 4.5.0, должно иметь следующий состав и характеристики программно-технического обеспечения:

1. Поддерживаемые ОС (только 64-bit):

- Astra Linux SE 1.7 (Воронеж, Орел);
- CentOS 7.5, 8.4.2105;
- CentOS Linux 8.5 (2111);
- CentOS Stream 9;
- Linux Mint 19.3, 20.3, 21.3;
- Ubuntu 18.04.6 LTS, 20.04.3 LTS, 22.04.4 LTS, 24.04 LTS.

2. Минимальная конфигурация ТС:
   - процессор: Intel или AMD с 2 логическими ядрами по 2 ГГц каждое;
   - ОЗУ — минимум 1 Гб;
   - ПЗУ — минимум 10 Гб;
   - сетевая карта.

Для установки агента DL oVirt Engine ТС с установленным СВ oVirt (версия 4.4.x) должно иметь следующий состав и характеристики программно-технического обеспечения:

1. Поддерживаемые ОС:
   - oVirt Node.
2. Минимальная конфигурация ТС:
   - процессор: Intel или AMD с 2 логическими ядрами по 2 ГГц каждое;
   - ОЗУ — минимум 4 Гб;
   - ПЗУ — минимум 25 Гб;
   - сетевая карта — минимум 1 Гбит/с.

Для установки агента DL oVirt Host ТС с установленным гипервизором oVirt (версия 4.4.x) должно иметь следующий состав и характеристики программно-технического обеспечения:

1. Поддерживаемые ОС:
   - oVirt Node.
2. Минимальная конфигурация ТС:
   - процессор: Intel или AMD с 2 логическими ядрами по 2 ГГц каждое;
   - ОЗУ — минимум 2 Гб;
   - ПЗУ — минимум 64 Гб;
   - сетевая карта — минимум 1 Гбит/с.

Для установки агента DL zVirt Engine ТС с установленным СВ zVirt (версий 4.1, 4.2) должно иметь следующий состав и характеристики программно-технического обеспечения:

1. Поддерживаемые ОС:
   - zVirt Node.
2. Минимальная конфигурация ТС:
   - процессор: двухъядерный x86-64 с поддержкой VT-x/AMD-V;
   - ОЗУ — минимум 4 Гб;
   - ПЗУ — минимум 94 Гб;
   - сетевая карта — минимум 1 Гбит/с.

Для установки агента DL zVirt Node ТС с установленным гипервизором zVirt (версий 4.1, 4.2) должно иметь следующий состав и характеристики программно-технического обеспечения:

1. Поддерживаемые ОС:
   - zVirt Node.
2. Минимальная конфигурация ТС:
   - процессор: двухъядерный x86-64 с поддержкой VT-x/AMD-V;
   - ОЗУ — минимум 4 Гб;
   - ПЗУ — минимум 94 Гб;
   - сетевая карта — минимум 1 Гбит/с.

Для установки агента DL RedVirt Engine ТС с установленным СВ RedVirt 7.3 должно иметь следующий состав и характеристики программно-технического обеспечения:

1. Поддерживаемые ОС:
   - RedVirt Node.
2. Минимальная конфигурация ТС:

- процессор: двухъядерный;
- ОЗУ — минимум 16 Гб;
- ПЗУ — минимум 80 Гб;
- сетевая карта — минимум 1 Гбит/с.

Для установки агента **DL** RedVirt Host ТС с установленным гипервизором RedVirt 7.3 должно иметь следующий состав и характеристики программно-технического обеспечения:

1. Поддерживаемые ОС:
   - RedVirt Node.
2. Минимальная конфигурация ТС:
   - процессор: двухъядерный;
   - ОЗУ — минимум 16 Гб;
   - ПЗУ — минимум 80 Гб;
   - сетевая карта — минимум 1 Гбит/с.

Для установки агента **DL** HOSTVM Engine ТС с установленным СВ HOSTVM должно иметь следующий состав и характеристики программно-технического обеспечения:

1. Поддерживаемые ОС:
   - HOSTVM Node.
2. Минимальная конфигурация ТС:
   - процессор: Intel или AMD с 2 логическими ядрами по 2 ГГц каждое;
   - ОЗУ — минимум 4 Гб;
   - ПЗУ — минимум 25 Гб;
   - сетевая карта — минимум 1 Гбит/с.

Для установки агента **DL** HOSTVM Host ТС с установленным гипервизором HOSTVM должно иметь следующий состав и характеристики программно-технического обеспечения:

1. Поддерживаемые ОС:
   - HOSTVM Node.
2. Минимальная конфигурация ТС:
   - процессор: Intel или AMD с 2 логическими ядрами по 2 ГГц каждое;
   - ОЗУ — минимум 2 Гб;
   - ПЗУ — минимум 64 Гб;
   - сетевая карта — минимум 1 Гбит/с.

2.3. Веб-консоль функционирует на стабильных версиях кроссплатформенных браузеров на основе движка Chromium с версией 114 и выше.

2.4. Для использования **СЗИ ВИ** необходимо настроить сетевой протокол TCP/IP.

2.5. **СЗИ ВИ Dallas Lock** может быть использована как в сетях с доменной организацией, так и в одноранговых сетях.

2.6. **СЗИ ВИ Dallas Lock** редакция «Расширенная» поддерживает следующие функций и инструменты управления серверами виртуализации для VMware vSphere.

- vCenter High Availability;
- Fault Tolerance;
- Enhanced Linked Mode.

2.7. Для модулей изделия **СЗИ ВИ Dallas Lock** предусмотрен механизм проверки наличия более новых версий.

2.8. **СЗИ ВИ Dallas Lock** соответствует требованиям руководящих и методических документов (требования безопасности информации ФСТЭК России):

- «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» (Гостехкомиссия России, 1992) — по 5 классу защищенности;
- «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (утвержден приказом ФСТЭК России № 76 от 2 июня 2020 г.) — по 4 уровню доверия.

2.9. При условии соблюдения ограничений, указанных в разделе 3 формуляра на данное изделие (ПФНА.501410.001 ФО) **СЗИ ВИ Dallas Lock** может быть использована:

- при создании защищенных автоматизированных систем до класса защищенности 1Г включительно (Руководящий документ «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» (Гостехкомиссия России, 1992));
- в информационных системах персональных данных до 1 уровня защищенности персональных данных включительно (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») (далее — приказ № 21);
- в государственных информационных системах до 1 класса защищенности включительно (Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах») (далее — приказ № 17);
- при создании защищенных автоматизированных систем управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды до 1 класса защищенности включительно (Приказ ФСТЭК России от 14 марта 2014 г. № 31 «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды»);
- защищенных значимых объектов критической информационной инфраструктуры до 1 категории значимости включительно (Приказ ФСТЭК России от 25 декабря 2017 г. № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации»).

3. ОПИСАНИЕ ЗАДАЧИ

3.1. Изделие разработано в соответствии с требованиями, описанными в документе «Технические условия» ПФНА.501410.001 ТУ (ТУ).

3.2. В соответствии с ТУ **СЗИ ВИ Dallas Lock** состоит из программного ядра и следующих подсистем:

- подсистема развертывания (установочные модули)
- подсистема администрирования;
- подсистема управления пользователями;
- подсистема управления доступом;
- подсистема контроля целостности;
- подсистема гарантированной очистки памяти;
- подсистема аудита;
- подсистема восстановления после сбоев;
- подсистема фильтрации трафика;
- подсистема лицензирования.

3.3. Подсистема управления пользователями

3.3.1. Реализована идентификация и аутентификация администраторов и пользователей в виртуальной среде по идентификатору (коду) и паролю условно-постоянного действия — на **ЦУ СЗИ ВИ**, серверах виртуализации vCSA, oVirt/zVirt/HOSTVM/RedVirt и гипервизорах KVM, oVirt/zVirt/HOSTVM/RedVirt. Контроль пользователей, имеющих право на вход на гипервизор, осуществляется посредством выполнения необходимых настроек на стороне **ЦУ СЗИ ВИ** и процесса синхронизации гипервизора с **ЦУ СЗИ ВИ**.

3.3.2. Изделие препятствует доступу к защищаемым ресурсам серверов виртуализации vCSA, oVirt/zVirt/HOSTVM/RedVirt и гипервизоров ESXi, KVM, oVirt, zVirt, RedVirt и HOSTVM неидентифицированных пользователей и пользователей, подлинность идентификации которых при аутентификации не подтвердилась. Контроль пользователей, имеющих право на доступ, осуществляется посредством выполнения необходимых настроек на стороне **ЦУ СЗИ ВИ** и процесса синхронизации с **ЦУ СЗИ ВИ**.

3.3.3. Реализовано управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов. В качестве идентификатора может выступать:

- имя локального пользователя ОС среды виртуализации vCSA/KVM/oVirt/zVirt/RedVirt/HOSTVM;
- имя доменного пользователя AD при условии, что на сервере виртуализации подключен контроллер домена в качестве возможного средства проверки авторизации. Вход доменных пользователей возможен только на серверах виртуализации vCSA, oVirt, zVirt, RedVirt и HOSTVM;
- имя пользователя ОС на гипервизоре ESXi.

3.3.4. Реализовано управление средствами аутентификации, в том числе хранение, выдача и инициализация для всех компонент защищаемой виртуальной инфраструктуры. Должна быть реализована защита аутентификационной информации субъектов доступа, хранящейся в компонентах виртуальной инфраструктуры от неправомерного доступа к ней, уничтожения или модифицирования. Также должно осуществляться блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации для **ЦУ СЗИ ВИ**, серверов виртуализации oVirt/zVirt/HOSTVM/RedVirt и гипервизоров KVM/oVirt/zVirt/RedVirt/HOSTVM.

3.3.5. Реализована блокировка доступа к компонентам виртуальной инфраструктуры для субъектов доступа, не прошедших процедуру аутентификации.

3.3.6. Для **ЦУ СЗИ ВИ** реализована защита обратной связи при вводе аутентификационной информации, посредством замены вводимых знаков на специальные символы, не позволяющих однозначно определить вводимые знаки.

3.3.7. Имеется возможность разделения полномочий (ролей, типов учетных записей) пользователей, администраторов и лиц, обеспечивающих функционирование **СЗИ ВИ Dallas Lock**.

3.3.8. Должно быть реализовано ограничение неуспешных попыток входа в **СЗИ ВИ Dallas Lock**.

3.3.9. Для веб-консоли **ЦУ СЗИ ВИ** реализовано ограничение числа параллельных сеансов доступа для каждой учетной записи пользователя.

3.4. Подсистема управления доступом

3.4.1. Разграничение доступа к объектам виртуальной инфраструктуры

3.4.1.1. Реализовано разграничение доступа к следующим компонентам виртуальной инфраструктуры — к **ЦУ СЗИ ВИ**. Разграничение доступа к СВ vCSA, гипервизорам ESXi и виртуальным машинам ESXi (файлам виртуальных машин) реализуется в пределах ролевой модели разграничения доступа vSphere 5.5, 6.0, 6.5, 6.7, 7.0, 8.0, к СВ oVirt и ВМ oVirt в рамках ролевой модели oVirt, к СВ zVirt и ВМ zVirt в рамках ролевой модели zVirt, к СВ RedVirt и ВМ RedVirt в рамках ролевой модели redVirt, к СВ HOSTVM и ВМ HOSTVM в рамках ролевой модели HOSTVM и к гипервизорам KVM и ВМ KVM в рамках ролевой модели KVM.

3.4.1.2. Осуществляется контроль доступа к операциям, выполняемым с помощью средств управления виртуальными машинами, в том числе к операциям создания, запуска, остановки, создания копий, удаления виртуальных машин, управления перемещением виртуальных машин, которые должны быть разрешены только назначенным пользователям.

3.4.2. Разграничение доступа к файлам и каталогам

3.4.2.1. Разграничение доступа к серверам виртуализации vCSA, гипервизорам ESXi, и виртуальным машинам (файлам виртуальных машин) реализуется в пределах ролевой модели разграничения доступа vSphere 5.5, 6.0, 6.5, 6.7, 7.0, 8.0 к СВ oVirt и ВМ oVirt в рамках ролевой модели oVirt, к СВ zVirt и ВМ zVirt в рамках ролевой модели zVirt, к СВ RedVirt и ВМ RedVirt в рамках ролевой модели redVirt, к СВ HOSTVM и ВМ HOSTVM в рамках ролевой модели HOSTVM и к гипервизорам KVM и ВМ KVM в рамках ролевой модели KVM.

3.4.2.2. Для каждой пары (субъект — объект) в **СЗИ ВИ Dallas Lock** задано явное и недвусмысленное перечисление допустимых типов доступа, т. е. тех типов доступа, которые являются санкционированными для данного субъекта (индивида или группы индивидов) к данному ресурсу информационной системы (объекту) или среды управления виртуализацией.

3.4.2.3. Механизм, реализующий дискреционный принцип контроля доступа, предусматривает возможности санкционированного изменения правил разграничения доступа, в том числе возможность санкционированного изменения списка пользователей информационной системы и списка защищаемых объектов.

3.4.2.4. Предусмотрены средства управления, ограничивающие распространение прав на доступ.

3.4.2.5. Реализованы функциональные возможности выделения сегментов безопасности[5] и меток субъектов доступа.

3.5. Подсистема гарантированной очистки памяти

3.5.1. При первоначальном назначении или при перераспределении внешней памяти **СЗИ ВИ Dallas Lock** предотвращает доступ субъекта к остаточной информации. Осуществляется очистка (обнуление, обезличивание) освобождаемых областей оперативной памяти ЭВМ, освобождаемых областей памяти внешних накопителей. Очистка осуществляется однократной произвольной записью в освобождаемую область памяти, ранее использованную для хранения защищаемых данных (файлов). На гипервизорах ESXi, KVM и oVirt/zVirt/HOSTVM/RedVirt осуществляется очистка остаточной информации по отношению к процессу удаления виртуальных машин и, соответственно, обеспечения невозможности восстановления информации, которую данные виртуальные машины содержали до удаления.

3.6. Подсистема контроля целостности

3.6.1. Осуществляется контроль целостности компонентов виртуальной среды на **ЦУ СЗИ ВИ** и серверах виртуализации vCSA (периодический, по расписанию, по запросу), на гипервизорах ESXi, KVM и СВ, созданных на базе oVirt (oVirt\zVirt\HOSTVM\RedVirt) (периодический, по запросу), на ВМ (периодический). По отношению к гипервизорам контроль целостности возможен к следующим защищаемым видам ресурсов:

[5] Настройка и управление сегментами безопасности осуществляется штатными средствами среды виртуализации.

- системные файлы;
- образы дисков виртуальных машин;
- конфигурационные файлы ВМ (виртуальное оборудование, настройки BIOS и пр.).

3.7. Подсистема аудита

3.7.1. Осуществляется регистрация входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее программного останова (для **ЦУ СЗИ ВИ** и серверов виртуализации vCSA, KVM и oVirt/zVirt/HOSTVM/RedVirt и гипервизоров KVM и oVirt/zVirt/HOSTVM/RedVirt). Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения АС.

3.7.2. Для серверов виртуализации vCSA, oVirt\zVirt\HOSTVM\RedVirt и гипервизоров ESXi, KVM, oVirt\zVirt\HOSTVM\RedVirt в пределах имеющейся информации в журналах серверов виртуализации, осуществляется регистрация попыток доступа программных средств (программ, процессов, задач, заданий) к защищаемым файлам. В параметрах регистрации указываются:

- дата и время попытки доступа к защищаемому файлу с указанием ее результата: успешная, неуспешная — несанкционированная;
- идентификатор субъекта доступа;
- спецификация защищаемого файла.

3.7.3. Для серверов виртуализации vCSA, гипервизоров ESXi, KVM и СВ, созданных на базе oVirt (oVirt\zVirt\HOSTVM\RedVirt), в пределах имеющейся информации в журналах серверов, осуществляется регистрация следующих событий:

- запуск, остановка и конфигурирование ВМ;
- запуск (завершение) работы компонентов виртуальной инфраструктуры;
- доступ субъектов доступа к компонентам виртуальной инфраструктуры;
- в составе и конфигурации компонентов виртуальной инфраструктуры во время их запуска, функционирования и аппаратного отключения.

Для каждого события регистрируется следующая информация:

- дата и время;
- субъект, осуществляющий регистрируемое действие;
- тип события (если регистрируется запрос на доступ, то следует отмечать объект и тип доступа);
- успешно ли осуществилось событие (обслужен запрос на доступ или нет).

3.7.4. Реализована возможность определения типов событий безопасности, подлежащих регистрации, для всех компонентов виртуальной инфраструктуры.

3.7.5. Для **ЦУ СЗИ ВИ** реализована возможность определения состава и содержания информации о событиях безопасности, подлежащих регистрации.

3.7.6. **СЗИ ВИ Dallas Lock** содержит средства выборочного ознакомления с регистрационной информацией.

3.7.7. Должна быть возможность просмотра и анализа информации о действиях отдельных пользователей в информационной системе (в т. ч. в среде виртуализации).

3.8. Подсистема фильтрации трафика

3.8.1. Реализовано обеспечение доверенного канала, маршрута внутри виртуальной инфраструктуры между администратором, пользователем и доверенным клиентом.

3.8.2. Реализована фильтрация сетевого трафика между компонентами виртуальной инфраструктуры.

3.9. Иные возможности существующих подсистем

3.9.1. **СЗИ ВИ Dallas Lock** блокирует подключения к СВ vCSA, KVM и к СВ oVirt, zVirt, HOSTVM и RedVirt с несанкционированных удаленных консолей.

3.9.2. Осуществляется использование предустановленных шаблонов типовых политик безопасности на основе требований руководящих документов.

3.9.3. Осуществляется взаимодействие **СЗИ ВИ Dallas Lock** с Единым центром управления **Dallas Lock** в части:

- отображения состояния **СЗИ ВИ Dallas Lock**;
- управления встроенными учетными данными пользователей **СЗИ ВИ Dallas Lock**;
- управления параметрами безопасности **ЦУ СЗИ ВИ Dallas Lock**;
- сбора информации с агентов **СЗИ ВИ Dallas Lock** в журналы Единого центра управления **Dallas Lock**;
- формирования заданий для **ЦУ СЗИ ВИ Dallas Lock**:
    - получение конфигурации;
    - применение конфигурации;
    - проверка обновлений;
    - получение отчета о параметрах безопасности **СЗИ ВИ**.

3.9.4. Осуществляется автоматическое снятие снапшотов ВМ.

4. ВХОДНЫЕ И ВЫХОДНЫЕ ДАННЫЕ

Входные данные

Входными данными являются:

- дерево объектов для каждой из развернутых и защищаемых виртуальных инфраструктур;
- список субъектов доступа, идентифицируемых логином (локальные пользователи, доменные пользователи, локальные пользователи гипервизоров, пользователи доменов vsphere.local, vsphere.common);
- настроенный набор ролей, определяющих полномочия по использованию объектов виртуальной инфраструктуры и их администрированию;
- список служб гипервизоров.

Выходные данные

Выходными данными являются:

- журнал СВ, создаваемые сервером в процессе работы, журнал событий, журналы гипервизора, анализируемые и собираемые **ЦУ СЗИ ВИ**, собственный журнал событий безопасности **ЦУ СЗИ ВИ**;
- значения контрольных сумм объектов, на которых установлен контроль целостности;
- файлы конфигураций модулей **СЗИ ВИ Dallas Lock**;
- сообщения **СЗИ ВИ Dallas Lock** в случае сигнализации при попытках несанкционированного доступа.

В журналах событий отслеживаются и отображаются такие данные, как дата, время, имя пользователя, имя объекта виртуальной инфраструктуры, тип события, результат, характер ошибки, фиксируются действия служб гипервизоров и иная информация.