УТВЕРЖДЕНО
ПФНА.501410.001 31-ЛУ

СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ В ВИРТУАЛЬНЫХ ИНФРАСТРУКТУРАХ

Dallas Lock

(версия 4.68)

Описание применения

ПФНА.501410.001 31

Листов 16

Аннотация

Данный документ 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 СОКРАЩЕНИЯ

Принятые сокращения

Сокращение	Полная формулировка
АУД	агент управления доступом
ВИ	виртуальная инфраструктура Dallas Lock
ВМ	виртуальная машина
ДБ	домен безопасности
ОС	операционная система
ОЗУ	оперативное запоминающее устройство
ПЗУ	постоянное запоминающее устройство
ПК	персональный компьютер
ОТК	отдел технического контроля
СВ	сервер виртуализации
СЗИ ВИ	система защиты информации в виртуальных инфраструктурах
ТС	техническое средство
ТУ	технические условия
ЦУ СЗИ ВИ	центр управления СЗИ ВИ.

Общая терминология

Сокращение	Полная формулировка
FQDN	Fully Qualified Domain Name. Доменное имя, которое не имеет неоднозначностей в определении. FQDN включает в себя доменные имена родительских доменов иерархии DNS
Гипервизор	программа или аппаратная схема, обеспечивающая или позволяющая одновременное, параллельное выполнение нескольких ОС на одном ТС

Терминология СЗИ ВИ Dallas Lock

Сокращение	Полная формулировка
Агент DL ESXi	компонент защиты гипервизора ESXi
Агент DL HOSTVM Engine	компонент защиты сервера виртуализации HOSTVM
Агент DL HOSTVM Host	компонент защиты гипервизора HOSTVM
Агент DL Hyper-V	компонент защиты гипервизора Hyper-V
Агент DL Hyper-V Cluster	компонент защиты для контроля кластера гипервизоров Hyper-V
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 Engine	компонент защиты сервера виртуализации RedVirt

Сокращение	Полная формулировка
Агент DL RedVirt Host	компонент защиты гипервизора RedVirt
Агент DL vCenter for Windows	компонент защиты сервера vCenter
Агент DL vCSA	компонент защиты сервера vCSA
Агент DL VMM	компонент защиты для ПО Microsoft System Center Virtual Machine Manager
Агент DL zVirt Engine	компонент защиты сервера виртуализации zVirt
Агент DL zVirt Host	компонент защиты гипервизора zVirt
АУД	агент управления доступом. Компонент СЗИ ВИ Dallas Lock, устанавливаемый на объекты ВИ (сервер vCenter for Windows, гипервизор Hyper-V, SC VMM, кластеры Hyper-V) для обеспечения выполнения политик безопасности
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
Домен безопасности	организация единой политики безопасности совокупностью ЦУ СЗИ ВИ и агентов управления доступом, 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 vCenter, СВ vCSA, гипервизор ESXi, гипервизор Hyper-V, виртуальная машина
ЦУ СЗИ ВИ	Центр управления СЗИ ВИ. Совокупность программных компонентов АУД и ядра СЗИ ВИ, управляемая с помощью Консоли

Терминология VMware

Сокращение	Полная формулировка
ESXi	гипервизор ESXi. Средство виртуализации VMware vSphere
vCenter	VMware vCenter Server. Сервер централизованного управления средством виртуализации ESXi (vCenter for Windows)
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

Терминология Hyper-V

Сокращение	Полная формулировка
Hyper-V	гипервизор Hyper-V. Средство виртуализации Microsoft Hyper-V
Microsoft Hyper-V	платформа (среда) виртуализации серверов/рабочих станций 64х ОС Windows

Терминология KVM

Сокращение	Полная формулировка
KVM	Kernel-based Virtual Machine. Программное решение, обеспечивающее виртуализацию в среде Linux

Терминология oVirt

Сокращение	Полная формулировка
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

Терминология Виртуализации zVirt

Сокращение	Полная формулировка
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

Терминология HOSTVM

Сокращение	Полная формулировка
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

Терминология РЕД Виртуализация

Сокращение	Полная формулировка
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

1 НАЗНАЧЕНИЕ

Изделие предназначено для защиты среды виртуализации на базе 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), KVM, использующей библиотеки libvirt (версии не ниже 4.5.0) в качестве инструмента управления гипервизором, oVirt (версии 4.4.x), Виртуализация zVirt (версий 3.0, 3.1, 3.3, 4.0), РЕД Виртуализация 7.3 и HOSTVM от несанкционированного доступа при работе в многопользовательских автоматизированных системах, 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.

2 УСЛОВИЯ ПРИМЕНЕНИЯ

Изделие СЗИ ВИ Dallas Lock включает в себя следующие компоненты:

- ядро системы защиты информации в виртуальных инфраструктурах;
- агент управления доступом (далее — АУД);
- веб-сервер ЦУ СЗИ ВИ;
- агент DL ESXi для гипервизора ESXi;
- агент DL vCenter for Windows для СВ vCenter;
- агент DL vCSA для СВ vCSA;
- агент DL Hyper-V для гипервизора Hyper-V;
- агент DL Hyper-V Cluster для контроля кластера гипервизоров Hyper-V;
- агент DL VMM для ПО Microsoft System Center Virtual Machine Manager;
- 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 RedVirt;
- агент DL RedVirt Host для гипервизора RedVirt;
- агент DL HOSTVM Engine для СВ HOSTVM;
- агент DL HOSTVM Host для гипервизора HOSTVM.

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

ТС с установленным ЦУ СЗИ ВИ должно иметь в составе аппаратный идентификатор, содержащий лицензионный ключ для изделия СЗИ ВИ Dallas Lock. 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 64-bit:
   - Windows 7 (SP 1) (Ultimate, Enterprise, Professional, Home Premium, Home Basic, Starter);
   - Windows 8 (Pro, Enterprise);
   - Windows 8.1 (Pro, Enterprise);
   - Windows 10 (Enterprise, Education, Pro, Home);
   - Windows 11 (Enterprise, Education, Pro, Home).
2. Минимальная конфигурация ТС:
   - процессор: Intel или AMD с 2 логическими ядрами по 2 ГГц каждое;
   - ОЗУ — минимум 2 Гб;
   - ПЗУ — минимум 20 Гб;
   - сетевая карта.
3. Поддерживаемые серверные ОС 64-bit:
   - Windows Server 2008 R2 (SP 1) (Foundation, Standard, Web, Enterprise, Datacenter);
   - Windows Server 2012 (Foundation, Essentials, Standard, Datacenter);
   - Windows Server 2012 R2 (Foundation, Essentials, Standard, Datacenter);
   - Windows Server 2016 (Multipoint Premium Server, Essentials, Standard, Datacenter, Storage Server);
   - Windows Server 2019 (Essentials, Standard, Datacenter);
   - Windows Server 2022 (Standard, Datacenter).
4. Минимальная конфигурация ТС с серверной ОС:
   - процессор: Intel или AMD с 2 логическими ядрами по 2 ГГц каждое;
   - ОЗУ — минимум 4 Гб;
   - ПЗУ — минимум 40 Гб;
   - сетевая карта.

Для установки агента DL vCenter for Windows ТС с установленным VMware vCenter Server 6.0/6.5/6.7 должно иметь следующий состав и характеристики программно-технического обеспечения:

1. Поддерживаемые ОС (64-bit):
   - Windows Server 2008 R2 (Foundation, Standard, Enterprise, Datacenter, Web Server 2008, Storage Server 2008);
   - Windows Server 2008 R2 (SP 1) (Foundation, Standard, Web, Enterprise, Datacenter);

- Windows Server 2012 (Foundation, Essentials, Standard, Datacenter);
- Windows Server 2012 R2 (Foundation, Essentials, Standard, Datacenter);
- Windows Server 2016 (Essentials, Standard, Datacenter).

2. Минимальная конфигурация ТС:
   - процессор: Intel или AMD с 2-мя логическими ядрами по 2 ГГц каждое;
   - ОЗУ — минимум 12 Гб;
   - ПЗУ — минимум 60 Гб;
   - сетевая карта.

Для установки агента DL vCSA ТС с установленным VMware vCSA 6.5/6.7/7.0 должно иметь следующий состав и характеристики программно-технического обеспечения:

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

Для установки агента DL ESXi ТС с установленным гипервизором VMWare ESXi 6.0/6.5/6.7/7.0 должно иметь следующий состав и характеристики программно-технического обеспечения:

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

Для установки агентов DL Hyper-V, DL Hyper-V Cluster ТС с установленным Windows Server (Hyper-V) (версий 2012, 2012 R2, 2016, 2019) 64-bit должно иметь следующий состав и характеристики программно-технического обеспечения:

- процессор: Intel или AMD с 2-мя логическими ядрами по 2 ГГц каждое;
- ОЗУ — минимум 2 Гб;
- ПЗУ — минимум 32 Гб;
- сетевая карта.

Для установки агента DL VMM ТС с установленным ПО Microsoft System Center Virtual Machine Manager должно иметь следующий состав и характеристики программно-технического обеспечения:

- процессор: Intel или AMD с 2 логическими ядрами по 2 ГГц каждое;
- ОЗУ — минимум 2 Гб;
- ПЗУ — минимум 32 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 1.6;
   - Astra Linux 2.12;
   - CentOS 7.5;
   - Linux Mint 18.3;
   - Ubuntu 18.04.2 LTS.
2. Минимальная конфигурация ТС:
   - процессор: Intel или AMD с 2-мя 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-мя 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-мя 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 3.0, 3.1, 3.3, 4.0) 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 Host ТС с установленным гипервизором zVirt (версий 3.0, 3.1, 3.3, 4.0) должно иметь следующий состав и характеристики программно-технического обеспечения:

1. Поддерживаемые ОС (только 64-bit):
   - 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-мя 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 (только x64 версии):
   - HOSTVM Node.
2. Минимальная конфигурация ТС:

- процессор: Intel или AMD с 2-мя логическими ядрами по 2 ГГц каждое;
- ОЗУ — минимум 2 Гб;
- ПЗУ — минимум 64 Гб;
- сетевая карта — минимум 1 Гбит/с.

Средства управления виртуальной инфраструктурой могут быть использованы как в сетях с доменной организацией, так и в одноранговых сетях.

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

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.

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

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

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.

3.1 Подсистема управления пользователями

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 vCenter, vCSA, Hyper-V, oVirt/zVirt/HOSTVM/RedVirt и гипервизорах KVM, oVirt/zVirt/HOSTVM/RedVirt (требование мер защиты информации согласно приказам № 21, № 17, обозначение и номер меры — «ЗСВ.1»). Контроль пользователей, имеющих право на вход на гипервизор, должен осуществляться посредством выполнения необходимых настроек на стороне ЦУ СЗИ ВИ и процесса синхронизации гипервизора с ЦУ СЗИ ВИ.
2. Обеспечивает запрет доступа к защищаемым ресурсам серверов виртуализации vCenter, vCSA, Hyper-V, 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 к гипервизору ESXi при условии успешной авторизации, должен осуществляться посредством выполнения необходимых настроек на стороне ЦУ СЗИ ВИ и процесса синхронизации с ЦУ СЗИ ВИ.
3. Реализовано управление идентификаторами, в том числе создание, присвоение, уничтожение идентификаторов. В качестве идентификатора может выступать:
   - имя локального пользователя ОС среды виртуализации vCenter/vCSA/Hyper-V/KVM/oVirt/zVirt/RedVirt/HOSTVM;
   - имя доменного пользователя AD при условии, что ЦУ СЗИ ВИ, сервер виртуализации vCenter (или Hyper-V) введены под управление AD и на сервере виртуализации подключен контроллер домена в качестве возможного средства проверки авторизации. Вход доменных пользователей возможен только на ЦУ СЗИ ВИ и серверах виртуализации vCenter, vCSA, Hyper-V, oVirt, zVirt, RedVirt и HOSTVM;
   - имя пользователя ОС на гипервизоре ESXi.
4. Реализовано управление средствами аутентификации, в том числе хранение, выдача и инициализация для всех компонент защищаемой виртуальной инфраструктуры. Реализована защита аутентификационной информации субъектов доступа, хранящейся в компонентах виртуальной инфраструктуры от неправомерных доступа к ней, уничтожения или модифицирования. Осуществляется блокирование средств аутентификации и принятие мер в случае утраты и (или) компрометации средств аутентификации для ЦУ СЗИ ВИ, серверов виртуализации vCenter, vCSA, Hyper-V, oVirt/zVirt/HOSTVM/RedVirt и гипервизоров KVM/oVirt/zVirt/RedVirt/HOSTVM. Реализована блокировка доступа к компонентам виртуальной инфраструктуры для субъектов доступа, не прошедших процедуру аутентификации.
5. 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.
6. Реализована возможность разделения полномочий (ролей, типов учетных записей) пользователей, администраторов и лиц, обеспечивающих функционирование СЗИ ВИ Dallas Lock.
7. В программном обеспечении изделия реализовано ограничение неуспешных попыток входа в СЗИ ВИ Dallas Lock.
8. Для ЦУ СЗИ ВИ и сервера виртуализации vCenter и гипервизора Hyper-V реализовано ограничение числа параллельных сеансов доступа для каждой учетной записи пользователя.

3.2 Подсистема управления доступом

Разграничение доступа к объектам виртуальной инфраструктуры

1. Реализовано разграничение доступа к следующим компонентам виртуальной инфраструктуры — ЦУ СЗИ ВИ, серверам виртуализации vCenter и Hyper-V. Разграничение доступа к серверам виртуализации vCSA, к гипервизорам ESXi и виртуальным машинам ESXi (файлам виртуальных машин) реализуется в пределах ролевой модели разграничения доступа vSphere, 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.
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. Реализованы методы предоставления доступа к виртуальным машинам, обеспечивающие возможность доступа с использованием одних аутентификационных данных только к одной виртуальной машине с одного АРМ пользователя или эксплуатационного персонала.
4. Реализовано принудительное прерывание и блокировка сессии пользователя при работе с ВМ для сред виртуализации VMware vSphere и Hyper-V.

Разграничение доступа к файлам и каталогам

1. Реализовано разграничение доступа по дискреционному принципу к объектам файловой системы и устройствам в виртуальной среде — на ЦУ СЗИ ВИ, сервере виртуализации vCenter и Hyper-V. Разграничение доступа к серверам виртуализации vCSA, к гипервизорам ESXi и виртуальным машинам (файлам виртуальных машин) реализуется в пределах ролевой модели разграничения доступа vSphere, 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.
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. 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.
4. Предусмотрены средства управления, ограничивающие распространение прав на доступ.
5. Реализованы функциональные возможности выделения сегментов безопасности и меток субъектов доступа.

3.3 Подсистема гарантированной очистки памяти

При первоначальном назначении или при перераспределении внешней памяти СЗИ ВИ Dallas Lock предотвращает доступ субъекту к остаточной информации. Осуществляется очистка (обнуление, обезличивание) 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, KVM, oVirt, zVirt, RedVirt, HOSTVM и Hyper-V осуществляется очистка остаточной информации по отношению к процессу удаления виртуальных машин и, соответственно, обеспечения невозможности восстановления информации, которую данные виртуальные машины содержали до удаления.

3.4 Подсистема контроля целостности

1. Осуществляется контроль целостности компонентов виртуальной среды — на ЦУ СЗИ ВИ и серверах виртуализации vCenter, vCSA и Hyper-V (периодический, по расписанию, по запросу), на гипервизорах ESXi, KVM и СВ созданных на базе oVirt (oVirt\zVirt\HOSTVM\RedVirt) (периодический, по запросу), на ВМ (периодически). По отношению к гипервизорам ESXi и KVM контроль целостности возможен к следующим защищаемым видам ресурсов:
   - системные файлы;
   - образы дисков виртуальных машин;
   - конфигурационные файлы виртуальных машин (виртуальное оборудование, настройки BIOS и пр.).

2. Осуществляется контроль целостности аппаратной части гипервизора.
3. Осуществляется контроль целостности настроек параметров безопасности виртуальной машины при ее запуске, в качестве сред виртуализации при создании виртуальных машин должны использоваться VMware vSphere и Hyper-V.

3.5 Подсистема фильтрации трафика

1. Реализовано обеспечение доверенного канала, маршрута внутри виртуальной инфраструктуры между администратором, пользователем и доверенным клиентом.
2. Реализована фильтрация сетевого трафика между компонентами виртуальной инфраструктуры.

3.6 Подсистема администрирования

Управление параметрами безопасности для всех защищенных СЗИ ВИ Dallas Lock компонентов виртуальной инфраструктуры осуществляется из единого Центра управления СЗИ ВИ Dallas Lock.

3.7 Подсистема восстановления после сбоев

Имеется возможность сохранения и применения файла конфигурации настроек ЦУ СЗИ ВИ из Консоли.

3.8 Подсистема аудита

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 vCenter, vCSA, Hyper-V, 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. В параметрах регистрации указываются:
   - дата и время входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы;
   - результат попытки входа: успешная или неуспешная — несанкционированная;
   - идентификатор (код или фамилия) субъекта, предъявленный при попытке доступа;
   - код или пароль, предъявленный при неуспешной попытке.
2. Для всех компонентов виртуальной инфраструктуры с ОС семейства Windows (включая сервер виртуализации vCenter и Hyper-V) осуществляется регистрация запуска (завершения) программ и процессов (заданий, задач), предназначенных для обработки защищаемых файлов. В параметрах регистрации указываются:
   - дата и время запуска;
   - имя (идентификатор) программы (процесса, задания);
   - идентификатор субъекта доступа, запросившего программу (процесс, задание);
   - результат запуска (успешный, неуспешный — несанкционированный).
3. Для сервера виртуализации vCenter и Hyper-V и гипервизора ESXi, в пределах имеющейся информации в журналах, 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.
4. Для серверов виртуализации vCenter, vCSA и Hyper-V и гипервизорам ESXi, KVM и СВ, созданных на базе oVirt (oVirt\zVirt\HOSTVM\RedVirt) в пределах имеющейся информации в журналах, осуществляется регистрация следующих событий:
   - запуск, остановка и конфигурирование ВМ;
   - запуск (завершение) работы компонентов виртуальной инфраструктуры;
   - доступ субъектов доступа к компонентам виртуальной инфраструктуры;
   - изменения 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).

5. Для всех компонентов виртуальной инфраструктуры реализована возможность определения типов событий безопасности, подлежащих регистрации, для всех компонентов виртуальной инфраструктуры с ОС семейства Windows.
6. Для ЦУ СЗИ ВИ реализована возможность определения состава и содержания информации о событиях безопасности, подлежащих регистрации.
7. СЗИ ВИ Dallas Lock содержит средства выборочного ознакомления с регистрационной информацией.
8. В СЗИ ВИ Dallas Lock реализована возможность просмотра и анализа информации о действиях отдельных пользователей в информационной системе (в т. ч. среде виртуализации).

3.9 Подсистема развертывания

Осуществляется локальное и удаленное (средствами Консоли) развертывание компонентов защиты СЗИ ВИ Dallas Lock.

3.10 Доработка существующих подсистем

1. СЗИ ВИ Dallas Lock блокирует подключения к СВ vCenter, vCSA, Hyper-V, KVM и к СВ oVirt, zVirt, HOSTVM и RedVirt с несанкционированных удаленных консолей.
2. Осуществляется использование предустановленных шаблонов типовых политик безопасности на основе требований руководящих документов.
3. Осуществляется взаимодействие СЗИ ВИ Dallas Lock с Единым центром управления Dallas Lock в части:
   - отображения состояния СЗИ ВИ Dallas Lock;
   - управления учетными данными пользователей (кроме KMV, zVir, oVirt, RedVirt и HOSTVM);
   - сбора информации с агентов СЗИ ВИ Dallas Lock в журналы Единого центра управления Dallas Lock;
   - формирования заданий для агентов СЗИ ВИ Dallas Lock;
   - настройки лицензирования.
4. Осуществляется автоматическое снятие снапшотов ВМ.

4 ВХОДНЫЕ И ВЫХОДНЫЕ ДАННЫЕ

4.1 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.

4.2 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.