УТВЕРЖДЕНО
ПФНА.501410.001 34-ЛУ

СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ В ВИРТУАЛЬНЫХ ИНФРАСТРУКТУРАХ

Dallas Lock

(версия 5.87.1695.0)

Руководство оператора (пользователя)

ПФНА.501410.001 34

Листов 12

Содержание

ВВЕДЕНИЕ

Система защиты информации в виртуальных инфраструктурах **Dallas Loc**k включает в себя следующие компоненты:

- ядро системы защиты информации в виртуальных инфраструктурах (далее — Ядро **СЗИ ВИ**);
- 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.

Ядро **СЗИ ВИ** представляет собой компонент Центра управления **СЗИ ВИ Dallas Lock**, обеспечивающий защиту серверов виртуализации посредством взаимодействия с агентами DL. Реализовано в виде службы.

В руководстве содержатся сведения, необходимые пользователю для работы на компьютерах с установленными компонентами защиты **СЗИ ВИ**.

Руководство подразумевает наличие у пользователя навыков работы с Linux-подобными системами.

В руководстве представлены элементы веб-интерфейса **СЗИ ВИ**.

ТЕРМИНЫ И СОКРАЩЕНИЯ

Некоторые термины, содержащиеся в тексте руководства, уникальны для **СЗИ ВИ**, другие используются для удобства, третьи выбраны из соображений краткости.

Термины *компьютер* и *ПК* считаются эквивалентными и используются в тексте руководства.

Принятые сокращения

Сокращение	Полная формулировка
BIOS	базовая система ввода-вывода, реализованная в виде микропрограмм, записанных в ПЗУ (постоянное запоминающее устройство) компьютера. Это — первая программа, которую компьютер использует сразу же после включения. Задача — опознать устройства (процессор, память, видео, диски и т. д.), проверить их исправность, инициировать
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 Engine	компонент защиты сервера виртуализации RedVirt
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
Гипервизор	программа или аппаратная схема, обеспечивающая или позволяющая одновременное, параллельное выполнение нескольких ОС на одном ТС
ОС	операционная система
ПК	персональный компьютер
Центр управления СЗИ ВИ Dallas Lock	совокупность программных компонентов АУД и Ядра **СЗИ ВИ**, управляемая с помощью Консоли

1. ОБЩИЕ СВЕДЕНИЯ О СИСТЕМЕ ЗАЩИТЫ

1.1 Назначение системы защиты

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.

В соответствии с требованиями безопасности предприятия лицами, ответственными за установку и эксплуатацию **СЗИ ВИ**, настраиваются соответствующие параметры и политики безопасности, механизмы которых реализованы в **СЗИ ВИ**. Подробное описание настройки механизмов администрирования **СЗИ ВИ** содержится в документе ПФНА.501410.001 РЭ «Руководство по эксплуатации».

Оператором (пользователем) **СЗИ ВИ** является пользователь, осуществляющий ввод и обработку информации любыми программными средствами на персональном компьютере, на котором установлен один из компонентов **СЗИ ВИ**.

1.2 Условия работы

1.2.1 Данные учетной записи

Чтобы получить доступ к веб-интерфейсу **СЗИ ВИ**, необходимо иметь зарегистрированную в **СЗИ ВИ** учетную запись. Регистрация учетных записей осуществляется администратором безопасности.

Учетная запись пользователя, зарегистрированного в **СЗИ ВИ**, имеет следующие атрибуты, которые необходимы непосредственно для входа на веб-интерфейс (авторизации):

Основные	
Имя (логин)	За пользователем закрепляется условное имя (идентификатор), необходимое для идентификации его в системе защиты
Пароль	Пользователю сообщается пароль, который необходим для подтверждения того, что именно он является пользователем, зарегистрированным под этим именем (происходит аутентификация)

Чтобы приступить к работе на компьютере, необходимо:

1. Уточнить у администратора безопасности все авторизационные данные для входа на защищенный компьютер.
2. Запомнить свое имя в системе защиты и пароль.
3. Никому не сообщать пароль.

Авторизация пользователя осуществляется при каждом входе.

При вводе имени и пароля необходимо соблюдать следующие правила:

- **для имени:**
  a. максимальная длина имени — 300 символов;
  b. имя может содержать латинские символы, символы кириллицы, цифры и специальные символы;

[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.

c. разрешается использовать различные регистры клавиатуры, при этом регистр не учитывается, то есть заглавные и прописные буквы воспринимаются как одинаковые (User и user являются одинаковыми именами).

- **для пароля:**
  a. пароль может содержать латинские символы, символы кириллицы, цифры и специальные символы;
  b. разрешается использовать различные регистры клавиатуры, при этом нужно помнить, что заглавные и прописные буквы воспринимаются как различные (Password и password являются разными паролями).

1.2.2 Права для работы под учетной записью

Также необходимо выяснить у администратора безопасности, какими именно правами и привилегиями обладает оператор (пользователь), к каким ресурсам может иметь доступ и с какими программами и приложениями работать.

Во всех сложных ситуациях, связанных с работой **СЗИ ВИ**, которые оператор (пользователь) не в состоянии разрешить самостоятельно, необходимо обращаться к администратору. Так, в частности, если имеющихся прав доступа к ресурсам недостаточно для эффективного выполнения должностных обязанностей (запрещающие сообщения), необходимо обратиться к администратору безопасности или другому должностному лицу, отвечающему за распределение прав доступа к ресурсам компьютера и сети.

2. ВХОД НА ЗАЩИЩЕННЫЙ КОМПЬЮТЕР

2.1 Вход в операционную систему

При загрузке компьютера, на который установлен один из компонентов **СЗИ ВИ**, в зависимости от ОС, появляется экран приветствия (приглашение на вход в операционную систему) (рис. 1).

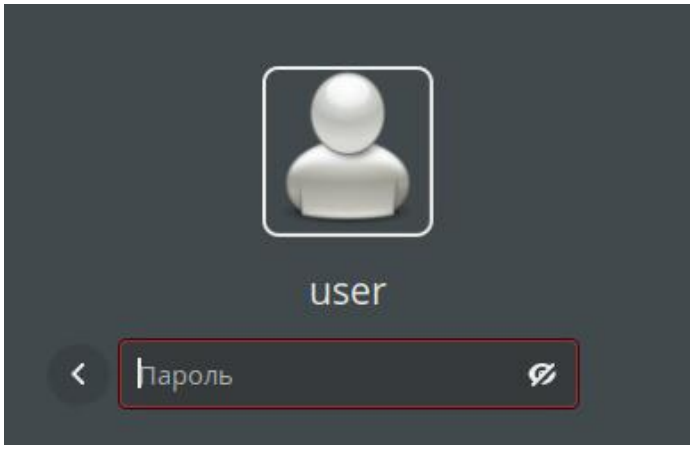

Рис. 1. Экран приветствия в ОС RedOS

Для входа на компьютер, с установленным **СЗИ ВИ**, каждому оператору (пользователю) предлагается выполнить следующую последовательность шагов.

1. Заполнить поле имени пользователя, под которым он зарегистрирован в системе защиты. В зависимости от настроек в этом поле может оставаться имя пользователя, выполнившего вход последним.
2. Ввести пароль. При вводе пароля, поле для ввода является текстовым. Однако на экране вместо символа, соответствующего каждой нажатой клавише, появляется символ «●» (точка). При вводе пароля следует помнить, что строчные и прописные буквы различаются. Допущенные ошибки при вводе исправляются так же, как и при заполнении текстового поля.
3. Нажать кнопку **Enter**.

После нажатия кнопки **Enter** осуществляется проверка наличия в системе защиты зарегистрированного пользователя с указанным именем. После чего проверяется правильность указанного пользователем пароля. В случае успеха проверки пользователю разрешается вход.

Для входа в веб-консоль **СЗИ ВИ**, каждому оператору (пользователю) предлагается выполнить следующую последовательность шагов.

1. Заполнить поле имени пользователя, под которым он зарегистрирован в системе защиты. В зависимости от настроек в этом поле может оставаться имя пользователя, выполнившего вход последним.
2. Ввести пароль. При вводе пароля, поле для ввода является текстовым. Однако на экране вместо символа, соответствующего каждой нажатой клавише, появляется символ «●» (точка). При вводе пароля следует помнить, что строчные и прописные буквы различаются. Допущенные ошибки при вводе исправляются так же, как и при заполнении текстового поля (Рис. 2).

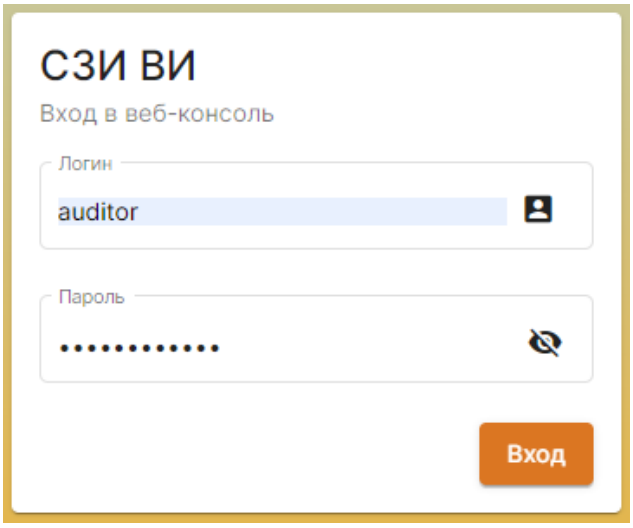

Рис. 2. Экран входа в веб-интерфейс СЗИ ВИ

3. Нажать на клавиатуре **Enter** или на интерфейсе кнопку **Вход**.

2.2 Ошибки, возникающие при входе

Попытка входа оператора (пользователя) в веб-интерфейс, на который установлен **СЗИ ВИ**, может быть неудачной, к чему приводит ряд событий. При этом на экран могут выводиться сообщения о характере события или соответствующие сообщения предупреждающего характера.

Если введенный пароль неверен, то на экране появится сообщение об ошибке, после чего система защиты предоставит возможность повторно ввести имя и пароль (Рис. 3).

Рис. 3. Сообщение при вводе неправильного пароля

Возможна ситуация, при которой оператор (пользователь) забыл свой пароль. В этом случае он также должен обратиться к администратору, который имеет право назначить оператору (пользователю) новый пароль.

Так же при ошибочном вводе данных в поле имени могут возникнуть соответствующие сообщения (Рис. 4).

Рис. 4. Ошибка авторизации

Администратор может отключить учетную запись, тогда при авторизации система защиты выведет соответствующее предупреждение (Рис. 5).

Рис. 5. Сообщение при отключенной учетной записи

В такой ситуации необходимо обратиться к администратору системы защиты.

При отключении компьютера, на котором установлен **СЗИ ВИ** во время авторизации может появиться предупреждение (Рис.6).

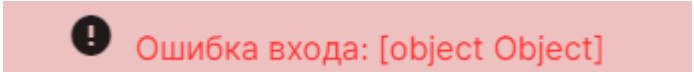

Рис.6. Предупреждение о нарушенной целостности

3. ЗАВЕРШЕНИЕ СЕАНСА РАБОТЫ

3.1 Завершение работы

> Компьютер, на котором установлен Центр управления **СЗИ ВИ Dallas Lock**, предназначен для режима беспрерывной работы. Выключение данного компьютера влечет за собой нештатную ситуацию в работе **СЗИ ВИ**.

При завершении сеанса работы оператора (пользователя) на компьютере, из которого осуществляется доступ к веб-интерфейсу **СЗИ ВИ**, выход оператора (пользователя) из системы выполняется в штатном для используемой ОС режиме. Для этого нужно (при работе в ОС RedOS Murom):

1. Сохранить все данные и завершить работу всех приложений.
2. В главное меню в нижнем правом углу нажать кнопку выхода из системы и выбрать пункт **Завершить сеанс**.
3. После нажатия кнопки **Завершить сеанс** сеанс текущего оператора (пользователя) будет завершен, а на экране появится диалог для повторной авторизации в ОС.

При завершении сеанса работы оператора (пользователя) в веб-интерфейсе:

1. Нажать на кнопку (Рис. 7).
2. Выбрать пункт **Выход**.

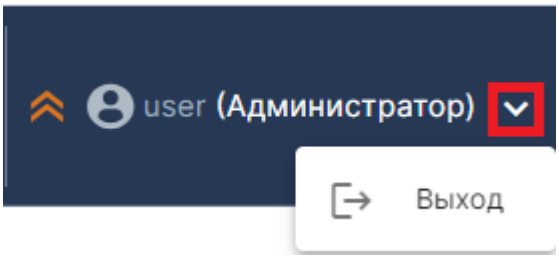

Рис. 7. Выход из веб-интерфейса СЗИ ВИ

3.2 Смена пользователя

Возможно, что завершение сеанса пользователя необходимо для смены пользователя веб-интерфейса **СЗИ ВИ**, то есть для входа в систему под другой учетной записью.

Для завершения сеанса и смены пользователя достаточно выйти из веб-интерфейса, после чего зайти под новыми учетными данными.

4. СМЕНА ПАРОЛЯ

Оператор (пользователь) не может самостоятельно сменить свой пароль для авторизации в **СЗИ ВИ**. В этом случае он должен обратиться к администратору, который имеет право назначить оператору (пользователю) новый пароль.

В соответствии с политиками безопасности могут быть включены настройки сложности паролей. Сложные пароли при их регулярной смене снижают вероятность успешной атаки на пароль. Поэтому при смене пароля пользователю необходимо выяснить у администратора безопасности дополнительные требования для установления паролей. К таким требованиям относятся:

- максимальный срок действия пароля;
- минимальная длина пароля (количество символов);
- необходимое наличие спецсимволов (*, #, @, %, ^, & и пр.);
- необходимое наличие строчных и прописных букв;
- необходимое наличие цифр;
- необходимое отсутствие цифры в первом и последнем символе.

5. ДОПОЛНИТЕЛЬНЫЕ ВОЗМОЖНОСТИ

СЗИ ВИ предоставляет пользователю несколько дополнительных возможностей, позволяющих увеличить уровень защищенности информации.

5.1 Работа с логами

СЗИ ВИ позволяет получать расширенные логи в случае возникновения непредвиденных инцидентов для предоставления их технической поддержке.

При предоставлении логов технической поддержке необходимо в сопроводительном письме предоставить подробное описание ситуации (окружение, время, порядок действий), при которой возникла та или иная нештатная ситуация (ошибка).

Для включения логов на агентах Linux (ESXi, vCSA, KVM/oVirt/zVirt/HOSTVM/RedVirt) нужно создать пустой файл в директории /tmp/ командой *touch dlneedlog* в директории /tmp/

Файл пропадает после перезагрузки гипервизора/сервера виртуализации.

Далее необходимо выполнить перезапуск службы DL командой *sudo systemctl restart confident-vicored*

Логи агента буду расположены по пути: */etc/confident/vicored.log.*

Чтобы открыть файлы логов, возможно, нужно будет выдать дополнительные права: *sudo chmod 777 vicored.log.*

5.2 Работа с отчетом о параметрах безопасности

СЗИ ВИ Dallas Lock позволяет сформировать отчет в формате HTML о параметрах безопасности, содержащий перечень защищаемых объектов, список пользователей/групп и их ролей, а также параметры политик безопасности.

Для создания отчета необходимо открыть дополнительное меню Консоли, выбрать пункт **Отчет о параметрах безопасности СЗИ ВИ** и нажать **Сгенерировать**, после чего дождаться построения отчета. Затем в пункте **Отчет о параметрах безопасности СЗИ ВИ** выбрать **Список отчетов** и, нажав на кнопку  , стоящую напротив нужного отчета, скачать его и просмотреть.

Отчет начинается с перечня атрибутов:

- «Дата построения»;
- «Имя компьютера»;
- «Название подразделения»;
- «Наименование АС»;
- «Рабочее место»;
- «Операционная система»;
- «Версия Dallas Lock»;
- «Номер лицензии Dallas Lock»;
- «Максимальное кол-во терминальных сессий»;
- «Номер системного блока».

Далее следует информация о редакции **СЗИ ВИ** («Стандартная\Расширенная»), наличии подключения к **ЕЦУ**.

Последующие разделы содержат информацию о субъектах и объектах доступа домена безопасности, включая параметры безопасности хоста с установленным ЦУ **СЗИ ВИ** и параметры элементов домена: платформы виртуализации (oVirt, vSphere, KVM), установленные агенты, роли, политики безопасности.