УТВЕРЖДЕНО
ПФНА.501410.001 РЭ-ЛУ

СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ В ВИРТУАЛЬНЫХ ИНФРАСТРУКТУРАХ

Dallas Lock

(версия 5.87.1695.0)

Руководство по эксплуатации

ПФНА.501410.001 РЭ

Листов 160

Аннотация

Данное руководство по эксплуатации освещает вопросы по установке, настройке и сопровождению системы защиты информации в виртуальных инфраструктурах **Dallas Lock** и предназначено для лиц, ответственных за ее эксплуатацию.

Руководство по эксплуатации подразумевает наличие у пользователя навыков работы в операционных системах Linux, с платформами VMware vSphere и oVirt/zVirt/HOSTVM/RedVirt, гипервизорами VMware ESXi и KVM.

В документе представлены элементы графических интерфейсов, которые соответствуют эксплуатации Центра управления **СЗИ ВИ** в веб-интерфейсе. Следует обратить внимание, что элементы графического интерфейса могут иметь незначительные отличия от представленных.

Содержание

ВВЕДЕНИЕ

Данное руководство предназначено для администратора программного продукта «Система защиты информации в виртуальных инфраструктурах **Dallas Lock**.

В руководстве содержатся сведения, необходимые для получения общего представления о системе защиты, ее функциональных возможностях, а также для установки, настройки и управления работой в соответствии с требованиями безопасности.

В данном руководстве описание работы с системой носит процедурный характер, то есть основное внимание сосредоточено на порядке выполнения тех или иных действий.

На сайте продукта (www.dallaslock.ru) можно получить дополнительную информацию о системе защиты в виртуальных инфраструктурах **Dallas Lock**, в предыдущих версиях, а также заказать комплекс услуг по проектированию, внедрению и сопровождению продукта.

Обращения в службу технической поддержки системы защиты в виртуальных инфраструктурах **Dallas Lock** осуществляются по электронному адресу: helpdesk@confident.ru.

Сайт компании-разработчика системы защиты в виртуальных инфраструктурах **Dallas Lock ООО «Конфидент»** доступен по ссылке: www.confident.ru.

ТЕРМИНЫ И СОКРАЩЕНИЯ

Термины *компьютер, ПК, рабочая станция, ТС* считаются эквивалентными и используются в тексте руководства.

Принятые сокращения

Сокращение	Полная формулировка
ВИ	виртуальная инфраструктура
ВМ	виртуальная машина
ДБ	домен безопасности
ЕЦУ	Единый Центр Управления **Dallas Lock** (**ЕЦУ Dallas Lock**)
Консоль	веб-консоль Центра управления **СЗИ ВИ Dallas Lock**
КЦ	контроль целостности
ЛВС	локальная вычислительная сеть
МЭ	межсетевой экран
ОС	операционная система
ПЗУ	постоянное запоминающее устройство, энергонезависимая память, используемая для хранения массива неизменяемых данных
ПК	персональный компьютер
СВ	сервер виртуализации
Сервер УД	сервер управления доступом
СЗИ ВИ	система защиты информации в виртуальных инфраструктурах
ТС	техническое средство
УЦ	удостоверяющий центр
ФС	файловая система
ЦУ СЗИ ВИ	центр управления **СЗИ ВИ**
AD	Active Directory

Общая терминология

Сокращение	Полная формулировка
Виртуальная инфраструктура	информационная система, состоящая из целевых элементов (виртуальных машин, виртуальных коммутаторов и т.д.) и обеспечивающих их работу вспомогательных элементов (гипервизоров, серверов виртуализации, устанавливаемых на них ОС), позволяющая более эффективно управлять аппаратными ресурсами по сравнению с обычной ИТ-инфраструктурой (физическими серверами, рабочими станциями, коммутаторами и т.д.)
Гипервизор	программа или аппаратная схема, обеспечивающая или позволяющая одновременное, параллельное выполнение нескольких ОС на одном ТС
Объекты ВИ	элементы ВИ, такие как: СВ vCSA, СВ oVirt/zVirt/HOSTVM/RedVirt, гипервизор oVirt/zVirt/HOSTVM/RedVirt, гипервизор ESXi, гипервизор KVM, виртуальная машина, введенные под контроль данного Центра управления СЗИ ВИ и образующие домен безопасности
Платформа виртуализации	программное решение для создания виртуальной инфраструктуры (vSphere, KVM, oVirt, zVirt, HOSTVM, RedVirt), предоставляющее набор целевых и вспомогательных элементов для ее построения
Сервер виртуализации	вспомогательный компонент ВИ, сервер или ВМ с установленным на нем средством управления системой виртуализации
Контроль целостности	проверка соответствия контролируемого объекта эталонному образцу с использованием контрольных сумм

Сокращение	Полная формулировка
Контрольная сумма	некоторое значение, рассчитанное по набору данных путём применения определённого алгоритма и используемое для проверки целостности данных при их передаче или хранении
Снапшот	моментальный снимок, копия файлов и каталогов файловой системы на определённый момент времени

Терминология СЗИ ВИ Dallas Lock

Сокращение	Полная формулировка
Агент DL KVM	компонент защиты гипервизора KVM
Агент DL Engine	компонент защиты сервера виртуализации oVirt, zVirt, HOSTVM и RedVirtуализации
Агент DL Host	компонент защиты гипервизора oVirt, zVirt, HOSTVM и RedVirtуализации
Веб-сервер СЗИ ВИ	позволяет подключаться через веб-интерфейс из любого браузера с любого АРМ к Ядру ЦУ **СЗИ ВИ** для выполнения функций администрирования **СЗИ ВИ**. Является частью ядра **СЗИ ВИ**
Домен безопасности	организация политик безопасности совокупностью Центра управления **СЗИ ВИ** и агентов управления доступом на множестве объектов ВИ
Веб-консоль центра управления СЗИ ВИ	компонент Центра управления **СЗИ ВИ Dallas Lock**, средство администрирования **СЗИ ВИ**
Параметры безопасности (политики безопасности)	совокупность правил по обеспечению безопасности информации, выраженные настраиваемыми категориями системы защиты
Сервер управления доступом (Сервер УД)	компонент Центра управления **СЗИ ВИ Dallas Lock**, обеспечивающий защиту серверов виртуализации посредством взаимодействия с агентами DL. Входит в состав Ядра **СЗИ ВИ**
СЗИ ВИ Dallas Lock	программный комплекс, состоящий из Центра управления **СЗИ ВИ** и работающих под его управлением агентов DL, устанавливаемых в виртуальные инфраструктуры с целью обеспечения безопасности путем включения в **ДБ** их элементов
Центр управления СЗИ ВИ	совокупность программных компонентов агентов DL, сервера УД и ядра **СЗИ ВИ**, управляемая с помощью Консоли
Ядро СЗИ ВИ	компонент Центра управления **СЗИ ВИ Dallas Lock**, обеспечивающий централизованное управление объектами виртуальной инфраструктуры. Реализовано в виде службы

Терминология VMware

Сокращение	Полная формулировка
ESXi	гипервизор ESXi, средство виртуализации VMware vSphere
vCSA	VMware vCenter Server Appliance, сервер централизованного управления средством виртуализации ESXi, состоит из службы vCenter выполняющейся на ОС Photon, установленной в виртуальную машину внутри ВИ, доступ к службе vCenter осуществляется через веб-браузер с поддержкой Flash/HTML5
Linked Mode	механизм, который объединяет серверы vCenter и позволяет использовать единое пространство объектов в географически распределенных датацентрах

Сокращение	Полная формулировка
Enhanced Linked Mode (ELM)	технология, позволяющая объединить серверы vCSA и vCenter, используя один или несколько внешних серверов PSC для репликации ролей, разрешений, лицензий, политик
Embedded Linked Mode	технология, позволяющая объединить серверы vCSA со встроенным PSC в общий домен для синхронизации, репликации и резервного копирования данных
Hybrid Linked Mode (HLM)	технология, с помощью которой осуществляется работа облачного сервиса VMware Cloud on AWC (VMC) с локальным доменом vCenter Single Sign-On
Platform Services Controller (PSC)	сервис vSphere, выполняющий функции безопасности инфраструктуры, такие как лицензирование и управление сертификатами
VMware Fault Tolerance	технология, предназначенная для защиты виртуальных машин с помощью кластеров непрерывной доступности

Терминология KVM

Сокращение	Полная формулировка
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)
QEMU	Quick Emulator, программа с открытым исходным кодом для эмуляции аппаратного обеспечения различных платформ

Терминология oVirt

Сокращение	Полная формулировка
oVirt	свободная, кроссплатформенная система управления виртуализацией, базирующаяся на технологии KVM
oVirt Engine	средство мониторинга и управления вычислительными узлами, хранилищами, сетями и виртуальными машинами. Далее по тексту сервер виртуализации oVirt (СВ oVirt)
oVirt Node	минимальная операционная система, основанная на CentOS, которая предназначена для работы в качестве гипервизора в среде oVirt
oVirt Host	вычислительный узел (гипервизор), на котором выполняются ВМ, а также могут быть размещены локальные хранилища. Далее по тексту гипервизор oVirt

Терминология zVirt

Сокращение	Полная формулировка
zVirt	система безопасного управления средой виртуализации. Построена на open source продуктах, создана на базе высокопроизводительного гипервизора KVM (Kernel-based Virtual Machine) и системы управления zVirt
zVirt Engine	средство мониторинга и управления вычислительными узлами, хранилищами, сетями и виртуальными машинами. Далее по тексту сервер виртуализации zVirt (СВ zVirt)
zVirt Node	минимальная операционная система, основанная на CentOS, которая предназначена для работы в качестве гипервизора в среде zVirt
zVirt Host	вычислительный узел (гипервизор), на котором выполняются ВМ, а также могут быть размещены локальные хранилища. Далее по тексту гипервизор zVirt

Терминология HOSTVM

Сокращение	Полная формулировка
HOSTVM	платформа виртуализации корпоративного уровня на основе гипервизора KVM для виртуализации серверов, рабочих столов и приложений
HOSTVM Manager	средство мониторинга и управления вычислительными узлами, хранилищами, сетями и виртуальными машинами. Далее по тексту сервер виртуализации HOSTVM (СВ HOSTVM)
HOSTVM	вычислительный узел (гипервизор), на котором выполняются ВМ, а также могут быть размещены локальные хранилища. Далее по тексту гипервизор HOSTVM

Терминология RedVirt

Сокращение	Полная формулировка
RedVirt	Система управления виртуализацией серверов и рабочих станций. Базируется на гипервизоре KVM (kernel-based virtual machine) и открытой платформе управления виртуальной инфраструктурой
RedVirt Engine	средство мониторинга и управления вычислительными узлами, хранилищами, сетями и виртуальными машинами. Далее по тексту сервер виртуализации RedVirt (СВ RedVirt)
RedVirt Node	минимальная операционная система, основанная на РЕД ОС, которая предназначена для работы в качестве гипервизора в среде RedVirt
RedVirt Host	вычислительный узел (гипервизор), на котором выполняются ВМ, а также могут быть размещены локальные хранилища. Далее по тексту гипервизор RedVirt

1 НАЗНАЧЕНИЕ И ВОЗМОЖНОСТИ СЗИ ВИ

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]), RedVirt 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.

СЗИ ВИ Dallas Lock имеет три редакции: «Ограниченная», «Стандартная» и «Расширенная». Редакция **СЗИ ВИ Dallas Lock** «Расширенная» имеет ряд преимуществ перед редакцией «Стандартная» (подробнее см. п. 2.2.1 «Различие редакций СЗИ ВИ»).

1.1 Возможности

СЗИ ВИ Dallas Lock предоставляет следующие возможности:

Возможности подсистемы управления пользователями:

1. Идентификация и аутентификация 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 KVM, oVirt, zVirt, HOSTVM и РЕД Вирт. 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**.
2. Запрет доступа к защищаемым ресурсам не идентифицированных пользователей и пользователей, подлинность идентификации которых при аутентификации не подтвердилась. Контроль пользователей, имеющих право на доступ к гипервизору, при условии успешной авторизации должен осуществляться посредством выполнения необходимых настроек на стороне **ЦУ СЗИ ВИ** и процесса синхронизации гипервизора с **ЦУ СЗИ ВИ**.
3. 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 oVirt, СВ zVirt, СВ HOSTVM, СВ РЕД Вирт и гипервизоров KVM, oVirt, zVirt, HOSTVM и РЕД Вирт.
4. Для решения проблемы «простых паролей» система 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.
5. В **СЗИ ВИ** реализована система контроля целостности параметров ТС.

Для агентов DL KVM, DL Engine и Host обеспечивается:

- контроль целостности файлов в директориях, указанных в переменной PATH;
- контроль целостности файлов в директориях «/lib» (включая все поддиректории) и «/usr/lib» (без поддиректорий);
- файлы агентов DL KVM, DL Engine и DL Host.

Для контроля целостности используются контрольные суммы, вычисленные по одному из алгоритмов на выбор: CRC32, MD5.

Кроме того, **СЗИ ВИ** выполняет периодический контроль целостности ВМ.

6. СЗИ ВИ позволяет производить настройку правил фильтрации сетевого трафика гипервизора ESXi.

[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.

7. **СЗИ ВИ** в рамках поддержки требований безопасности для финансовых организаций в соответствии с ГОСТ Р 57580.1-2017 обеспечивает выполнение следующих требований[5]:
   - Разделение виртуальной инфраструктуры vSphere на сегменты безопасности, состоящие из ВМ, ограничивается сетевое взаимодействие между сегментами посредством технологии VLAN.
8. Реализовано разграничение доступа к компонентам виртуальной инфраструктуры – к ЦУ **СЗИ ВИ**, СВ oVirt, СВ zVirt, СВ HOSTVM, СВ РЕД Вирт и гипервизорам 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 6.5/6.7/7.0/8.0. 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.
9. 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.
10. Разграничение доступа к гипервизорам ESXi и файлам виртуальных машин реализуется в пределах ролевой модели разграничения доступа vSphere 6.5/6.7/7.0/8.0. 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.
11. На гипервизорах ESXi, oVirt, zVirt, HOSTVM и РЕД Вирт осуществляется очистка остаточной информации по отношению к дискам виртуальных машин.
12. Доступно создание снапшотов как в ручном режиме, так и в автоматическом (по расписанию и/или с заданным интервалом).
13. В СЗИ ВИ реализовано ведение следующих журналов:
    - Журнал ЦУ СЗИ ВИ. В журнал заносятся события, связанные непосредственно с работой ЦУ СЗИ ВИ.
    - 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 vCSA. Журнал содержит информацию об изменениях состояния управляемых объектов на СВ vCSA. События включают в себя действия системы и пользователей, которые происходят на объектах ВИ.
    - Журнал сервера виртуализации KVM. Журнал содержит информацию об изменениях состояния 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. Журнал включает в себя системные события на гипервизоре ESXi.
14. Для облегчения работы с журналами есть возможность фильтрации записей по определенному признаку и экспортирования журналов. 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.

[5] Данные требования реализованы для среды виртуализации vSphere.

15. 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).

Иные возможности существующих подсистем:

16. 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**.

2 РАЗВЕРТЫВАНИЕ И УДАЛЕНИЕ СЗИ ВИ

Развертывание **СЗИ ВИ Dallas Lock** заключается в установке Центра управления **СЗИ ВИ Dallas Lock** на рабочую станцию, агентов управления доступом – в виртуальные инфраструктуры и включении их в домен безопасности.

Подробные характеристики ОС и аппаратной платформы см. в п. 2.1 «Требования к аппаратному и программному обеспечению»). Веб-консоль является основным средством администрирования изделия (подробное описание см. в разделе «Описание средств администрирования»).

Поддерживаемые платформы виртуализации (VMware vSphere, KVM, oVirt, zVirt, HOSTVM, RedVirt) различаются количеством и типами элементов ВИ, но в общем случае обязательно включают в себя гипервизор и систему управления гипервизором.

2.1 Требования к аппаратному и программному обеспечению

Для установки Центра управления **СЗИ ВИ Dallas Lock** минимальная и оптимальная конфигурация определяется требованиями к версии операционной системы. Для установки **ЦУ СЗИ ВИ** необходимо минимум 1 Гб свободного дискового пространства на системном разделе жесткого диска.

1. Поддерживаемые ОС:
   - РЕД ОС 7.3;
   - РЕД ОС 8.0;
   - Альт 8 СП релиз 10 (Рабочая станция, Сервер);
   - Альт Рабочая станция 10.1;
   - Альт Сервер 10;
   - Альт Рабочая станция К;
   - Astra Linux Special Edition 1.7 (SE) (Воронеж) (Server/Desktop)
   - РОСА «КОБАЛЬТ» 7.9 (Рабочая станция/Сервер);
   - РОСА «ХРОМ» 12.4 (Рабочая станция/Сервер);
   - Debian 11;
   - Ubuntu 22.04 LTS;
   - Ubuntu 24.04 LTS.
2. Минимальная комплектация (для 10 хостов и 100 ВМ):
   - 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.
3. Минимальная комплектация (для 100 хостов и 1000 ВМ):
   - ОЗУ — минимум 4 ГБ;
   - ПЗУ — минимум 30 ГБ.
4. Минимальная комплектация (для 200 хостов и 5000 ВМ):
   - ОЗУ — минимум 8 ГБ;
   - ПЗУ — минимум 40 ГБ.
5. Минимальная комплектация (для более 200 хостов и более 5000 ВМ):
   - ОЗУ — минимум 16 ГБ;
   - ПЗУ — минимум 60 ГБ.

Для ввода в домен безопасности (безагентская поддержка) 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:

1. Минимальная комплектация:
   - процессор: Intel или AMD с 2 логическими ядрами по 2 ГГц каждое, только x64, с поддержкой VT-x/AMD-V;
   - 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.

1. Минимальная конфигурация (до 10 хостов и до 100 ВМ):
   - процессор: Intel или AMD с 2-мя логическими ядрами по 2 ГГц каждое, только x64;
   - видеоадаптер: поддержка режима SVGA800x600;
   - ОЗУ — минимум 12 ГБ;
   - ПЗУ — более 350-4500 ГБ;
   - ЦП — 2 vCPU;
   - сетевая карта.
2. Минимальная конфигурация (до 100 хостов и до 1000 ВМ):
   - ОЗУ — минимум 20 ГБ;
   - ПЗУ — более 700-5000 ГБ;
   - ЦП — 4 vCPU.
3. Минимальная конфигурация (до 200 хостов и до 5000 ВМ):
   - ОЗУ — минимум 24 ГБ;
   - ПЗУ — более 800-5500 ГБ;
   - ЦП — 8 vCPU.
4. Минимальная конфигурация (более 200 хостов и более 5000 ВМ):
   - ОЗУ — минимум 32 ГБ;
   - ПЗУ — более 700-5000 ГБ;
   - ЦП — 16 vCPU.

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:
   - Astra Linux SE 1.7 (Орел, Воронеж);
   - CentOS 7.5;
   - CentOS 8.4.2105;
   - CentOS Stream 9;
   - CentOS Linux 8.5 (2111);
   - Linux Mint 19.3.
   - Linux Mint 20.3;
   - Linux Mint 21.3;
   - Ubuntu 18.04.6 LTS;
   - Ubuntu 20.04.3 LTS;
   - Ubuntu 22.04.4 LTS;
   - Ubuntu 24.04 LTS;
2. Минимальная комплектация:
   - 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 Engine ТС с установленным СВ oVirt (версия 4.4.x)/СВ zVirt (версий 4.1, 4.2)/HOSTVM/РедВиртуализация 7.3 должно иметь следующий состав и характеристики программно-технического обеспечения:

1. Поддерживаемые ОС:
   - oVirt Node;
   - zVirt Node;
   - HOSTVM Node;
   - РЕД ОС 7.3.

2. Минимальная конфигурация (до 10 хостов и до 100 ВМ):
   - процессор: двухъядерный x86-64 с поддержкой VT-x/AMD-V;
   - ОЗУ — минимум 16 ГБ;
   - ПЗУ — минимум 94 ГБ;
   - сетевая карта — минимум 1 Гбит/с.
3. Минимальная конфигурация (до 100 хостов и до 1000 ВМ):
   - ОЗУ — минимум 16 ГБ;
   - ПЗУ — минимум 94 ГБ.
4. Минимальная конфигурация (до 200 хостов и до 5000 ВМ):
   - ОЗУ — минимум 16 ГБ;
   - ПЗУ — минимум 94 ГБ.
5. Минимальная конфигурация (более 200 хостов и более 5000 ВМ):
   - ОЗУ — минимум 16 ГБ;
   - ПЗУ — минимум 94 ГБ.

Для установки агента DL Host TC с установленным гипервизором oVirt (версия 4.4.x)/zVirt (версий 4.1, 4.2)/HOSTVM/РедВиртуализация 7.3 должно иметь следующий состав и характеристики программно-технического обеспечения:

1. Поддерживаемые ОС:
   - oVirt Node;
   - zVirt Node;
   - HOSTVM Node;
   - РЕД ОС 7.3.
2. Минимальная комплектация (до 10 хостов и до 100 ВМ):
   - процессор: двухъядерный x86-64 с поддержкой VT-x/AMD-V;
   - ОЗУ — минимум 16 ГБ;
   - ПЗУ — минимум 94 ГБ;
   - сетевая карта — минимум 1 Гбит/с.
3. Минимальная комплектация (до 100 хостов и до 1000 ВМ):
   - ОЗУ — минимум 16 ГБ;
   - ПЗУ — минимум 94 ГБ.
4. Минимальная комплектация (до 200 хостов и до 5000 ВМ):
   - ОЗУ — минимум 16 ГБ;
   - ПЗУ — минимум 94 ГБ.
5. Минимальная комплектация (более 200 хостов и более 5000 ВМ):
   - ОЗУ — минимум 16 ГБ;
   - ПЗУ — минимум 94 ГБ.

Веб-интерфейс **СЗИ ВИ** корректно отображается в следующих веб-браузерах:

- Chrome (Windows, Linux) 129.0.6668.89;
- Firefox 131.0;
- Edge (Windows, Linux) 129.0.2792.79;
- Яндекс.Браузер 24.7.6.970;
- Safari 18.0;
- Chromium-gost 129.0.6668.70;
- Opera 115.0.5297.0.

Для установки компонентов **СЗИ ВИ** необходимо минимум 1 Гб свободного дискового пространства на системном разделе жесткого диска.
Для использования **СЗИ ВИ** необходимо настроить сетевой протокол TCP/IP.

2.2 Ограничения при установке и эксплуатации

СЗИ ВИ Dallas Lock редакции «Ограниченная», «Стандартная» и «Расширенная» имеют следующие ограничения по установке и эксплуатации:

1. **СЗИ ВИ:**

1) При использовании изделия при создании защищенных АС до класса защищенности 1Г включительно[6] на ТС, на которых выполняется обработка защищаемой информации, необходимо включить опции, отвечающие за выполнение следующих условий:
   - осуществление идентификации при входе в систему по паролю условно-постоянного действия, длиной не менее шести буквенно-цифровых символов;
   - включение регистрации входов (выходов) пользователей в систему (из системы).
2) Должен быть установлен пароль на BIOS ПК, на котором установлен какой-либо компонент **СЗИ ВИ Dallas Lock** и выполняется обработка защищаемой информации.
3) Перед установкой Ядра **СЗИ ВИ** необходима предварительная настройка локалей в ОС. Сделать это можно, включив en_US.UTF-8 UTF-8 и ru_RU.UTF-8 UTF-8 в /etc/locale.gen и далее запустить locale-gen.
4) Количество устанавливаемых программных модулей **СЗИ ВИ Dallas Lock** необходимо производить в соответствии с договором и отгрузочными документами (накладная, акт передачи прав и т.д.) с обязательной соответствующей записью в разделе 13 «Особые отметки» формуляра на изделие.
5) Дополнительная установка **СЗИ ВИ Dallas Lock** (сверх указанного количества) допускается только при переносе соответствующих модулей **СЗИ ВИ Dallas Lock** на другое ТС или их восстановлении.
6) Суперпользователь (root, администратор среды виртуализации) и пользователи с аналогичными правами обладают привилегиями, с помощью которых могут внести изменения в **СЗИ ВИ** и ее настройки, способные нарушить корректность выполнения функций **СЗИ ВИ** вплоть до ее неработоспособности. Контроль привилегированных пользователей должен осуществляться посредством применения организационных мер защиты.
7) Необходимо периодически проводить проверку контроля целостности образов виртуальных машин[7]. Для проведения необходимо на уровне гипервизора в категории **Состояние** → **Контроль целостности** → выбрать пункт **Конфигурация** для ВМ и нажать левой кнопкой мыши и выбрать пункт из контекстного меню **Проверить** (подробнее см. п. 6.1 «Контроль целостности файлов»).
8) В процессе эксплуатации изделия необходимо использовать сертифицированные обновления по результатам испытаний, вызванных внесением изменений в **СЗИ ВИ**.
9) Доступ к сертифицированным обновлениям по результатам испытаний, вызванных внесением изменений в **СЗИ ВИ** возможен только в рамках действующего технического сопровождения.
10) В процессе эксплуатации **СЗИ ВИ Dallas Lock** запрещается:
    - коммерческое тиражирование **СЗИ ВИ Dallas Lock**;
    - модификация, декомпиляция или дизассемблирование **СЗИ ВИ Dallas Lock**;
    - обработка компакт-диска с **СЗИ ВИ Dallas Lock** системными программами и утилитами, работающими на низком уровне.

2. ЦУ СЗИ ВИ:

1) Для корректной работы веб-консоли необходимо добавить разрешения для TCP порта 4564.
2) На время установки и удаления **СЗИ ВИ** необходимо отключить программные антивирусные средства, а при возникновении ошибок, необходимо удалить антивирусные средства на время установки и удаления **СЗИ ВИ**.
3) Имя и пароль пользователя указанные при первом входе в веб-консоль будут использованы для создания соответствующего встроенного пользователя с правами Суперадминистратора.

3. vSphere/vCSA:

1) Не допускается использование **СЗИ ВИ** на компьютерах, введенных в домен AD с зарезервированным именем «vsphere.common», vsphere.local.
2) При установке VMware vCSA не допускается использовать имя «vsphere.common» для домена SSO (Single Sign-On).
3) Для vCSA 6.5, 6.7, 7.0.0, 7.0.1 и 7.0.2 требуется предварительная настройка количества сессий до ввода в **ДБ СЗИ ВИ**. Для этого в файле /etc/ssh/sshd_config нужно внести изменения в параметр «MaxSessions». Параметр должен быть включен (раскомментирован) и установлено к нему значение равное 32. После чего выполнить перезагрузку службы SSH, введя команду в консоль: sudo service sshd restart.

[6] Руководящий документ «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» (Гостехкомиссия России, 1992).

[7] Периодический контроль целостности образа виртуальной машины определяется в рамках действующих положений ИБ по организации, в котором указывается период выполнения ручной проверки КС.

4) В штатном режиме функционирования **СЗИ ВИ** запрещается использовать локальный вход на СВ vCSA.
5) **СЗИ ВИ** автоматические меняет shell для PhotonOS VCSA. При этом будет произведена запись в журнале **ЦУ СЗИ ВИ** об изменении настройки shell (см. п. 2.5.2 «Развертывание СЗИ ВИ для VmWare vSphere/vCSA»).
6) Запрет на ssh соединение с сервером ESXi блокирует работу функции «удалить и зачистить» − перед применением функции следует убедиться в доступности функции соединения с хостом по SSH.

4. oVirt/zVirt/HOSTVM/РЕД Виртуализация:

1) Обязательным условием является установка агента DL oVirt/zVirt/redVirt/HOSTVM Engine на все СВ oVirt/zVirt/redVirt/HOSTVM.
2) Обязательным условием является установка агента DL oVirt/zVirt/redVirt/HOSTVM Host на все гипервизоры oVirt/zVirt/redVirt/HOSTVM.
3) Рекомендуется перед добавлением инфраструктуры oVirt/zVirt/HOSTVM/РЕД Виртуализация в **ДБ СЗИ ВИ** завести встроенные учетные записи (internal) и доменные учетные записи для использования их при работе с виртуальной инфраструктурой.
4) При работе с платформами виртуализации oVirt/zVirt/РЕД Виртуализации поддерживаются только конфигурации Standalone и Self-hosted.
5) При работе с платформой виртуализации HOSTVM поддерживается только конфигурации Self-hosted.
6) При работе с платформой виртуализации zVirt 4.2 поддерживается только конфигурации с использованием провайдера по умолчанию - AAA-JDBC.
7) При обновлении СВ oVirt/zVirt/redVirt/HOSTVM необходимо выполнить удаление агента DL oVirt/zVirt/redVirt/HOSTVM Engine, выполнить обновление, после чего установить агент DL oVirt/zVirt/redVirt/HOSTVM Engine.
8) При обновлении гипервизора oVirt/zVirt/redVirt/HOSTVM необходимо выполнить удаление агента DL oVirt/zVirt/redVirt/HOSTVM Host, выполнить обновление, после чего установить агент DL oVirt/zVirt/redVirt/HOSTVM Host.

5. KVM:

1) Обязательным условием является установка агента DL KVM на все гипервизоры KVM и СВ KVM.
2) При обновлении гипервизора KVM или СВ KVM необходимо выполнить удаление агента DL KVM, выполнить обновление, после чего установить агент DL KVM.
3) Агентом DL KVM не поддерживается режим работы socket activation mode для всех ОС.
4) При работе с KVM в консоли **СЗИ ВИ** недоступны к управлению и не отображаются ВМ пользователей (доступны только qemu:///system). Для создания и использования ВМ пользователей необходимо выключить политику **KVM: Блокировать запуск ВМ в пространстве пользователя**.
5) При установке виртуализации QEMU/KVM в Astra Linux Special Edition автоматически будет установлена и настроена система управления сетевым трафиком «firewalld».
6) Для предоставления доступа пользователю к управлению ВМ необходимо добавить данного пользователя в следующие группы:
   - Для ОС Linux Mint – libvirt.
   - Для ОС Ubuntu – libvirt, kvm.
   - Для ОС Astra Linux – kvm, libvirt, libvirt-qemu, libvirt-admin.
   - Для ОС CentOS – libvirt, kvm.

2.2.1 Различие редакций СЗИ ВИ

СЗИ ВИ Dallas Lock редакции «Расширенная» имеет следующие преимущества в функциональных возможностях:

- Мониторинг событий в виртуальной инфраструктуре с помощью графической панели;
- Поддержка серверов управления vCenter Linked Mode;
- Поддержка vSphere High Availability;
- Поддержка vCenter High Availability;
- Поддержка VMware Fault Tolerance;
- Поддержка oVirt High Availability (zVirt, РЕД Виртуализация, HOSTVM).

«Ограниченное» издание имеет только возможность работы в веб-интерфейсе для загрузки файла-ключа. Все остальные функции заблокированы!

2.3 Порядок развертывания компонентов

2.3.1 Порядок развертывания СЗИ ВИ для VMware vSphere vCSA

№ п/п	Шаг развертывания	Описание
1	Установить Центр управления **СЗИ ВИ Dallas Lock** на компьютер, предназначенный для ЦУ **СЗИ ВИ**	см. раздел 2.5.1
2	Ввести сервер виртуализации в домен безопасности	см. раздел 2.5.2

2.3.2 Порядок развертывания СЗИ ВИ для KVM

№ п/п	Шаг развертывания	Описание
1	Установить Центр управления **СЗИ ВИ Dallas Lock** на компьютер, предназначенный для ЦУ **СЗИ ВИ**	см. раздел 2.5.1
2	Ввести сервер виртуализации в домен безопасности	см. раздел 2.5.3

2.3.3 Порядок развертывания СЗИ ВИ для oVirt/zVirt/HOSTVM/RedVirt

№ п/п	Шаг развертывания	Описание
1	Установить Центр управления **СЗИ ВИ Dallas Lock** на компьютер, предназначенный для ЦУ **СЗИ ВИ**	см. раздел 2.5.1
2	Установить агент **DL** Engine	см. раздел 2.5.4.2
3	Ввести сервер виртуализации в домен безопасности	см. раздел 2.5.4.2
4	Установить агент **DL** Host на гипервизор oVirt/zVirt/HOSTVM/RedVirt	см. раздел 2.5.4.3

2.4 Подготовка к установке СЗИ ВИ

2.4.1 Предварительная подготовка

Перед развертыванием **СЗИ ВИ** необходимо выполнить следующие действия:

1. Если в BIOS компьютера включена антивирусная защита, то на время установки ее необходимо отключить.
2. Рекомендуется произвести дефрагментацию жесткого диска.
3. Необходимо убедиться, что на диске имеется необходимое свободное пространство для установки системы защиты.
4. Проверить компьютер на отсутствие вирусов.
5. Проверить корректность установленной даты и времени на всех компонентах среды виртуализации.
6. Перед установкой системы защиты необходимо выгрузить из памяти все резидентные антивирусы.
7. Конфигурацию протоколов TLS на серверах vCenter и хостах ESXi необходимо производить штатной утилитой VMware перед развертыванием **СЗИ ВИ**.
8. Проверить актуальность паролей для VMware vCSA для учетных записей administrator@vsphere.local и root и срока их действия
9. Перед установкой Центра управления **СЗИ ВИ Dallas Lock** необходимо убедиться, что на компьютерах, на которых будет производиться установка данных компонентов, в BIOS отключена функция Secure Boot.

2.4.2 Особенности установки

Устанавливать компоненты **СЗИ ВИ** на компьютер может только пользователь, обладающий правами администратора на данном компьютере. Это может быть локальный или доменный пользователь.

Локальную установку необходимо выполнять только из-под сессии текущего авторизованного пользователя. Запуск установки от имени другого пользователя не допускается.

Пользователь, установивший систему защиты, автоматически становится привилегированным пользователем – *суперадминистратором***.** Необходимо запомнить имя и пароль этого пользователя, так как некоторые операции можно выполнить только из-под его учетной записи. Изменять учетную запись суперадминистратора средствами ОС запрещено.

Имя и пароль пользователя для входа в операционную систему, выполнившего установку, автоматически становятся именем и паролем для первого входа на компьютер с установленным **СЗИ ВИ**, пользователем в качестве суперадминистратора.

Если будут использоваться сторонние firewall-программы, то необходимо добавить разрешения для TCP портов 80, 443, 514, 8080, 17491, 17492, 17493, 17495, 17497, 11111 в их настройках вручную и убедиться, что открыты порты, необходимые для работы компонентов VMware vSphere, а также для иного используемого стороннего программного обеспечения (подробнее о добавлении разрешений см. п. 5.1 «Удаленный доступ к СВ».

Необходимо добавить разрешения для TCP портов 4564, 443, 514, 1514, 22, 4563, 19779 в их настройках вручную и убедиться, что открыты порты, необходимые для работы компонентов VMware vSphere.

ЦУ СЗИ ВИ не осуществляет контроль пользователей доменной группы *ESX Admins*, использующейся для авторизации доменных пользователей на гипервизорах ESXi, введенных в домен AD. В группу AD *ESX Admins* следует включать только высоко доверенных пользователей.

При назначении пользователю число сессий, можно установить флаг *Без ограничений*.

2.5 Развертывание СЗИ ВИ

Доступно 2 варианта развертывания **ЦУ СЗИ ВИ**:

- Установка компонента из установочного файла.
- Установка через пакетный менеджер с помощью командной строки.

На ТС предназначенное для установки **ЦУ СЗИ ВИ** скопировать файл *confident-vicored.rpm* или *confident-vicored.deb*.

2.5.1 Установка компонента «Центр управления СЗИ ВИ Dallas Lock»

2.5.1.1 Установка компонента из установочного файла

1. Запустить установочный файл *confident-vicored* двойным кликом.
2. После завершения настройки запустится окно установщика, с помощью которого в программе установки необходимо выполнять действия по подсказкам программы.

2.5.1.2 Установка через пакетный менеджер DEB

1. Открыть консоль или подключиться по SSH.
2. Перейти в каталог с файлом *confident-vicored.deb*.
3. Выполнить команду *sudo dpkg -i confident-vicored.deb*.

2.5.1.3 Установка через пакетный менеджер RPM

4. Открыть консоль или подключиться по SSH.

5. Перейти в каталог с файлом *confident-vicored.rpm*.
6. Выполнить команду *sudo rpm -i confident-vicored.rpm*.

2.5.1.4 Первый вход в веб-консоль ЦУ СЗИ ВИ

Работа с веб-консолью осуществляется из окна браузера. Для вызова веб-консоли необходимо открыть браузер и в адресной строке ввести ip-адрес или полное доменное имя ТС с установленным компонентом **ЦУ СЗИ ВИ Dallas Lock** или, если доступ осуществляется непосредственно с ТС с установленным компонентом, указать в строке адреса localhost с указанием порта 4564. Например, https://192.168.100.2:4564 или https://szivi.dl.local:4564 или https://localhost:4564. Обязательно необходимо ввести "https://" перед ip-адресом или полным доменным именем.

По умолчанию на этапе установки **СЗИ ВИ** не создается никакой учетной записи.

> **!** При первом подключении к **ЦУ СЗИ ВИ** будет создана учетная запись Суперадминистратора **СЗИ ВИ**. Под данной учетной записью осуществляется только первичная настройка и создание других учетных записей с ролью администратора.

Для создания учетной записи Суперадминистратора необходимо в окне авторизации ввести следующие данные:

- Имя учетной записи;
- Пароль учетной записи. (Длина пароля должна сосоставять не менее 8 символов.)

Для завершения создания пользователя необходимо нажать кнопку **Вход**. После успешного входа учетная запись появится на вкладке **Сервер УД − Встроенные учетные записи.**

> **!** Учетную запись Суперадминистратора нельзя удалить.

2.5.1.4.1 Авторизация в веб-консоли ЦУ СЗИ ВИ

Дальнейшие подключения к веб-консоли, после успешно созданной УЗ Суперадминистратора, проходят в штатном режиме.

Для авторизации требуется:

1. Ввести имя и пароль учетной записи;
2. Нажать кнопку **Вход**.

> **!** В случае неправильного входа в ЦУ **СЗИ ВИ** пользователем, учетная запись его автоматически блокируется. В этом случае разблокировать пользователя нельзя. Только автоматическая разблокировка по истечению установленного времени на основе политик безопасности (см. п. 4.4.1 «Настройка параметров безопасности»).

2.5.1.5 Активация продукта

Доступно 2 варианта активации **ЦУ СЗИ ВИ**:

- Через графический интерфейс веб-консоли.
- Копирование файла вручную на ТС с установленным **СЗИ ВИ**.

2.5.1.5.1 Активация продукта через веб-консоль СЗИ ВИ

Для активации продукта необходимо:

1. Авторизоваться в веб-консоли.
2. В **Общем меню** выбрать пункт **Настройки лицензирования − Выбор файла-ключа** (см. Рисунок 1).

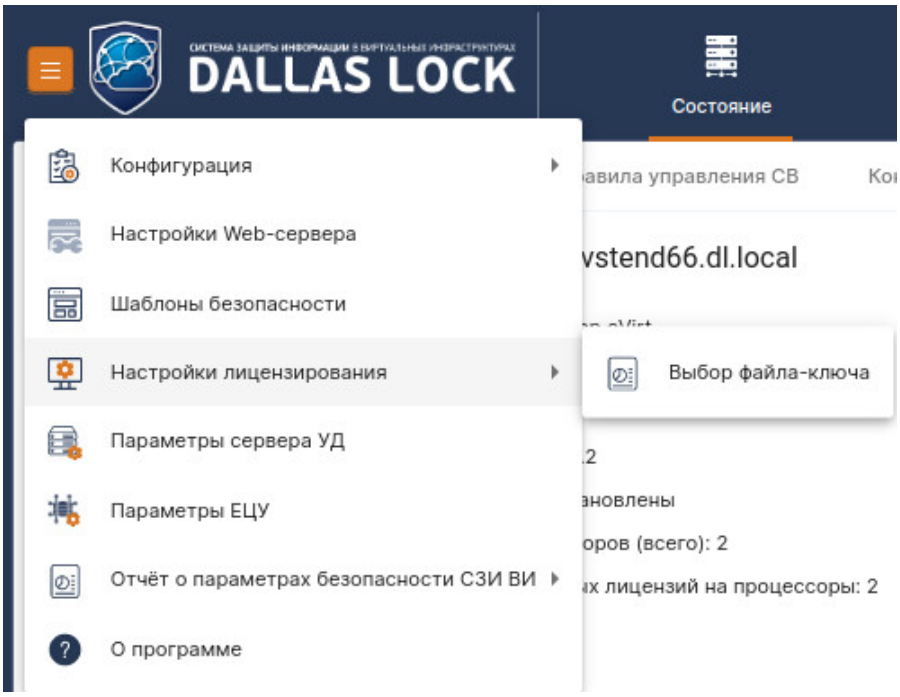

Рисунок 1. Выбор файла-ключа

3. Перенести файл с лицензией в область появившегося окна или указать путь к файлу на диске (кнопка **Выбрать на диске**) (см. Рисунок 2).

Рисунок 2. Применение файла лицензий

4. Нажать кнопку **Применить**.
5. Обновить страницу, убедиться, что редакция **СЗИ ВИ** изменила состояние с «Ограниченная» (см. Рисунок 3) на «Стандартная» (см. Рисунок 4) или «Расширенная» (см. Рисунок 5) в соответствии с приобритенной лицензией.

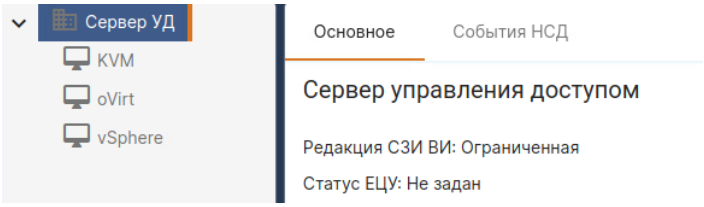

Рисунок 3. Редакция СЗИ ВИ: Ограниченная

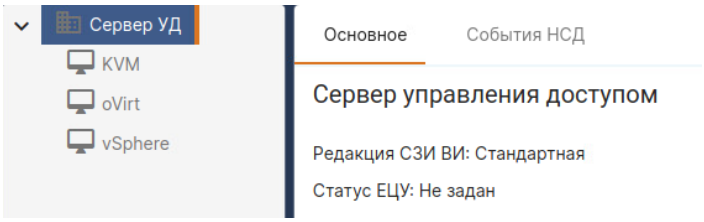

Рисунок 4. Редакция СЗИ ВИ: Стандартная

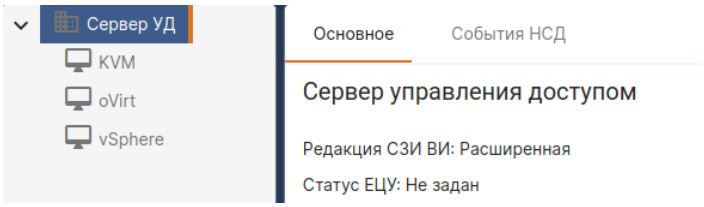

Рисунок 5. Редакция СЗИ ВИ: Расширенная

2.5.1.5.2 Активация продукта на ТС с установленным СЗИ ВИ

Для активации продукта необходимо:

1. Скопировать файл с лицензией на ТС с установленным Ядром **СЗИ ВИ**.
2. Перезапустить службу ядра, выполнив следующую команду: *sudo systemctl restart confident-vicored*.
3. Проверить статус службы после перезапуска, выполнив следующую команду: *sudo systemctl status confident-vicored*.
4. Авторизоваться в веб-консоли и убедиться, что редакция **СЗИ ВИ** изменила состояние с «Ограниченная» на «Стандартная» или «Расширенная» в соответствии с приобритенной лицензией.

2.5.2 Развертывание СЗИ ВИ для VmWare vSphere/vCSA

Перед вводом СВ vCSA, необходимо применить файл лицензий и убедится, что редакция **СЗИ ВИ** изменила состояние с «Ограниченная» на «Стандартная» или «Расширенная» в соответствии с приобритенной лицензией. В противном случае установка компонентов и ввод в **ДБ** будет невозможен.

Подробнее см. п. 2.5.1.5.1 «Активация продукта через веб-консоль СЗИ ВИ».

Перед вводом vCSA 7.0 **СЗИ ВИ** автоматически меняет shell. Запись об изменении shell будет отображаться в журнале **ЦУ СЗИ ВИ**.

Перед вводом vCSA 8.0 требуется ручная настройка shell.

2.5.2.1 Установка компонента «Центр управления СЗИ ВИ Dallas Lock»

Порядок установки компонента **Центр управления СЗИ ВИ Dallas Lock** указан в п. 2.5.1 «Установка компонента «Центр управления СЗИ ВИ Dallas Lock»».

2.5.2.2 Установка и ввод в домен безопасности сервера виртуализации vSphere/vCSA

Для ввода сервера виртуализации vCSA в домен безопасности с помощью Консоли необходимо:

1. Открыть вкладку *Сервер УД* в дереве объектов и выбрать вкладку *Состояние*.
2. В блоке *Действие* открыть вкладку *Добавить СВ*.
3. В появившемся окне требуется ввести (Рисунок 6):
   - полное DNS-имя или IP-адрес сервера виртуализации и нажать **Проверить адрес**, в случае успеха нажать **Далее**;
   - выбрать тип платформы виртуализации «VmWare vCSA (без агента)» и нажать **Далее**;
   - ввести учётные данные администратора ОС, и нажать **Проверить адрес**, в случае успеха нажать **Далее**;
   - ввести учетные данные администратора виртуализации.

В случае, если IP-адрес сервера виртуализации vCSA является динамическим, его DNS-имя не должно содержать кириллические символы.

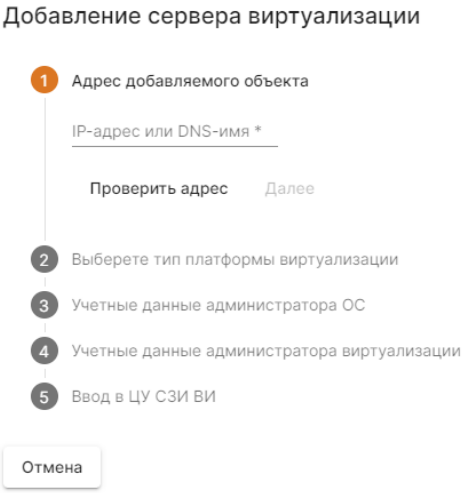

Рисунок 6. Установка агента DL и ввод в домен безопасности сервера виртуализации

4. Проверить правильность введённых данных и нажать кнопку **Ввести в домен**.

Если операция завершилась успешно, то на панели дерева объектов в ветке vSphere появятся значки новых объектов ВИ.

2.5.2.3 Установка и удаление ESXi на Сервере УД

Включение режима Lockdown Mode на гипервизоре существенно повышает уровень безопасности ВИ.

Подготовка к установке:

Перед установкой необходимо убедиться, что к СВ открыт доступ по SSH и отключена политика **Вход: блокировать протокол SSH** (подробнее см. п. 5.3.1.1 «Параметры входа для vSphere»). Чтобы установить ESXi в Сервер УД, необходимо указать учетные данные администратора гипервизора. Для этого требуется:

1. Открыть дерево агентов.

2. Выбрать уровень гипервизора и открыть категорию **Основное** → **Управление**.

3. Нажать кнопку **Установить учетные данные**.

4. В появившемся окне ввести учетные данные гипервизора (см. Рисунок 7).

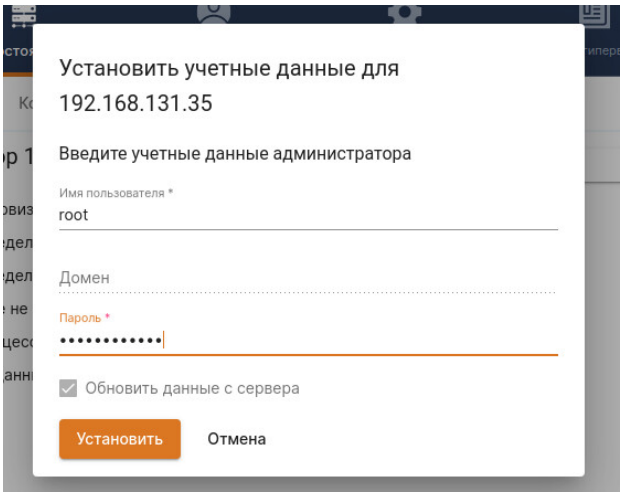

Рисунок 7. Установка учетных данных гипервизора

5. Чтобы автоматически обновить данные с сервера необходимо установить флаг *Обновить данные с сервера*.

6. Нажать кнопку **ОК**.

Если операция завершилась успешно, то на панели дерева объектов в ветке KVM появятся значки новых объектов ВИ.

Для удаления гипервизора из домена безопасности необходимо выделить сервер виртуализации в

дереве агентов ВИ, открыть вкладку *Состояние*, нажать *Управление* и выбрать **Удалить учетные данные**.

В случае если учетные данные уже установлены (об этом свидетельствует надпись «*Учетные данные установлены*»), то необходимо нажать кнопку **Установить агент на гипервизоре**.

Статус учетных данных и агента отображаются на рабочей области (см. Рисунок 8).

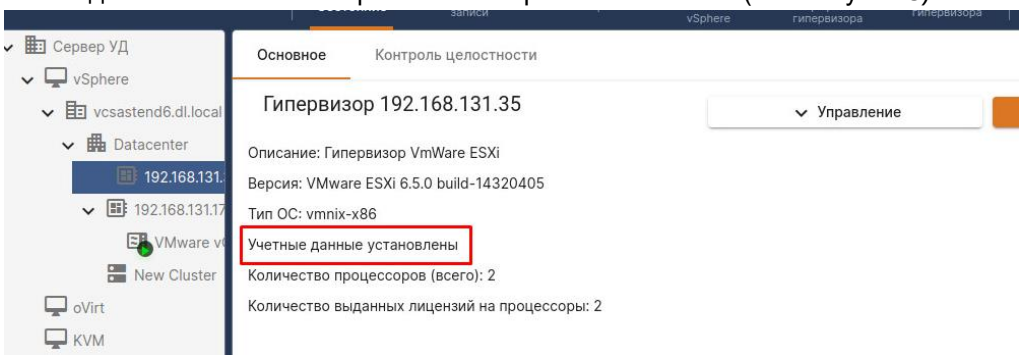

Рисунок 8. Статус учетных данных и агента DL

Для вывода из управления гипервизора из домена безопасности необходимо выделить гипервизор в дереве, открыть вкладку *Состояние*, *Основное*, нажать *Управление* и выбрать из выпадающего списка пункт **Удалить агент**.

2.5.3 Развертывание СЗИ ВИ для KVM

2.5.3.1 Установка компонента «Центр управления СЗИ ВИ Dallas Lock»

Порядок установки компонента Центр управления **СЗИ ВИ Dallas Lock** указан в п. 2.5.1 «Установка компонента «Центр управления СЗИ ВИ Dallas Lock»».

2.5.3.2 Установка и удаление агента DL KVM и ввод в домен безопасности сервера виртуализации KVM

> **!** Если в системе используется система управления сетевым трафиком ufw, то перед установкой виртуализации следует сохранить настройки и удалить ufw командами:
> *sudo apt remove ufw*
> *sudo systemctl stop ufw*

Перед установкой агента DL KVM, необходимо убедиться, что к гипервизору открыт доступ по SSH и отключена политика **Политики авторизации: блокировать протокол SSH** (подробнее см. п. 4.3.1.2 «Параметры авторизации для KVM»). Далее необходимо указать учетные данные администратора KVM. Для этого требуется:

1. Открыть вкладку *KVM* или *Сервер УД* в дереве объектов.
2. В блоке *Действие* открыть вкладку *Добавить СВ* (см. Рисунок 9).

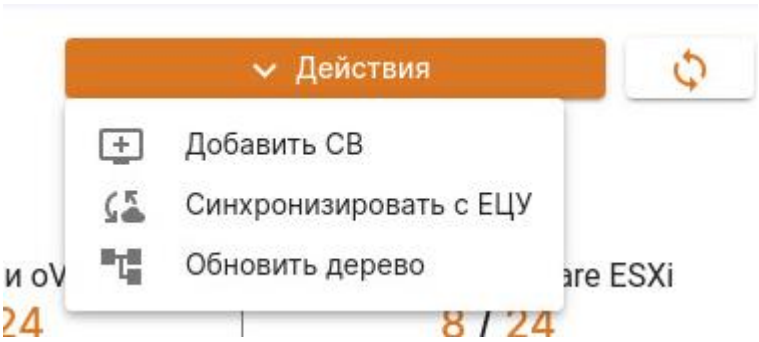

Рисунок 9. Добавление KVM на уровне Сервера УД

3. В появившемся окне требуется ввести (см. Рисунок 10):
   - полное DNS-имя или IP-адрес сервера виртуализации и нажать **Проверить адрес**, в случае успеха нажать **Далее**;
   - выбрать тип платформы виртуализации «агент KVM» и нажать **Далее**;
   - ввести учётные данные администратора ОС, и нажать **Проверить адрес**, в случае успеха нажать **Далее**;
   - ввести учетные данные администратора виртуализации.

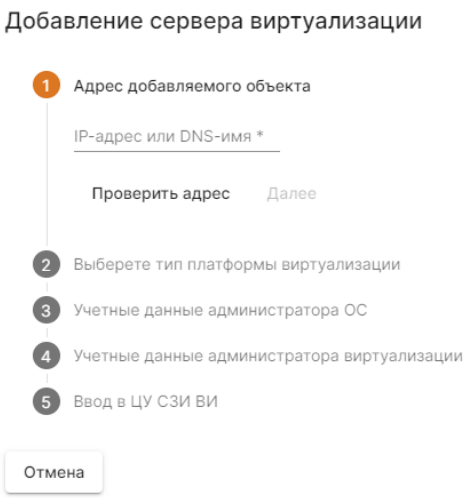

Рисунок 10. Ввод данных для добавления KVM

4. Проверить правильность введённых данных и нажать кнопку **Ввести в домен**.

Если операция завершилась успешно, то на панели дерева объектов в ветке KVM появятся значки новых объектов ВИ.

> После добавления СВ KVM для возможности агентского управления необходимо на уровне СВ назначить пользователю «root» роль Администратора, иначе при попытке управления из веб-консоли появляется ошибка с фиксацией НСД.

Для удаления гипервизора из домена безопасности и агента DL KVM необходимо выделить сервер виртуализации в дереве агентов ВИ, открыть вкладку *Состояние*, нажать «Управление» и выбрать «Удалить учетные данные».

2.5.4 Развертывание СЗИ ВИ для oVirt/zVirt/HOSTVM/RedVirt

2.5.4.1 Установка компонента «Центр управления СЗИ ВИ Dallas Lock»

Порядок установки компонента **Центр управления СЗИ ВИ Dallas Lock** указан в п. 2.5.1 «Установка компонента «Центр управления СЗИ ВИ Dallas Lock»».

2.5.4.2 Установка и удаление агента DL Engine и ввод в домен безопасности сервера виртуализации oVirt/zVirt/HOSTVM/RedVirt

2.5.4.2.1 Установка агента DL Engine Ввод в домен безопасности сервера виртуализации oVirt/zVirt/HOSTVM/RedVirt

Перед установкой необходимо убедиться, что к СВ открыт доступ по SSH и отключена политика **Вход: блокировать протокол SSH** (подробнее см. п. 4.3.1.3 «Параметры входа для oVirt/zVirt/HOSTVM/RedVirt»). Чтобы установить oVirt/zVirt/HOSTVM/RedVirt в Сервер УД, необходимо указать учетные данные администратора гипервизора. Для этого требуется:

1. Открыть вкладку *Сервер УД* в дереве объектов.

2. В блоке *Действие* открыть вкладку **Добавить СВ** (см. Рисунок 11).

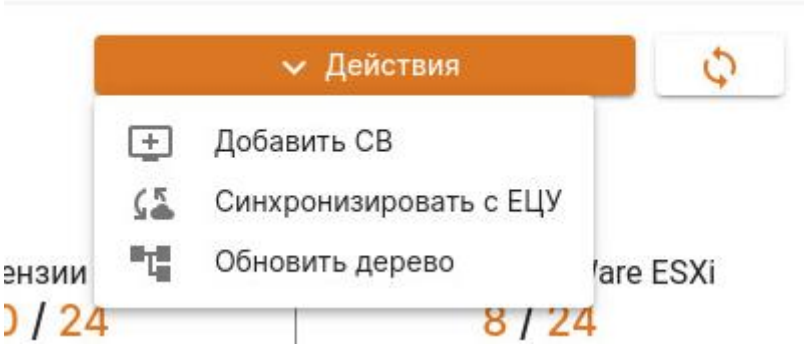

Рисунок 11. Добавление сервера виртуализации

3. В появившемся окне требуется (см. Рисунок 12):
   - полное DNS-имя или IP-адрес сервера виртуализации и нажать **Проверить адрес**, в случае успеха нажать **Далее**;
   - выбрать тип платформы виртуализации «oVirt/zVirt», «HOSTVM» или «RedVirt» и нажать **Далее**;
   - ввести учётные данные администратора ОС и нажать **Проверить учетные данные**, в случае успеха нажать **Далее**;
   - ввести учётные данные администратора виртуализации, и нажать **Проверить учетные данные**, в случае успеха нажать **Далее**.

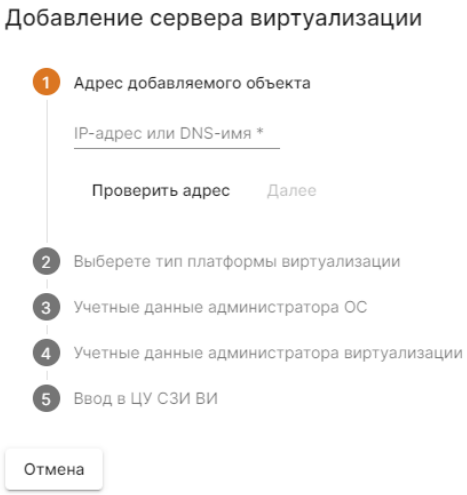

Рисунок 12. Ввод данных для добавления СВ

4. Проверить правильность введённых данных и нажать кнопку **Ввести в домен**.

Если операция завершилась успешно, то на панели дерева объектов в ветке oVirt появятся значки новых объектов ВИ.

2.5.4.2.2 Удаление агента DL Engine Ввод в домен безопасности сервера виртуализации oVirt/zVirt/HOSTVM/RedVirt

Для удаления СВ из домена безопасности необходимо

1. Выбрать уровень сервера виртуализации в дереве и открыть вкладку **Состояние** → **Основное**.
2. В блоке *Управление* выбрать пункт **Вывести из-под управления**. В случае возникновения ошибок при удалении можно активировать пункт **Вывести принудительно**, который позволяет очистить дерево объектов ВИ от удаленного СВ.

2.5.4.3 Установка и удаление агента DL Host на гипервизоре oVirt/zVirt/HOSTVM/RedVirt

2.5.4.3.1 Установка агента DL Host на гипервизоре oVirt/zVirt/HOSTVM/RedVirt

Чтобы установить агент DL Host на гипервизор, необходимо указать учетные данные администратора гипервизора. Для этого требуется:

1. Выбрать уровень гипервизора и открыть категорию **Состояние** → **Основное**.
2. В блоке *Управление* выбрать пункт **Установить агент**. В появившемся окне необходимо ввести данные пользователя. Затем нажать кнопку **Установить** (см. Рисунок 13).

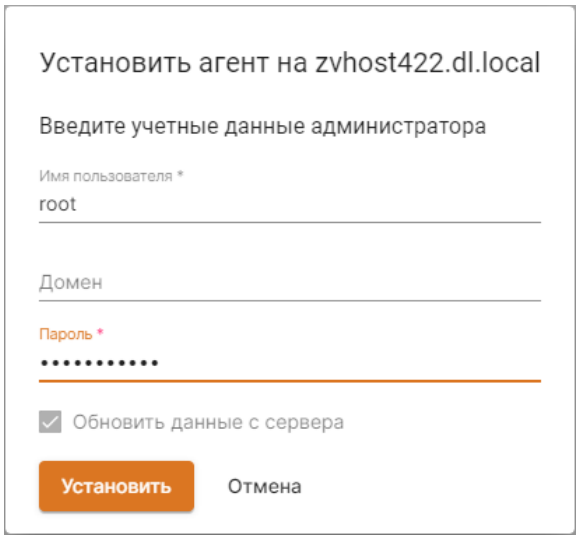

Рисунок 13. Установка агента на хост

3. При успешной установке появится всплывающее уведомление.

2.5.4.3.2 Удаление агента DL Host на гипервизоре oVirt/zVirt/HOSTVM/RedVirt

1. Выбрать уровень гипервизора и открыть категорию **Состояние** → **Основное**.
2. В блоке *Управление* нажать кнопку **Удалить агент**. В появившемся окне подтвердить удаление, нажав кнопку **Да** (см. Рисунок 14).

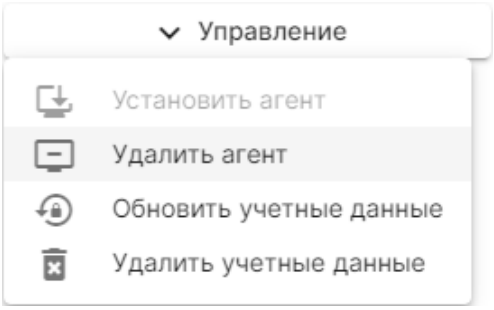

Рисунок 14. Удаление агента с хоста

2.6 Установка учетных данных

Установка учетных данных для введенных в ДБ СВ и гипервизоров необходима в случаях смены данных учетной записи администратора объекта ВИ, изменении разрешений, списков пользователей и прочих локальных параметров.

2.6.1 Установка учетных данных для vSphere/vCSA

Чтобы установить учетные данные для СВ необходимо на уровне СВ в блоке *Управление* нажать кнопку **Обновить учетные данные**. В появившемся окне необходимо ввести данные пользователя и установить флаг в поле *Обновить данные с сервера* (см. Рисунок 15). Затем нажать кнопку **Установить**.

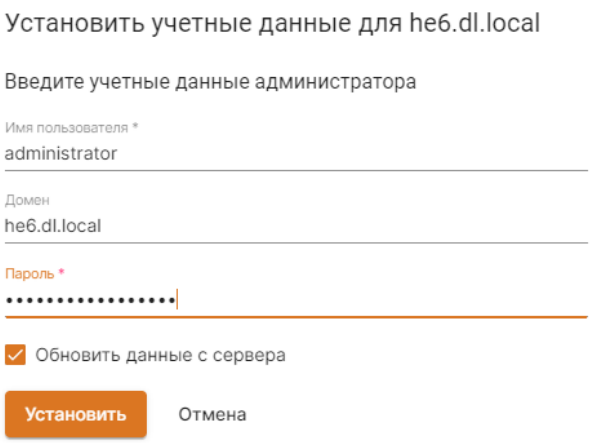

Рисунок 15. Установка учетных на данных ESXi

2.6.1.1 Установка учетных данных для гипервизора ESXi

Установка учетных данных для гипервизора описана в п. 2.5.2.3 «Установка и удаление ESXi ».

2.6.2 Установка и обновление учетных данных для гипервизора KVM

Перед установкой учетных данных для гипервизора KVM, необходимо убедиться, что к гипервизору открыт доступ по SSH и отключена политика **Вход: блокировать протокол SSH** (подробнее см. п. 5.3.1.2 «Параметры входа для KVM»).

Чтобы установить учетные данные для СВ необходимо на уровне СВ в блоке *Управление* нажать кнопку **Обновить учетные данные**. В появившемся окне необходимо ввести данные пользователя и установить флаг в поле *Обновить данные с сервера* (Рисунок 16). Затем нажать кнопку **Установить**.

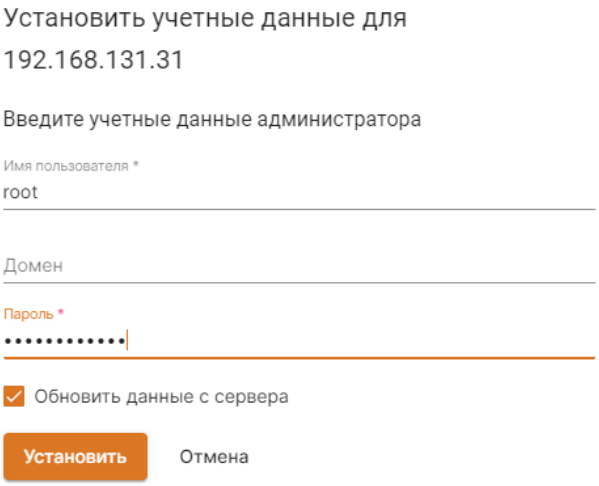

Рисунок 16. Установка учетных данных гипервизора KVM

2.6.3 Установка, обновление и удаление учетных данных для СВ oVirt/zVirt/HOSTVM/RedVirt

Установка учетных данных происходит в момент установки агента DL Engine и ввода СВ в домен безопасности (подробнее см. п. 2.5.4.2 «Установка и удаление агента DL Engine и ввод в домен безопасности сервера виртуализации oVirt/zVirt/HOSTVM/RedVirt»).

Обновление учетных данных требуется в случае их смены штатными средствами среды виртуализации или для перевычитки списка учетных записей пользователей ВИ, ролей и т.д. Переустановка агента в данном случае не требуется. Для обновления учетных данных необходимо:

1. Выбрать уровень СВ и открыть категорию **Состояние** → **Основное**.
2. В блоке *Управление* выбрать пункт **Обновить учетные данные**.
3. В появившемся окне ввести данные пользователя и установить флаг в поле *Обновить данные с сервера*. Затем нажать кнопку **Установить** (см. Рисунок 17).

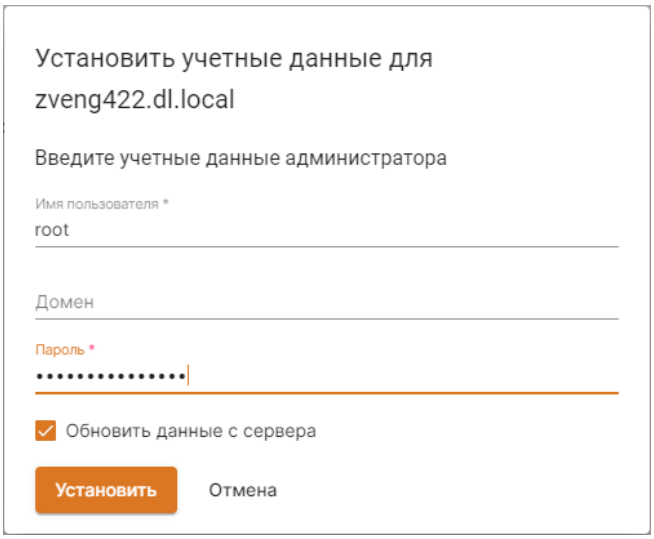

Рисунок 17. Установка учетных на данных СВ oVirt/zVirt/HOSTVM/RedVirt

Удаление учетных данных может потребоваться, если планируется вывести СВ из-под управления и повторно ввести в **ДБ СЗИ ВИ** без переустановки **ЦУ СЗИ ВИ**. Для удаления учетных данных необходимо:

1. Выбрать уровень СВ и открыть категорию **Состояние** → **Основное**.
2. В блоке *Управление* выбрать пункт **Удалить учетные данные**.
3. В появившемся окнеподтвердить удаление, нажав кнопку **ОК**.

2.6.3.1 Установка, обновление и удаление учетных данных для гипервизора oVirt/zVirt/HOSTVM/RedVirt

Перед обновлением учетных данных для гипервизора oVirt/zVirt/HOSTVM, необходимо убедиться, что к гипервизору открыт доступ по SSH и отключена политика «Вход: блокировать протокол SSH» (подробнее см. п. 4.3.1.3 «Параметры входа для oVirt/zVirt/HOSTVM/RedVirt»).

Установка учетных данных происходит в момент установки агента DL Host и ввода СВ в домен безопасности (подробнее см. п. 2.5.4.3 «Установка и удаление агента DL Host на гипервизоре oVirt/zVirt/HOSTVM/RedVirt»).

Обновление учетных данных требуется в случае их смены штатными средствами среды виртуализации или для перевычитки списка учетных записей пользователей ВИ, ролей и т.д. Переустановка агента в данном случае не требуется. Для обновления учетных данных необходимо:

1. Выбрать уровень гипервизора и открыть категорию **Состояние** → **Основное**.
2. В блоке *Управление* выбрать пункт **Обновить учетные данные**.
3. В появившемся окне ввести данные пользователя и установить флаг в поле *Обновить данные с сервера*. Затем нажать кнопку **Установить** (см. Рисунок 18).

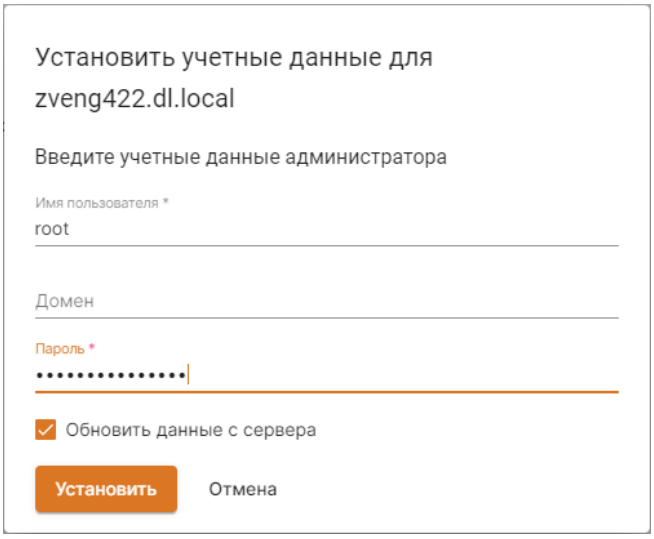

Рисунок 18. Обновление учетных на данных СВ oVirt/zVirt/HOSTVM/RedVirt

Удаление учетных данных может потребоваться, если планируется вывести СВ из-под управления и повторно ввести в **ДБ СЗИ ВИ** без переустановки **ЦУ СЗИ ВИ**. Для удаления учетных данных необходимо:

1. Выбрать уровень СВ и открыть категорию **Состояние** → **Основное**.
2. В блоке *Управление* выбрать пункт **Удалить учетные данные**.
3. В появившемся окне подтвердить удаление, нажав кнопку **ОК**.

2.7 Вывод серверов виртуализации из домена безопасности

Перед выводом СВ из-под управления рекомендуется:

1. Очистить список клиентов управления СВ (подробнее см. п. 5.1.2 «Клиенты управления СВ»).
2. Скорректировать правила управления СВ (подробнее см. п. 5.1.1 «Правила управления СВ»).
3. Открыть доступ по SSH, отключив следующие политики безопасности в зависимости от платформы виртуализации:
   - vCSA: Блокировать протокол SSH;
   - ESXi: Блокировать протокол SSH;
   - KVM: Блокировать протокол SSH.
4. Открыть доступ к штатному управлению виртуализацией, от отключив следующие политики безопасности в зависимости от платформы виртуализации:
   - vCSA: Разрешить вход на Web-клиент vCSA Management Interface (VAMI);
   - vCSA: Разрешить локальный вход с консоли;
   - vSphere: Запрет на работу через Web-клиент;
   - KVM: блокировать доступ к Cockpit Web Interface.

Для вывода сервера виртуализации из домена безопасности необходимо:

1. Открыть дерево агентов.
2. Выбрать нужну группу и во вкладке *Параметры безопасности* проверить отключены ли политики (см. Рисунок 19).

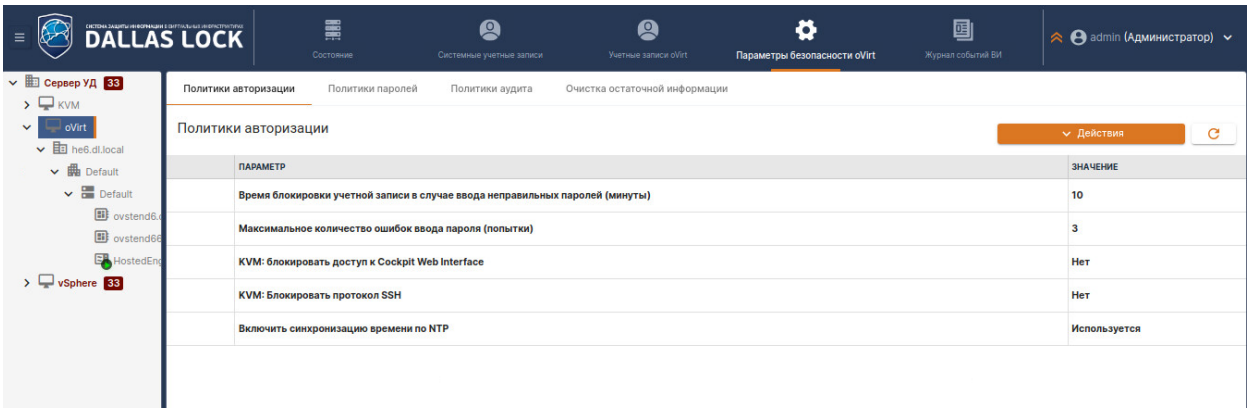

Рисунок 19. Отключение политик перед выводом СВ

3. Вычистить доверенные клиенты, учетные записи и агенты (см. п. 2.5.4 «Установка и удаление агента DL Engine и ввод в домен безопасности сервера виртуализации oVirt/zVirt/HOSTVM/RedVirt»).
4. Выбрать уровень Сервера виртуализации и открыть категорию **Состояние** → **Основное**.
5. Нажать кнопку **Вывести из-под управления** в блоке *Управление* (см. Рисунок 20).

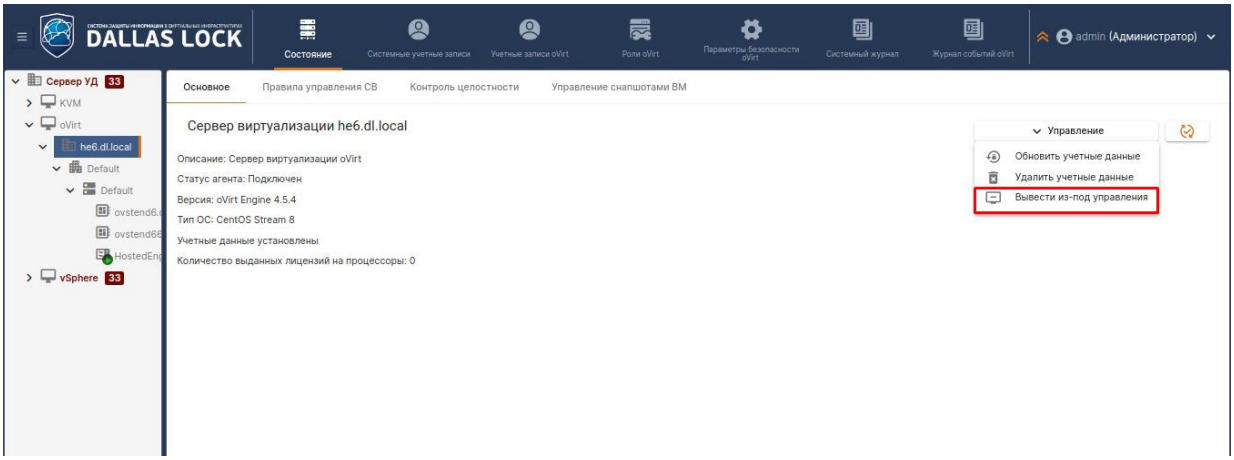

Рисунок 20. Удаление сервера виртуализации из ВИ

При отсутствии связи с СВ рекомендуется выводить с установленной галочкой *Вывести принудительно* (см. Рисунок 21), иначе агент будет удален, но в дереве СВ и агенты всё равно будет отображаться.

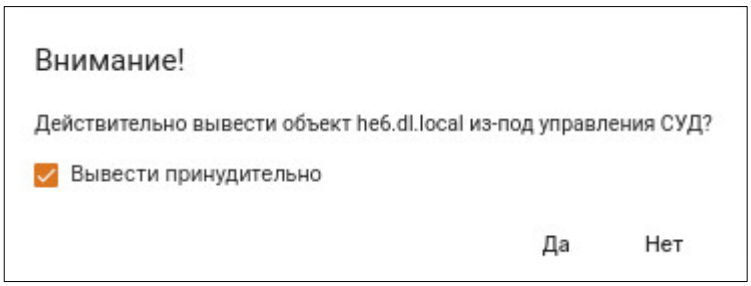

Рисунок 21. Принудительный вывод

6. Подтвердить запрос на вывод сервера виртуализации из домена, нажав кнопку **Да**.

После вывода СВ из-под управления **СЗИ ВИ** настройки, политики учетные записи, роли, разрешения и т.д. остаются теми, которые были установлены при вводе СВ под управление **СЗИ ВИ**.

2.8 Удаление СЗИ ВИ

2.8.1 Удаление компонента «Центр управления СЗИ ВИ Dallas Lock»

Для того чтобы правильно и полностью удалить **СЗИ ВИ**, требуется выполнить поочередные

действия.

Для начала следует удалить агентов на хостах. Это можно сделать, перейдя в дереве на агент/гипервизор. Во вкладке *Состояние*, в разделе *Основное* нажать на блок *Управление*. В открывшемся окне блока *Управление* выбрать **Удалить агент** (см. Рисунок 22). Подтвердить нажатием на **Ок**.

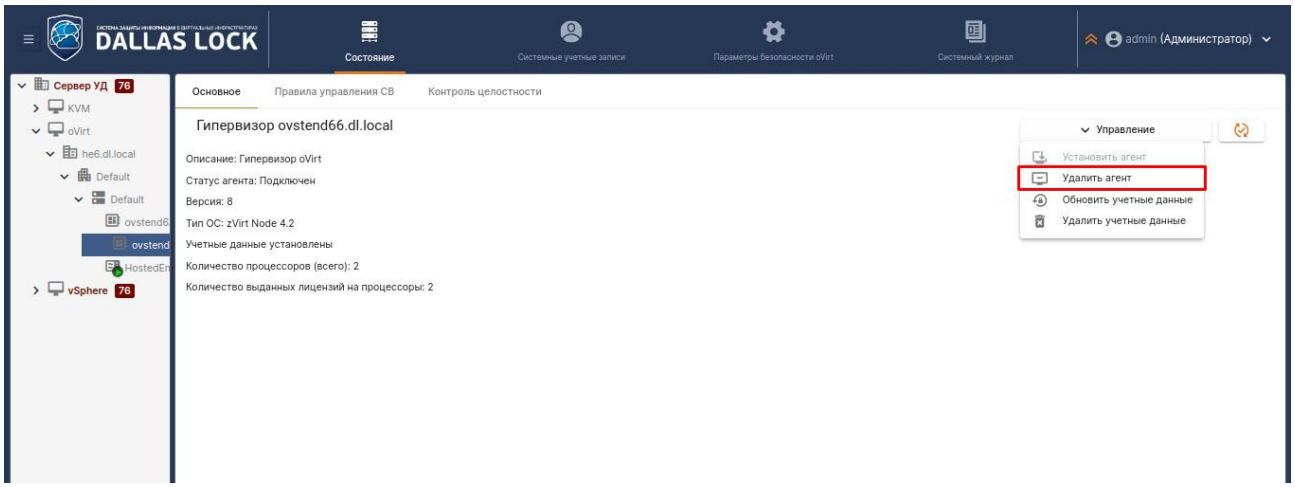

Рисунок 22. Уаление агента

Далее, в дереве нужно выбрать Сервер Виртуализации. Во вкладке *Состояние* в разделе **Основное**, в блоке *Управление* выбрать **Вывести из-под управления** (см. 2.7 «Вывод серверов виртуализации из домена безопасности»). Подтвердить действие нажатием на **Да**. После этих действий следует переходить к удалению ядра **СЗИ ВИ**.

2.8.1.1 Удаление через пакетный менеджер DEB

1. Откройте консоль и введите команду:
   sudo dpkg -r confident-vicored
   или
   sudo dpkg -P confident-vicored

2.8.1.2 Удаление через пакетный менеджер RPM

1. Откройте консоль и введите команду:
   sudo rpm -e confident-vicored
   или
   sudo rpm -U confident-vicored

2.8.2 Удаление агента DL KVM

1. Откройте консоль и введите команду:
   /opt/confident/bin/uninstall_agent.sh

2.9 Обновление системы защиты

Обновление установленной системы защиты выполняется путем удаления **СЗИ ВИ** и ее компонентов защиты с объектов ВИ и установки обновленного дистрибутива с последующей установкой агентов DL.

Перед удалением рекомендуется воспользоваться функцией сохранения конфигурации предыдущей версии **СЗИ ВИ** (подробнее см. п. 10.1 «Сохранение конфигурации ЦУ СЗИ ВИ»).

> **!** Сохранение и применение файла конфигурации ЦУ **СЗИ ВИ** осуществляется только на соответствующем ЦУ **СЗИ ВИ** с соответствующей версией, на котором данная конфигурация была сформирована. Использовать данный механизм для обновления **СЗИ ВИ** на более старшую версию не рекомендуется.

Перед установкой обновленного дистрибутива необходимо выполнить проверку подлинности электронной подписи (согласно инструкции, представленной на сайте www.dallaslock.ru) и расчет и сверку контрольных сумм полученного пакета обновлений с контрольными суммами, указанными на сайте.

Информация о появлении обновленной версии **СЗИ ВИ** отображается на сайте www.dallaslock.ru.

Так же реализован механизм проверки наличия более новых версий **СЗИ ВИ** с использованием открытого канала связи (протокол http).

Для проверки наличия обновления необходимо выполнить следующие действия:

1. Открыть дополнительное меню Консоли и нажать кнопку **О программе**.
2. В появившемся окне нажать кнопку **Проверить обновление**.
3. Будет произведена проверка наличия обновления. В открывшемся окне будет отображено сообщение о результатах проверки.

Для получения обновления необходимо выполнить следующие действия:

1. Обратиться в службу технической поддержки **ООО «Конфидент»** (обновление предоставляется только при наличии действующей (оплаченной) лицензией).
2. Получить от сотрудника технической поддержки **ООО «Конфидент»** ссылку на архив, расположенный на ftp-сервере **ООО «Конфидент»**. Архив содержит в себе обновленный дистрибутив **СЗИ ВИ**.
3. Сохранить и распаковать указанный архив на жесткий диск ПК (либо на другой накопитель), на котором требуется обновить **СЗИ ВИ**.

2.10 О программе

Со следующими сведениями о **СЗИ ВИ** можно ознакомиться в информационном окне **О программе**, вызвав его из списка дополнительных функций кнопки главного меню (см. Рисунок 23):

- полное наименование и редакция **СЗИ ВИ**;
- номер версии и дата сборки **ЦУ СЗИ ВИ**;
- путь и наименование файла ключа лицензии;
- номер лицензии;
- редакция лицензии;
- код технической поддержки;
- дата завершения технической поддержки;
- адрес сайта компании-разработчика;
- адрес сайта продуктовой линейки **Dallas Lock**;
- адрес электронной почты коммерческого департамента;
- номер телефона коммерческого департамента;
- адес личного кабинета на портале технической поддержки;
- адрес электронной почты технической поддержки;
- номер телефона технической поддержки;
- ссылка на телеграмм-бота.

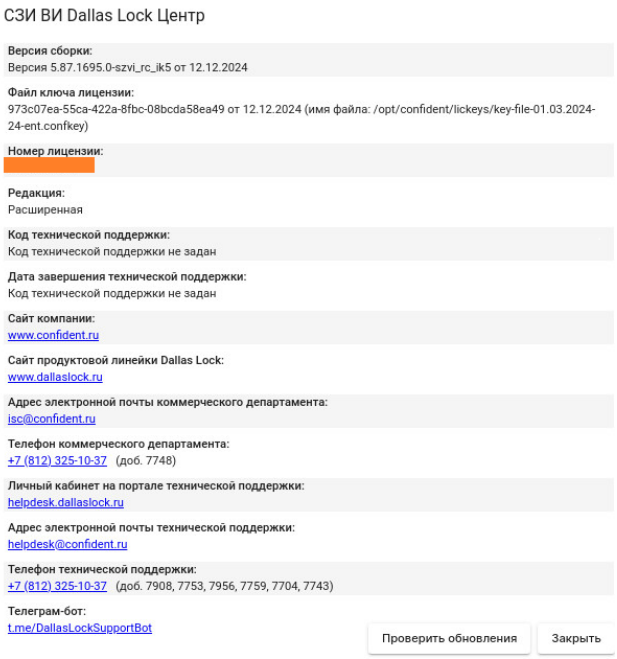

Рисунок 23. Окно «О программе»

Процесс обновления **СЗИ ВИ** с помощью кнопки **Проверить обновление** описан в п. 2.9 «Обновление системы защиты».

Действующий код технической поддержки является условием предоставления помощи в установке

и настройке **СЗИ ВИ** специалистами компании-разработчика, а также условием доступа к сертифицированным обновлениям.

3 ОПИСАНИЕ СРЕДСТВ АДМИНИСТРИРОВАНИЯ

3.1 Консоль

Администрирование установленной **СЗИ ВИ** осуществляется из веб-Консоли **ЦУ СЗИ ВИ**.

Контроль доступа к веб-консоли **ЦУ СЗИ ВИ** осуществляется средствами ролевой модели разграничения доступа (подробнее см. п. 3.4 «Встроенные учетные записи Сервера УД»).

Работа с веб-консолью осуществляется из окна браузера. Для вызова веб-консоли необходимо открыть браузер и в адресной строке ввести ip-адрес «https://<vi-core-ip>:4564/» или «https://localhost:4564/» ТС с установленным компонентом **ЦУ СЗИ ВИ Dallas Lock**. В окне подключения к **ЦУ СЗИ ВИ** требуется ввести следующие данные (см. Рисунок 24):

- Логин учетной записи;
- Пароль учетной записи.

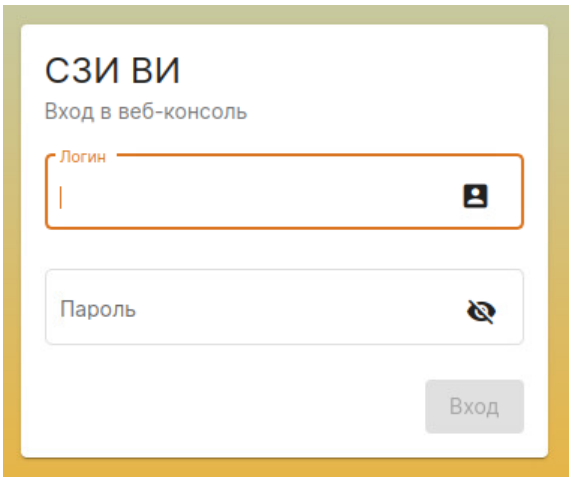

Рисунок 24. Ввод пароля учетной записи для входа в веб-консоль

Главное окно веб-консоли содержит следующие рабочие области (см. Рисунок 25):

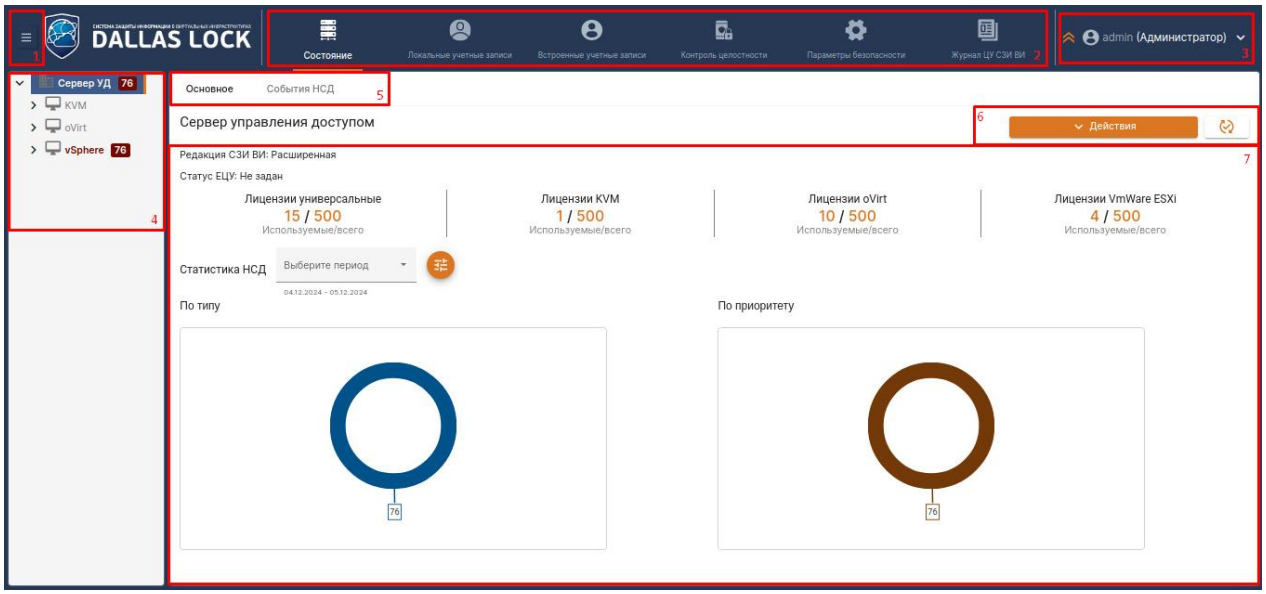

Рисунок 25. Окно Веб-Консоли

1. Кнопка дополнительного меню.
2. Категории параметров основного меню.
3. Меню выбора пользователя.
4. Проводник в виде дерева объектов, отображающий список клиентов, групп клиентов и объектов ВИ (см. Рисунок 26).
5. Вкладки выбранных категорий основного меню.
6. Панель действий.
7. Рабочая область, содержащая списки параметров или объектов текущей категории.

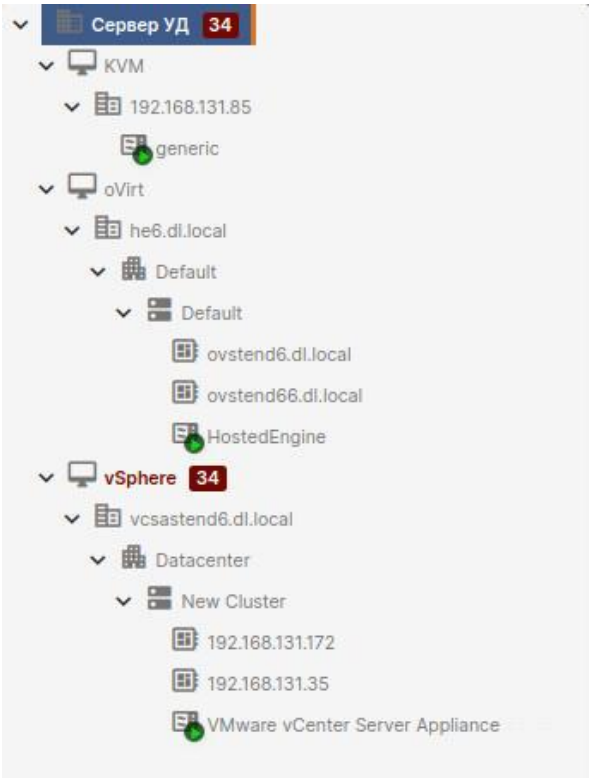

Рисунок 26. Объекты ВИ

С помощью Консоли можно настроить параметры безопасности для следующих объектов ВИ:

- — Сервер УД;
- — Уровень группы;
- — Сервер виртуализации;
- — Дата центр;
- — Гипервизор;
- — Кластер;
- — Виртуальная машина и ее состояние (выключена);
- — Виртуальная машина и ее состояние (включена);
- — Пул ресурсов (Resource pool);
- — Хранилища;
- — VM Network;
- — Папка.

Для обновления дерева агентов ВИ необходимо перейти на уровень Сервера УД в категорию **Состояние** → **Основное** и нажать кнопку *Действия* и выбрать кнопку **Синхронизация СВ и гипервизоров**.

Для каждого из объектов в верхней части основного меню Консоли формируется свой список вкладок. При выборе вкладки в рабочей области открывается страница с соответствующими параметрами и меню.

Контекстное меню дерева Консоли позволяет на уровне vSphere добавлять сервера виртуализации vCSA, на уровне KVM добавлять гипервизоры KVM, СВ oVirt/zVirt/HOSTVM/RedVirt и гипервизоры oVirt/zVirt/HOSTVM/ RedVirt и синхронизировать их по команде администратора **ЦУ СЗИ ВИ**.

3.2 Информационная панель

3.2.1 Информационная панель групп ВИ

Группы элементов *vSphere*, *oVirt* и *KVM* единообразно отображают информацию о себе. При выборе группы состояние объектов группы отображается в рабочей области (см. Рисунок 27):

1. Наименование Сервера УД.
2. Редакция **СЗИ ВИ** (Ограниченная/Стандартная/Расширенная).

3. Информация о подключении к серверу **ЕЦУ**.
4. Информация о лицензиях.
5. Статистика НСД (выбор периода).
6. Кнопка вызова настройки отображения (назначение приоритета и цвета).
7. Круговые диаграммы (события НСД по типу и по приоритету).

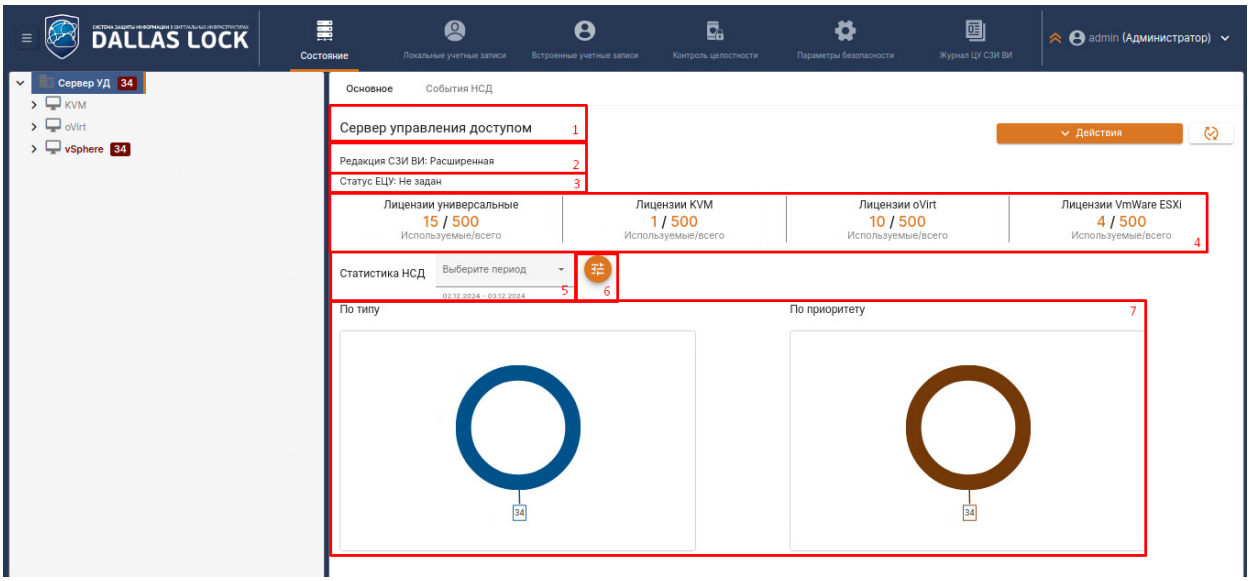

Рисунок 27. Сводная информация по элементу «Сервер УД»

При нажатии на кнопку настроек приоритетов и оформления круговых диаграмм (6)  откроется окно с настройками отображения типов событий по приоритетам (Рисунок 28) и по цветам (Рисунок 29).

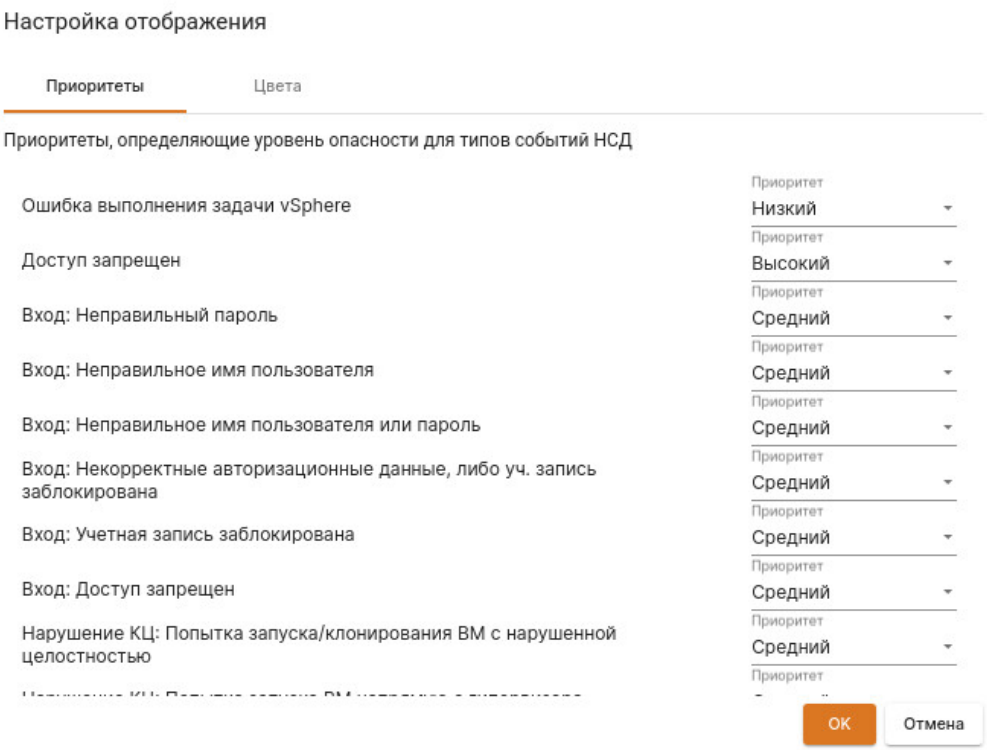

Рисунок 28. Настройка приоритетов типов событий НСД

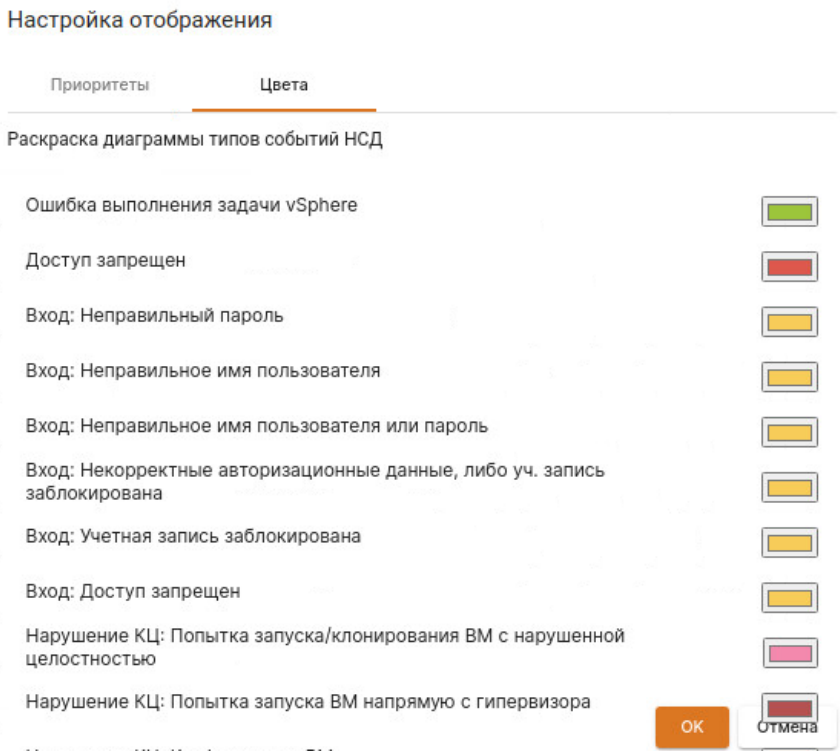

Рисунок 29. Сопоставление цветов типам событий НСД

Окна отображают перечень типов событий НСД, регистрация которых включена для выбранного элемента дерева – Сервера УД или одной из групп. Для изменения перечня регистрируемых событий см. п. 3.6 «Сигнализация об НСД».

3.2.1.1 Информационная панель Сервера УД

Группы элементов *vSphere*, *oVirt* и *KVM* единообразно настраиваются и отображают информацию о себе. При выборе группы в дереве состояние объектов группы отображается в рабочей области (Рисунок 30)[8].

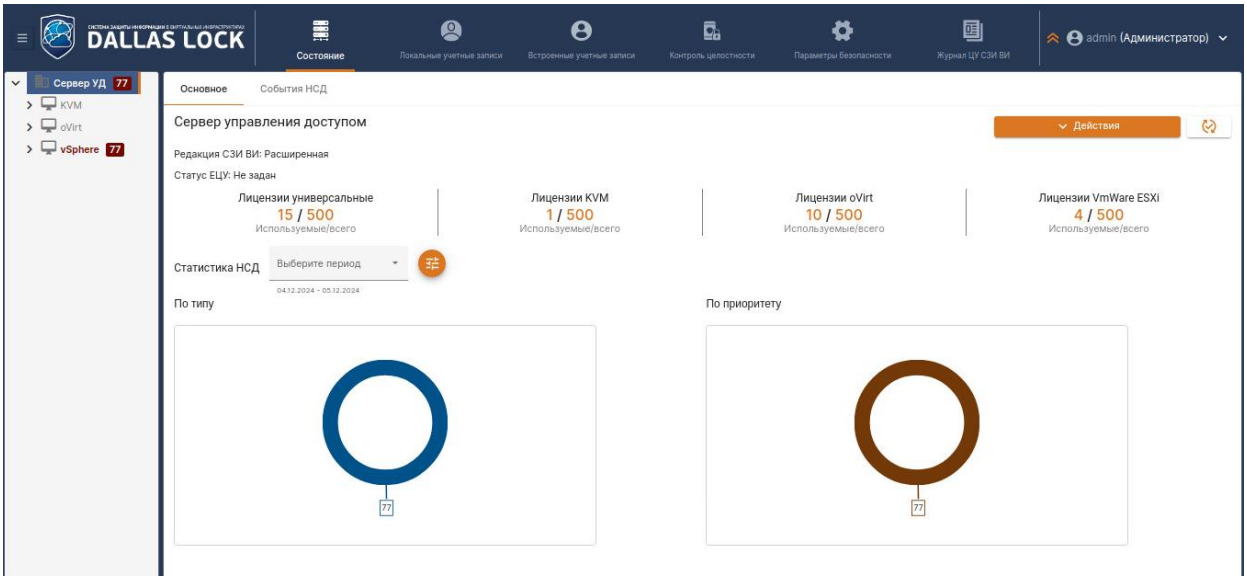

Рисунок 30. Информационная панель Сервера УД

Доступны следующие действия с группами:

- добавление сервера виртуализации;
- синхронизация параметров безопасности всех объектов группы по команде администратора (см. п. 3.5 «Синхронизация»).

3.2.1.2 Информационная панель групп ВИ

Группы элементов *vSphere*, *oVirt* и *KVM* единообразно настраиваются и отображают информацию о

[8] Круговые диаграммы (события НСД по типу и по приоритету) доступны только в редакции «Расширенная».

себе. При выборе группы в дереве агентов состояние объектов группы отображается в рабочей области (см. Рисунок 31).

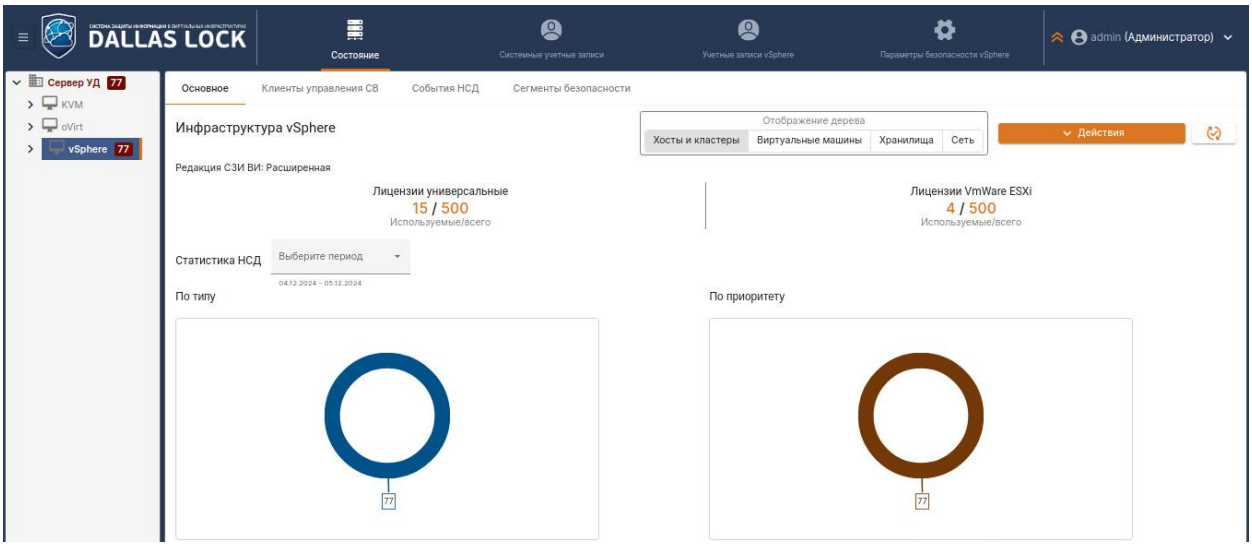

Рисунок 31. Сводная информация групп ВИ

Доступны следующие действия с группами:

- добавление сервера виртуализации;
- синхронизация параметров безопасности всех объектов группы по команде администратора (см. п. 3.5 «Синхронизация»);

Для группы объектов ВИ *vSphere* есть возможность изменить отображение дерева объектов.

Доступны следующие режимы отображения дерева ВИ группы vSphere:

- Хосты и кластеры – наиболее полный режим отображения.
- Виртуальные машины – отображаются виртуальные машины и их вышестоящая иерархия.
- Хранилища – datastores и пр.
- Сеть – объекты сети (виртуальные коммутаторы и пр.).

По умолчанию дерево отображается в режиме **Хосты и кластеры**.

3.2.1.3 Информационная панель СВ vSphere/vCSA

Просмотр основных параметров СВ vSphere происходит на уровне Сервера виртуализации в категории **Состояние** → **Основное**.

Данная категорию содержит элементы управления СВ, а также отображает статус учетных данных, описание, версию СВ vSphere и тип ОС (см. Рисунок 32).

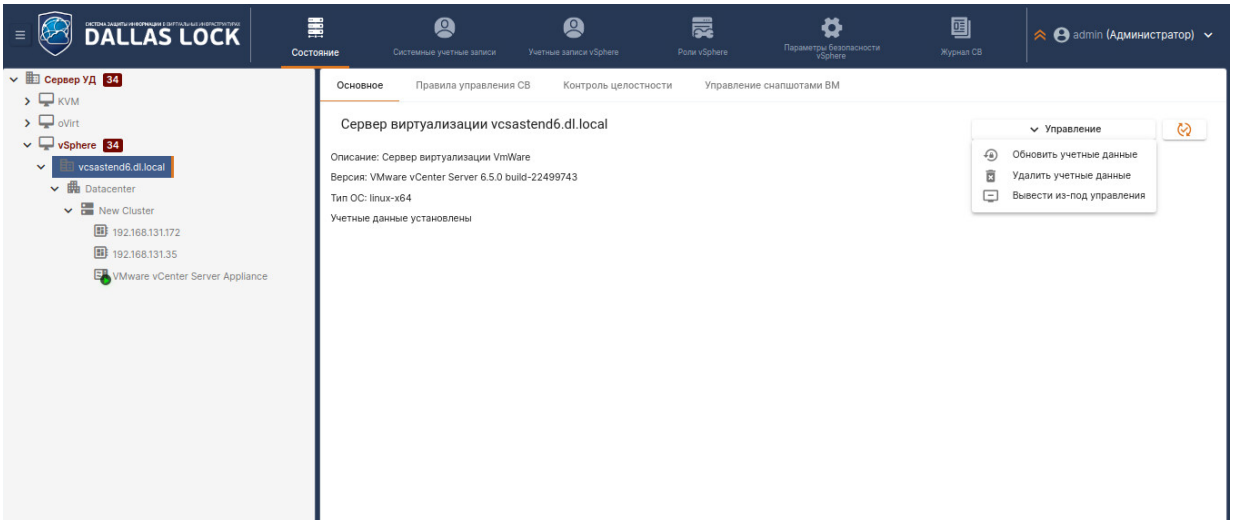

Рисунок 32. Рабочая область СВ vCSA

Доступны следующие действия с Сервером виртуализации:

- обновление/удаление учетных данных;
- вывод из-под управления СВ;
- синхронизация параметров безопасности Сервера виртуализации с **ЦУ СЗИ ВИ** (см. п. 3.5 «Синхронизация»).

3.2.1.4 Информационная панель гипервизора ESXi

Просмотр основных параметров гипервизора происходит на уровне гипервизора ESXi в категории **Состояние → Основное**.

Данная категорию содержит элементы управления гипервизора, а также отображает описание гипервизора, версию VMware ESXi, тип ОС, статус учётных данных, количество процессоров на гипервизоре и количество выданных лицензий на процессоры (см. Рисунок 33).

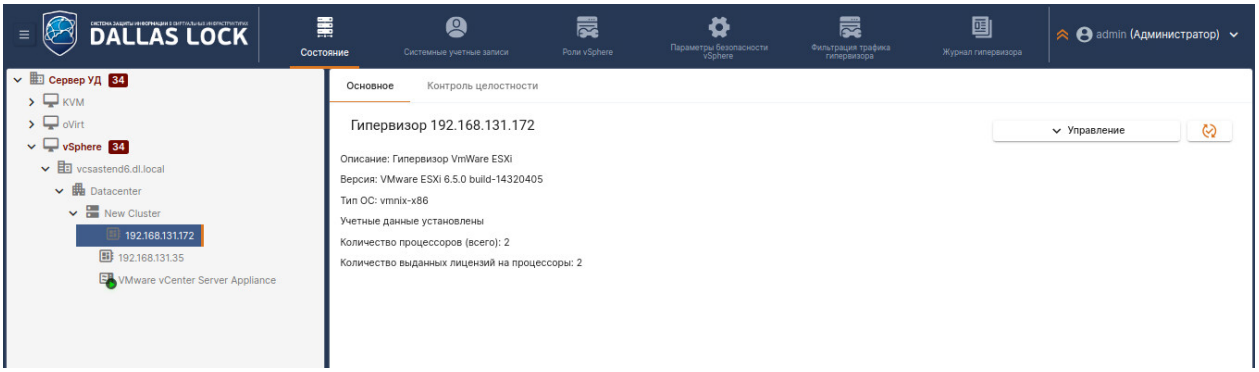

Рисунок 33. Рабочая область гипервизора ESXi

Доступны следующие действия с гипервизором:

- установка/обновление/удаление учетных данных;
- синхронизация параметров безопасности с **ЦУ СЗИ ВИ** (см. п. 3.5 «Синхронизация»).

3.2.1.5 Информационная панель гипервизора KVM

Просмотр основных параметров гипервизора происходит на уровне гипервизора KVM в категории **Состояние → Основное**.

Данная категорию содержит описание, статус агента, версию, тип ОС, а также отображает статус учетных данных, статус и версию агента QEMU и количество выданных лицензий на процессоры (см. Рисунок 34).

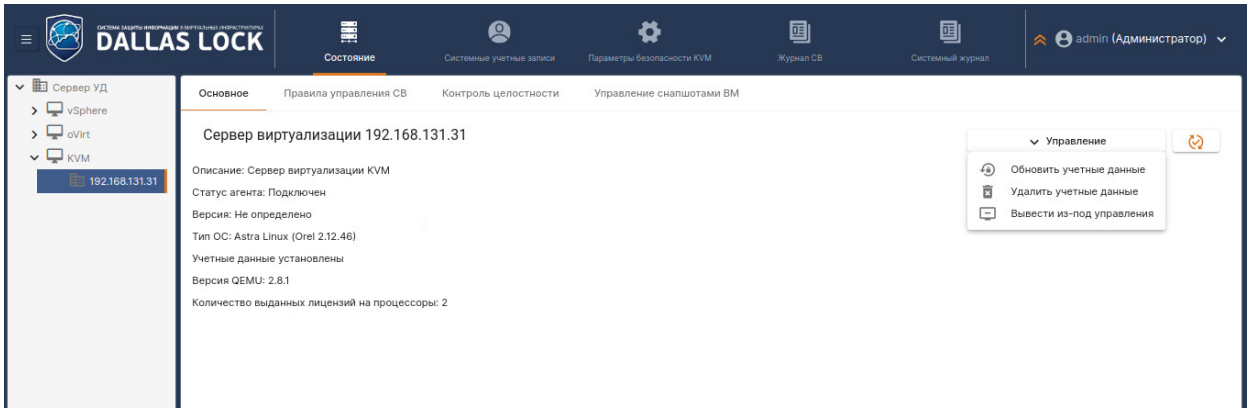

Рисунок 34. Рабочая область гипервизора KVM

Доступны следующие действия с гипервизором:

- обновление/удаление учетных данных;
- вывод из-под управления;
- синхронизация параметров безопасности с **ЦУ СЗИ ВИ** (см. п. 3.5 «Синхронизация»).

3.2.1.6 Информационная панель групп СВ oVirt/zVirt/HOSTVM/RedVirt

Просмотр основных параметров СВ oVirt/zVirt/HOSTVM/RedVirt происходит на уровне Сервера виртуализации в категории **Состояние → Основное**.

Данная категорию содержит элементы управления СВ, а также отображает описание, статус агента, версию, тип ОС, статус учётных данных и количество выданных лицензий на процессоры (см. Рисунок 35).

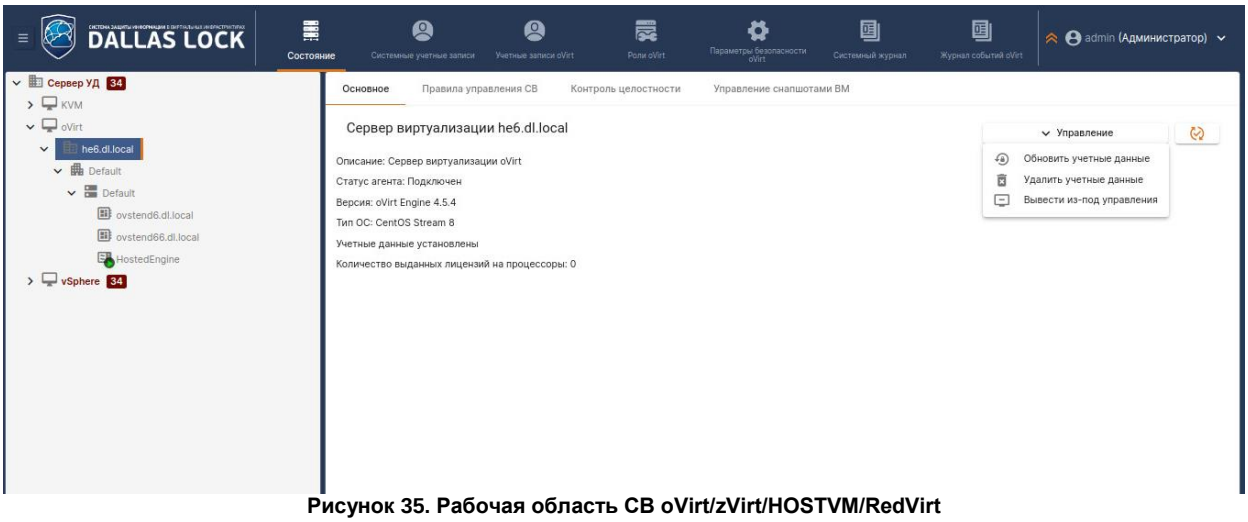

Рисунок 35. Рабочая область СВ oVirt/zVirt/HOSTVM/RedVirt

Доступны следующие действия с СВ:

- обновить/удалить учетные данные;
- вывести из-под управления;
- синхронизация параметров безопасности с **ЦУ СЗИ ВИ** (см. п. 3.5 «Синхронизация»).

3.2.1.7 Информационная панель гипервизора oVirt/zVirt/HOSTVM/RedVirt

Просмотр основных параметров гипервизора oVirt/zVirt/HOSTVM/RedVirt происходит на уровне гипервизора в категории **Состояние** → **Основное**.

Данная категорию содержит элементы управления гипервизора, а также отображает описание, статус агента, версию, тип ОС, статус учетных данных, количество процессоров и количество выданных лицензий на процессоры (см. Рисунок 36).

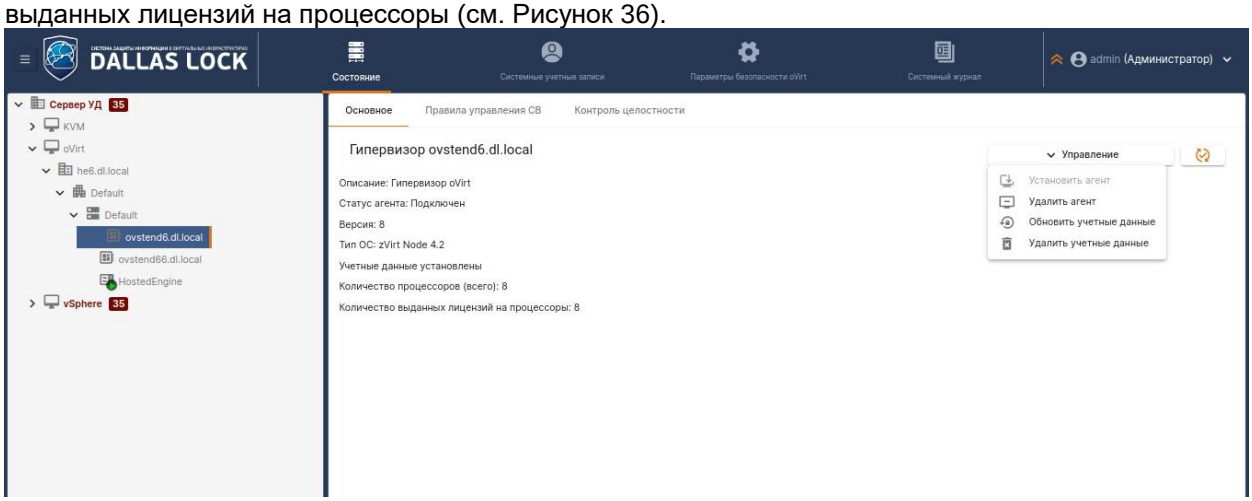

Рисунок 36. Рабочая область гипервизора oVirt/zVirt/HOSTVM/RedVirt

Доступны следующие действия с гипервизором:

- обновление статуса агента;
- установка (переустановка) агента DL Host на гипервизоре;
- удаление агента DL Host на гипервизоре;
- синхронизация параметров безопасности с **ЦУ СЗИ ВИ** (см. п. 3.5 «Синхронизация»).

3.3 Основные параметры

Настройка основных параметров функционирования **СЗИ ВИ** осуществляется в **Общем меню** и выбором пункта **Параметры сервера УД** в дополнительном меню Консоли (см. Рисунок 37). В открывшемся окне путем выбора соответствующих вкладок в меню можно задать определенные настройки и параметры Сервера УД, vSphere, oVirt, KVM (см. Рисунок 38).

Рисунок 37. Дополнительное меню Консоли СЗИ ВИ

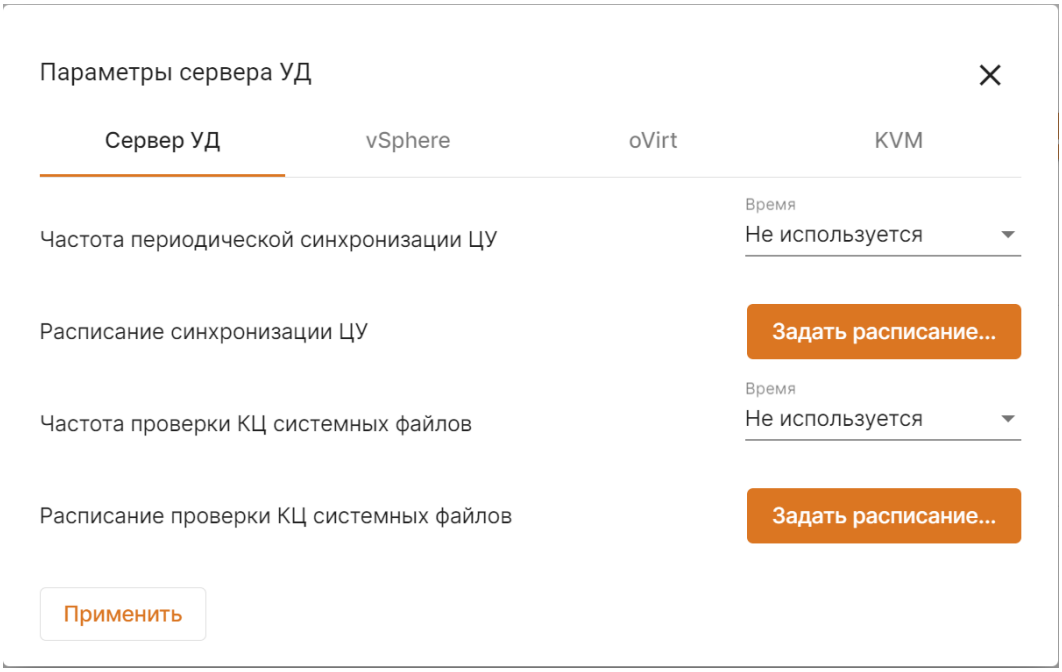

Рисунок 38. Окно настройки параметров сервера УД

3.3.1 Основные параметры работы

Для настройки параметров работы агентов необходимо выбрать вкладку *Сервер УД* в меню. Ниже отобразится перечень доступных настроек:

- частота периодической синхронизации ЦУ;
- расписание синхронизации ЦУ;
- частота проверки КЦ системных файлов;
- расписание проверки КЦ системных файлов.

После внесения изменений необходимо нажать кнопку **Применить**.

3.3.2 Основные параметры группы СВ vSphere

В окне настройки параметров сервера УД для группы vSphere доступны следующие настраиваемые

параметры (см. Рисунок 39):

- максимальное кол-во клиентов управления;
- частота проверки КЦ системных файлов (необходимо выбрать период времени);
- расписание проверки КЦ системных файлов;
- частота периодической синхронизации СВ;
- расписание синхронизации СВ;
- частота периодического сбора журналов СВ;
- расписание сбора журналов СВ.

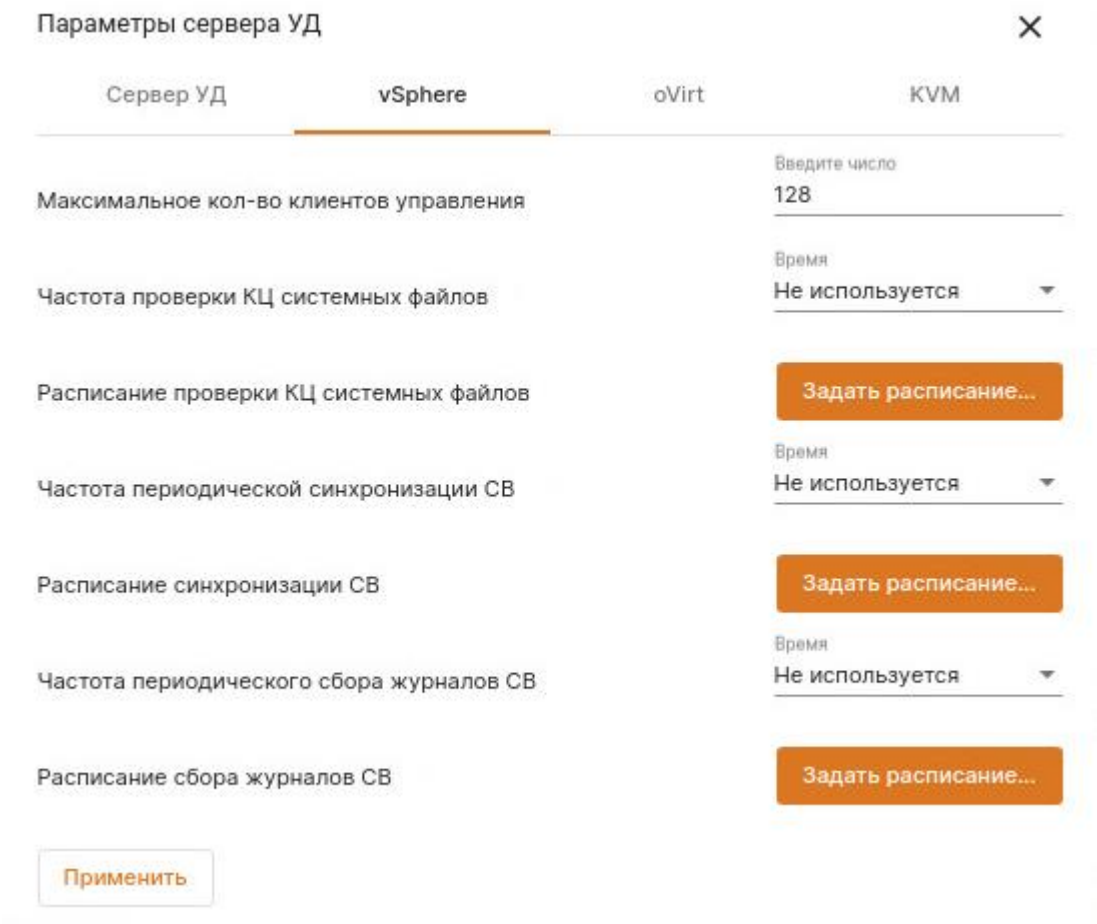

Рисунок 39. Окно настройки параметров группы vSphere

После внесения изменений необходимо нажать кнопку **Применить**.

3.3.3 Основные параметры группы СВ oVirt

В окне настройки параметров сервера УД для группы oVirt доступны следующие настраиваемые параметры (см. Рисунок 40):

- максимальное количество клиентов управления;
- частота проверки КЦ системных файлов (необходимо выбрать период времени);
- расписание проверки КЦ системных файлов;
- частота периодической синхронизации СВ;
- расписание синхронизации СВ;
- частота периодического сбора журналов СВ;
- расписание сбора журналов.

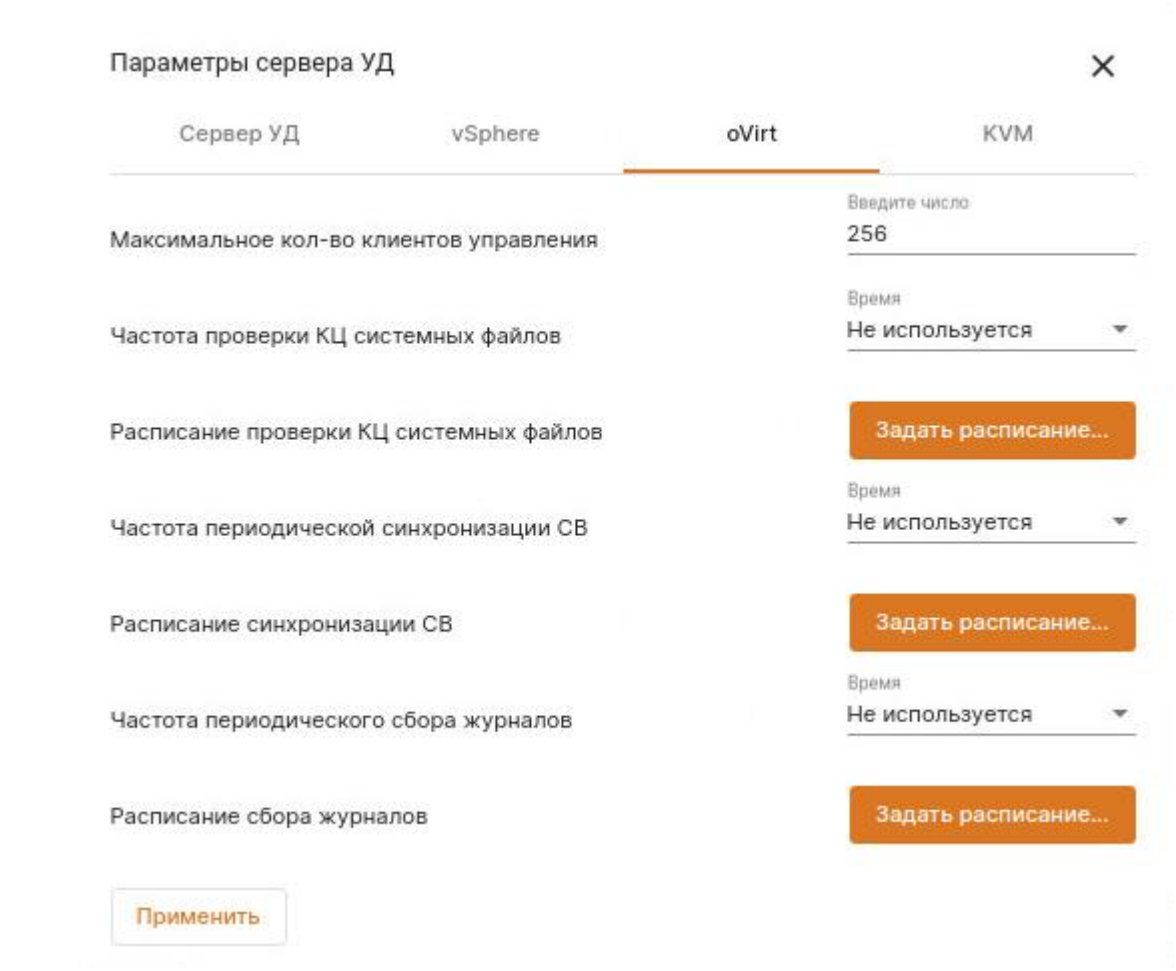

Рисунок 40. Окно настройки параметров группы oVirt

После внесения изменений необходимо нажать кнопку **Применить**.

3.3.4 Основные параметры группы KVM

В окне настройки параметров сервера УД для группы KVM доступны следующие настраиваемые параметры (см. Рисунок 41):

- максимальное кол-во клиентов управления;
- частота проверки КЦ системных файлов (необходимо выбрать период времени);
- расписание проверки КЦ системных файлов;
- частота периодической синхронизации СВ;
- расписание синхронизации СВ.

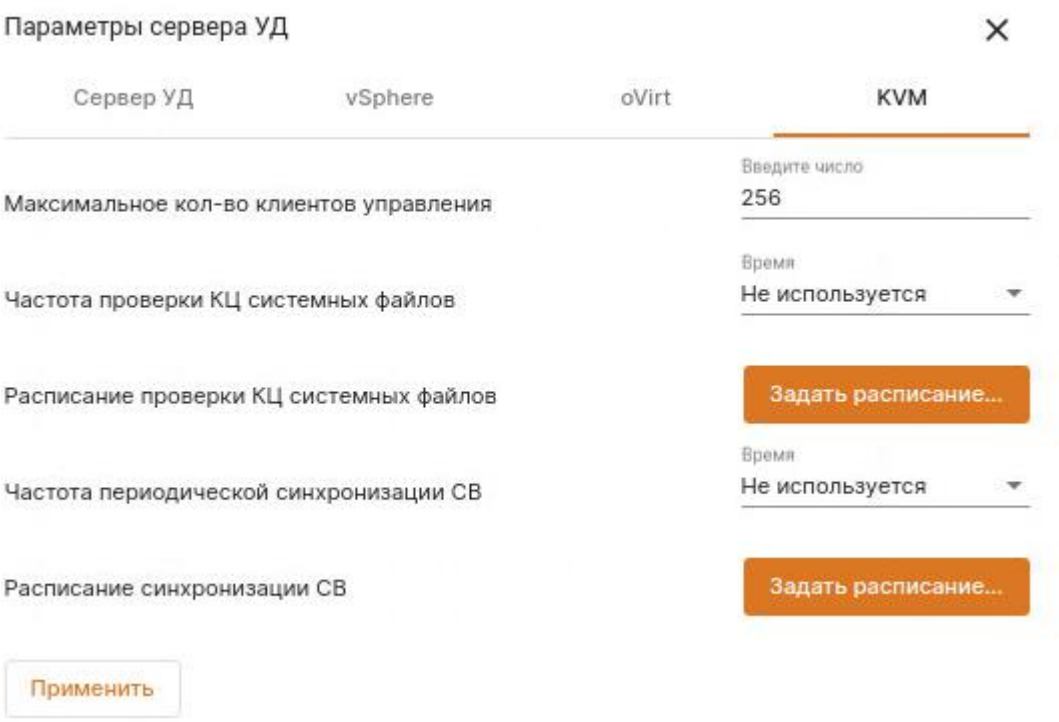

Рисунок 41. Окно настройки параметров группы KVM

После внесения изменений необходимо нажать кнопку **Применить**.

3.4 Встроенные учетные записи Сервера УД

Контроль доступа к **ЦУ СЗИ ВИ** осуществляется средствами ролевой модели разграничения доступа. Для работы с ролями необходимо на уровне Сервера УД перейти в категорию **Встроенные учётные записи** (см. Рисунок 42).

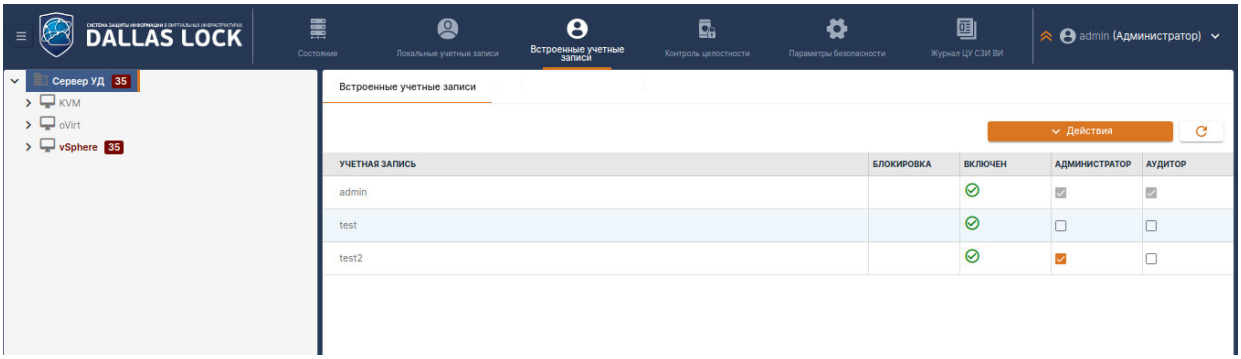

Рисунок 42. Встроенные учетные записи

Роль представляет собой совокупность привилегий – полномочий по выполнению действий в части администрирования **ЦУ СЗИ ВИ**. Для удобства привилегии группируются в несколько категорий в зависимости от области применения.

Различным учетным записям (или группам пользователей) **СЗИ ВИ** имеется возможность присвоить определенную роль.

Рабочая область категории **Встроенные учётные записи** состоит из разделов: *Учётная запись*, *Блокировка*, *Включён*, *Администратор* и *Аудитор* (см. Рисунок 42).

Для доменной роли осуществляется автоматическое наследование назначения на более низкоуровневых узлах.

В **ЦУ СЗИ ВИ** существуется одна предустановленная роль суперадминистратора, которую невозможно отредактировать или удалить.

3.4.1 Создание, изменение и удаление назначений ролей

Назначение предустановленных ролей пользователям происходит в блоке *Действия* (см. Рисунок 43).

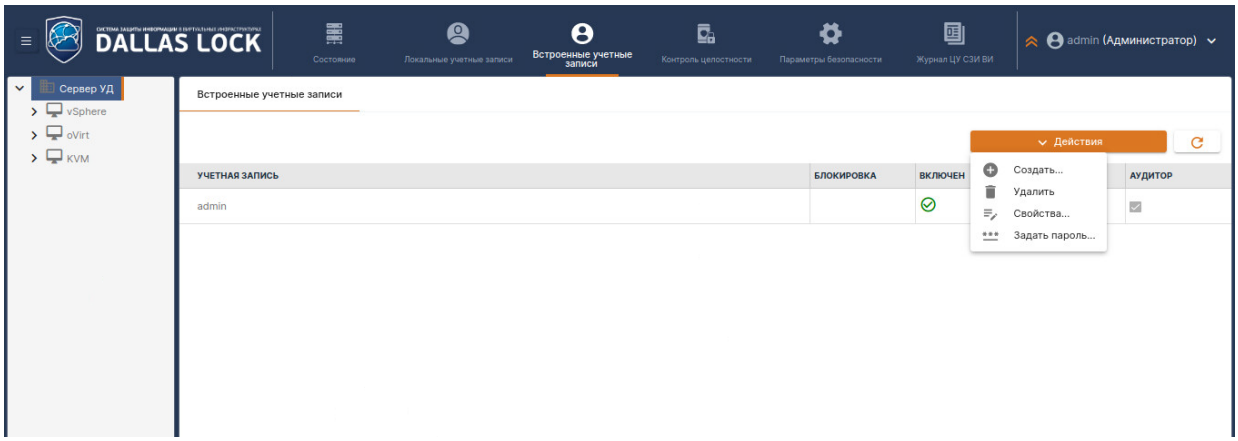

Рисунок 43. Назначение предустановленных ролей

Для назначения одной из предустановленных ролей для пользователя, необходимо нажать на кнопку **Создать** в блоке *Действия*. В появившемся окне указать имя пользователя, отметить выбранную для него роль, состояние учётной записи, указать максимальное число сессий и нажать кнопку **ОК** (см. Рисунок 44). Далее **СЗИ ВИ** запросит подтвердить пароль для нового пользователя. Есть возможность как сгенерировать пароль, так и написать вручную (см. Рисунок 45).

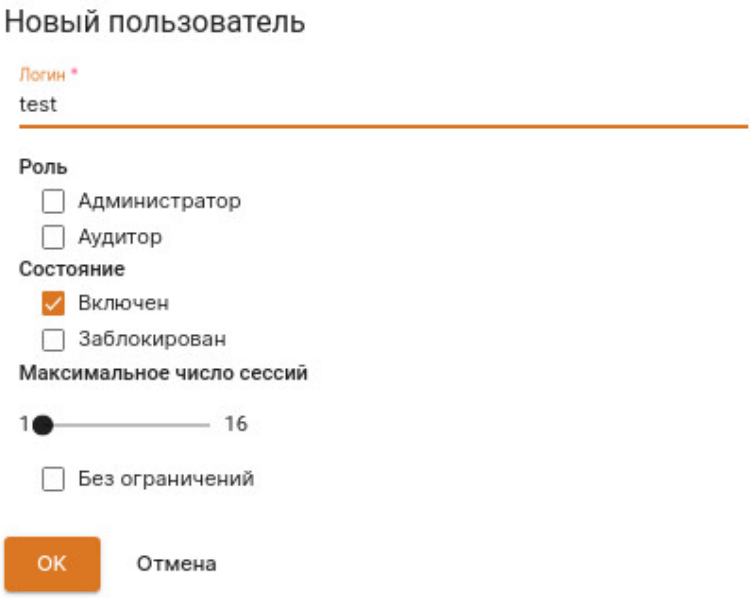

Рисунок 44. Администрирование. Создание пользователя

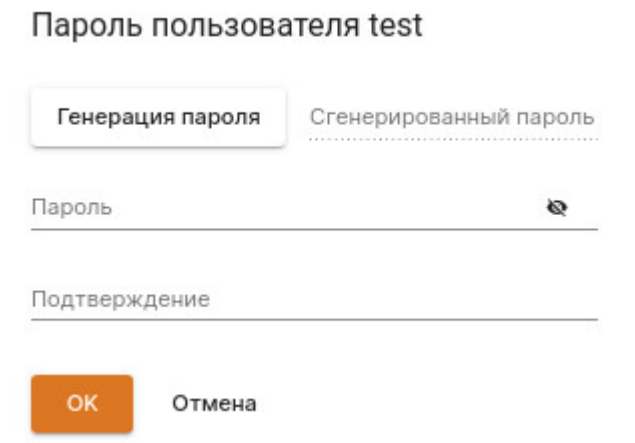

Рисунок 45. Генерация пароля

При назначении пользователю число сессий, можно установить флаг *Без ограничений*.

После этого в списке учетных записей и групп отобразится созданная учетная запись.

После входа в веб-консоль под учетной записью пользователя с правами аудитора параметры безопасности будут отображены, но не будет возможности их редактировать, производить настройки и действия; кнопки, отвечающие за настройки, будут недоступны.

Смена роли для учетной записи осуществляется при помощи выделения ее в таблице и нажатия кнопки **Свойства** в блоке *Действия*. При этом открывается диалоговое окно с выпадающим списком для выбора назначаемой роли (см. Рисунок 46).

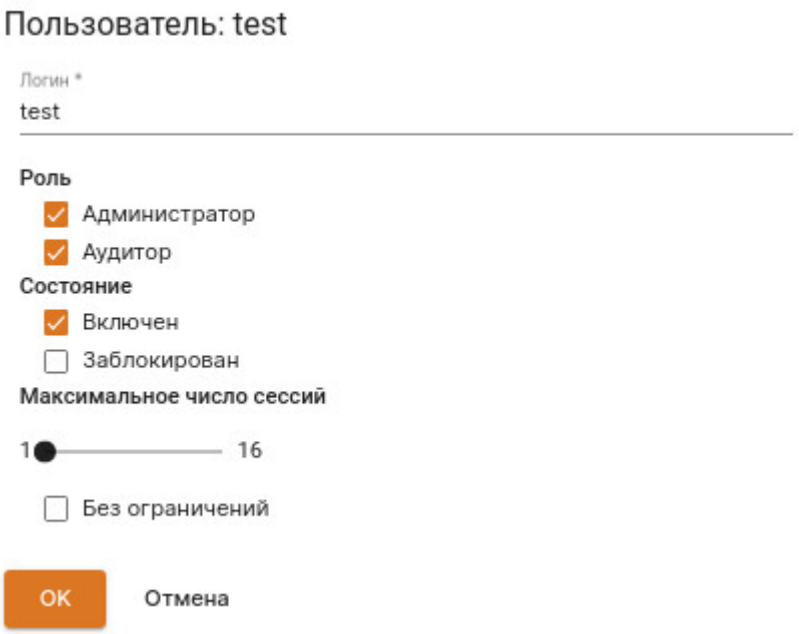

Рисунок 46. Смена роли для учетной записи

При назначении роли для учетной записи или группы, для которых назначение уже было создано, происходит переназначение данной роли.

Для удаления учетной записи с ролью назначения необходимо выделить пользователя, на панели сверху нажать кнопку **Удалить** в блоке *Действия* и подтвердить действие в появившемся диалогом окне (см. Рисунок 47).

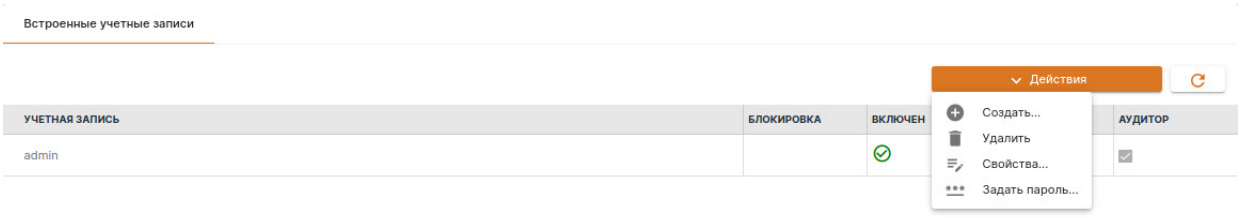

Рисунок 47. Удаление учетной записи

Также настройка и редактирование предустановленной модели происходит на уровне группы KVM, на уровне СВ (oVirt, vSphere/vCSA, гипервизорах ESXi) (подробнее см. п. 5.2 «Ролевая модель учетных записей СВ»).

3.5 Синхронизация

Синхронизация – это ключевое понятие в концепции **ЦУ СЗИ ВИ**. Под синхронизацией понимается процесс проверки соответствия настройки объектов ВИ с внутренней базой данных **ЦУ СЗИ ВИ**, являющейся эталонной настройкой ВИ. При обнаружении несоответствия к настройкам объектов ВИ применяются эталонные настройки **ЦУ СЗИ ВИ**.

Синхронизацию по команде администратора возможно произвести для определенного сервера

виртуализации или всей ВИ. Для этого необходимо выбрать уровень vSphere, KVM, oVirt, СВ или гипервизор, открыть вкладку *Состояние* нажать рядом с кнопкой *Действия* кнопку **Синхронизация СВ и гипервизоров**.

3.6 Сигнализация об НСД

Ситуации несанкционированного доступа на *Объектах ВИ* отслеживаются и сопровождаются сигнализацией на Сервере УД. Сообщения о событиях НСД заносятся в журнал Событий НСД. При попытке НСД на ПК с установленной **СЗИ ВИ** воспроизводится звуковой сигнал, выводится соответствующее всплывающее сообщение в области уведомлений (см. Рисунок 48).

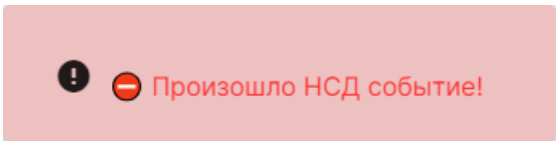

Рисунок 48. Сигнализация об НСД в области уведомлений

Также количество событий НСД отображается в квадратных скобках рядом с элементами дерева агентов (см. Рисунок 49).

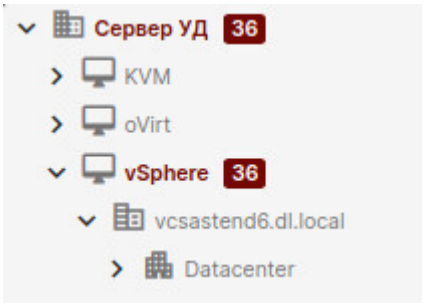

Рисунок 49. Сигнализация об НСД в дереве агентов

События, зафиксированные на объектах нижнего уровня, суммируются на объектах более высокого уровня, вплоть до объекта *Сервер УД*, который может отображать все события НСД всех объектов структуры дерева **СЗИ ВИ**.

При прочтении одного события НСД в списке событий НСД на том или ином уровне, количество событий НСД, отображаемое на этом уровне, уменьшается на единицу и все суммируемые события НСД на более высоких уровнях так же уменьшается на единицу. При прочтении большего количества событий НСД, отображаемые в дереве непрочитанные события уменьшатся на количество прочитанных событий НСД.

Для того чтобы произвести настройку уведомлений, получаемых от соответствующих агентов, необходимо:

1. В дереве агентов выбрать **Сервер УД** → **Параметры безопасности** → **Политики аудита**, после чего задать значения необходимых параметров (см. Рисунок 50).

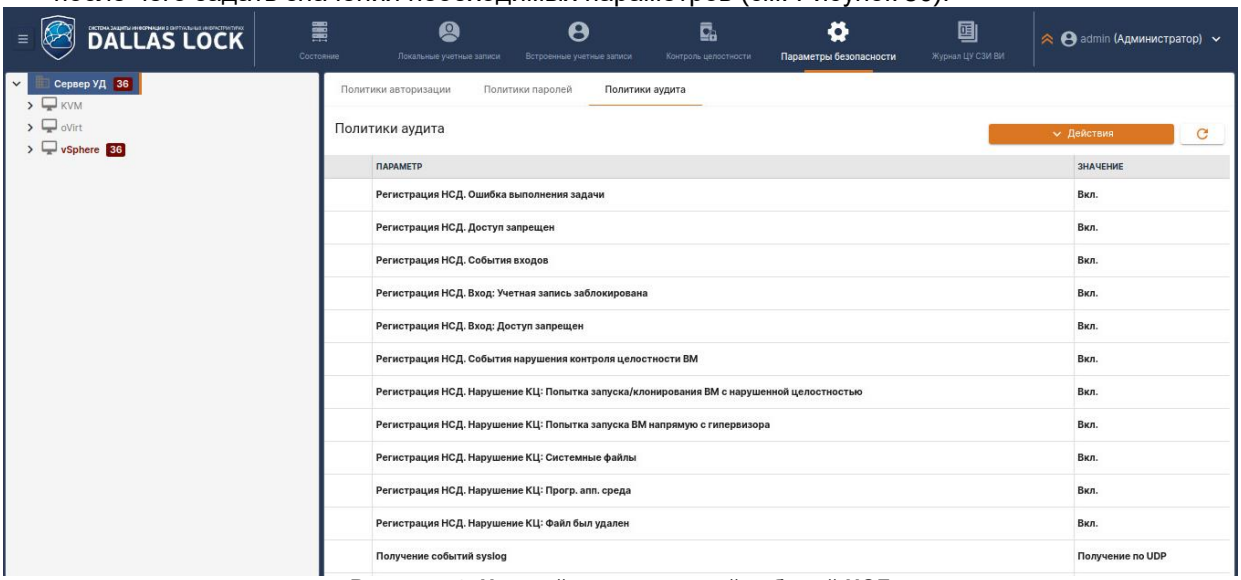

Рисунок 50. Настройка уведомлений событий НСД

2. После установки параметров нажать кнопку *Действия* и выбрать **Сохранить**.
3. Затем нажать кнопку *Действия* и выбрать **Обновить**.

Сигнализация при нарушении целостности происходит при ее проверке. Частота периодической проверки КЦ системных файлов гипервизора редактируется только для всех гипервизоров (см. п. 3.3.2 «Основные параметры группы СВ vSphere»). Частота периодической проверки КЦ для ВМ редактируется при настройке КЦ для ВМ (см. п. 6.2 «Настройка контроля целостности ВМ»).

При многократной проверке объекта ВИ с нарушенной целостностью сигнализация происходит только при первом обнаружении нарушения. Повторная сигнализация о том же нарушении не произойдет!

Просмотр событий сигнализации доступен для групп ВИ:

1. Для просмотра событий сигнализации на сервере виртуализации необходимо в дереве агентов на уровне клиента открыть категорию **Журнал СВ**.
2. Для просмотра событий сигнализации на клиентах **ВИ** необходимо в дереве на уровне группы oVirt/KVM/vSphere открыть категорию **Состояние** → **События НСД** (см. Рисунок 51).

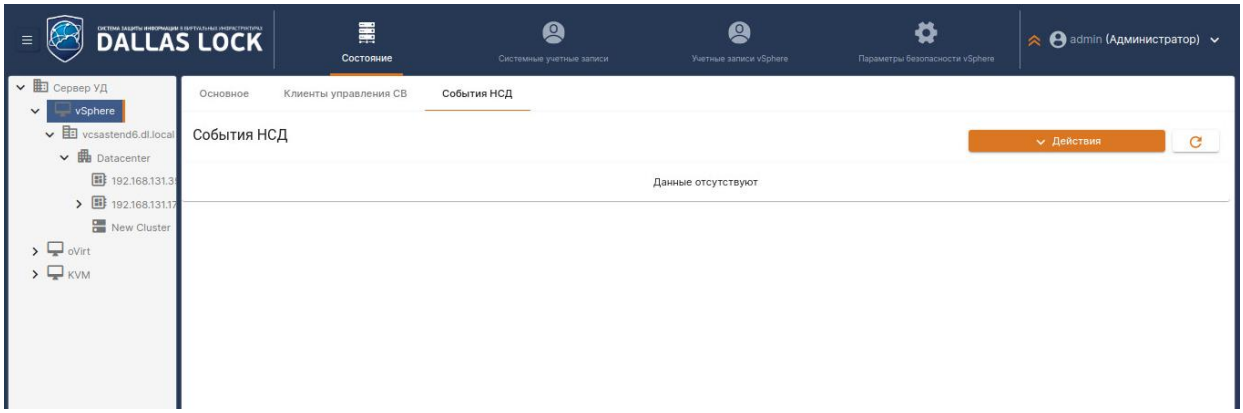

Рисунок 51. Журнал событий сигнализации об НСД на примере vSphere

С помощью панели действий и контекстного меню для списка событий НСД возможно отметить все записи прочитанными или непрочитанными, обновить и очистить список, загрузить сообщения о событиях НСД из текущего журнала. Двойной клик по событию откроет запись в отдельном окне, в списке данное событие будет помечено как прочитанное.

3.7 Наследование настроек

Дочерние объекты **ВИ** могут наследовать установленные настройки от родительской или принимать индивидуальные значения следующим образом:

1. Параметры, для которых отмечено наследование, примут значения, установленные для родительского объекта ВИ в дереве агентов ВИ. В этом случае параметры будут отображаться серым цветом.
2. Параметры, для которых выбраны и установлены оригинальные настройки, будут отображаться черным цветом.

Для того чтобы установить наследование настроек требуется:

1. Чтобы параметры дочернего объекта наследовали значения, установленные для родительского объекта ВИ, необходимо открыть вкладку *Параметры безопасности*, затем выбрать нужный раздел политик безопасности и нажать *Действия*, после чего выбрать **Наследовать всё**.

4 ПОДСИСТЕМА УПРАВЛЕНИЯ ПОЛЬЗОВАТЕЛЯМИ

4.1 Управление учетными записями

В **СЗИ ВИ** возможна регистрация пользователей следующих видов:

1. Пользователь, созданный средствами ОС на СВ.
2. Пользователь, созданный средствами СЗИ ВИ на СВ.
3. Пользователей, созданных средствами службы Active Directory (если компьютер находится под управлением Контроллера домена) для vSphere.
4. Пользователь домена vSphere (например, vsphere.local, VSPHERE.COMMON).
5. Пользователь гипервизора.

4.1.1 Полномочия на управление учетными записями

Регистрировать и удалять пользователей, а также просматривать и редактировать учетные записи может только пользователь, наделенный соответствующими полномочиями по администрированию.

Полномочиями для создания, удаления и изменения учетных записей пользователей в системе защиты обладают: суперадминистратор и пользователи, указанные в списке разрешенных параметра **Встроенные учётные записи** (подробнее см. п. 3.4 «Встроенные учетные записи Сервера УД»).

4.1.2 Управление учетными записями домена

Управление учетными записями клиентов осуществляется в разделе *Доступ к авторизации*.

4.1.2.1 Создание локальных учетных записей на ТС с СЗИ ВИ

Перед созданием новой учетной записи необходимо убедиться в том, что нужная учетная запись еще не создана в операционной системе. В таком случае, достаточно будет ее просто зарегистрировать, выбрав из списка, вызываемого кнопкой поиска.

Для создания нового пользователя в системе защиты необходимо:

1. Выбрать уровень Сервера УД и открыть вкладку **Локальные учетные записи → категория Доступ к авторизации** (см. Рисунок 52).

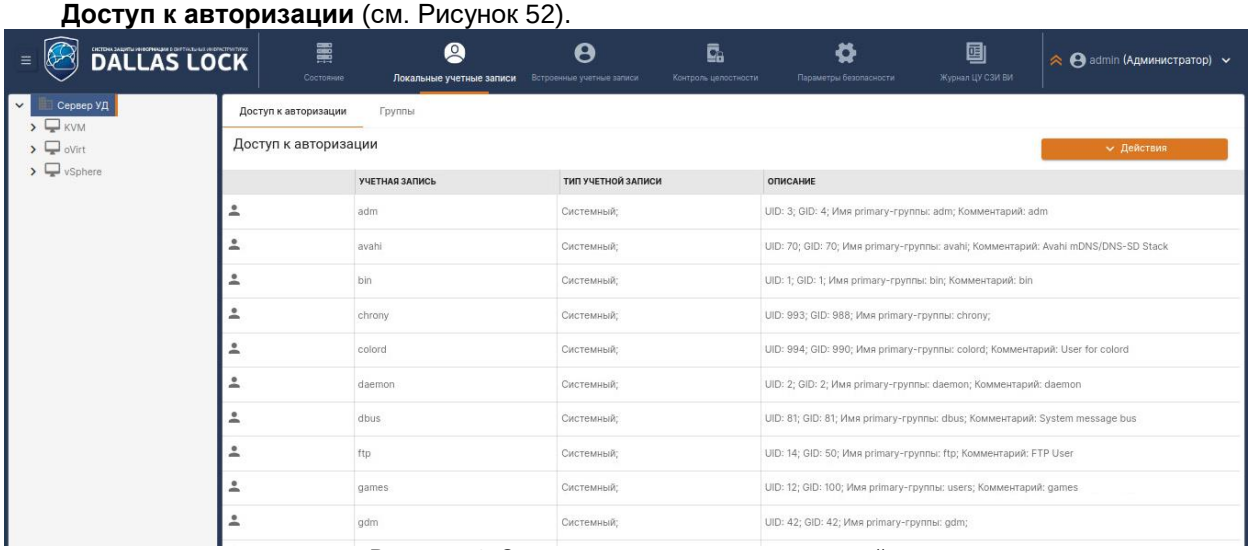

Рисунок 52. Список локальных учетных записей

2. Выбрать блок *Действия* и нажать кнопку **Создать**.
3. В появившемся окне ввести имя учетной записи (см. Рисунок 53).
   - Заполнить *Полное имя* пользователя.
   - В поле *Описание* ввести любой комментарий. Длина комментария не более 256 символов.
   - Вводить комментарий и полное имя не обязательно.
   - Отметки *Не синхронизируемый* и *Системный* задаются при необходимости.
   - Флаг в поле *Не синхронизируемый пользователь* устанавливает статус, при котором данная учетная запись не синхронизируется с **ЦУ СЗИ ВИ** (см. п. 3.5 «Синхронизация»).

   При вводе имени присутствуют ограничения той системы, в которой оно создаётся.

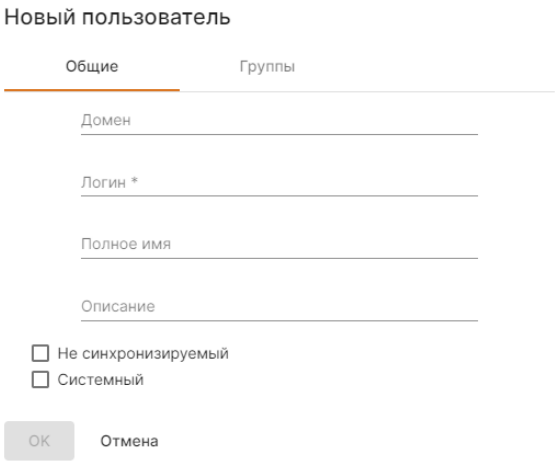

Рисунок 53. Окно создания локальной учетной записи

4. Далее, в процессе создания или регистрации нового локального пользователя администратор имеет возможность включить его в определенную группу. В окне закладки *Группы* отображены названия групп, в которые включен пользователь (см. Рисунок 54). По умолчанию, каждый новый пользователь входит в группу *Пользовательская*.

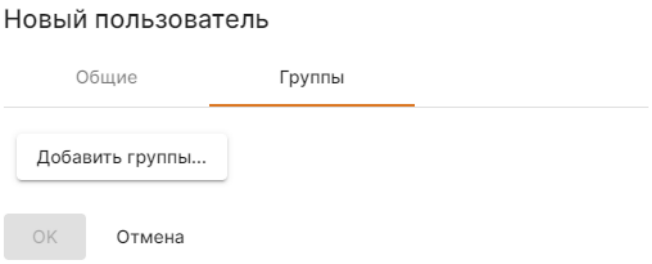

Рисунок 54. Окно добавление групп для локальной учетной записи

5. В появившемся окне нажать **Добавить группы**.
6. Чтобы включить пользователя в определенную группу необходимо выбрать его в разделе *Доступ к авторизации* и нажать левой кнопкой мыши. После чего из выпадающего списка выбрать *Свойства*, перейти в графу *Группы* и выбрать **Изменить группы**. Появится список всех групп пользователей, имеющихся в системе, (см. Рисунок 55). Необходимо отметить нужные группы и нажать **ОК**.

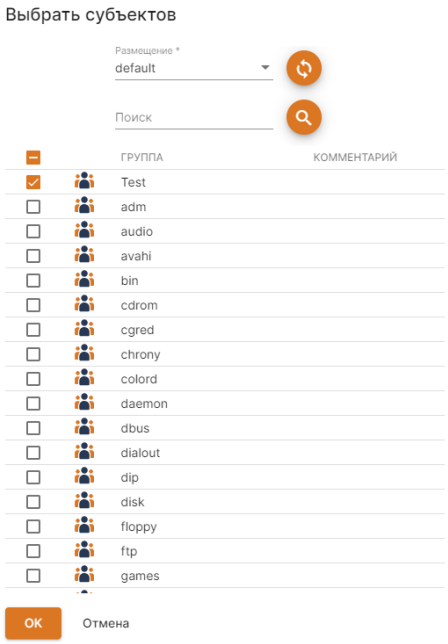

Рисунок 55. Окно выбора групп для учетной записи

7. В поле *Размещение* необходимо оставить значение *Локальный*.

Кнопка поиска в данном окне помогает найти необходимые группы по названию или его части.

Завершающей операцией по созданию учетной записи пользователя является назначение пароля. Назначение пароля предлагается системой защиты после заполнения всех необходимых параметров в окне создания локальной учетной записи и нажатия кнопки **ОК** (см. Рисунок 56).

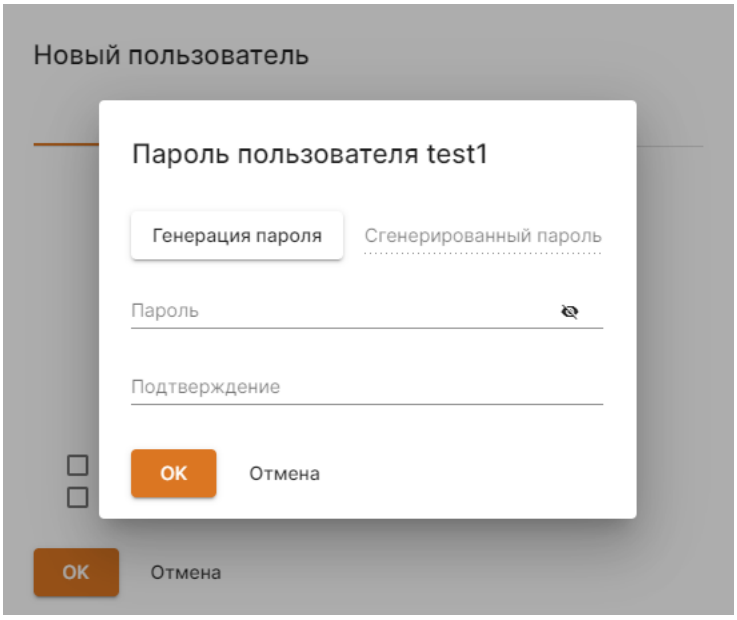

Рисунок 56. Окно генерации пароля для локальной учетной записи

При вводе пароля необходимо руководствоваться следующими правилами:

- пароль может содержать латинские символы, символы кириллицы, цифры и специальные символы (список допустимых символов см. в описании политики безопасности **Пароли: необходимо наличие спец. символов** в п. 4.4.1 «Настройка параметров »);
- сложность пароля (наличие определенных символов, длина, срок действия и прочие) регулируется специальными политиками безопасности, которые устанавливаются администратором (см. п. 4.4.1 «Настройка параметров »).

Для создания пароля, отвечающего всем установленным требованиям политик безопасности, можно воспользоваться помощью генератора паролей системы защиты. Для этого нажать кнопку с надписью **Генерация пароля**. Система автоматически создаст случайный пароль, удовлетворяющий политикам сложности пароля, значение которого автоматически вводится в поля *Пароль* и *Подтверждение*.

Дополнительная кнопка изменит явные символы на скрытые. Подтверждение пароля в этом случае не потребуется и соответствующее поле будет скрыто.

Если в **СЗИ ВИ** регистрируется пользователь, учетная запись которого уже имеется на локальном компьютере, то его пароль для входа в ОС автоматически становится паролем для входа в систему защиты, поэтому операция по назначению пароля не предлагается. При необходимости пароль можно изменить средствами **СЗИ ВИ**.

Для использования созданной учетной записи требуется ее активация (подробнее см. п. 4.1.4 «Активация и деактивация учетных записей»).

Изменения вступят в силу при следующей синхронизации (подробнее п. 3.5 «Синхронизация»).

Создание учетных записей путем копирования

При создании учетной записи пользователя, которая имеет одинаковые свойства с другой учетной записью, можно воспользоваться функцией копирования. Для этого необходимо выбрать учетную запись в списке и нажать левой кнопкой мыши на неё, после чего выбрать **Копировать** из выпадающего списка (см. Рисунок 57). Данные действия доступны на уровне сервера УД, на уровне группы клиентов и на уровне клиента.

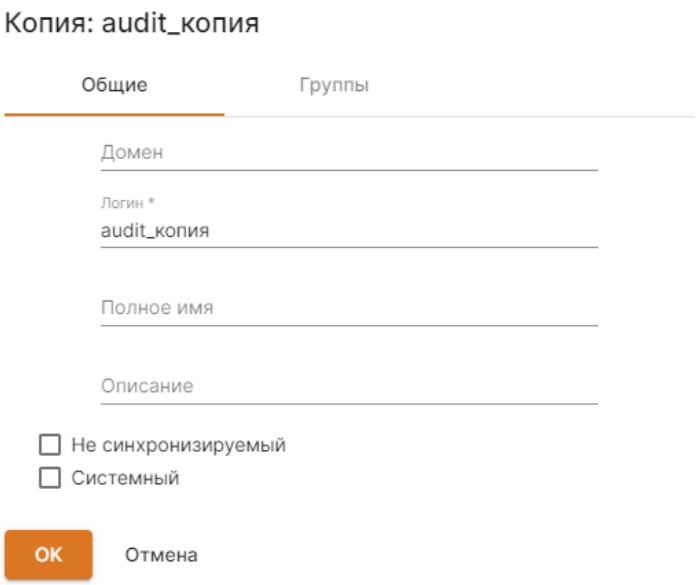

Рисунок 57. Копирование учетной записи

В появившемся окне ввести имя учетной записи. Далее, в разделе *Группы* для создаваемой учетной записи будут установлены свойства и список групп с копируемой учетной записи, их можно отредактировать. Далее необходимо задать пароль.

Для использования созданной учетной записи требуется ее активация (подробнее см. п. 4.1.4 «Активация и деактивация учетных записей»).

Изменения вступят в силу при следующей синхронизации (подробнее см. п. 3.5 «Синхронизация»).

Редактирование учетных записей

Для редактирования необходимо выбрать учетную запись из списка и кликом левой кнопки мыши вызвать выпадающий список, после чего выбрать пункт *Свойства*. Дальнейшие действия полностью идентичны действиям, описанным в п. 4.1.2.1 «Создание локальных учетных записей» начиная с п. 5. Изменения вступят в силу при следующей синхронизации (подробнее см. п. 3.5 «Синхронизация»).

4.1.3 Управление учетными записями ВИ

Управление учетными записями ВИ осуществляется в дереве агентов.

4.1.3.1 Создание учетных записей vSphere

Для того чтобы создать учетную запись серверов виртуализации необходимо:

1. Выбрать уровень группы vSphere и открыть категорию **Учетные записи vSphere** → **Учетные записи vSphere** (см. Рисунок 58).

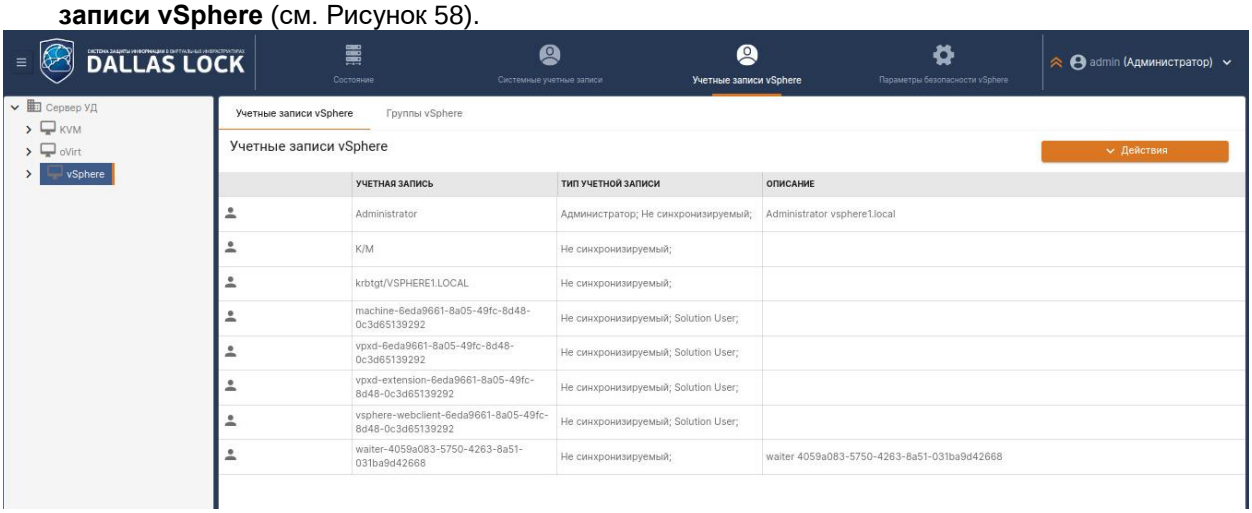

Рисунок 58. Список учетных записей vSphere

2. В категории «Действия» нажать кнопку **Создать…**.
3. В появившемся окне имя учетной записи и заполнить остальные поля при необходимости, после чего нажать кнопку **ОК** (см. Рисунок 59).

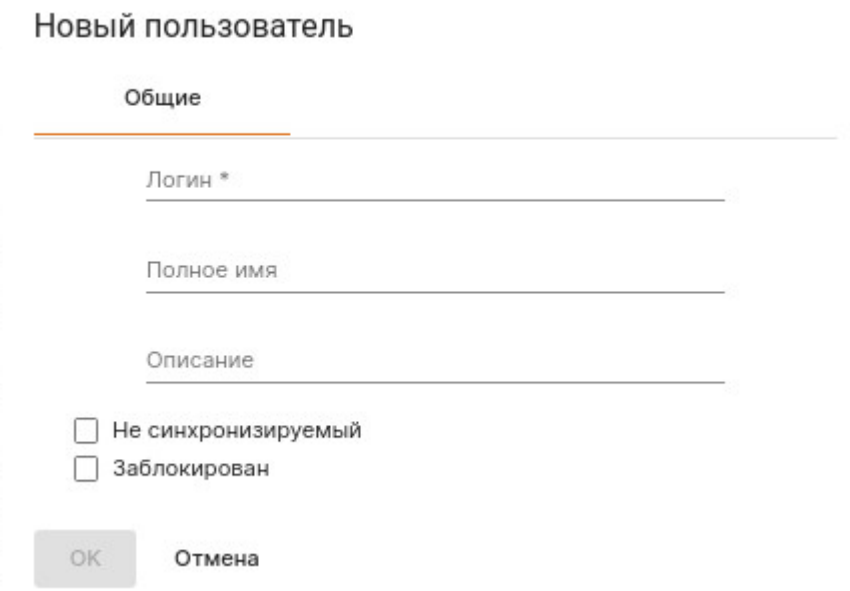

Рисунок 59. Создание учетной записи СВ vSphere

При вводе имени в системе существуют следующие правила:

- максимальная длина имени – 300 символов;
- имя может содержать латинские символы, символы кириллицы, цифры и специальные символы (кроме запрещенных: « / \ [ ] : | < > + = ; , ? @ * #);
- 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).

4. В появившемся окне выбрать расположение и назначить пароль, который соответствует заданным парольным политикам, после чего нажать **ОК** (см. Рисунок 60).

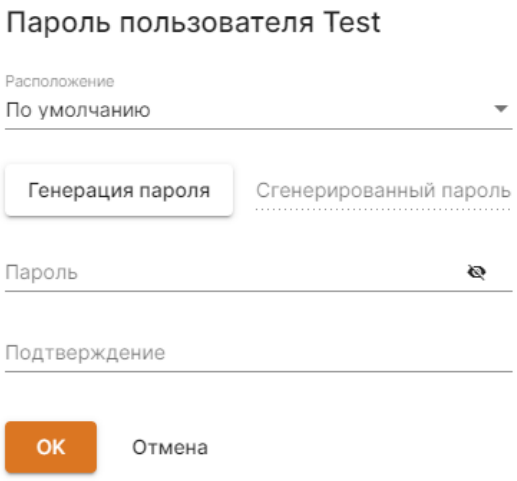

Рисунок 60. Окно генерации пароля

При вводе пароля необходимо руководствоваться следующими правилами:

- требования к сложности пароля определяются политиками безопасности, политики паролей;
- пароль может содержать латинские заглавные и строчные символы, цифры, спецсимволы, символы кириллицы, цифры и специальные символы (список допустимых символов см. в описании политики безопасности **[Сервер виртуализации] Пароли: минимальное количество специальных символов** в п. 4.3.1.1 «Параметры входа для vSphere»);
- сложность пароля (наличие определенных символов, длина, срок действия и прочие) регулируется специальными политиками безопасности, которые устанавливаются администратором (см. п. 4.3.1.1 «Параметры входа для vSphere»).

Для создания пароля, отвечающего всем установленным требованиям политик безопасности, можно воспользоваться помощью генератора паролей системы защиты. Для этого нажать кнопку **Генерация пароля**. Система автоматически создаст случайный пароль, удовлетворяющий

парольным политикам сложности пароля выбранного объекта дерева **ВИ**, значение которого необходимо ввести в поля *Пароль* и «*Подтверждение*.

Дополнительная кнопка изменит скрытые символы на явные. Подтверждение пароля в этом случае не потребуется и соответствующее поле будет скрыто.

Изменения вступят в силу при следующей синхронизации (подробнее см. п. 3.5 «Синхронизация»).

Далее следует активировать учетную запись на уровне соответствующих СВ (подробнее см. п. 4.1.4 «Активация и деактивация учетных записей»).

4.1.3.2 Создание учетных записей гипервизора ESXi

Для того чтобы создать учетную запись гипервизора необходимо:

1. Выбрать уровень *vSphere* и открыть категорию **Системные учетные записи → Учетные записи ESXi** (см. Рисунок 61).

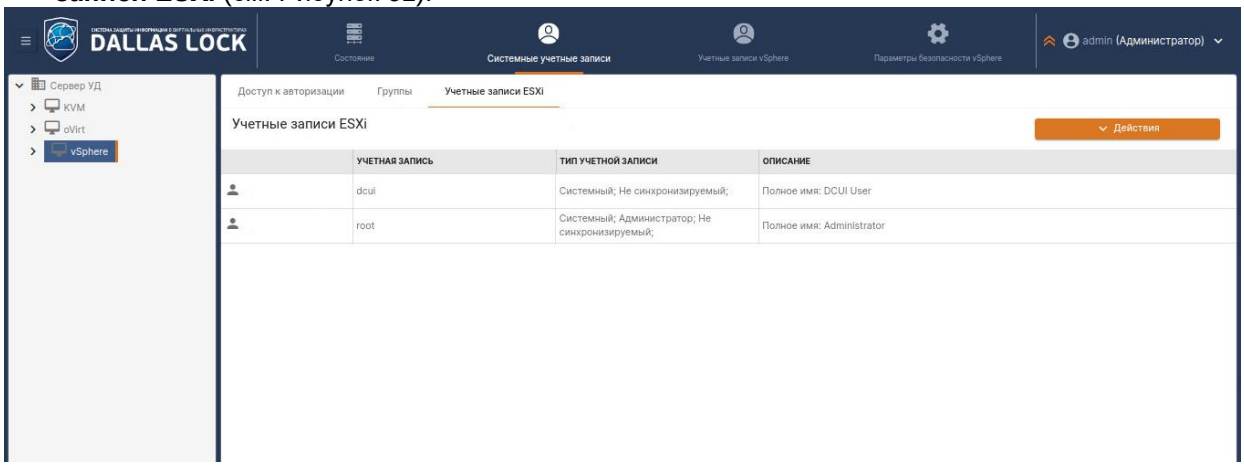

Рисунок 61. Список учетных записей гипервизора

2. В категории *Действия* нажать кнопку **Создать…**.
3. В появившемся окне имя учетной записи и заполнить остальные поля при необходимости, после чего нажать кнопку **ОК** (см. Рисунок 62).

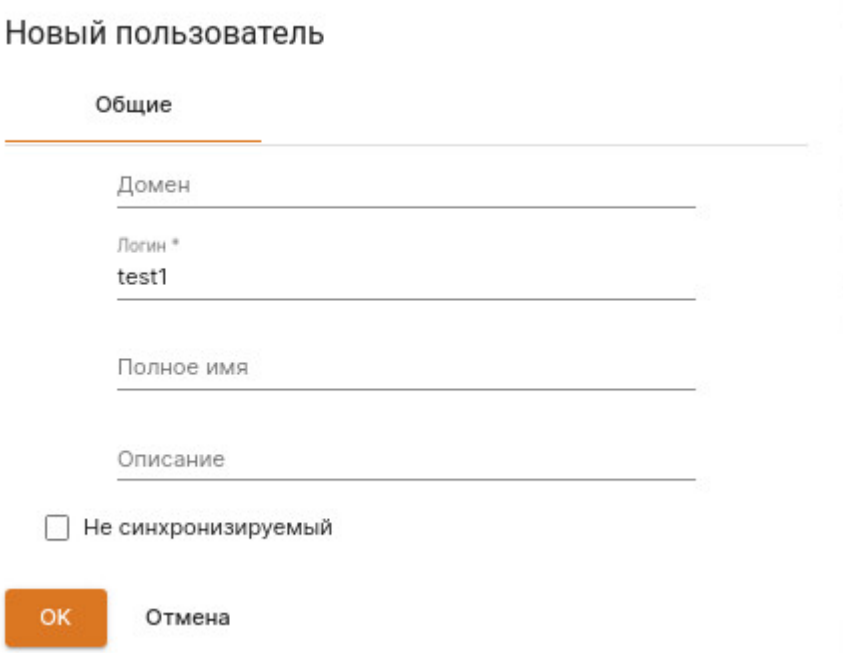

Рисунок 62. Создание пользователя гипервизора ESXi

При вводе имени в системе существуют следующие правила:

- максимальная длина имени – 300 символов;
- имя может содержать латинские символы, символы кириллицы, цифры и специальные символы (кроме запрещенных: « / \ [ ] : | < > + = ; , ? @ * #);
- 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).

4. В появившемся окне выбрать сервер, где будет располагаться учётная запись и назначить пароль, который соответствует заданным парольным политикам, после чего нажать **ОК** (см. Рисунок 63).

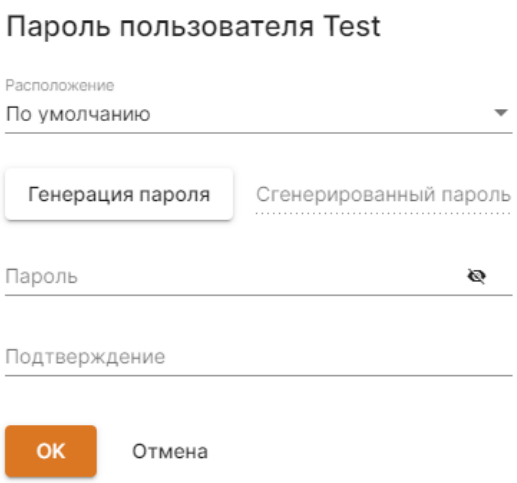

Рисунок 63. Форма ввода пароля

При вводе пароля необходимо руководствоваться следующими правилами:

- пароль может содержать латинские символы, символы кириллицы, цифры и специальные символы (список допустимых символов см. в описании политики безопасности **[Сервер виртуализации] Минимальное количество специальных символов** в п. 4.3.1.1 «Параметры входа для vSphere»);
- сложность пароля (наличие определенных символов, длина, срок действия и прочие) регулируется специальными политиками безопасности, которые устанавливаются администратором (см. п. 4.3.1.1 «Параметры входа для vSphere»).

Для создания пароля, отвечающего всем установленным требованиям политик безопасности, можно воспользоваться помощью генератора паролей системы защиты. Для этого нажать кнопку **Генерация пароля**. Система автоматически создаст случайный пароль, удовлетворяющий парольным политикам сложности пароля выбранного объекта дерева ВИ, значение которого необходимо ввести в поля *Пароль* и *Подтверждение*.

Дополнительная кнопка изменит скрытые символы на явные. Подтверждение пароля в этом случае не потребуется и соответствующее поле будет скрыто.

Изменения вступят в силу при следующей синхронизации (подробнее см. п. 3.5 «Синхронизация»).

4.1.3.3 Создание учетных записей гипервизора KVM

Для того чтобы создать учетную запись гипервизора необходимо:

1. Выбрать уровень гипервизора *KVM* и открыть вкладку **Системные учетные записи → Доступ к авторизации** (см. Рисунок 64).

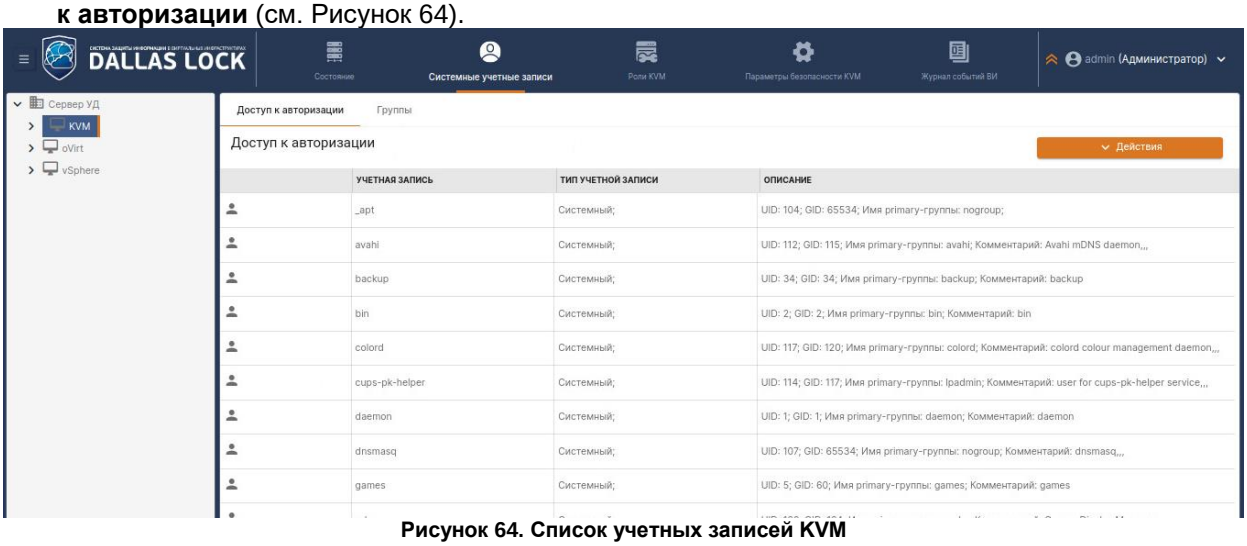

Рисунок 64. Список учетных записей KVM

2. Нажать кнопку **Создать…** на панели действия.
3. В появившемся окне ввести имя учетной записи, после чего нажать кнопку **ОК** (см. Рисунок 65).

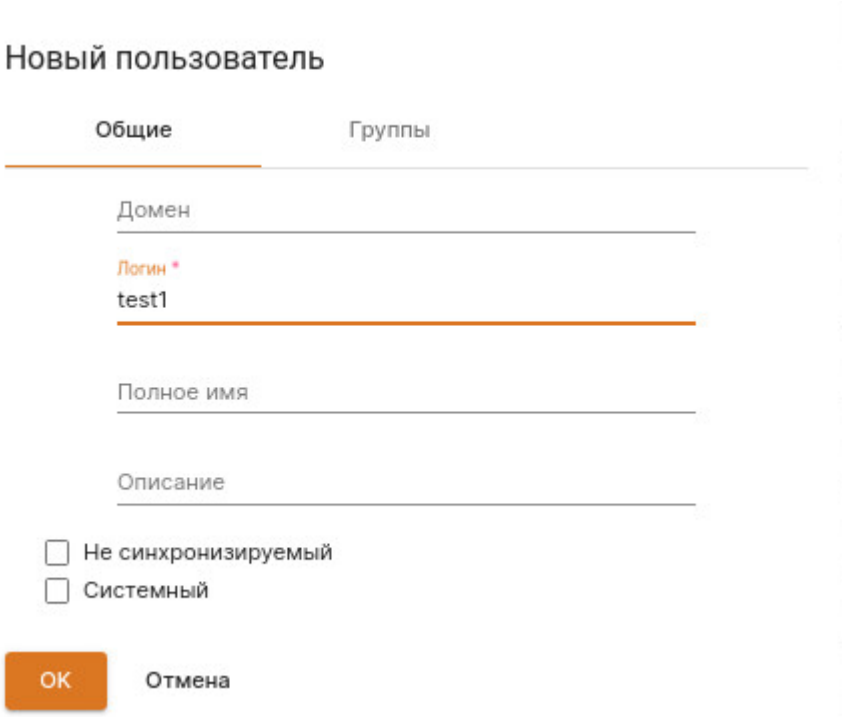

Рисунок 65. Создание пользователя гипервизора KVM

4. Далее следует назначить пароль (см. Рисунок 66).

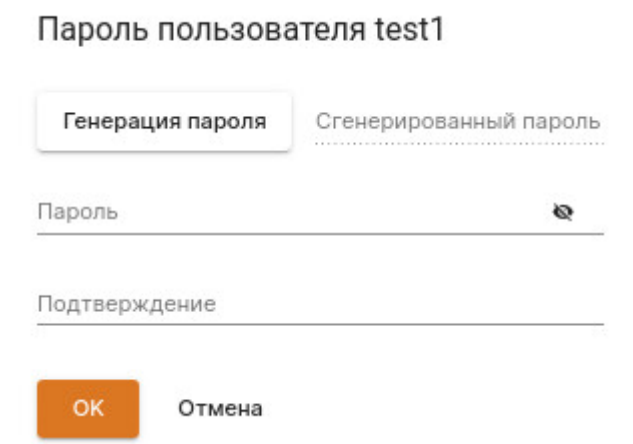

Рисунок 66. Форма ввода пароля

Для создания пароля, отвечающего всем установленным требованиям политик безопасности, можно воспользоваться помощью генератора паролей системы защиты. Для этого нажать кнопку **Генерация пароля**. Система автоматически создаст случайный пароль, удовлетворяющий политикам сложности пароля, значение которого необходимо ввести в поля *Пароль* и *Подтверждение*.

Дополнительная кнопка 👁 изменит скрытые символы на явные. Подтверждение пароля в этом случае не потребуется и соответствующее поле будет скрыто.

5. Далее необходимо нажать кнопку **Сохранить**.
6. Для использования созданной учетной записи требуется ее активация (подробнее см. п. 4.1.4 «Активация и деактивация учетных записей»).
7. Изменения вступят в силу при следующей синхронизации (подробнее см. п. 3.5 «Синхронизация»).

Для предоставления доступа новому пользователю к управлению ВМ необходимо добавить данного пользователя в следующие группы:

1. Для ОС Linux Mint – libvirt.
2. Для ОС Ubuntu – libvirt, kvm.
3. Для ОС Astra Linux (Орел 1.7) – kvm, libvirt, libvirt-qemu.
4. Для ОС Astra Linux (Смоленск 1.7) – kvm, libvirt, libvirt-qemu, libvirt-admin.
5. Для ОС CentOS – libvirt, kvm.

4.1.3.4 Создание учетных записей oVirt/zVirt/HOSTVM/RedVirt

Для того чтобы создать учетную запись сервера виртуализации необходимо:

1. Выбрать уровень группы oVirt в дереве объектов ВИ и открыть категорию **Учетные записи oVirt** → **Учетные записи oVirt** (см. Рисунок 67).

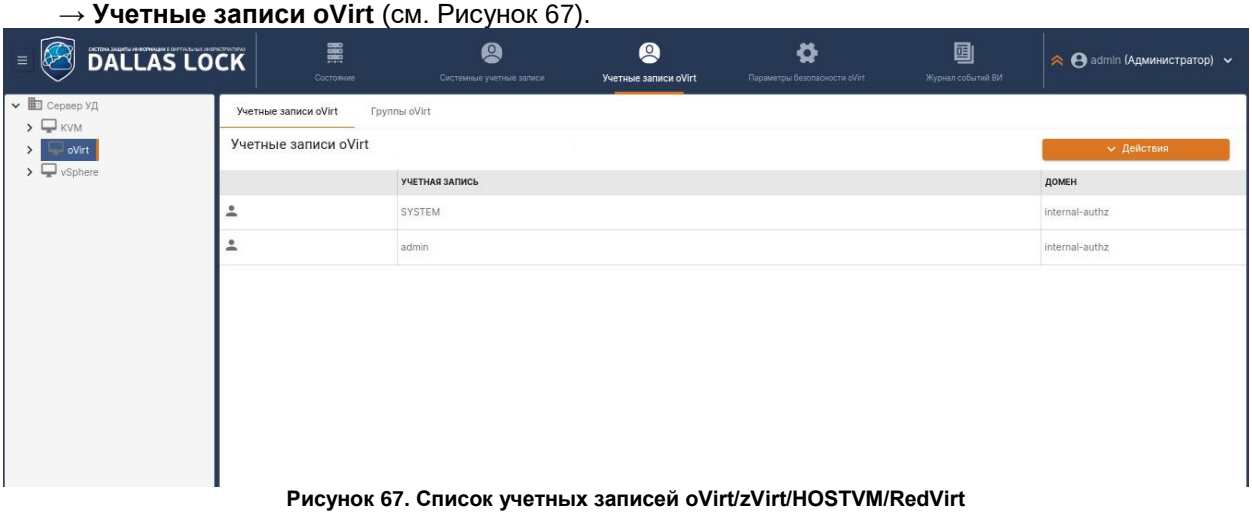

Рисунок 67. Список учетных записей oVirt/zVirt/HOSTVM/RedVirt

2. В категории *Действия* нажать кнопку **Создать**.
3. В появившемся окне имя учетной записи и заполнить остальные поля при необходимости, после чего нажать кнопку «**ОК**» (см. Рисунок 68).

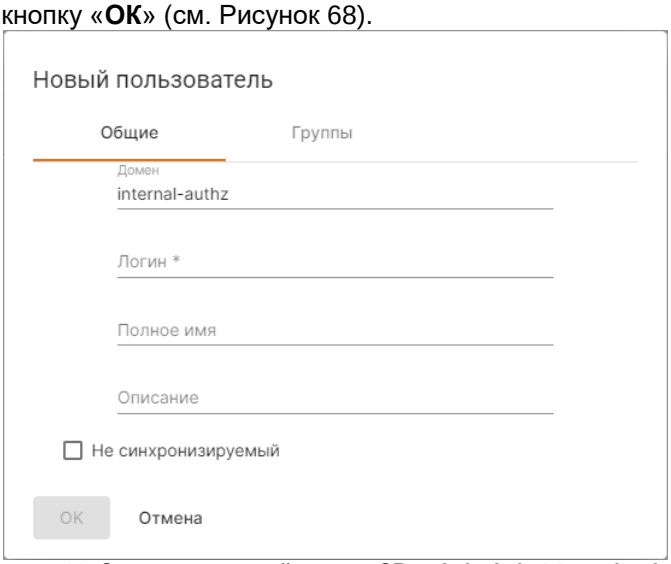

Рисунок 68. Создание учетной записи СВ oVirt/zVirt/HOSTVM/RedVirt

4. Далее следует назначить пароль (см. Рисунок 69):

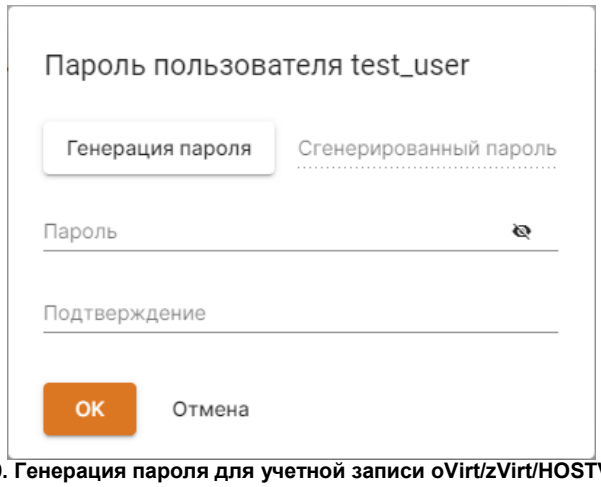

Рисунок 69. Генерация пароля для учетной записи oVirt/zVirt/HOSTVM/RedVirt

Для создания пароля, отвечающего всем установленным требованиям политик безопасности, можно воспользоваться помощью генератора паролей системы защиты. Для этого нажать кнопку **Генерация пароля**. Система автоматически создаст случайный пароль, удовлетворяющий политикам сложности пароля, значение которого необходимо ввести в поля *Пароль* и *Подтверждение*.

Дополнительная кнопка изменит скрытые символы на явные. Подтверждение пароля в этом случае не потребуется и соответствующее поле будет скрыто.

5. Для использования созданной учетной записи требуется ее активация (подробнее см. п. 4.1.4 «Активация и деактивация учетных записей»).
6. Изменения вступят в силу при следующей синхронизации (подробнее см. п. 3.5 «Синхронизация»).

4.1.3.5 Создание системных учетных записей oVirt/zVirt/HOSTVM/RedVirt

Для того чтобы создать системную учетную запись СВ или гипервизора необходимо:

1. Выбрать уровень СВ или гипервизора oVirt/zVirt/HOSTVM/RedVirt и открыть вкладку **Системные учетные записи** → **Доступ к авторизации** (см. Рисунок 70).

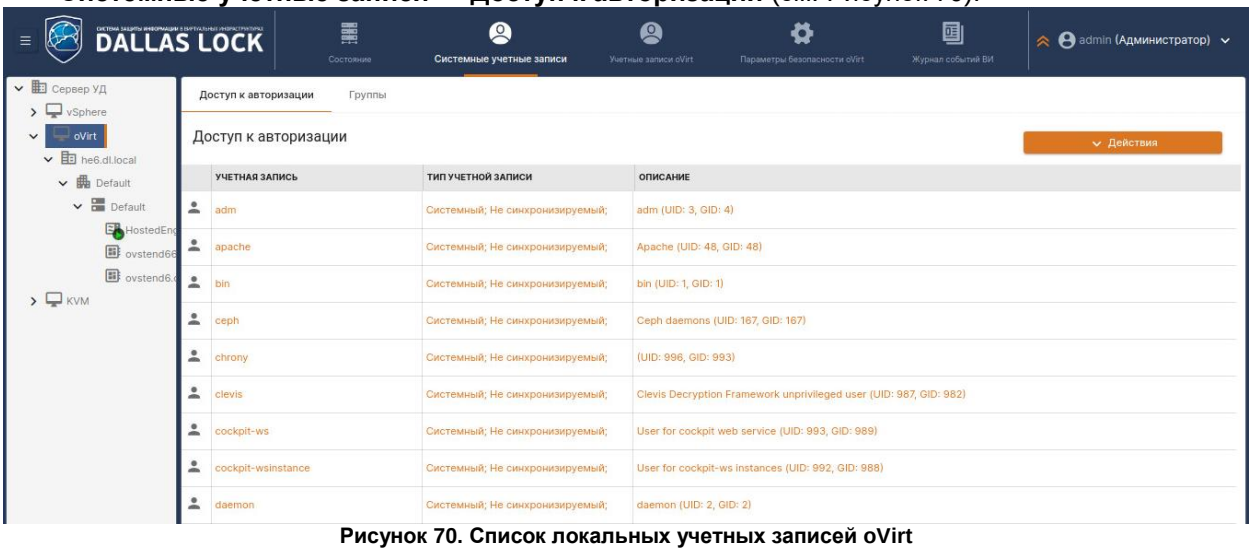

Рисунок 70. Список локальных учетных записей oVirt

2. Нажать кнопку **Создать…** на панели действия.
3. В появившемся окне ввести имя учетной записи, и заполнить остальные поля при необходимости, после чего нажать кнопку **ОК** (см. Рисунок 71).

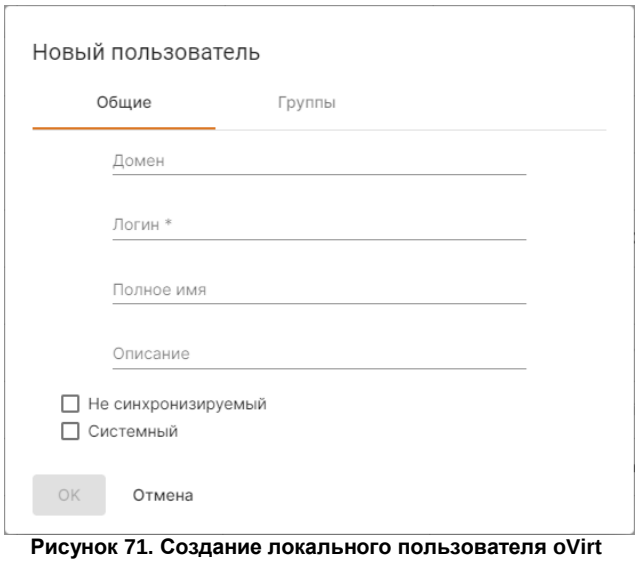

Рисунок 71. Создание локального пользователя oVirt

4. Далее следует назначить пароль (см. Рисунок 72):

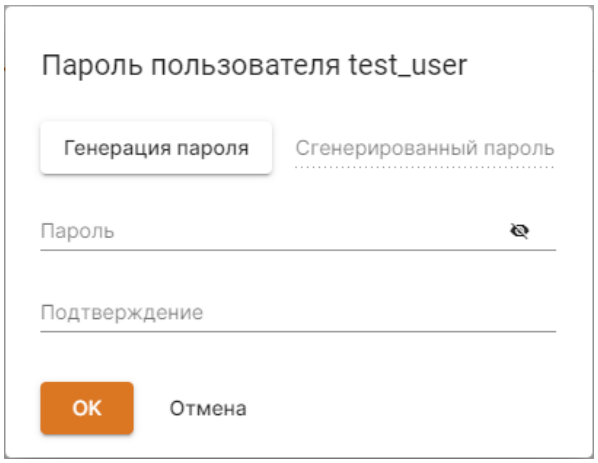

Рисунок 72. Форма ввода пароля

Для создания пароля, отвечающего всем установленным требованиям политик безопасности, можно воспользоваться помощью генератора паролей системы защиты. Для этого нажать кнопку **Генерация пароля**. Система автоматически создаст случайный пароль, удовлетворяющий политикам сложности пароля, значение которого необходимо ввести в поля *Пароль* и *Подтверждение*.

Дополнительная кнопка изменит скрытые символы на явные. Подтверждение пароля в этом случае не потребуется и соответствующее поле будет скрыто.

5. Для использования созданной учетной записи требуется ее активация (подробнее см. п. 4.1.4 «Активация и деактивация учетных записей»).

6. Изменения вступят в силу при следующей синхронизации (подробнее см. п. 3.5 «Синхронизация»).

4.1.4 Активация и деактивация учетных записей

Включение учетных записей необходимо для формирования списка учетных записей на клиентах.

Блокирование учетной записи необходимо для временной приостановки использования учетной записи без ее удаления.

Чтобы включить или заблокировать учетную запись необходимо выделить её, нажать *Действие* и выбрать **Свойства**. Поставить флаг напротив соответствующей записи. Затем необходимо нажать кнопку **ОК**. Учетная запись будет активирована или деактивирована при следующей синхронизации (подробнее см. п. 3.5 «Синхронизация»).

- — отмеченное флагом поле означает, что данная учетная запись активна имеет доступ к выбранному объекту;
- — пустое поле означает, что учетная запись отключена для работы на выбранном объекте.

4.1.4.1 Активация и деактивация учетных записей vSphere

Активация и деактивация учетных записей vSphere происходит в дереве агентов на уровне СВ во вкладке **Учетные записи vSphere → Учетные записи vSphere**. Выберите из списка нужную учетную запись и слева в первом столбце укажите/снимите флаг (галочку).

4.1.4.2 Активация и деактивация учетных записей vCSA

1. Активация и деактивация учетных записей vSphere/vCSA происходит в дереве на уровне СВ во вкладке **Учетные записи → Учетные записи vSphere**.
   1.1. Активация и деактивация учетных записей локальной ОС vSphere/vCSA для доступа к авторизации в ОС СВ vSphere/vCSA локально или через SSH происходит в дереве на уровне СВ во вкладке **Системные учетные записи → Доступ к авторизации**.
      1.1.1. Для включения или отключения доступа к авторизации в SSO (Single Sign-On), а значит возможности работы через web-клиент и PowerCli, локальных учетных записей ОС vCSA нужно настроить членство в соответствующих группах vsphere.local[9] vCSA. Это происходит в дереве на уровне СВ во вкладке **Учетные записи → Группы**.
   1.2. Активация и деактивация учетных записей vCSA домена vsphere.local[9] для доступа к авторизации в SSO (Single Sign-On) (web-клиент или PowerCli) происходит в дереве на уровне СВ во вкладке **Учетные записи → Учетные записи vSphere**.
      1.2.1. Для включения или отключения доступа к авторизации в SSO (Single Sign-On), а значит возможности работы через web-клиент и PowerCli, учетных записей домена vsphere.local[9] vCSA нужно настроить членство в соответствующих группах vsphere.local[9] vCSA. Это происходит в дереве на уровне СВ во вкладке **Учетные записи → Группы vSphere vCSA.**

4.1.4.3 Активация и деактивация учетных записей гипервизора ESXi

Активация и деактивация учетных записей гипервизора происходит в дереве агентов на уровне гипервизора во вкладке **Системные учетные записи → Учетные записи ESXi**.

4.1.4.4 Активация и деактивация учетных записей гипервизора KVM

Активация и деактивация учетных записей гипервизора происходит в дереве на уровне гипервизора во вкладке **Системные учетные записи → Доступ к авторизации**.

4.1.4.5 Активация и деактивация учетных записей СВ oVirt/zVirt/HOSTVM/RedVirt

Активация и деактивация учетных записей происходит в дереве объектов ВИ на уровне СВ во вкладке **Учетные записи oVirt/zVirt/HOSTVM/RedVirt → Учетные записи oVirt**.

4.1.4.6 Активация и деактивация локальных учетных записей гипервизора/СВ oVirt/zVirt/HOSTVM/RedVirt

Активация и деактивация учетных записей гипервизора происходит в дереве объектов ВИ на уровне гипервизора/СВ во вкладке **Системные учетные записи → Доступ к авторизации**.

4.1.5 Разблокирование и заблокированные пользователи

4.1.5.1 Блокирование учетных записей СВ vCSA/vSphere

Учетная запись пользователя по разным причинам может быть заблокирована, например, вследствие неправильного ввода пароля несколько раз.

4.1.5.2 Разблокирование учетных записей СВ vCSA/vSphere

Нет возможности разблокировать учетную запись на уровне СВ vSphere/vCSA.

4.1.5.3 Разблокирование учетных записей гипервизора ESXi

Нет возможности разблокировать учетную запись на уровне гипервизора ESXi.

4.1.5.4 Разблокирование учетных записей гипервизора KVM

Для того, чтобы разблокировать учетную запись с правами доступа к авторизации на гипервизоре необходимо:

1. Выбрать уровень гипервизора и открыть вкладку *Системные учетные записи*.
2. Выбрать категорию **Доступ к авторизации**.
3. Нажать кнопку **Разблокировать всех**.

[9] Имя домена *vsphere.local* приводится в качестве примера, имя домена задается на этапе установки сервера виртуализации и может отличаться от указанного в руководстве.

4. Нажать кнопку **Сохранить**.
5. Изменения вступят в силу при следующей синхронизации (подробнее см. п. 3.5 «Синхронизация»).

4.1.5.5 Разблокирование учетных записей СВ oVirt/zVirt/HOSTVM/RedVirt

Для того, чтобы разблокировать учетную запись СВ вследствие превышения числа попыток ввода пароля при авторизации через web-клиент необходимо:

1. Выбрать уровень СВ и открыть вкладку *Учетные записи oVirt/zVirt/HOSTVM/RedVirt*.
2. Выбрать категорию **Учетные записи oVirt**.
3. В блоке *Управление* выбрать пункт *Разблокировать всех*.
4. Нажать кнопку **Сохранить**.
5. Изменения вступят в силу при следующей синхронизации (подробнее см. п. 3.5 «Синхронизация»).

4.1.5.6 Разблокирование локальных учетных записей гипервизора oVirt/zVirt/HOSTVM/RedVirt

Для того, чтобы разблокировать учетную запись с правами доступа к авторизации на гипервизоре необходимо:

1. Выбрать уровень гипервизора и открыть вкладку *Системные учетные записи*.
2. Выбрать категорию *Доступ к авторизации*.
3. В блоке *Управление* выбрать пункт *Разблокировать всех*.
4. Нажать кнопку **Сохранить**.
5. Изменения вступят в силу при следующей синхронизации (подробнее см. п. 3.5 «Синхронизация»).

4.1.6 Удаление учетных записей

Для удаления учетной записи из **ВИ** вне зависимости от того, какими средствами она создана или зарегистрирована в самой системе защиты, необходимо выделить ее имя в списке главного окна программы, в выпадающем списке нажать кнопку **Удалить**. Подтвердить операцию, после чего синхронизировать, открыв вкладку *Состояние* и нажав кнопку **Действия** выбрать **Синхронизация СВ и гипервизоров**. Учетная запись будет удалена из **ЦУ СЗИ ВИ** и из самого Сервера виртуализации.

Следует отметить, что при удалении самой **СЗИ ВИ**, учетные записи, созданные средствами **ЦУ СЗИ ВИ**, остаются на сервере виртуализации.

4.1.7 Смена пароля

В некоторых ситуациях, например, когда пользователь забыл свой пароль, администратору бывает необходимо задать пользователю новый пароль, не зная старого. Для это необходимо:

1. Открыть одну из категорий для редактирования учетных записей
   - Для vSphere - в дереве агентов на уровне группы **vSphere** → **Учетные записи vSphere**;
   - Для KVM - в дереве на уровне группы или гипервизора **KVM** → **Системные учетные записи**;
   - Для oVirt/zVirt/HOSTVM/RedVirt - в дереве на уровне группы **oVirt/zVirt/HOSTVM/RedVirt** → **Системные учетные записи**.
2. Выделить учетную запись в списке и в выпавшем списке нажать кнопку **Задать пароль**.
3. Далее следует назначить пароль, который соответствует заданным парольным политикам и нажать кнопку **ОК**.

При вводе пароля необходимо руководствоваться следующими правилами:

- пароль может содержать латинские символы, символы кириллицы, цифры и специальные символы (список допустимых символов см. в описании политики безопасности **[Сервер виртуализации] Пароли: минимальное количество специальных символов** в п. 4.3.1.1 «Параметры входа для vSphere»);
- сложность пароля (наличие определенных символов, длина, срок действия и прочие) регулируется специальными политиками безопасности, которые устанавливаются администратором (см. п. 4.3.1.1 «Параметры входа для vSphere»).

Для создания пароля, отвечающего всем установленным требованиям политик безопасности, можно воспользоваться помощью генератора паролей системы защиты. Для этого нажать кнопку **Генерация пароля**. Система автоматически создаст случайный пароль, удовлетворяющий парольным политикам сложности пароля выбранного объекта дерева **ВИ**, значение которого необходимо ввести в поля *Пароль*» и *Подтверждение*.

Дополнительная кнопка изменит скрытые символы на явные. Подтверждение пароля в этом случае не потребуется и соответствующее поле будет скрыто.

Изменения вступят в силу при следующей синхронизации (подробнее см. п. 3.5 «Синхронизация»).

4. Открыть вкладку *Состояние* и нажать кнопку *Действие*, где нужно выбрать кнопку **Синхронизация СВ и гипервизоров**.

При изменении пароля администратора СВ vSphere/ oVirt/zVirt/HOSTVM/RedVirt или гипервизора ESXi/KVM/oVirt/zVirt/HOSTVM/RedVirt штатными средствами, учетные данные которого были установлены при подключении к **СЗИ ВИ**, необходимо выполнить повторную установку учетных данных (см. п. 2.6.1 «Установка учетных данных для vSphere», п. 2.6.2 «Установка и обновление учетных данных для гипервизора KVM», п. 2.6.3 «Установка, обновление и удаление учетных данных для СВ »).

4.2 Управление группами пользователей

Группы предназначены для объединения пользователей со схожими правами безопасности. Такое объединение может упростить работу администратора, при выполнении настроек **СЗИ ВИ**.

Группы упрощают управление Сервером виртуализации. Можно добавлять пользователей к группам и назначать этим группам определенную роль, удалять пользователей из групп в соответствии с потребностями этих пользователей.

4.2.1 Управление группами пользователей Сервера УД

4.2.1.1 Создание групп Сервера УД

Для создания новой группы необходимо:

1. Выбрать уровень *Сервера УД* и открыть категорию **Локальные учетные записи** → **Группы** (см. Рисунок 73).

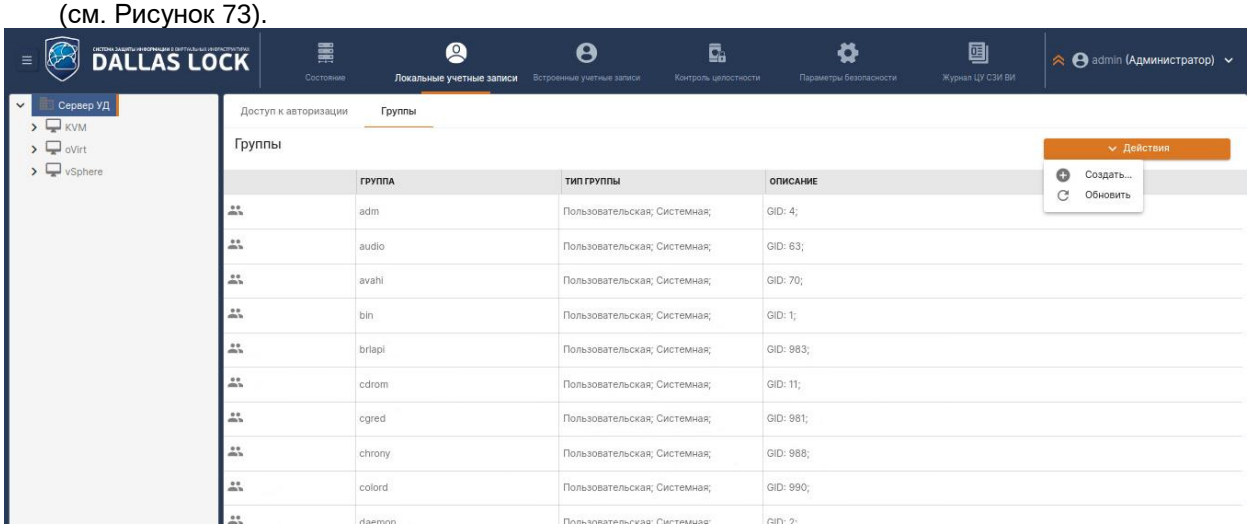

Рисунок 73. Список групп Сервера УД

2. Выбрать блок *Действия* и нажать кнопку **Создать…**.
3. В появившемся окне ввести имя группы и заполнить поля *Домен* и *Описание* при необходимости, после чего нажать кнопку **ОК** (см. Рисунок 74).

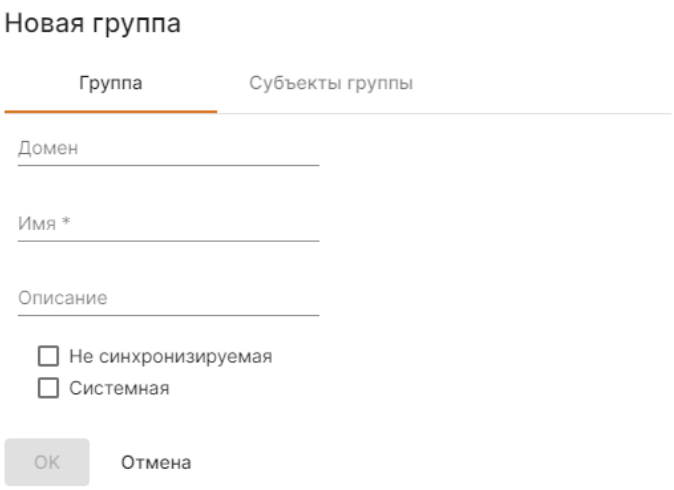

Рисунок 74. Окно создания новой группы

Изменить описание группы можно, используя кнопку **Свойства** или выбрав данное действие из контекстного меню.

Назначить все необходимые политики безопасности для созданной группы можно, редактируя параметры безопасности различных категорий параметров.

4.2.2 Управление группами пользователей ВИ

4.2.2.1 Управление группами домена vSphere/vCSA

Для создания новой группы vSphere необходимо:

1. Выбрать уровень vSphere и открыть категорию **Учетные записи vSphere** → **Группы vSphere** (см. Рисунок 75).

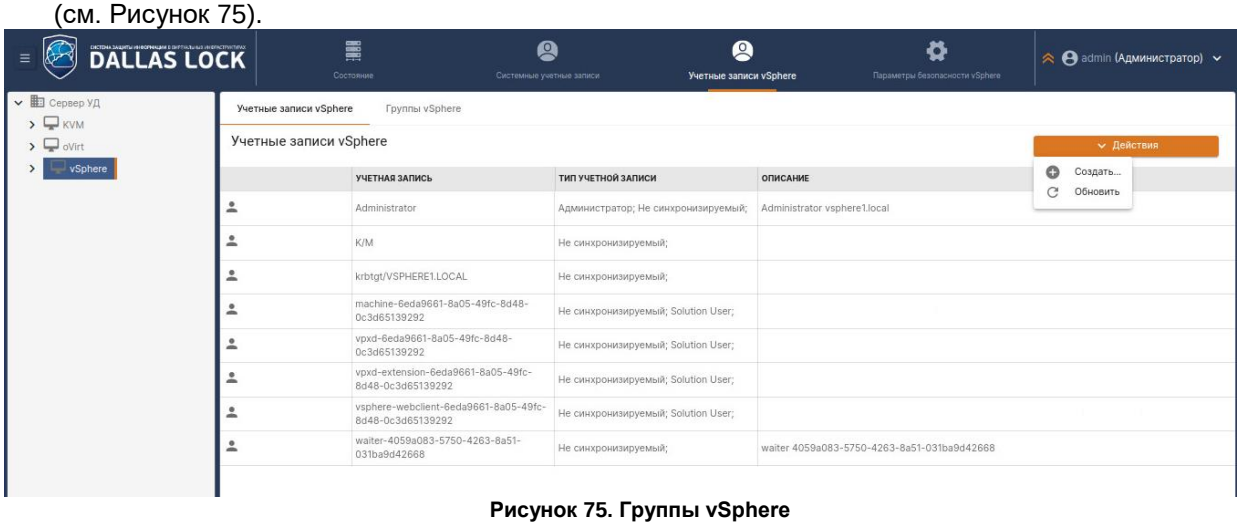

Рисунок 75. Группы vSphere

2. В категории действия нажать кнопку *Действия* и выбрать **Создать…**.
3. В появившемся окне ввести имя группы. Далее, при необходимости, заполнить поля *Домен* и *Описание* и добавить субъекты группы (см. ниже).
4. Завершить процесс создания группы, нажав кнопку **ОК** (см. Рисунок 76).

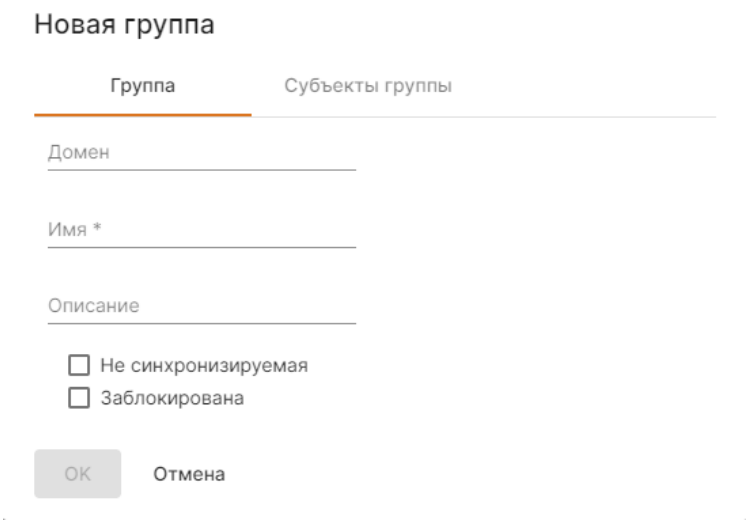

Рисунок 76. Окно создания новой группы

5. Изменения вступят в силу при следующей синхронизации (подробнее см. п. 3.5 «Синхронизация»).

4.2.2.2 Управление группами домена KVM

Для создания новой группы KVM необходимо:

1. Выбрать уровень KVM и открыть вкладку **Системные учетные записи** → **Группы** (см. Рисунок 77).

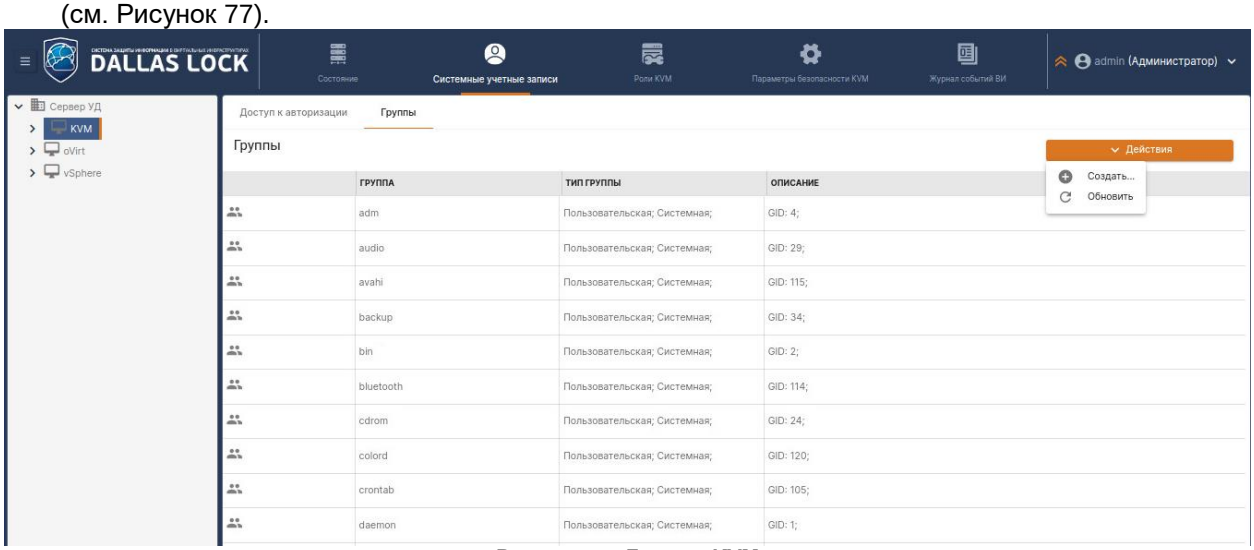

Рисунок 77. Группы KVM

2. Нажать кнопку **Создать…**.

3. В появившемся окне ввести имя группы (см. Рисунок 78).

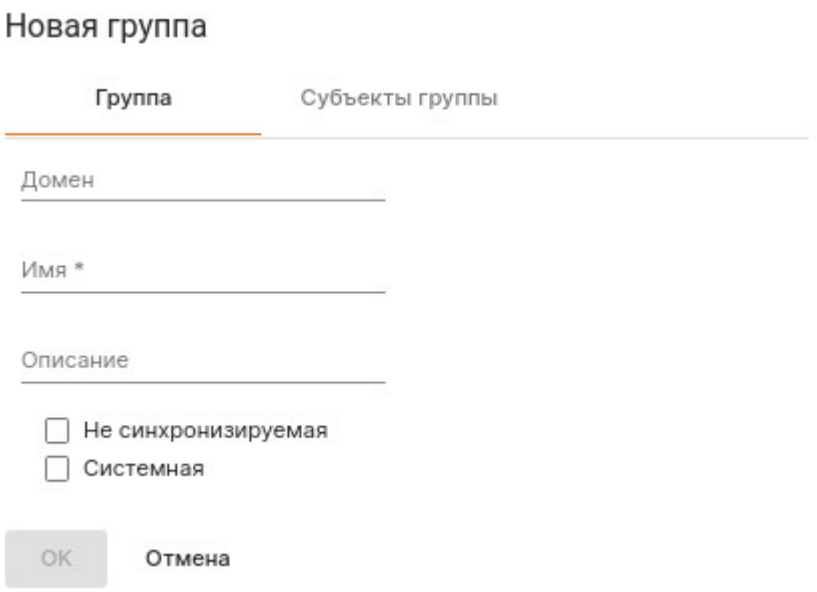

Рисунок 78. Окно создания новой группы KVM

4. Завершить процесс создания группы, нажав кнопку **OK**.
5. Изменения вступят в силу при следующей синхронизации (подробнее см. п. 3.5 «Синхронизация»).

4.2.2.3 Управление группами oVirt/zVirt/HOSTVM/RedVirt

Для создания новой группы oVirt/zVirt/HOSTVM/RedVirt необходимо:

1. Выбрать уровень oVirt и открыть вкладку **Учетные записи oVirt** → **Группы oVirt** (см. Рисунок 79).

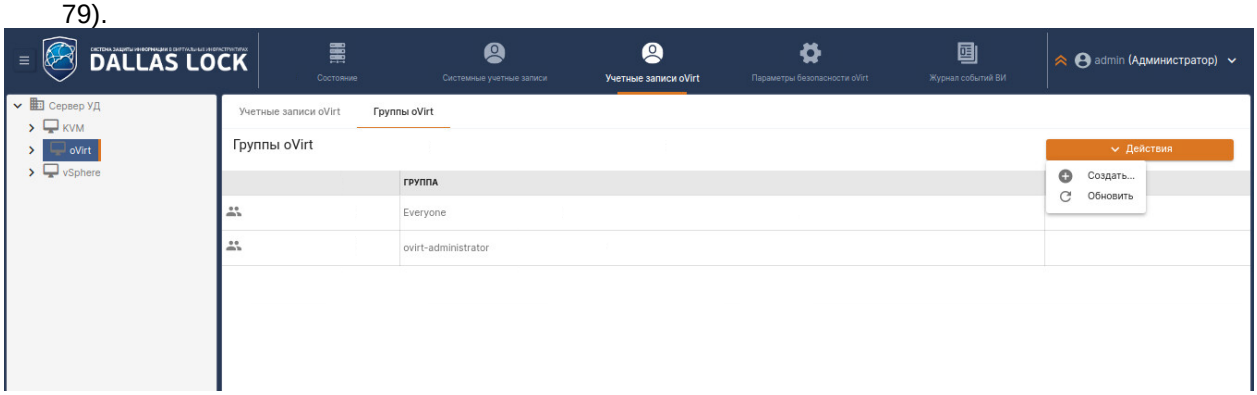

Рисунок 79. Группы oVirt/zVirt/HOSTVM/RedVirt

2. Нажать кнопку **Создать…**.
3. В появившемся окне ввести имя группы (см. Рисунок 80).

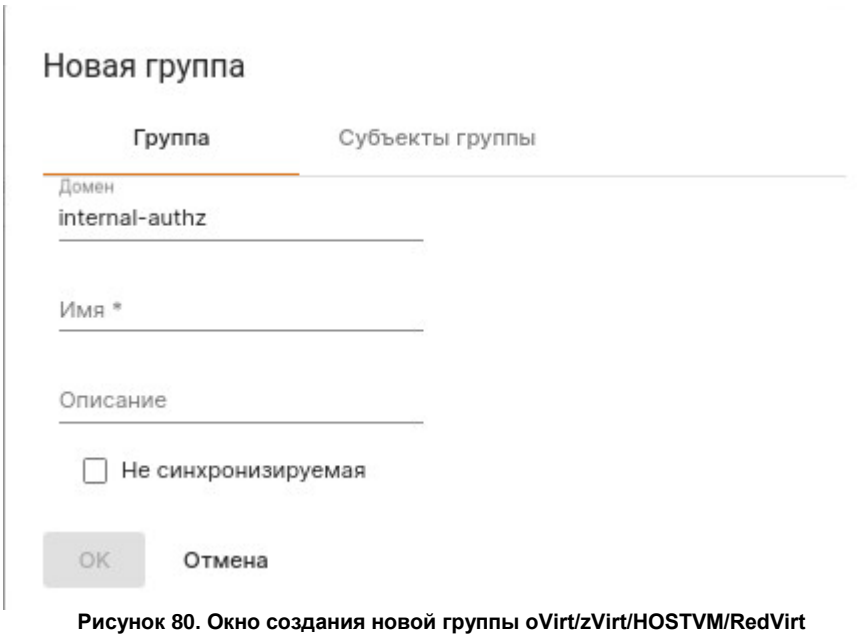

Рисунок 80. Окно создания новой группы oVirt/zVirt/HOSTVM/RedVirt

4. Завершить процесс создания группы, нажав кнопку **OK**.
5. Изменения вступят в силу при следующей синхронизации (подробнее см. п. 3.5 «Синхронизация»)

Создание локальной группы гипервизора/СВ oVirt/zVirt/HOSTVM/RedVirt

Для создания новой локальной группы oVirt/zVirt/HOSTVM/RedVirt необходимо:

1. Выбрать уровень oVirt и открыть вкладку **Системные учетные записи** → **Группы** (см. Рисунок 81).

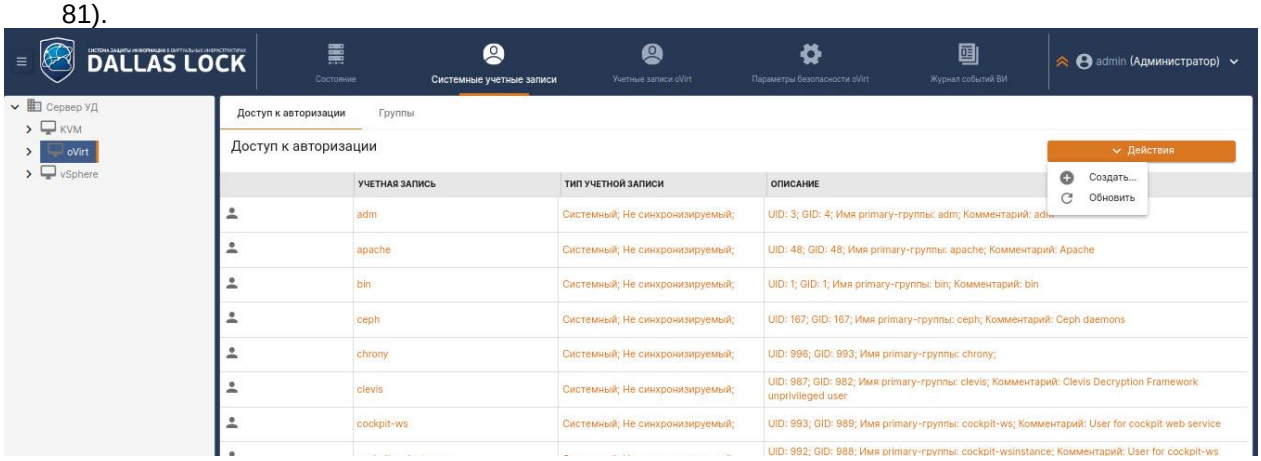

Рисунок 81. Локальные группы oVirt/zVirt/HOSTVM/RedVirt

2. Нажать кнопку **Создать**.
3. В появившемся окне ввести имя группы (см. Рисунок 82).

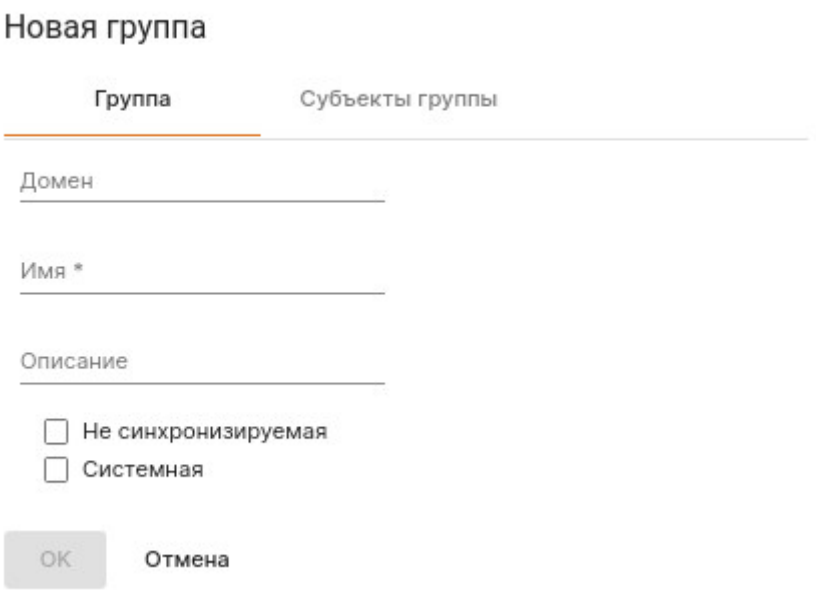

Рисунок 82. Окно создания новой группы oVirt/zVirt/HOSTVM/RedVirt

4. Завершить процесс создания группы, нажав кнопку **OK**.
5. Изменения вступят в силу при следующей синхронизации (подробнее см. п. 3.5 «Синхронизация»).

4.2.3 Удаление группы

Для удаления группы необходимо выделить соответствующую группу, нажать кнопку **Удалить** или выбрать данное действие в контекстном меню. На экране отобразится подтверждение на удаление.

Изменения вступят в силу при следующей синхронизации (подробнее см. п. 3.5 «Синхронизация»).

4.3 Настройки параметров безопасности для объектов ВИ

4.3.1 Настройки параметров безопасности

4.3.1.1 Параметры входа для vSphere

Просмотр и редактирование параметров входа для объектов ВИ vSphere происходит на уровне vSphere в категории **Параметры безопасности vSphere → Политики авторизации** (см. Рисунок 83).

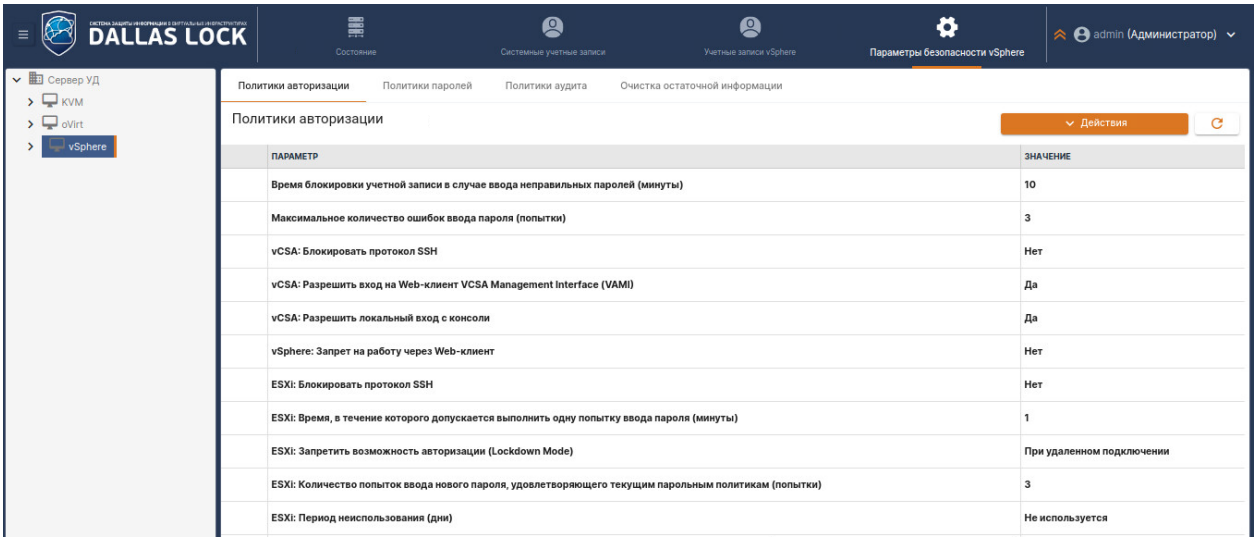

Рисунок 83. Параметры входа vSphere

Данные параметры входа применимы только для сервера виртуализации и гипервизора.

Параметры настройки политики авторизации vSphere представлены ниже.

Время блокировки учетной записи в случае ввода неправильных паролей

Данный параметр позволяет установить, сколько времени учетная запись будет заблокирована после того, как пользователь ввел неверный пароль больше допустимого числа раз.

По истечении указанного времени учетная запись автоматически разблокируется, и пользователь снова получит возможность ввести пароль.

Значение «900», установленное по умолчанию, указывает на то, что срок блокировки будет равняться 10 минутам.

Данная политика работает применительно к учетным записям, принадлежащим домену vsphere.local.

Значение данной политики определяется в диапазоне от «60 секунд» (1 минута) до «18000 секунд» (5 часов).

Максимальное количество ошибок ввода пароля

Значение, установленное для этого параметра, регламентирует, сколько раз пользователь имеет право ошибаться при вводе пароля. По умолчанию данное значение равно 3.

Если при входе на сервер виртуализации или гипервизор пользователь вводит неверный пароль и число ошибок превысит больше допустимого, учетная запись будет заблокирована. Сбросить автоматическую блокировку досрочно может только администратор безопасности или пользователь, обладающий правом редактирования учетных записей.

vCSA: Блокировать протокол SSH

Параметр контролирует удаленный доступ в vCSA по протоколу SSH.

По умолчанию значение данного параметра: **Нет**.

vCSA: Разрешить вход на Web-клиент VCSA Management Interface

Данный параметр позволяет настроить разрешение входа на Web-клиент VCSA Management Interface (VAMI).

По умолчанию значение данного параметра: **Нет**.

Данная политика может влиять на отображение ноды vCSA в интерфейсе vSphere client. Рекомендуется разрешить вход на Web-клиент VCSA Management Interface для исключения подобного поведения.

Актуально только для vSphere 7.0.3.

vCSA: Разрешить локальный вход с консоли

Данный параметр позволяет настроить разрешение локального входа с консоли.

По умолчанию значение данного параметра: **Да**.

vSphere: Запрет на работу через Web-клиент

Данный параметр позволяет заблокировать возможность подключения к серверу виртуализации или гипервизору ESXi через Web-клиент VMware vSphere.

По умолчанию значение данного параметра: **Нет**.

ESXi: Блокировать протокол SSH

Если разрешено использование ESXi Shell, то его можно запустить непосредственно на гипервизоре ESXi через DCUI или удаленно по SSH. Данный параметр блокирует такую возможность.

По умолчанию значение данного параметра: **Нет**.

ESXi: Время, в течение которого допускается выполнить одну попытку ввода пароля

Данный параметр позволяет установить, количество времени в течение которого допускается выполнить одну попытку ввода пароля. Если произошла неудачная попытка ввода пароля, то выполнить новую попытку ввода пароля возможно будет только через указанный период времени.

По умолчанию значение данного параметра: **1 мин**.

ESXi: Запретить возможность авторизации (Lockdown Mode)

Данный параметр позволяет настроить запрет возможности авторизации. Возможно установить запрет при удаленном подключении, при прямом и удаленном подключении. По умолчанию значение данного параметра: **При удаленном подключении**.
ESXi: Количество попыток ввода нового пароля, удовлетворяющего текущим парольным политикам
Значение, установленное для этого параметра, регламентирует, сколько раз пользователь имеет право ошибаться при вводе нового пароля. По умолчанию значение данного параметра: 3**.**
ESXi: Период неиспользования
Данным параметром устанавливается период времени, через который будут отключены неиспользуемые учетные записи. Сбросить автоматическую блокировку досрочно может только администратор безопасности или пользователь, обладающий правом редактирования учетных записей. По умолчанию значение данного параметра: **Не используется**.
Включить синхронизацию времени по NTP
Данный параметр позволяет отключить синхронизацию времени между **СЗИ ВИ** и гипервизорами. По умолчанию значение данного параметра **Используется**.
vCSA: Время, в течение которого подсчитываются ошибки ввода пароля
Данный параметр позволяет установить количество времени, в течение которого подсчитываются ошибки ввода пароля. Если за данный период времени количество неудачных попыток входа достигнет максимального количества ошибок ввода пароля, учетная запись будет заблокирована на время, заданное в параметре **[Общее] Вход: время блокировки учетной записи в случае ввода неправильных паролей**. В случае, если за установленное время количество неудачных попыток входа не достигло заданного максимального количества ошибок ввода пароля – счетчик неудачных попыток обнуляется. По умолчанию значение данного параметра: **1 мин**.

Параметры настройки политики паролей vSphere представлены ниже.

vSphere: Максимальный срок действия пароля
Данным параметром устанавливается максимальный срок действия пароля для всех пользователей. По истечении установленного срока, пользователь должен сменить пароль при входе на сервер виртуализации или гипервизор. По умолчанию значение данного параметра: **180 дн**.
vSphere: Минимальная длина пароля
Данным параметром устанавливается ограничение на минимальную длину пароля. При регистрации новой учетной записи и при изменении старого пароля **СЗИ ВИ DL** контролирует длину вводимого пароля. Если число символов в пароле меньше установленного значения, то на экране появится предупреждение *Пароль не соответствует политикам! Слишком короткий пароль*. Следует иметь в виду, что если в процессе работы изменить значение длины пароля (например, увеличить), то у зарегистрированных учетных записей она останется прежней до первой смены пароля. По умолчанию значение данного параметра: **6 симв**.
ESXi: Напоминать о смене пароля за
С помощью данного параметра **СЗИ ВИ** позволит напоминать пользователю о том, что через определенное количество дней необходимо сменить пароль. Напоминание о предстоящей смене пароля будет появляться на экране при загрузке ОС данным пользователем, начиная с того момента, когда до смены пароля (фактически до истечения максимального времени действия пароля) осталось количество дней, равное установленному значению для этой политики. По умолчанию значение данного параметра: **Не используется**.
ESXi: Минимальное количество классов символов
Данный параметр определяет количество классов символов (буквы в верхнем и нижнем регистре,

цифры и специальные символы), которые должны присутствовать в пароле.

Этот параметр может принимать значения от 1 до 4. Значение «1» означает, что пароль может содержать любые символы, например, только цифры.

По умолчанию значение данного параметра: **Не используется**.

vCenter: Количество предыдущих паролей, которые пользователь не может использовать

Данным параметром устанавливается количество предыдущих паролей каждого пользователя, которые не могут быть выбраны ими при смене пароля. Например, значение «5», установленное по умолчанию, запрещает использовать пять предыдущих паролей для выбранного пользователя.

vCenter: Максимальная длина пароля

Данным параметром устанавливается ограничение на максимальную длину пароля.

По умолчанию значение данного параметра: **20 символов**.

vCenter: Максимально допустимое количество одинаковых символов, стоящих рядом

Данным параметром устанавливается максимально допустимое количество одинаковых символов, которые могут присутствовать при задании пароля, для учетной записи Сервера виртуализации.

По умолчанию значение данного параметра: **3 симв**.

vCenter: Минимальное количество прописных букв

Данным параметром устанавливается минимальное количество прописных (больших) букв, которые должны присутствовать при задании пароля, для учетной записи Сервера виртуализации.

По умолчанию значение данного параметра: **Не используется**.

vCenter: Минимальное количество символов алфавита

Данным параметром устанавливается минимальное количество символов алфавита, которые должны присутствовать при задании пароля, для учетной записи Сервера виртуализации.

По умолчанию значение данного параметра: **Не используется**.

vCenter: Минимальное количество специальных символов

Данным параметром устанавливается минимальное количество специальных символов («`», «~», «!», «@», «#», «$», «%», «^», «&», «*», «(», «)», «_», «-», «+», «{», «}», «[», «]», «\», «|», «:», «;», ««», «'«, «<«, «>», «,», «.», «?», «/»), которые должны присутствовать при задании пароля, для учетной записи Сервера виртуализации.

По умолчанию значение данного параметра: **Не используется**.

vCenter: Минимальное количество строчных букв

Данным параметром устанавливается минимальное количество строчных (маленьких) букв, которые должны присутствовать при задании, для учетной записи Сервера виртуализации.

По умолчанию значение данного параметра: **Не используется**.

vCenter: Минимальное количество цифр

Данным параметром устанавливается минимальное количество цифр, которые должны присутствовать при задании пароля, для учетной записи Сервера виртуализации.

По умолчанию значение данного параметра: **Не используется**.

Параметры настройки политики аудита vSphere представлены ниже.

vSphere: ESXi Shell (служба shell)

Данный параметр позволяет включить регистрацию событий и записей всех введенных команд в ESXi Shell.

По умолчанию значение данного параметра: **Выкл.**.

vSphere: Агент ESXi (служба hostd)

Данный параметр позволяет включить регистрацию сведений о действиях агента, который управляет и конфигурирует гипервизор виртуальные машины, а также включить регистрацию событий аутентификации на гипервизоре.

По умолчанию значение данного параметра: **Выкл.**.

vSphere: USB-устройства (служба usb)

Данный параметр позволяет включить регистрацию событий, связанных с подключаемыми USB-устройствами к гипервизору. По умолчанию значение данного параметра: **Выкл.**.
vSphere: Аутентификация (службы auth, login, vmauthd)
Данный параметр позволяет включить регистрацию событий, связанных с аутентификацией на гипервизоре. По умолчанию значение данного параметра: **Выкл.**.
vSphere: Системные события (служба syslog)
Данный параметр позволяет включить регистрацию общих сообщений журнала (Syslog), которые могут быть использованы для устранения неполадок. По умолчанию значение данного параметра: **Выкл.**.
vSphere: Виртуальные машины (службы vmauthd, vmkdevmgr, vmkernel, vmkeventd, vmksummary, vmkwarning)
Данный параметр позволяет включить регистрацию событий, связанных с виртуальными машинами и гипервизорами. По умолчанию значение данного параметра: **Выкл.**.
vSphere: Зачистка ФС (события eraser)
Данный параметр позволяет включить регистрацию событий, связанных с зачисткой файловой системы гипервизора. По умолчанию значение данного параметра: **Выкл.**.
Уведомления: Операции с виртуальными машинами
Данный параметр позволяет включить регистрацию событий, связанных с операциями с виртуальными машинами. По умолчанию значение данного параметра: **Выкл.**.
Уведомления: Операции со снапшотами
Данный параметр позволяет включить регистрацию событий, связанных с созданием снапшотов. По умолчанию значение данного параметра: **Выкл.**.
Уведомления: Операции с виртуальными дисками
Данный параметр позволяет включить регистрацию событий, связанных виртуальными дисками. По умолчанию значение данного параметра: **Выкл.**.
Уведомления: Операции с объектами виртуальной сети
Данный параметр позволяет включить регистрацию событий, связанных с объектами виртуальной сети. По умолчанию значение данного параметра: **Выкл.**.
Уведомления: Изменение общих настроек сервера виртуализации
Данный параметр позволяет включить регистрацию событий, связанных изменением настроек сервера виртуализации. По умолчанию значение данного параметра: **Выкл.**.

Параметры настройки политики очистки остаточной информации vSphere представлены ниже.

Количество циклов затирания
Данный параметр позволяет определить количество циклов затирания. По умолчанию значение данного параметра: **3**.

4.3.1.2 Параметры авторизации для KVM

Просмотр и редактирование параметров авторизации для объектов ВИ происходит в дереве на уровне Сервера УД и KVM в категории **Параметры безопасности (KVM)** → **Политики авторизации**. Подробное описание приведено в п. 4.4.1 «Настройка параметров ».

4.3.1.3 Параметры входа для oVirt/zVirt/HOSTVM/RedVirt

Просмотр и редактирование параметров входа для объектов ВИ oVirt/zVirt/HOSTVM/RedVirt происходит в дереве на уровне oVirt в категории **Параметры безопасности oVirt** → **Политики авторизации** (см. Рисунок 84).

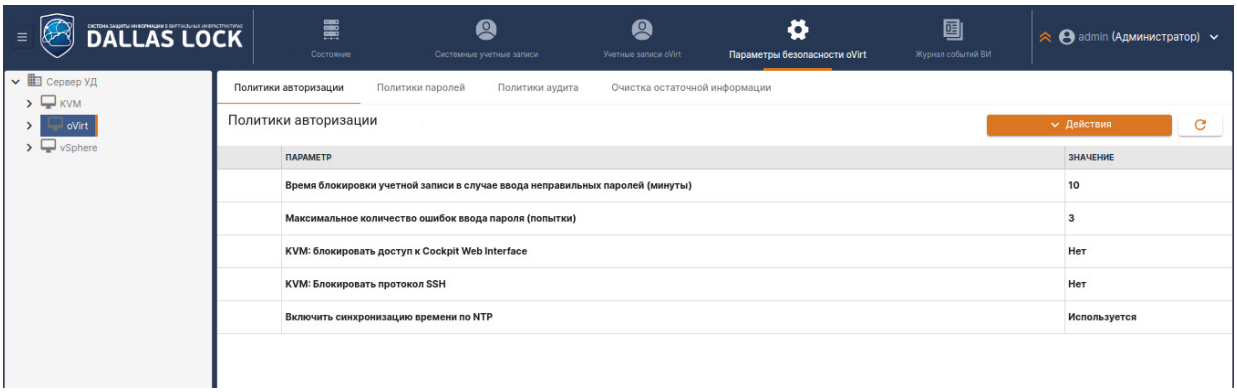

Рисунок 84. Параметры входа oVirt/zVitr/HOSTVM/RedVirt

Данные параметры входа применимы только для сервера виртуализации и гипервизора.

Максимальное количество ошибок ввода пароля (попытки)

Значение, установленное для этого параметра, регламентирует, сколько раз пользователь имеет право ошибаться при вводе пароля. По умолчанию данное значение равно 3.

Если при входе на сервер виртуализации или гипервизор пользователь вводит неверный пароль и число ошибок превысит больше допустимого, учетная запись будет заблокирована. Сбросить автоматическую блокировку досрочно может только администратор безопасности или пользователь, обладающий правом редактирования учетных записей.

Время блокировки учетной записи в случае ввода неправильных паролей (сек.)

Данный параметр позволяет установить, сколько времени учетная запись будет заблокирована после того, как пользователь ввел неверный пароль больше допустимого числа раз.

По истечении указанного времени учетная запись автоматически разблокируется, и пользователь снова получит возможность ввести пароль.

Значение 900, установленное по умолчанию, указывает на то, что срок блокировки будет равняться 10 минутам.

KVM: блокировать протокол SSH

Данный параметр блокирует удаленный доступ к СВ по протоколу SSH.

По умолчанию значение данного параметра: **Да**.

Для возможности удаленного подключения к клиенту по протоколу SSH помимо отключения данной политики необходимо добавить компьютер, с которого будет осуществляться подключение, в список клиентов управления СВ (подробнее см. п. 5.1.2.3 «Клиенты управления СВ KVM/oVirt/zVirt/HOSTVM»).

KVM: блокировать доступ к Cockpit Web Interface

Данный параметр позволяет настроить разрешение входа на Web-клиент Cockpit Web Interface.

По умолчанию значение данного параметра: **Нет**.

Включить синхронизацию времени по NTP

Данный параметр позволяет использовать NTP-сервера из заданного списка для синхронизации времени между сервером УД и агентами **СЗИ ВИ**.

По умолчанию значение данного параметра: **Используется**.

oVirt: Количество предыдущих паролей, которые пользователь не может использовать (штук)

Данным параметром устанавливается количество предыдущих паролей каждого пользователя, которые не могут быть выбраны ими при смене пароля. Например, значение «5», установленное по умолчанию, запрещает использовать пять предыдущих паролей для выбранного пользователя.

4.4 Настройки параметров для клиентов Сервера УД

4.4.1 Настройка параметров безопасности

Для настройки политик безопасности необходимо перейти на уровень Сервера УД во вкладку «Параметры безопасности» (см. Рисунок 85). Настройки входа будут установлены для всех клиентов.

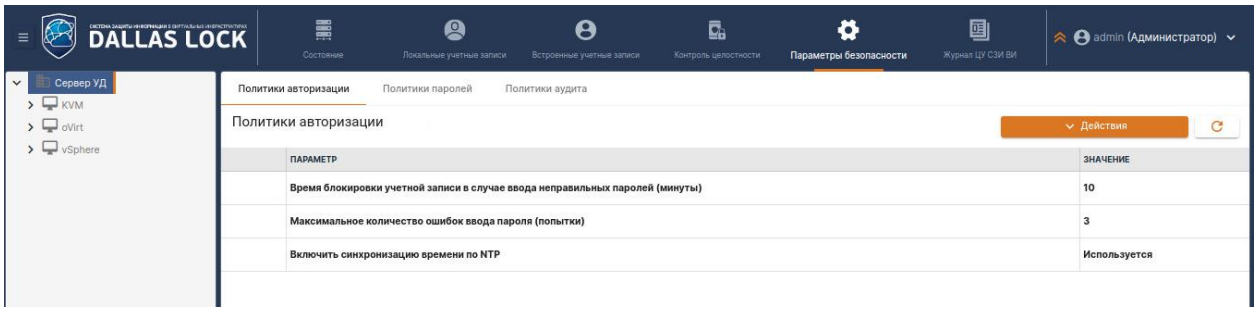

Рисунок 85. Настройка параметров безопасности на уровне Сервера УД

В соответствии с требованиями политики безопасности организации необходимо настроить все параметры, расположенные в списке параметров политики авторизации.

Время блокировки учетной записи в случае ввода неправильных паролей

Данный параметр позволяет установить, сколько времени учетная запись будет заблокирована после того, как пользователь ввел неверный пароль больше допустимого числа раз. В этот временной интервал пользователь не сможет загрузить компьютер и ОС, даже при верном вводе пароля.

По истечении указанного времени учетная запись автоматически разблокируется, и пользователь снова получит возможность ввести пароль. Сбросить автоматическую блокировку досрочно может только администратор безопасности или пользователь, обладающий правом редактирования учетных записей.

Если при настройке опции выбрано значение **Не используется**, то разблокировать учетную запись и тем самым позволить пользователю вновь работать на защищенном компьютере, может только администратор безопасности.

По умолчанию значение данного параметра: **15 минут**.

Максимальное количество ошибок ввода пароля

Значение, установленное для этого параметра, регламентирует, сколько раз пользователь имеет право ошибаться при вводе пароля. В выпадающем списке можно выбрать число попыток от 1 до 10.

Если при входе на защищенный компьютер или на этапе загрузки ОС пользователь ввел неверный пароль, то система выдаст предупреждение *Указан неверный пароль*. Если число ошибок больше допустимого, учетная запись будет заблокирована, и пользователь не сможет загрузить компьютер и ОС. При этом система защиты выдаст сообщение *Запись пользователя заблокирована*.

Способы разблокирования пользователей описаны в п. 4.1.5 «Разблокирование и заблокированные пользователи».

Если установлено значение **Не используется**, то пользователь может вводить неверный пароль неограниченное число раз.

По умолчанию значение данного параметра: **5**.

Включить синхронизацию времени по NTP

Данный параметр позволяет задать список NTP-серверов для синхронизации времени между сервером УД и агентами **СЗИ ВИ**.

По умолчанию значение данного параметра: **Используется**.

В соответствии с требованиями политики безопасности организации необходимо настроить все параметры, расположенные в списке параметров политики паролей (см. Рисунок 86).

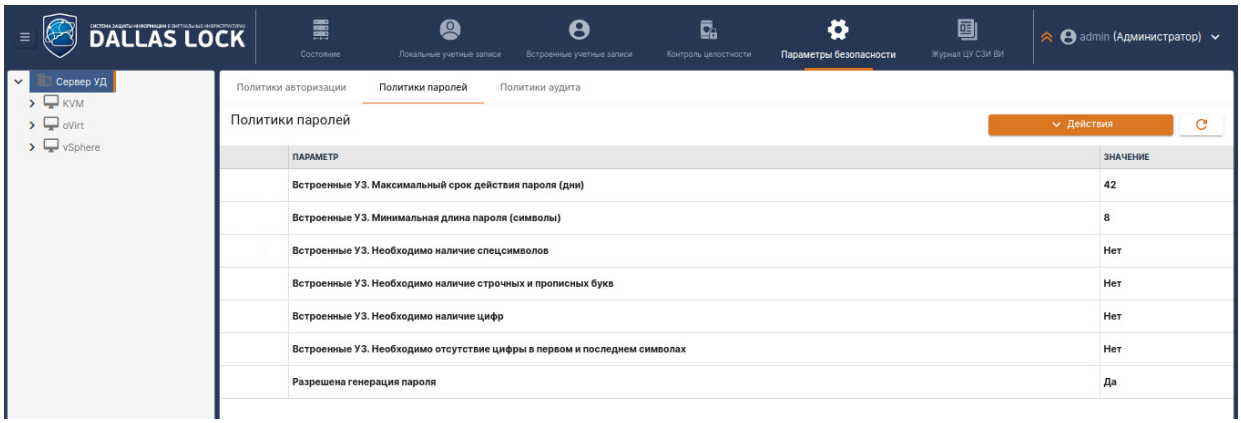

Рисунок 86. Политики паролей на уровне Сервера УД

Встроенные УЗ: Максимальный срок действия пароля

Данным параметром устанавливается максимальный срок действия пароля для всех пользователей. По истечении установленного срока **СЗИ ВИ** автоматически предложит пользователю сменить пароль при входе в ОС.

По умолчанию значение данного параметра: **42 дн**.

Встроенные УЗ: Минимальная длина пароля (символы)

Данным параметром устанавливается ограничение на минимальную длину пароля. Если число символов в пароле меньше установленного значения, то на экране появится предупреждение. При выборе значения **Не используется** устанавливаемый пароль может иметь пустое значение. При регистрации нового пользователя и при изменении старого пароля система защиты контролирует длину вводимого пароля. Если число символов в пароле меньше установленного значения, то на экране появится предупреждение «*Ввод пароля: введен слишком короткий пароль*».

Следует иметь в виду, что если в процессе работы изменено значение длину пароля (например, увеличена), то у зарегистрированных пользователей она останется прежней до первой смены ими пароля.

По умолчанию значение данного параметра: **8 симв**.

Встроенные УЗ: Необходимо наличие спец. символов

Если данный параметр включен (значение **Да**), то при создании пароля в нем должны присутствовать специальные символы из следующего списка: ` ~ ! @ # $ % ^ & * ( ) _ - + = { } [ ] \ | : ; ‘ “ < > , . ? /.

Действие параметра распространяется на значения паролей, PIN-кодов и ключей.

Пример. Если у пользователя имеется пароль «password1», и если вышеописанная опция активирована, то при смене пароля на «password2» выведется сообщение «*В пароле должны содержаться спецсимволы*». Правильной будет смена пароля, например, с «password1» на «password#».

По умолчанию значение данного параметра: **Нет**.

Встроенные УЗ: Необходимо наличие цифр

Если данный параметр включен (значение **Да**), то при создании пароля в нем должны присутствовать цифры. Действие параметра распространяется на значения паролей, PIN-кодов и ключей.

Пример: если у пользователя имеется пароль «password», если описанная выше опция активирована, то при смене пароля на «passwordd» выведется сообщение «*В пароле должны содержаться цифры*». Правильной будет смена пароля, например, с «password» на «password12».

По умолчанию значение данного параметра: **Нет**.

Встроенные УЗ: Необходимо наличие строчных и прописных букв

Если данный параметр включен (значение **Да**), то при создании пароля в нем должны присутствовать строчные и прописные буквы. Действие параметра распространяется на значения паролей, PIN-кодов и ключей.

Пример: если у пользователя имеется пароль «password1», и, если вышеописанная опция активирована, то при смене пароля на «pacsword1» выведется сообщение «*В пароле должны содержаться и строчные, и прописные буквы*». Если пользователь сменит пароль «password1»

на «paCsword1», то операция успешно завершится.
По умолчанию значение данного параметра: **Нет**.

Встроенные УЗ: Необходимо отсутствие цифры в первом и последнем символе

Если данный параметр включен (значение **Да**), то при создании пароля на месте первого и последнего символа в нем не должны присутствовать цифры. Действие параметра распространяется на значения паролей, PIN-кодов и ключей.
По умолчанию значение данного параметра: **Нет**.

Разрешена генерация пароля

Разрешение генерировать пароли системы защиты. Система автоматически создаст случайный пароль, удовлетворяющий политикам сложности пароля.
По умолчанию значение данного параметра: **Да**.

В соответствии с требованиями политики безопасности организации необходимо настроить все параметры, расположенные в списке параметров политики аудита (см. Рисунок 87).

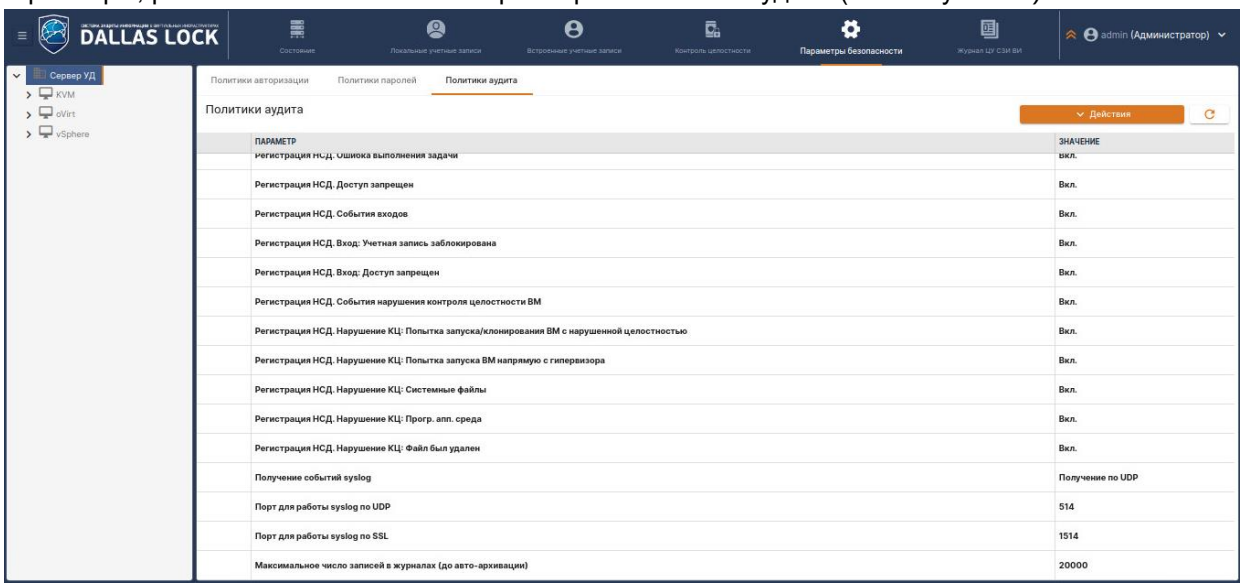

Рисунок 87. Политики аудита на уровне Сервера УД

Регистрация НСД: Ошибка выполнения задачи

Регистрация события НСД.
По умолчанию значение данного параметра: **Вкл**.

Регистрация НСД: Доступ запрещен

Регистрация события НСД.
По умолчанию значение данного параметра: **Вкл**.

Регистрация НСД: События входов

Регистрация события НСД.
По умолчанию значение данного параметра: **Вкл**.

Регистрация НСД: Вход: Учетная запись заблокирована

Регистрация события НСД.
По умолчанию значение данного параметра: **Вкл**.

Регистрация НСД: Вход: Доступ запрещен

Регистрация события НСД.
По умолчанию значение данного параметра: **Вкл**.

Регистрация НСД: События нарушения контроля целостности ВМ

Регистрация события НСД.
По умолчанию значение данного параметра: **Вкл**.

Регистрация НСД: КЦ: Попытка запуска/клонирования ВМ с нарушенной целостностью

Регистрация события НСД.
По умолчанию значение данного параметра: **Вкл**.

Регистрация НСД: КЦ: Попытка запуска ВМ напрямую с гипервизора
Регистрация события НСД. По умолчанию значение данного параметра: **Вкл**.
Регистрация НСД: Нарушение КЦ: Системные файлы
Регистрация события НСД. По умолчанию значение данного параметра: **Вкл**.
Регистрация НСД: Нарушение КЦ: Прогр. апп. среда
Регистрация события НСД. По умолчанию значение данного параметра: **Вкл**.
Регистрация НСД: Нарушение КЦ: Файл был удален
Регистрация события НСД. По умолчанию значение данного параметра: **Вкл**.
Получение событий syslog
Регистрация события НСД. По умолчанию значение данного параметра: **Получение по UDP**.
Порт для работы syslog по UDP
Регистрация события НСД. По умолчанию значение данного параметра: **514**.
Порт для работы syslog по SSL
Регистрация события НСД. По умолчанию значение данного параметра: **1514**.

5 ПОДСИСТЕМА УПРАВЛЕНИЯ ДОСТУПОМ

5.1 Удаленный доступ к СВ

По умолчанию, после развертывания **СЗИ ВИ**, удаленное подключение к СВ доступно только с **ЦУ СЗИ ВИ**.

5.1.1 Правила управления СВ

Просмотр и редактирование списка правил управления СВ происходит на уровне СВ в категории **Состояние → Правила управления СВ** (см. Рисунок 88).

В правилах управления СВ задается список блокируемых портов и тип протокола (TCP/UDP) для удаленного подключения к СВ. По умолчанию заданы все стандартные порты, используемые для подключения к СВ.

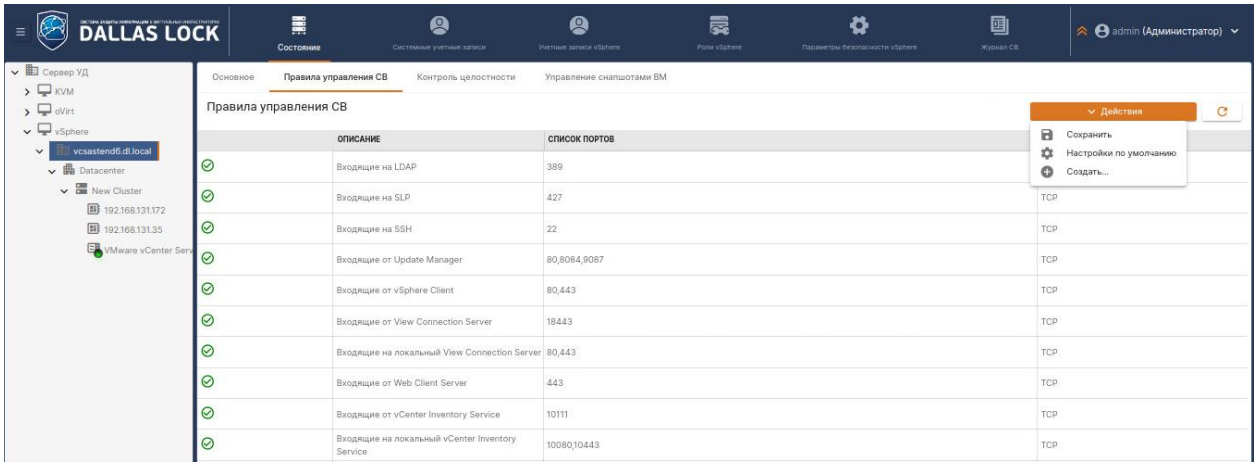

Рисунок 88. Правила управления СВ

Для того чтобы создать правило управления СВ необходимо:

1. Перейти на уровень СВ и открыть категорию **Состояние → Правила управления СВ**.
2. Нажать кнопку *Действия* и выбрать **Создать…**.
3. Ввести необходимые данные и нажать **Ок**.
4. Далее следует нажать кнопку *Действия* и выбрать **Сохранить**.

Для того, чтобы деактивировать правило необходимо выделить это правило и нажать кнопку **Отключить**, а затем нажать кнопку *Действия* и выбрать **Сохранить**.

Чтобы отменить все изменения и вернуться к исходным настройкам правил, необходимо в категории *Действия* нажать кнопку **Настройки по умолчанию**.

5.1.2 Клиенты управления СВ

Чтобы получить доступ к серверу виртуализации с удаленного компьютера, данный компьютер должен входить в список клиентов управления СВ.

5.1.2.1 Клиенты управления СВ vSphere

Просмотр и редактирование списка клиентов управления vSphere происходит на уровне *vSphere* в категории **Состояние → Клиенты управления СВ** (см. Рисунок 89).

Рисунок 89. Клиенты управления СВ vSphere

Для того чтобы добавить клиента управления сервером виртуализации необходимо:

1. Выбрать уровень группы *vSphere* и открыть категорию **Состояние → Клиенты управления СВ**.
2. Выбрать категорию *Действия* и нажать кнопку **Добавить клиента…**.

3. В появившемся окне ввести имя в сети или IP-адрес клиента управления, после чего нажать кнопку **ОК**.
4. Нажать кнопку *Действия*, после чего выбрать **Обновить**.

5.1.2.2 Клиенты управления СВ oVirt

Просмотр и редактирование списка клиентов управления oVirt происходит на уровне *oVirt* в категории **Состояние → Клиенты управления СВ** (см. Рисунок 90).

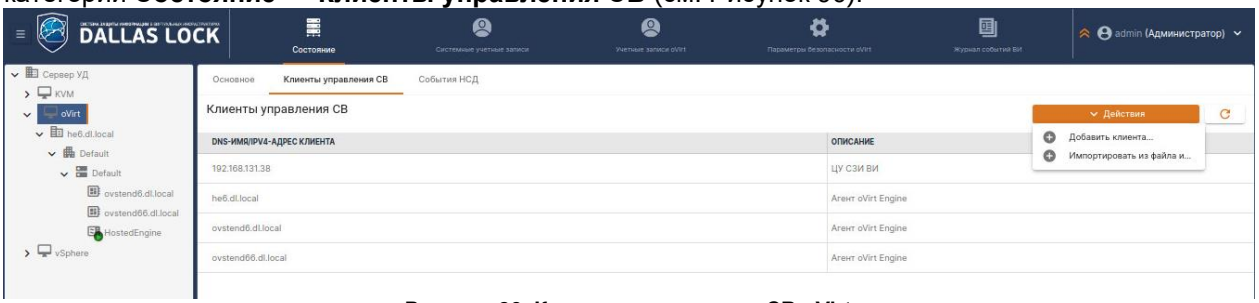

Рисунок 90. Клиенты управления СВ oVirt

Для того чтобы добавить клиента управления сервером виртуализации необходимо:

1. Выбрать уровень *oVirt* и открыть категорию **Состояние → Клиенты управления СВ**.
2. В категории **Действия с клиентами** и нажать кнопку **Добавить клиента**.
3. В появившемся окне ввести имя в сети или IP-адрес клиента управления, после чего нажать кнопку **ОК**.
4. Нажать кнопку **Синхронизация СВ и гипервизоров** в разделе **Основное** кнопка *Действия*.

> Не рекомендуется удалять или деактивировать правила из списка блокируемых портов для удаленного подключения к СВ (подробнее см. п. 5.1.1 «Правила управления СВ», сформированного по умолчанию.

5.1.2.3 Клиенты управления СВ KVM/oVirt/zVirt/HOSTVM/RedVirt

Просмотр и редактирование списка клиентов управления KVM происходит на уровне *KVM* в категории **Состояние → Клиенты управления СВ** (см. Рисунок 91).

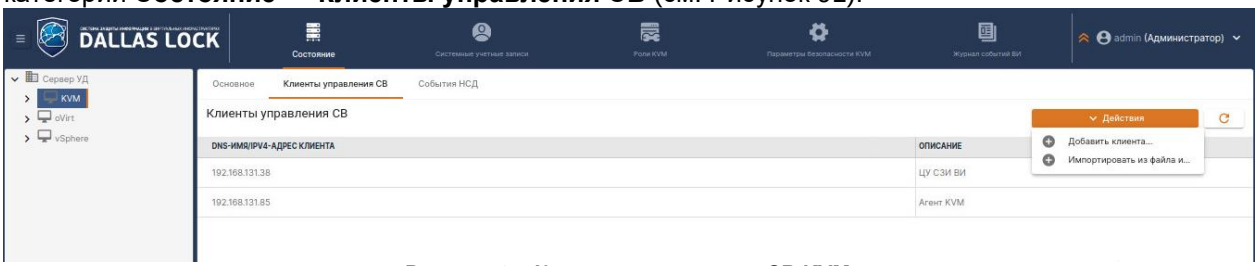

Рисунок 91. Клиенты управления СВ KVM

Для того чтобы добавить клиента управления сервером виртуализации необходимо:

1. Выбрать уровень «KVM» и открыть категорию **Состояние → Клиенты управления СВ**.
2. В категории **Действия с клиентами** и нажать кнопку **Добавить клиента**.
3. В появившемся окне ввести имя в сети или IP-адрес клиента управления, после чего нажать кнопку **ОК**.
4. Нажать кнопку **Синхронизация СВ и гипервизоров** в блоке *Действия* с KVM.

5.2 Ролевая модель учетных записей СВ

Роль представляет собой совокупность привилегий — полномочий по выполнению действий в части администрирования **СЗИ ВИ** и **ДБ**. Для удобства привилегии группируются в несколько категорий в зависимости от области применения.

Различным субъектам доступа (учетным записям или группам пользователей) **ДБ** ставится в соответствие роль, отображающая права данного субъекта в части администрирования средствами **СЗИ ВИ**.

Для субъекта доступа (пользователя или группы) может быть назначена только одна роль на объект **ВИ**, однако, разрешения для пользователя могут складываться, если он является членом нескольких групп, для которых назначены разные роли на объект. При этом, если роль явно назначается для учетной записи пользователя, она перекрывает все права, полученные от групп. Однако если пользователь состоит хотя бы в одной группе, которой явно была назначена роль *Нет*

доступа, все привилегии считаются снятыми.

5.2.1 Ролевая модель учетных записей vSphere

Настройки по правам администрирования доступа к гипервизорам, объектам ВИ и виртуальным машинам vSphere осуществляются средствами ролевой модели разграничения доступа. Для просмотра и редактирования параметров ролевого доступа необходимо в дереве на уровне группы vSphere перейти на вкладку *Роли vSphere* (см. Рисунок 92).

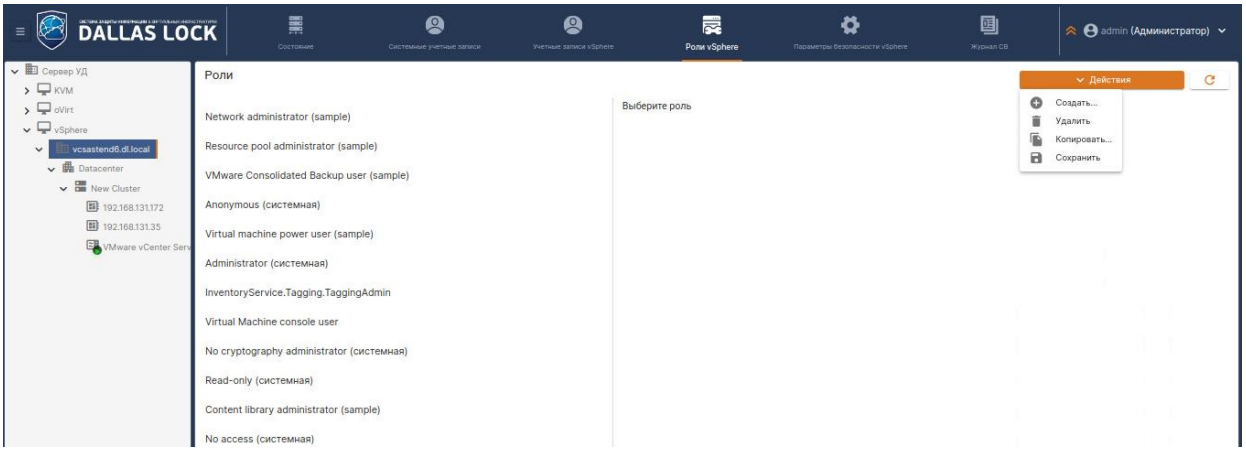

Рисунок 92. Роли сервера виртуализации vSphere

> Создавать и осуществлять настройку ролей может только суперадминистратор.

В группе vSphere на вкладке *Роли vSphere* присутствуют предустановленные роли, которые невозможно изменить (системные). Системные предустановленные роли, которые нельзя изменить или удалить, называются (Administrator (системная), Anonymous (системная), No access (системная), No cryptography administrator (системная), Read-only (системная), View (системная)).

Для системных ролей установлены следующие разрешающие привилегии:

- для роли A*dministrator*: включены все привилегии;
- для роли *Anonymous*: частично включена привилегия *System*, раздел *Anonymous*;
- для роли *No access*: все привилегии отключены;
- для роли *No cryptography administrator*: включены все привилегии, кроме *TrustedAdmin*;
- для роли *Read-only*: включена привилегия *System*. Используется для аудита (только просмотр детальной информации и состояния объекта);
- для роли *View*: частично включена привилегия *System*, раздел *Anonymous* и *View*.

5.2.1.1 Создание и редактирование ролей vSphere

Для создания новой роли на СВ необходимо:

1. Выбрать уровень СВ и открыть вкладку *Роли vSphere*.
2. Нажать кнопку *Действия* и выбрать **Создать…**, ввести имя для новой роли (см. Рисунок 93) и нажать **ОК**.
3. Выбрать необходимые привилегии для роли и нажать кнопку **Сохранить** в блоке *Действия*.
4. Открыть вкладку *Состояние* и нажать кнопку **Синхронизация СВ и гипервизоров** в блоке *Действия* (подробнее см. п. 3.5 «Синхронизация»).

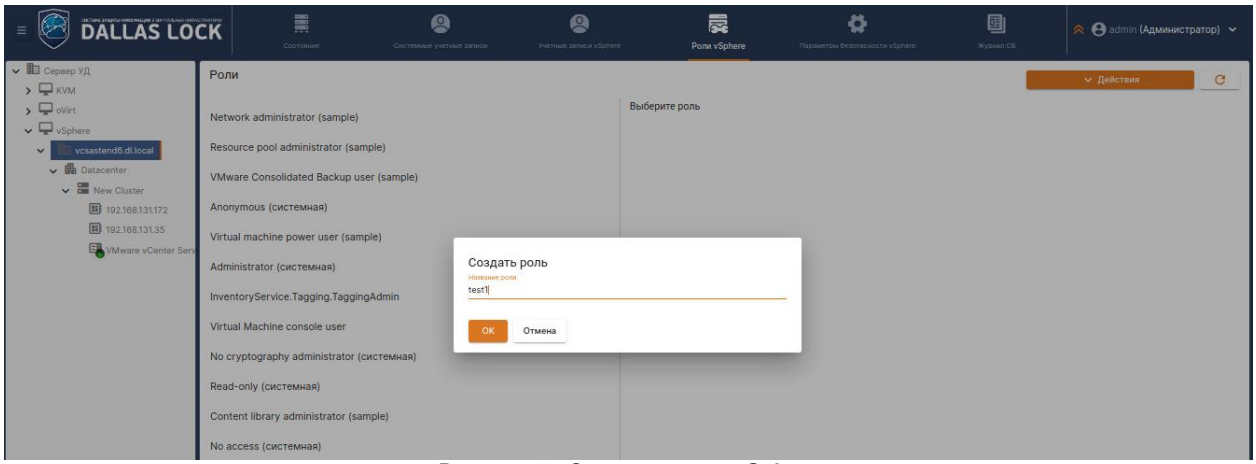

Рисунок 93. Создание роли vSphere

По умолчанию все привилегии для вновь созданных ролей отключены. Для назначения привилегий, необходимо корректно заполнить поле с привилегиями и нажать кнопку **Сохранить** в блоке *Действия*.

После внесения всех необходимых изменений, следует выполнить сохранение путем нажатия кнопки **Сохранить** в блоке *Действия* и произвести синхронизацию (подробнее см. п. 3.5 «Синхронизация»).

5.2.1.2 Удаление ролей vSphere

Для удаления роли необходимо выделить роль, которую следует удалить и выбрать **Удалить** после нажатия кнопки *Действия* (см. Рисунок 94).

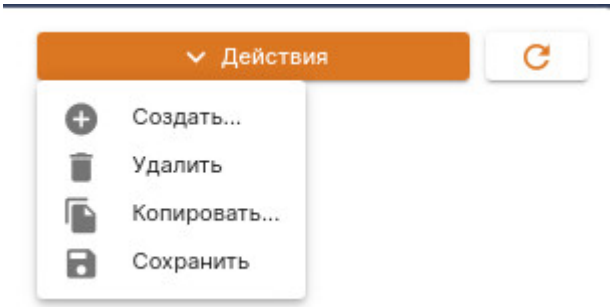

Рисунок 94. Удаление роли vSphere

После чего подтвердить операцию и произвести синхронизацию (подробнее см. п. 3.5 «Синхронизация»).

После удаления назначенной роли все назначения данной роли удаляются.

Для обновления списка ролей в категории *Действия* необходимо нажать кнопку **Обновить**.

5.2.1.3 Управление ролями гипервизора ESXi

Порядок действий для ролей гипервизоров аналогичен п. 5.2.1.1 (см. Рисунок 95).

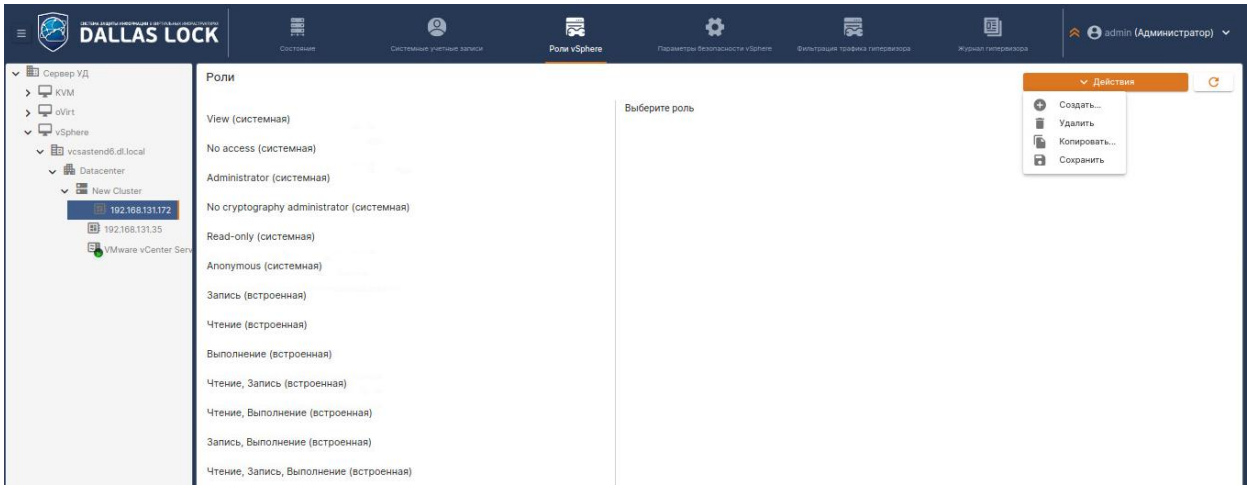

Рисунок 95. Роли гипервизора ESXi

5.2.2 Ролевая модель учетных записей oVirt

Настройки по правам администрирования доступа к гипервизорам, объектам ВИ и виртуальным машинам oVirt/zVirt/HOSTVM/RedVirt/KVM осуществляются средствами ролевой модели разграничения доступа. Для просмотра и редактирования параметров ролевого доступа необходимо в дереве уровне группы oVirt перейти на вкладку *Роли oVirt* (см. Рисунок 96).

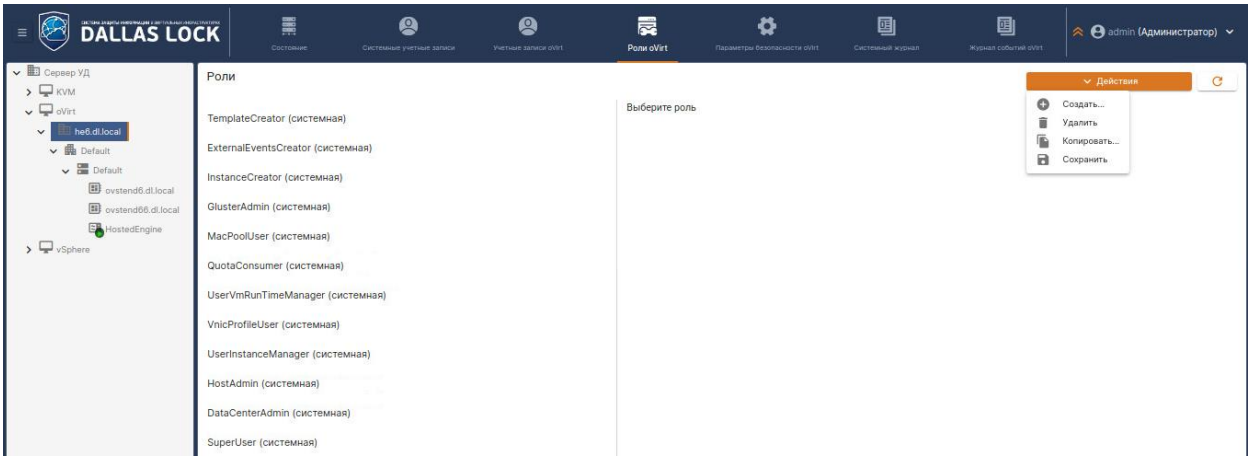

Рисунок 96. Роли oVirt

В дереве oVirt на вкладке *Роли oVirt* присутствуют предустановленные роли, которые невозможно изменить (системные), предустановленные роли, привилегии которых можно редактировать, а также существует возможность создания новых ролей.

Системные предустановленные роли нельзя изменить или удалить.

Также, следует учитывать, что редактирование ролей осуществляется на общем для всех СВ oVirt уровне, следовательно, на каждом СВ oVirt всегда создается одинаковый набор ролей.

5.2.2.1 Создание ролей oVirt

Для создания новой роли на СВ необходимо:

1. Выбрать уровень группы oVirt и открыть вкладку **Роли oVirt** → **Роли oVirt**.
2. Нажать кнопку *Действия* и **Создать…**, ввести имя для новой роли (см. Рисунок 97) и нажать кнопку **Ок**.
3. Выбрать необходимые привилегии для роли и нажать кнопку **Сохранить** в блоке *Действия*.
4. Открыть вкладку *Состояние* и нажать кнопку **Синхронизация СВ и гипервизоров** или выбрать соответствующий пункт из контекстного меню (подробнее см. п. 3.5 «Синхронизация»).

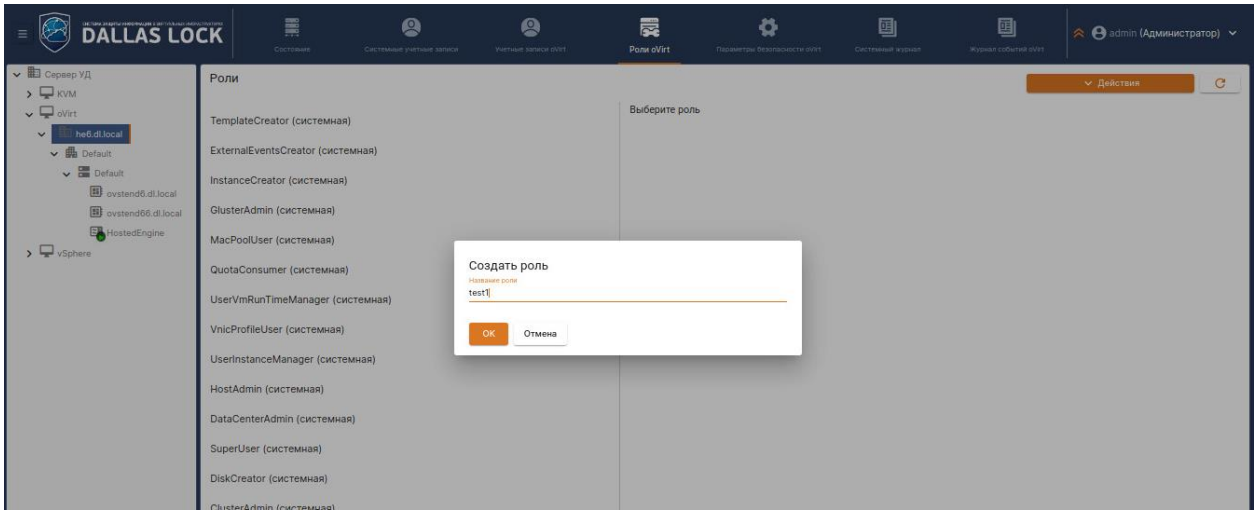

Рисунок 97. Создание роли oVirt

Все роли, за исключением системных ролей, можно переименовывать.

По умолчанию все привилегии для вновь созданных ролей отключены. Для назначения привилегий, необходимо корректно заполнить поле с привилегиями и нажать кнопку **Сохранить** в блоке *Действия*.

После внесения всех необходимых изменений, следует выполнить сохранение путем нажатия кнопки **Сохранить** в блоке *Действия*. Изменения будут применены после синхронизации (подробнее см. п. 3.5 «Синхронизация»).

5.2.2.2 Удаление ролей oVirt

Для удаления роли необходимо выделить роль, которую следует удалить и нажать кнопку **Удалить**. При этом на экране появится предупреждение (см. Рисунок 98).

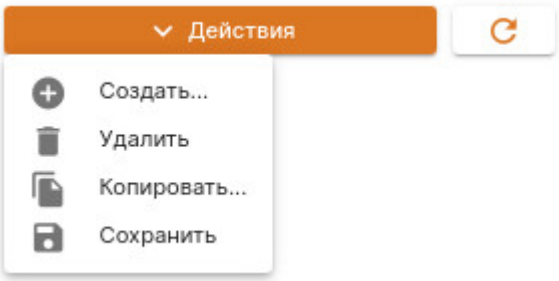

Рисунок 98. Удаление роли oVirt

После чего подтвердить операцию. Изменения вступят в силу при следующей синхронизации (подробнее см. п. 3.5 «Синхронизация»).

После удаления назначенной роли все назначения данной роли удаляются.

Для обновления списка ролей в категории *Действия* необходимо нажать кнопку **Обновить**.

5.2.3 Ролевая модель учетных записей KVM

Настройки по правам администрирования доступа к гипервизорам, объектам ВИ и виртуальным машинам KVM осуществляются средствами ролевой модели разграничения доступа. Для просмотра и редактирования параметров ролевого доступа необходимо в дереве на уровне группы KVM перейти на вкладку *Роли KVM* (см. Рисунок 99).

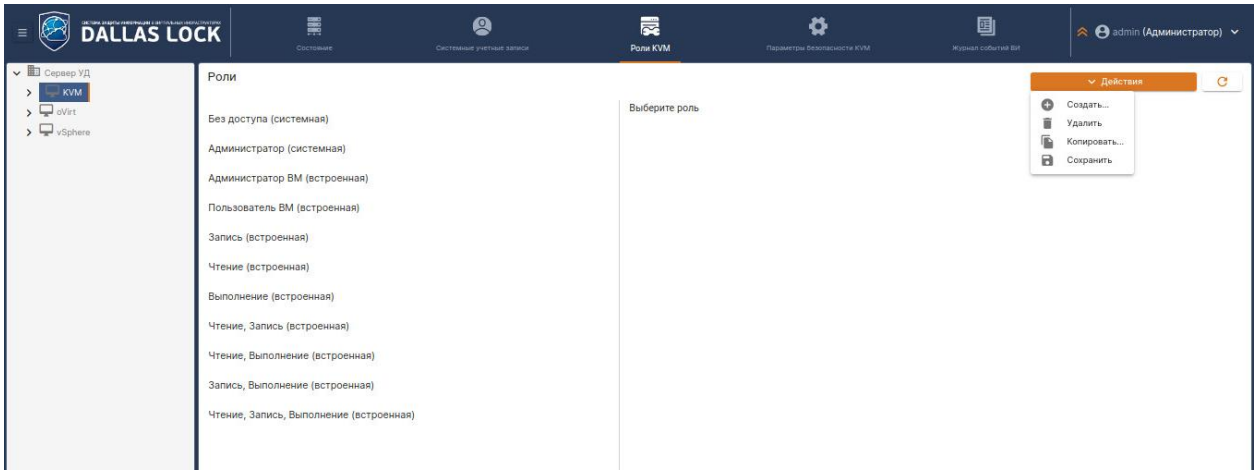

Рисунок 99. Роли KVM

В группе KVM на вкладке *Роли KVM* присутствуют предустановленные роли, которые невозможно изменить (системные). Системные предустановленные роли нельзя изменить или удалить.

Для системных ролей установлены следующие разрешающие привилегии:

- для роли *Администратор (системная)*: включены все привилегии;
- для роли *Без доступа (системная)*: все привилегии отключены.

Предустановленные роли, привилегии которых можно редактировать:

- Администратор ВМ;
- Пользователь ВМ;
- Чтение;
- Запись;
- Выполнение.

Также, следует учитывать, что редактирование ролей осуществляется на общем для всех СВ KVM уровне, следовательно, на каждом СВ KVM всегда создается одинаковый набор ролей.

5.2.3.1 Создание ролей KVM

Для создания новой роли необходимо:

1. Выбрать уровень группы KVM и открыть вкладку *Роли KVM*.
2. Нажать кнопку **Создать…**, ввести имя для новой роли (см. Рисунок 100) и нажать ккнопку **Ок**.

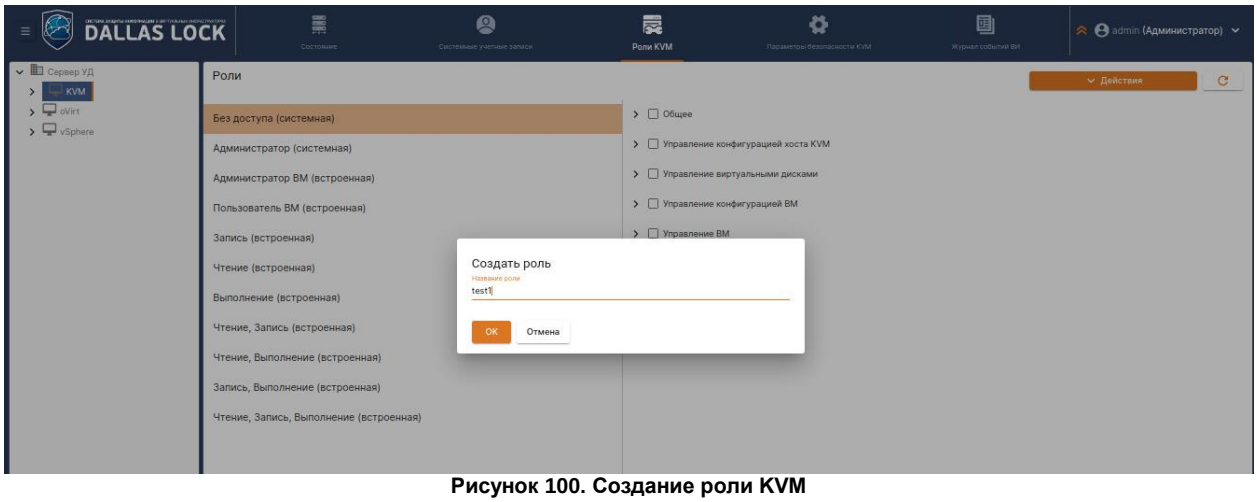

Рисунок 100. Создание роли KVM

3. Выбрать необходимые привилегии для роли и нажать кнопку **Сохранить** в блоке *Действия*.
4. Открыть вкладку *Состояние* и нажать кнопку **Синхронизация СВ и гипервизоров** или выбрать соответствующий пункт из контекстного меню (подробнее см. п. 3.5 «Синхронизация»).

Все роли, за исключением системных ролей, можно переименовывать.

По умолчанию все привилегии для вновь созданных ролей отключены. Для назначения привилегий, необходимо корректно заполнить поле с привилегиями и нажать кнопку **Сохранить** в блоке *Действия*.

После внесения всех необходимых изменений, следует выполнить сохранение путем нажатия кнопки **Сохранить** в блоке *Действия*. Изменения будут применены после синхронизации (подробнее см. п. 3.5 «Синхронизация»).

5.2.3.2 Удаление ролей KVM

Для удаления роли необходимо выделить роль, которую следует удалить и нажать кнопку **Удалить** (см. Рисунок 101).

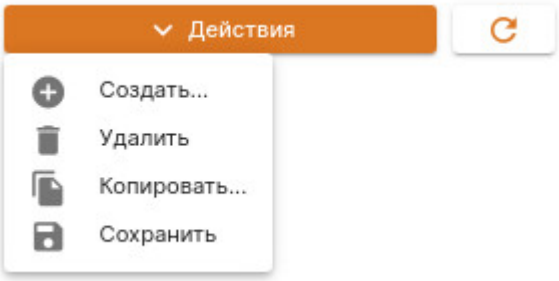

Рисунок 101. Удаление роли KVM

После чего подтвердить операцию. Изменения вступят в силу при следующей синхронизации (подробнее см. п. 3.5 «Синхронизация»).

После удаления назначенной роли все назначения данной роли удаляются.

Для обновления списка ролей в категории *Действия* необходимо нажать кнопку **Обновить**.

5.2.4 Ролевая модель учетных записей oVirt/zVirt/HOSTVM/RedVirt

Настройки по правам администрирования доступа к гипервизорам, объектам ВИ и виртуальным машинам oVirt/zVirt/HOSTVM/RedVirt осуществляются средствами ролевой модели разграничения доступа. Для просмотра и редактирования параметров ролевого доступа необходимо в дереве на уровне СВ oVirt/zVirt/HOSTVM/RedVirt перейти на вкладку *Роли oVirt/zVirt/HOSTVM/RedVirt* (см. Рисунок 102).

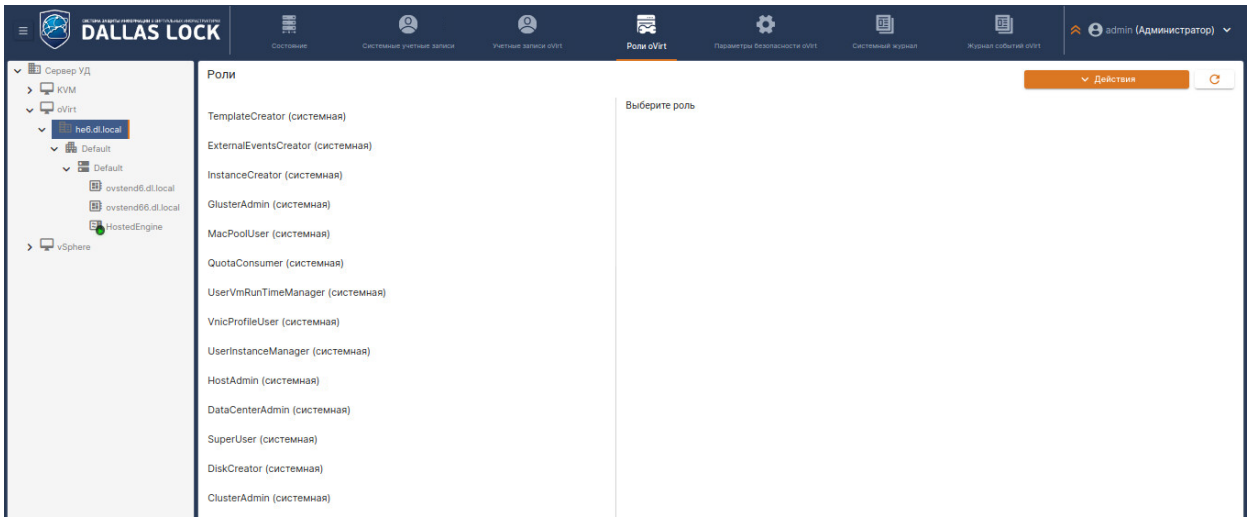

Рисунок 102. Роли oVirt/zVirt/HOSTVM/RedVirt

На уровне СВ oVirt/zVirt/HOSTVM/RedVirt на вкладке *Роли oVirt/zVirt/HOSTVM/RedVirt* присутствуют предустановленные роли, которые невозможно изменить (системные), предустановленные роли, привилегии которых можно редактировать, а также существует возможность создания новых ролей.

Системные предустановленные роли, которые нельзя изменить или удалить, полностью соответствуют стандартным предустановленным ролям oVirt/zVirt/HOSTVM/RedVirt.

5.2.4.1 Создание ролей oVirt/zVirt/HOSTVM/RedVirt

Для создания новой роли необходимо:

1. Выбрать уровень СВ oVirt/zVirt/HOSTVM/RedVirt и открыть вкладку *Роли oVirt/zVirt/HOSTVM/RedVirt*.
2. Нажать кнопку **Создать…** на панели *Действия*, ввести имя для новой роли (см. Рисунок 103) и нажать кнопку **Ок**.

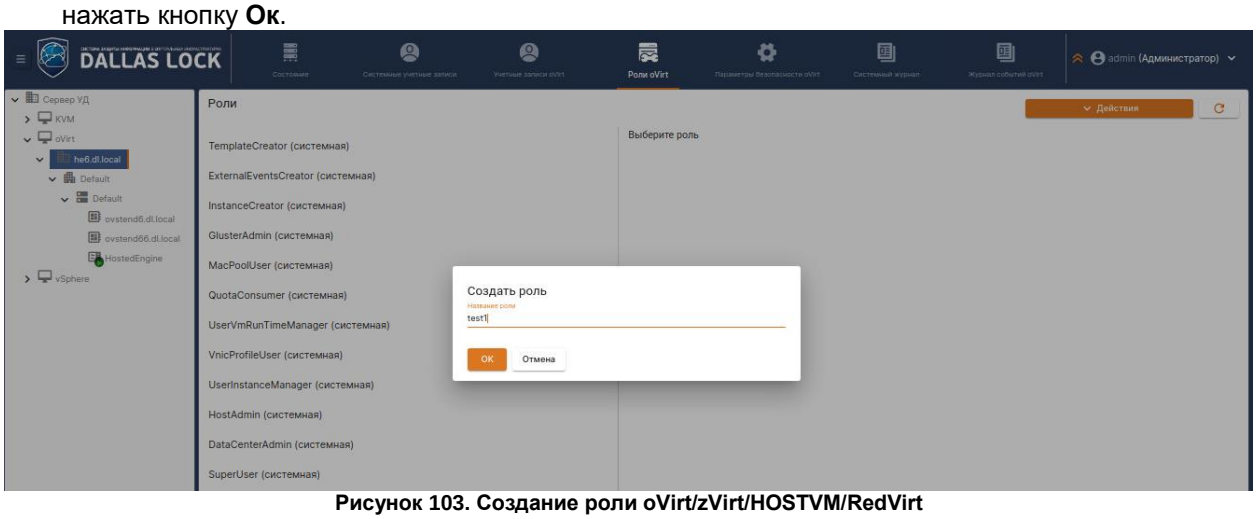

Рисунок 103. Создание роли oVirt/zVirt/HOSTVM/RedVirt

3. Выбрать необходимые привилегии для роли и нажать кнопку **Сохранить** в блоке *Действия*.
4. Открыть вкладку *Состояние* и нажать кнопку **Синхронизация СВ и гипервизоров** или выбрать соответствующий пункт из контекстного меню (подробнее см. п. 3.5 «Синхронизация»).

Все роли, за исключением системных и предустановленных ролей, можно переименовывать.

По умолчанию все привилегии для вновь созданных ролей отключены. Для назначения привилегий, необходимо корректно заполнить поле с привилегиями и нажать кнопку **Сохранить** в блоке *Действия*.

После внесения всех необходимых изменений, следует выполнить сохранение путем нажатия кнопки **Сохранить** в блоке *Действия*. Изменения будут применены после синхронизации (подробнее см. п. 3.5 «Синхронизация»).

5.2.4.2 Удаление ролей oVirt/zVirt/HOSTVM/RedVirt

Для удаления роли необходимо выделить роль, которую следует удалить и нажать кнопку **Удалить** во вкладке *Действия* (см. Рисунок 104).

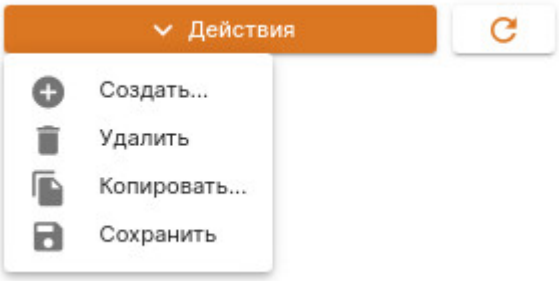

Рисунок 104. Удаление роли oVirt/zVirt/HOSTVM/RedVirt

После чего подтвердить операцию. Изменения вступят в силу при следующей синхронизации (подробнее см. п. 3.5 «Синхронизация»).

После удаления назначенной роли все назначения данной роли удаляются.

Для обновления списка ролей в категории *Действия* необходимо нажать кнопку **Обновить**.

5.2.5 Права пользователей

Назначение ролей может осуществляться на уровне СВ или гипервизора при этом настройки СВ могут наследоваться (подробнее см. п. 3.7 «Наследование настроек»).

Просмотр и редактирование прав пользователей для vSphere происходит на уровне Сервера виртуализации в категории **Параметры безопасности vSphere → Права пользователей** (см. Рисунок 105).

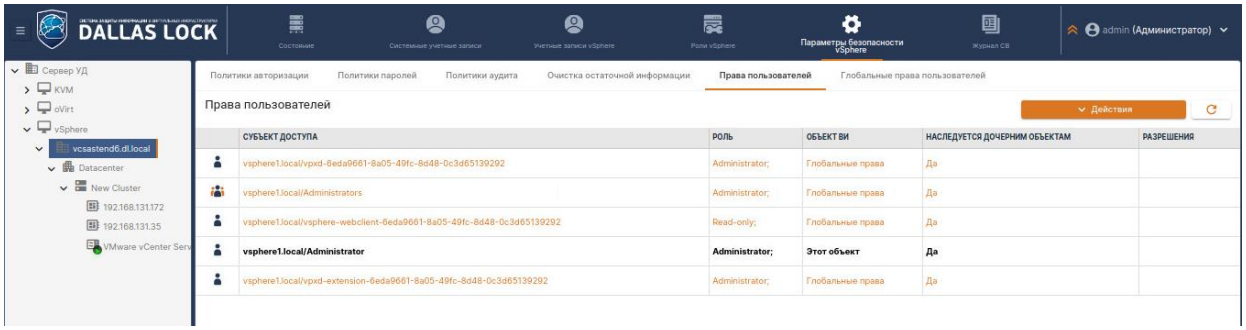

Рисунок 105. Права пользователей vSphere

Просмотр и редактирование прав пользователей для oVirt происходит на уровне Сервера виртуализации в категории **Параметры безопасности oVirt → Права пользователей** (см. Рисунок 106).

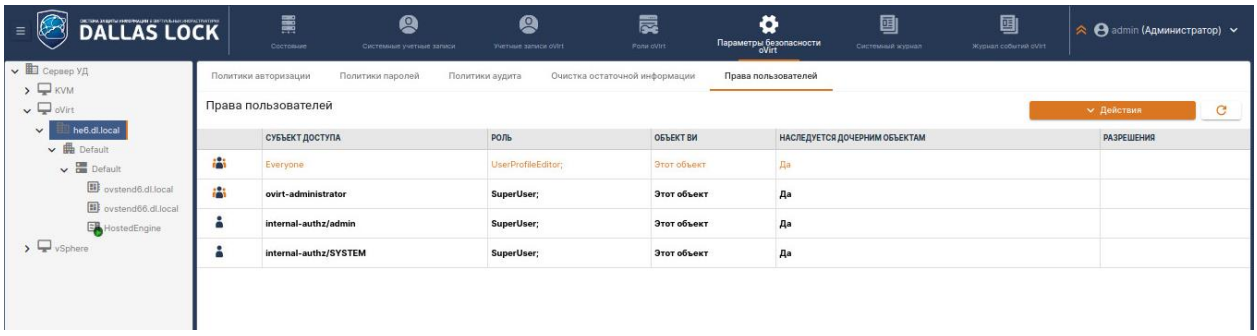

Рисунок 106. Права пользователей oVirt

Просмотр и редактирование прав пользователей для KVM происходит на уровне Сервера виртуализации в категории **Параметры безопасности KVM → Права пользователей** (см. Рисунок 107).

Для предоставления доступа новому пользователю к управлению ВМ необходимо добавить данного пользователя в следующие группы:

1. Для ОС Linux Mint – libvirt.
2. Для ОС Ubuntu – libvirt, kvm.
3. Для ОС Astra Linux (Орел 1.7) – kvm, libvirt, libvirt-qemu.
4. Для ОС Astra Linux (Смоленск 1.7) – kvm, libvirt, libvirt-qemu, libvirt-admin.
5. Для ОС CentOS – libvirt, kv

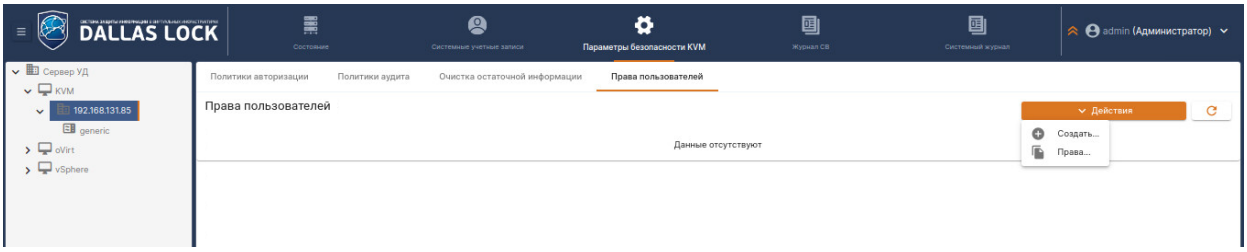

Рисунок 107. Права пользователей KVM

Просмотр и редактирование прав пользователей для oVirt/zVirt/HOSTVM/RedVirt происходит на уровне Сервера виртуализации в категории **Параметры безопасности oVirt → Права пользователей** (см. Рисунок 108).

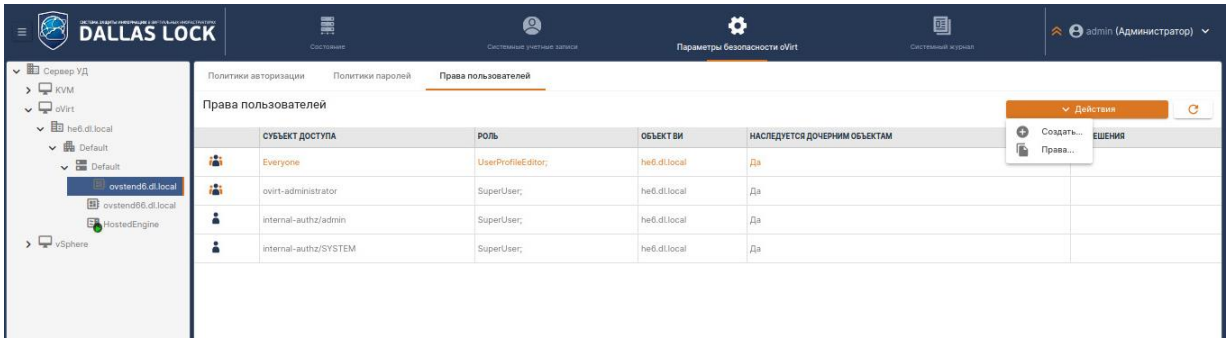

Рисунок 108. Права пользователей oVirt/zVirt/HOSTVM/RedVirt

Для пользователя или группы может быть назначена только одна роль на объект, однако, привилегии для пользователя могут суммироваться, если он состоит в нескольких группах, для которых назначены разные роли на объект.

Исключением является случай, когда роль явно назначается пользователю. В таком случае она перекрывает все привилегии, полученные от групп.

Чтобы задать пользователю или группе определенную роль необходимо:

1. Выбрать уровень Сервера виртуализации и открыть категорию **Параметры безопасности СВ → Права пользователей**.
2. Нажать кнопку **Создать…**, после чего появится окно со списком пользователей и групп, которым будет задана роль (см. Рисунок 109).

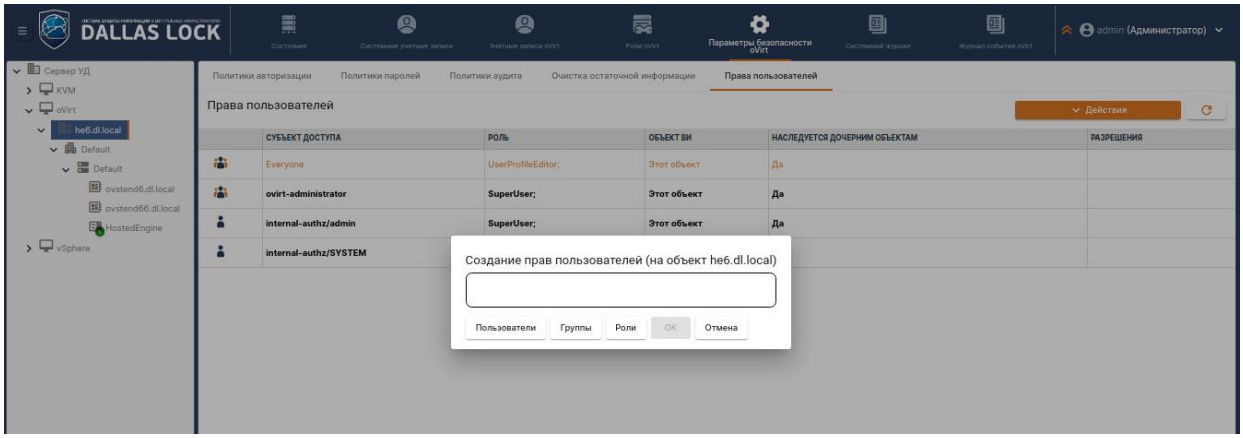

Рисунок 109. Выбор пользователей и групп

3. Далее требуется выбрать пользователей и группы, которым будет задана роль, после чего нажать **ОК** (см. Рисунок 110).

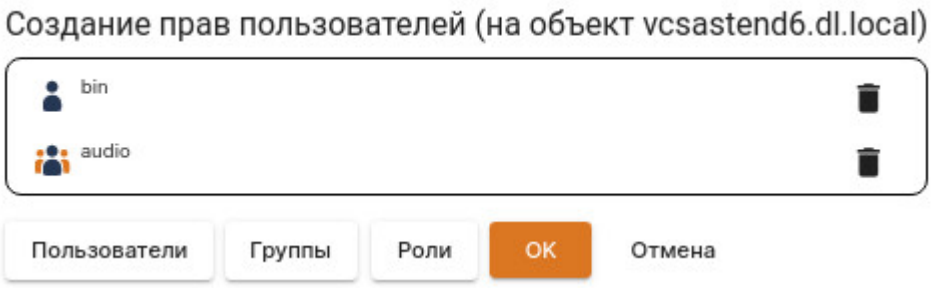

Рисунок 110. Выбор пользователей и групп

4. В появившемся окне выбрать роль из выпадающего списка (см. Рисунок 111).

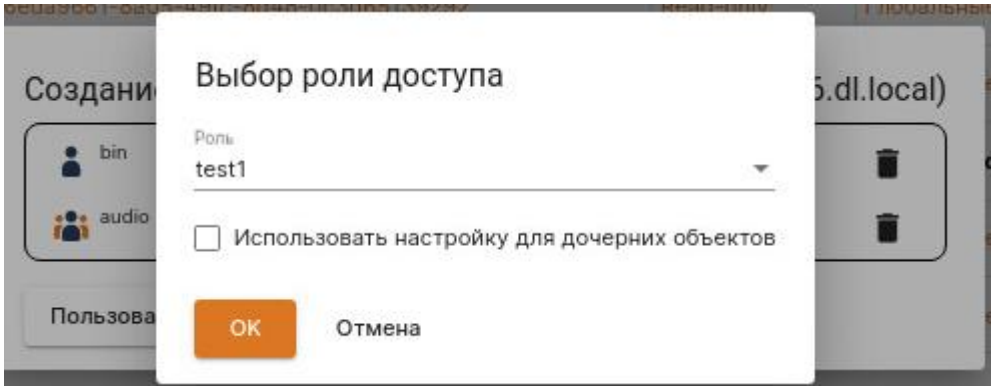

Рисунок 111. Выбор роли доступа

5. Чтобы распространить привилегии на дочерние объекты, необходимо установить флаг *Настройка действует на дочерние объекты*.

При назначении роли для KVM рекомендуется всегда устанавливать данный флаг.

6. Нажать кнопку **ОК**.
7. Сохранить изменения, нажав кнопку **Сохранить**.
8. Открыть вкладку *Состояние* и нажать кнопку **Синхронизация СВ и гипервизоров**.

Для редактирования прав пользователей необходимо:

1. Выделить нужную учетную запись или группу и выбрать действие **Редактировать**.
2. В появившемся окне выбрать роль из выпадающего списка.
3. Чтобы распространить привилегии на дочерние объекты, необходимо установить флаг *Настройка действует на дочерние объекты*.
4. Нажать кнопку **ОК**.
5. Сохранить изменения, нажав кнопку **Сохранить**.
6. Открыть вкладку *Состояние* и нажать кнопку **Синхронизация СВ и гипервизоров**.

Для удаления прав пользователей необходимо выбрать учетную запись или группу и нажать кнопку **Удалить**. После чего подтвердить операцию, сохранить изменения и синхронизировать.

Для обновления списка учетных записей в категории *Действия* необходимо нажать кнопку **Обновить**.

5.2.5.1 Глобальные права пользователей vSphere

Глобальные права доступа пользователей имеют наивысший приоритет и автоматически наследуются на дочерние объекты ВИ.

Осуществлять настройку глобальных прав пользователей может только суперадминистратор.

Для просмотра, добавления, удаления и редакции глобальных прав доступа пользователей необходимо на уровне Сервера виртуализации перейти к категории **Параметры безопасности vSphere → Глобальные права пользователей** (см. Рисунок 112).

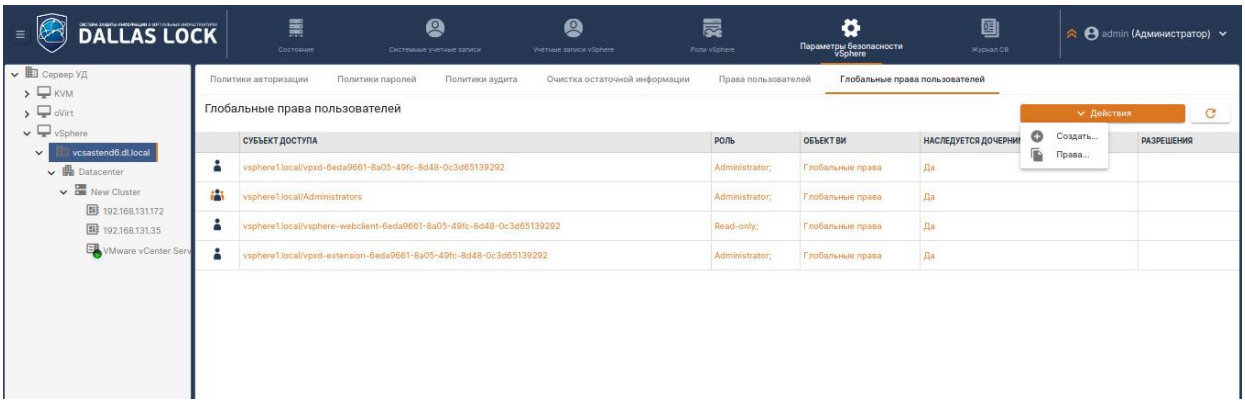

Рисунок 112. Глобальные права доступа пользователей vSphere

Глобальные права можно назначить пользователю либо группе пользователей. Для этого необходимо:

1. В категории «*Действия*» нажать кнопку **Создать…**.
2. В появившемся окне нажать кнопку **Группы**, **Пользователи** или **Роли**.
3. Выбрать одну или несколько групп, или пользователей (см. Рисунок 113), нажать кнопку **ОК**.

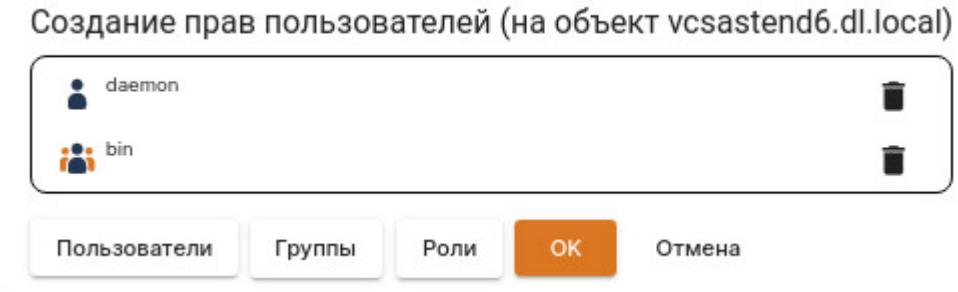

Рисунок 113. Добавление учетных записей

4. Нажать кнопку **ОК**.

Для изменения роли учетной записи и наследования настройки для дочерних объектов, необходимо выбрать учетную запись и в контекстном меню, вызываемом нажатием правой кнопкой мыши на учетной записи, нажать кнопку «Редактировать». В появившемся окне выбрать необходимые параметры, нажать кнопку **ОК**.

Для удаления учетной записи, которой назначены глобальные права, необходимо выбрать учетную запись и в контекстном меню, вызываемом нажатием правой кнопкой мыши на учетной записи, нажать кнопку **Удалить**.

Просмотр, добавление, удаление и редактирование учетных записей, наделенных глобальными правами на уровне гипервизоров, производится на вкладках **Параметры безопасности** → **Права пользователей**.

Изменения вступят в силу при следующей синхронизации (подробнее см. п. 3.5 «Синхронизация»).

5.2.5.2 Назначение прав пользователям vSphere

1. Для назначения разрешений пользователю, на уровне СВ следует перейти на вкладку *Параметры безопасности vSphere*, выбрать категорию **Права пользователей**, во вкладке действия нажать кнопку **Создать…** (см. Рисунок 114).

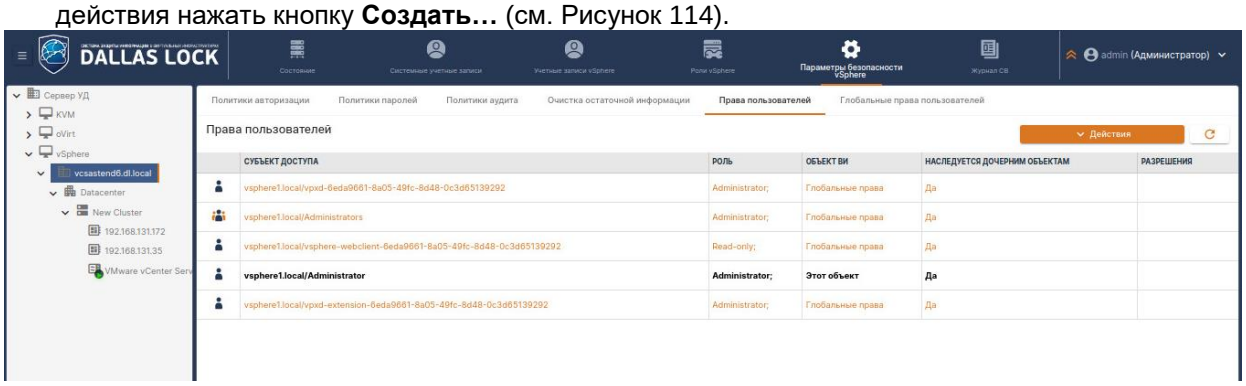

Рисунок 114. Добавление учетной записи

2. В появившемся окне нажать кнопку **Группы**, **Пользователи** или **Роли**.

3. Выбрать размещение группы или пользователя из выпадающего меню (см. Рисунок 115), после чего выбрать из списка одну или несколько групп, или пользователей и нажать кнопку **ОК**.

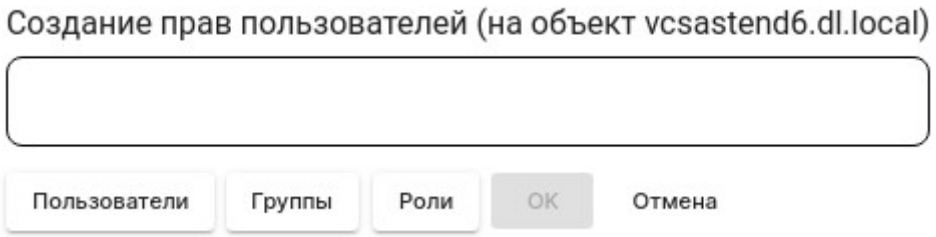

Рисунок 115. Выбор учетной записи

4. В появившемся окне выбрать роль для учетной записи из выпадающего списка и нажать на кнопку **ОК**.
5. Изменения вступят в силу при следующей синхронизации (подробнее см. п. 3.5 «Синхронизация»).

5.2.5.3 Назначение прав пользователям гипервизора ESXi

Назначение прав пользователям гипервизора осуществляется на уровне гипервизора во вкладке «Параметры безопасности vSphere».

Перед назначением прав пользователям, необходимо убедиться, что данные учетные записи активированы (подробнее см. п. 4.1.4 «Активация и деактивация учетных записей»).

1. Для назначения разрешений локальному пользователю гипервизора, следует выбрать категорию **Права пользователей гипервизоров**, в блоке *Действия* нажать кнопку **Создать…**.
2. В появившемся окне необходимо нажать кнопку **Пользователи**, после чего выбрать из списка учетную запись и нажать кнопку **ОК** в обеих окнах (см. Рисунок 116).

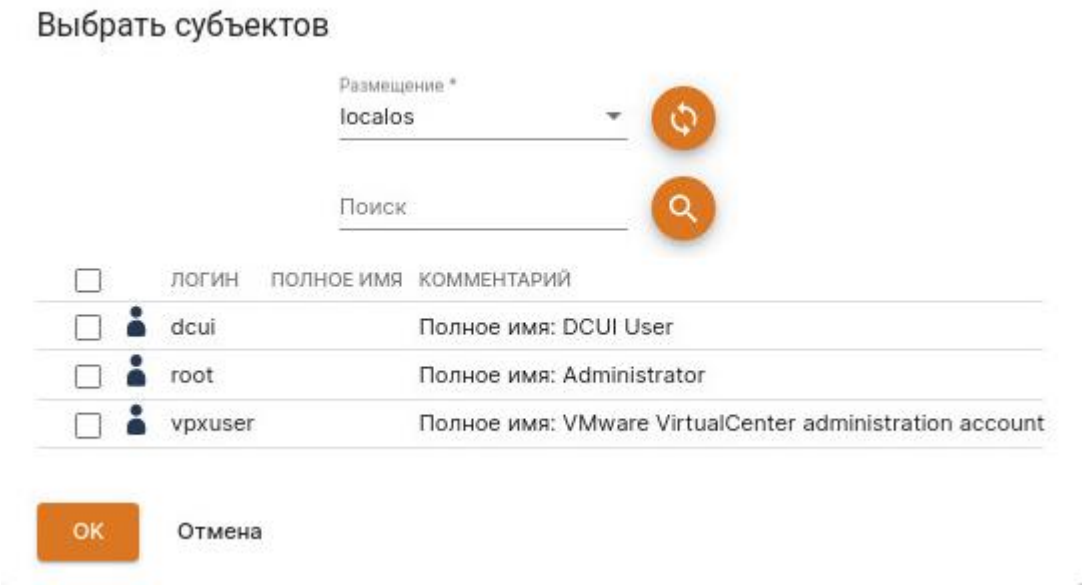

Рисунок 116. Выбор учетной записи

3. В появившемся окне выбрать роль из выпадающего меню для учетной записи из выпадающего списка (см. Рисунок 117) и нажать на кнопку **ОК**.

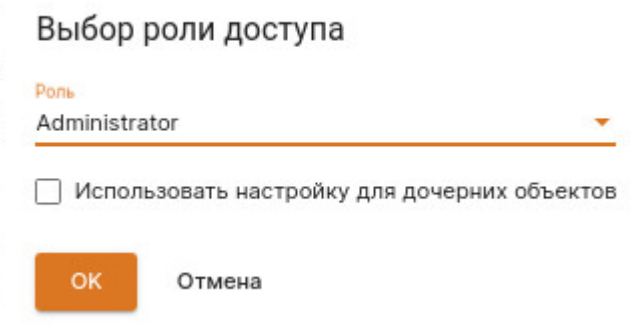

Рисунок 117. Выбор роли

4. Изменения вступят в силу при следующей синхронизации (подробнее см. п. 3.5 «Синхронизация»).

5.2.5.4 Назначение прав доменным пользователям гипервизора ESXi

1. Для назначения разрешений доменным пользователям или группам, следует выбрать категорию **Права пользователей**, в блоке *Действия* нажать кнопку **Создать…**.
2. В появившемся окне необходимо нажать кнопку **Группы** или **Пользователи**, после чего выбрать из выпадающего меню размещение групп или пользователей. Далее из списка выбрать одну или несколько групп, или пользователей и нажать кнопку **ОК** в обеих окнах (см. Рисунок 118).

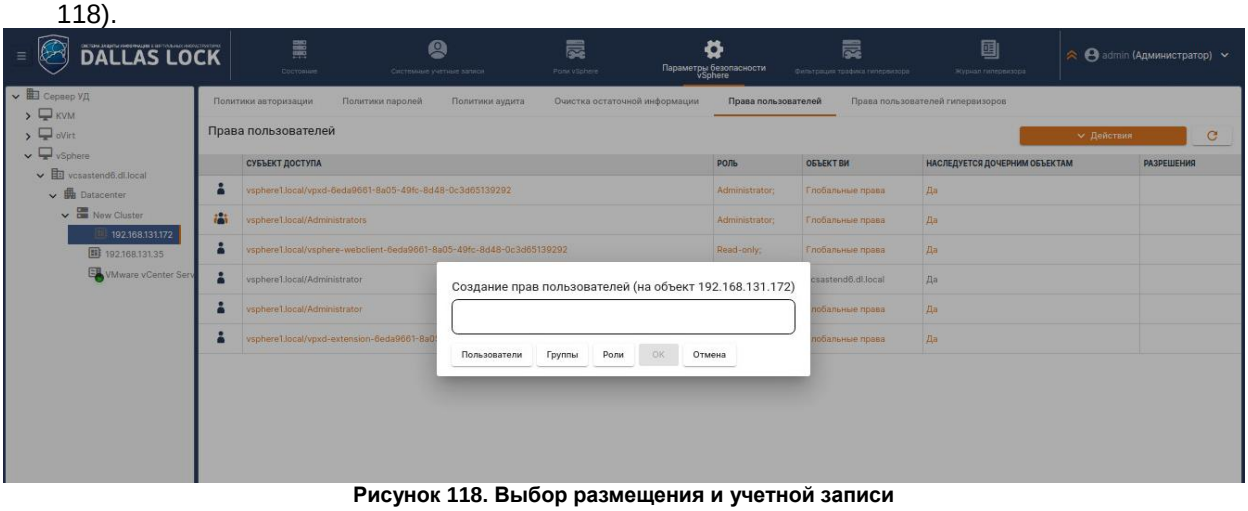

Рисунок 118. Выбор размещения и учетной записи

3. В появившемся окне выбрать роль из выпадающего меню для учетной записи из выпадающего списка и нажать на кнопку **ОК**. (см. Рисунок 119). Чтобы распространить привилегии на дочерние объекты, необходимо установить флаг *Использовать настройку для дочерних объектов*.

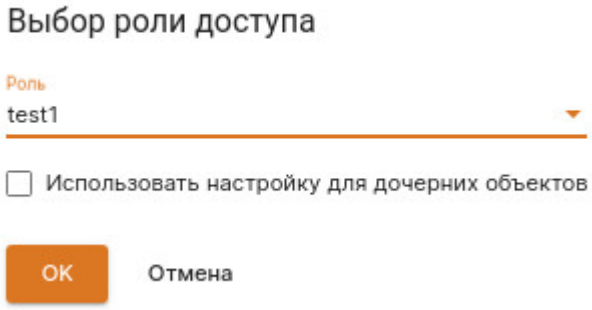

Рисунок 119. Выбор роли

4. Изменения вступят в силу при следующей синхронизации (подробнее см. п. 3.5 «Синхронизация»).

5.2.5.5 Упрощенное назначение прав доступа пользователям

Данная опция позволяет назначать права доступа пользователям к объектам ВИ по средствам выбора типа действия с объектом ВИ.

Доступны следующие типы действий:

- Чтение;
- Запись;
- Выполнение.

Для назначения прав доступа необходимо:

1. Выбрать уровень СВ, гипервизора или ВМ и открыть категорию **Параметры безопасности** → **Права пользователей**, в блоке *Действия* нажать кнопку **Права** (см. Рисунок 120).

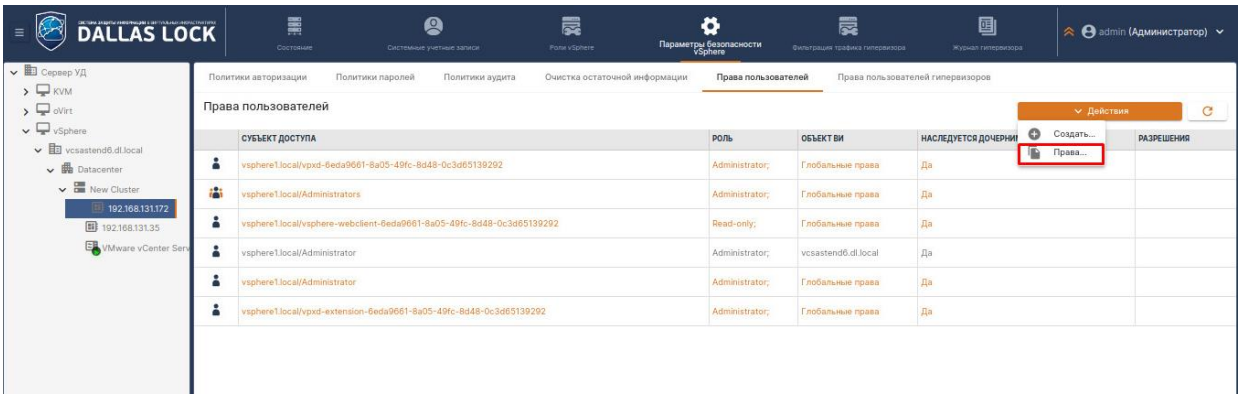

Рисунок 120. Упрощенное назначение прав

2. В появившемся окне нажать кнопку **Группы** либо **Пользователи**.
   Отметив пункт *Автоматический поиск пользователей/групп* при последующем нажатии кнопок **Пользователи** или **Группы** будет показан список всех возможных пользователей или групп для последующего назначения роли.
3. Выбрать размещение группы или пользователя из выпадающего меню (см. Рисунок 121), после чего выбрать из списка одну или несколько групп, или пользователей и нажать кнопку «ОК» в обеих окнах.

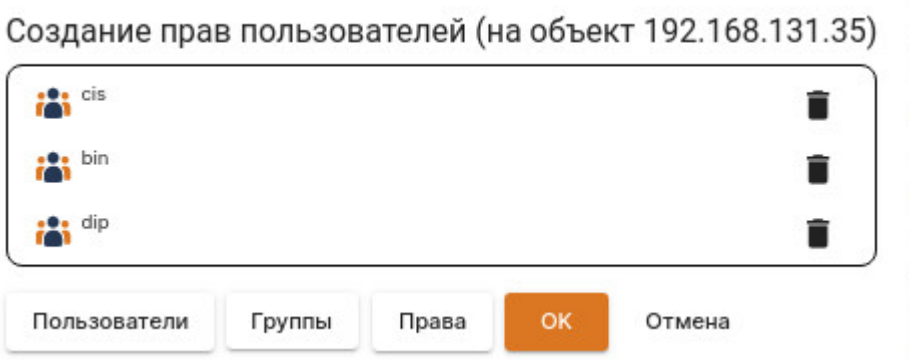

Рисунок 121. Выбор учетной записи

4. Далее нажать на кнопку **Права** и впоявившемся окне выбрать разрешенные действия, для назначения соответствующей роли и нажать на кнопку **ОК** (см. Рисунок 122). Чтобы распространить привилегии на дочерние объекты, необходимо установить флаг *Использовать настройку для дочерних объектов*.

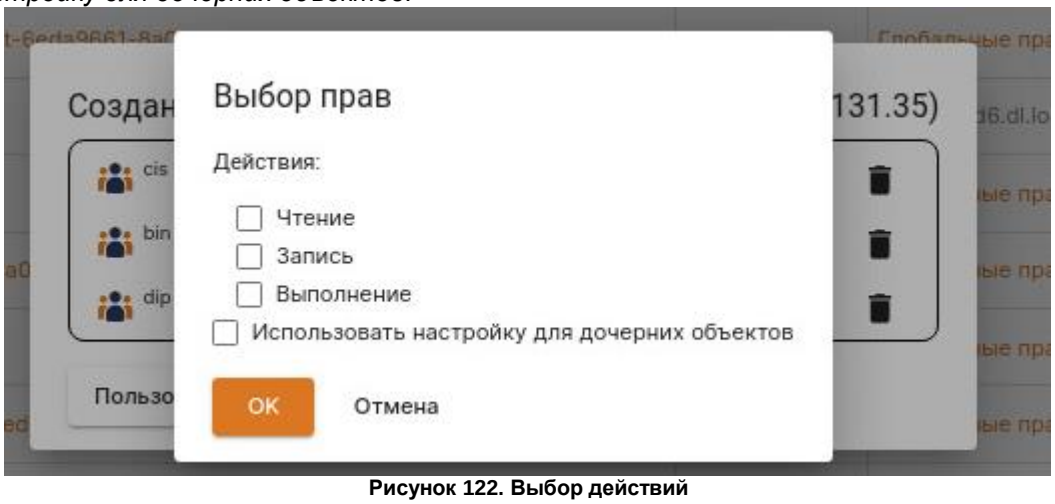

Рисунок 122. Выбор действий

5. Изменения вступят в силу при следующей синхронизации (подробнее см. п. 3.5 «Синхронизация»).

5.3 Настройка фильтрации трафика гипервизоров ESXi

Гипервизор ESXi включает в себя брандмауэр между интерфейсом управления и сетью. По умолчанию брандмауэр гипервизора настроен на блокирование входящего и исходящего трафика, за исключением трафика для его стандартных служб.

Просмотр и редактирование списка правил фильтрации трафика для всех гипервизоров происходит на уровне гипервизора ESXi на вкладке **Фильтрация трафика гипервизора** (см. Рисунок 123).

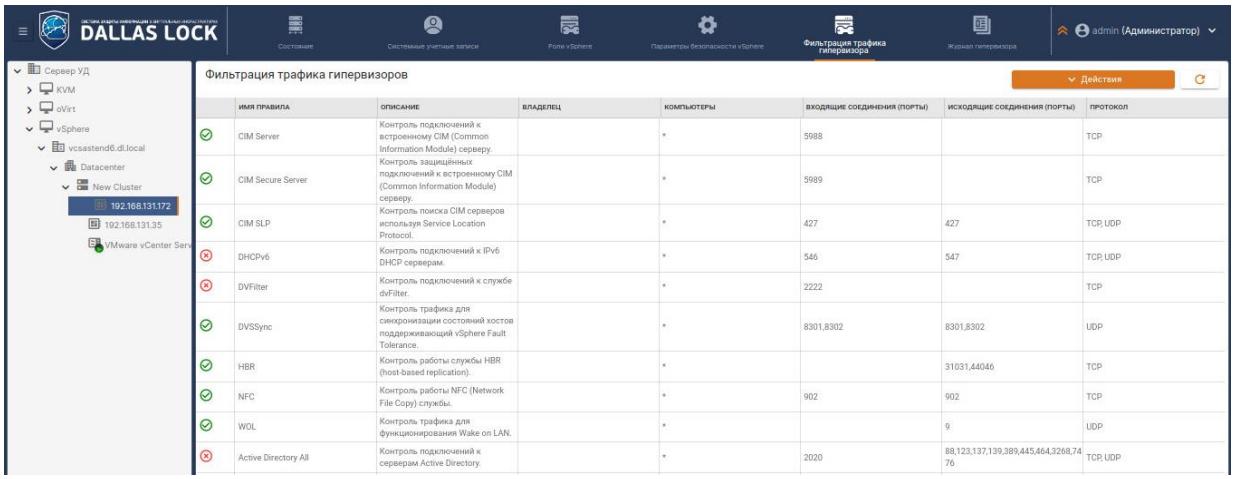

Рисунок 123. Фильтрация трафика гипервизора

После добавления гипервизора в ВИ DL выполняется вычитывание списка правил фильтрации гипервизора. Далее эти правила пополняют общий список правил **ЦУ СЗИ ВИ** на уровне гипервизора на вкладке *Фильтрация трафика гипервизора*. В общий список правил добавляются только новые правила с оригинальным именем.

Если при вычитывании правил, имя правила гипервизора совпадает с именем правила из общего списка, но имеет другое значение (порт, IP-адрес и т.д.), то данное правило не добавляется в общий список и отмечается на уровне добавленного гипервизора как оригинальное (т.е. не наследуется).

Если при вычитывании правил, имя правила гипервизора совпадает с именем правила из общего списка и имеет такое же значение, то данное правило отмечается на уровне гипервизора как наследуемое (см. п. 3.7 «Наследование настроек»).

Редакция (переопределение) правил фильтрации доступно для каждого отдельного гипервизора. Для этого необходимо перейти на уровень гипервизора во вкладку *Фильтрация трафика гипервизора* (см. Рисунок 124). Здесь:

— отмеченное таким значком поле означает, что правило включено.

— отмеченное таким значком поле означает, что правило выключено.

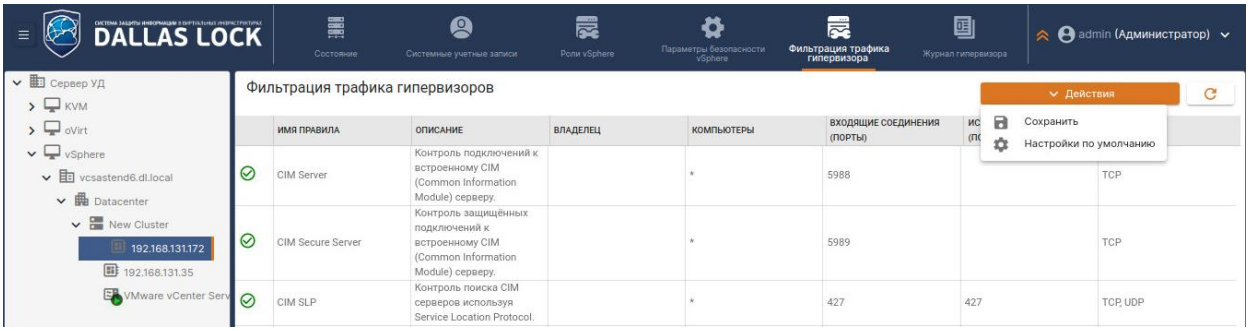

Рисунок 124. Переопределение правил фильтрации на гипервизоре

После формирования списка правил необходимо нажать кнопку **Сохранить** в блоке *Действия*, после чего перейти на вкладку *Состояние* и нажать кнопку **Синхронизация СВ и гипервизоров**.

Для работы с хранилищем данных NFS необходимо используя веб-консоль включить правило «NFS Client» (см. Рисунок 125).

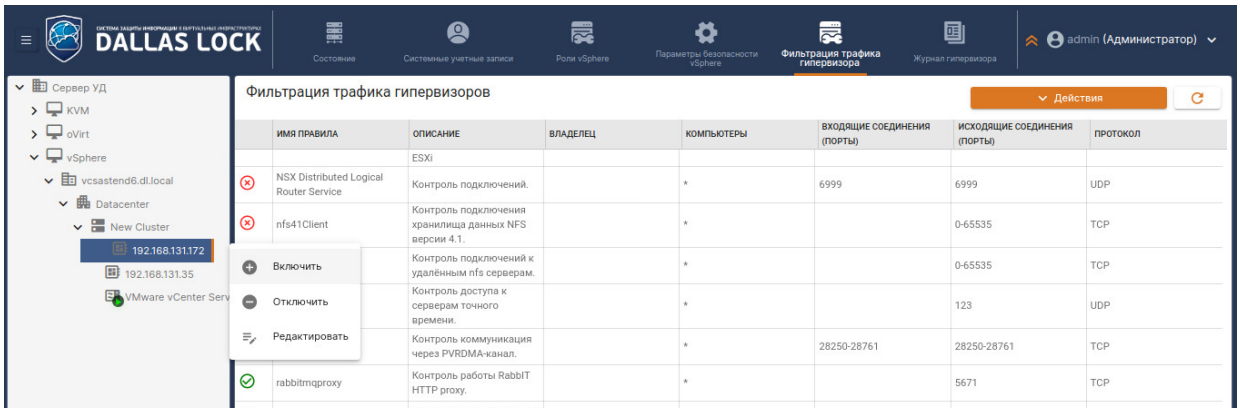

Рисунок 125. Правило «NFS Client»

Для редактирования правила фильтрации для всех гипервизоров ВИ, необходимо:

1. Выбрать уровень гипервизора и открыть вкладку *Фильтрация трафика гипервизора*.
2. Выделить необходимую службу и левой кнопкой мыши нажать на правило. Далее нажать кнопку **Редактировать**.
3. В появившимся окне **Изменение правила** можно будет посмотреть настройки правила (см. Рисунок 126). В этом окне можно изменить: описание, владелец, компьютеры. В строке компьютеры значком «*» показывается, что это правило включается для всех компьютеров.

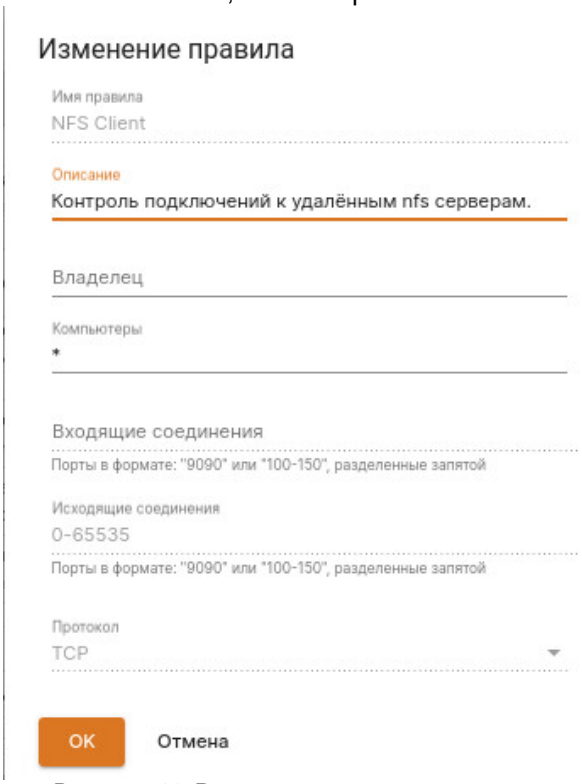

Рисунок 126. Вкладка редактирования правила

4. По завершению редактирования правила, необходимо нажать кнопку **ОК**.
5. Далее нажать кнопку **Сохранить** в блоке *Действия*.
6. Открыть вкладку *Состояние* и нажать кнопку **Синхронизация СВ и гипервизоров**.

5.4 Сегменты безопасности

СЗИ ВИ позволяет разделять виртуальные инфраструктуры (vSphere/vCSA) на сегменты безопасности.

После назначения сегмента безопасности пользователи могут работать только с теми объектами, доступ к которым им разрешен, и совершать над ними только санкционированные операции. По умолчанию все пользователи имеют доступ ко всем объектам. Механизм сегментов безопасности основывается на предоставлении пользователю прав на определенные операции с объектами.

В качестве объектов доступа, выделяемых в сегмент, выступают виртуальные машины (ВМ), виртуальный адаптер, виртуальный маршрутизатор и хранилище данных.

В качестве субъектов доступа к сегменту выступают следующие типы субъектов:

- локальные учетные записи/группы ОС Linux;
- учетные записи/группы, созданные средствами Active Directory.

5.4.1 Настройка сегментов безопасности на уровне группы vSphere

Просмотр и редактирование сегментов безопасности происходит на уровне группы vSphere во вкладке *Состояние* в категории **Сегменты безопасности** (см. Рисунок 127).

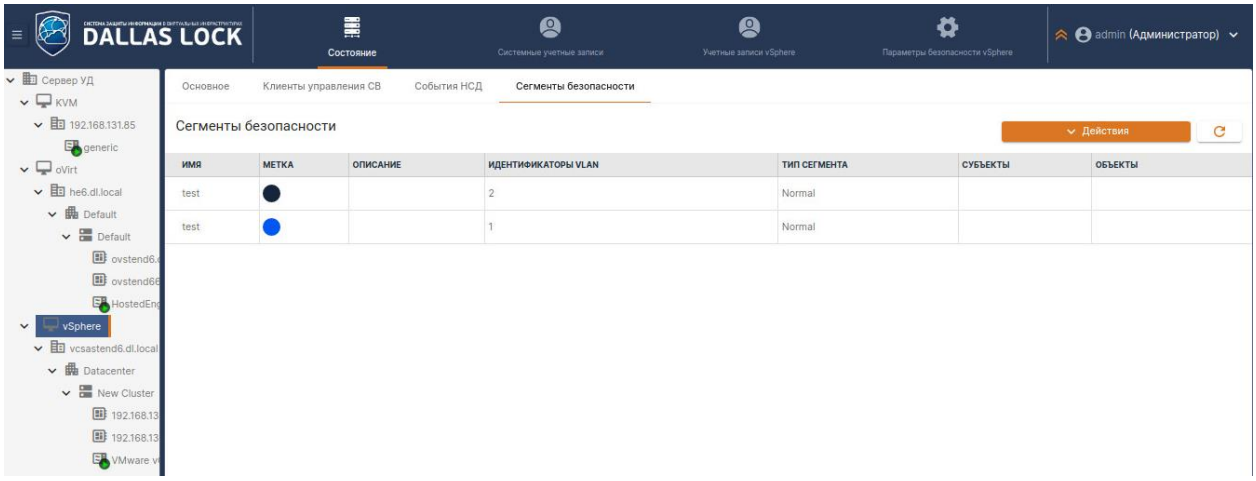

Рисунок 127. Сегменты безопасности на уровне группы

5.4.1.1 Создание сегмента безопасности на уровне группы vSphere

Для создания метки безопасности необходимо:

1. Развернуть блок *Действия* и выбрать кнопку **Создать** (см. Рисунок 128):

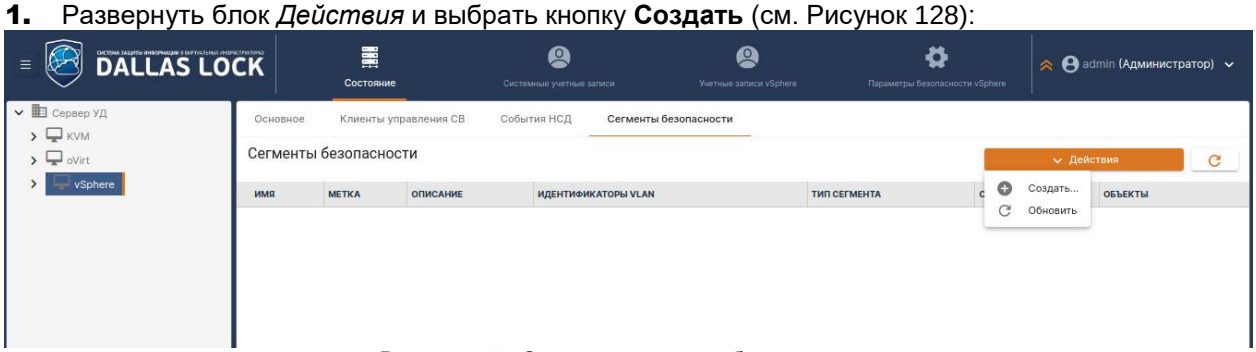

Рисунок 128. Создание сегмента безопасности

2. В появившемся окне (см. Рисунок 129) ввести имя сегмента, описание (опционально), если требуется, поле *Идентификаторы VLAN* (активна если убрать чекбокс *Генерировать vlan*), выбрать цвет метки (см. Рисунок 130), после чего нажать кнопку **ОК**.

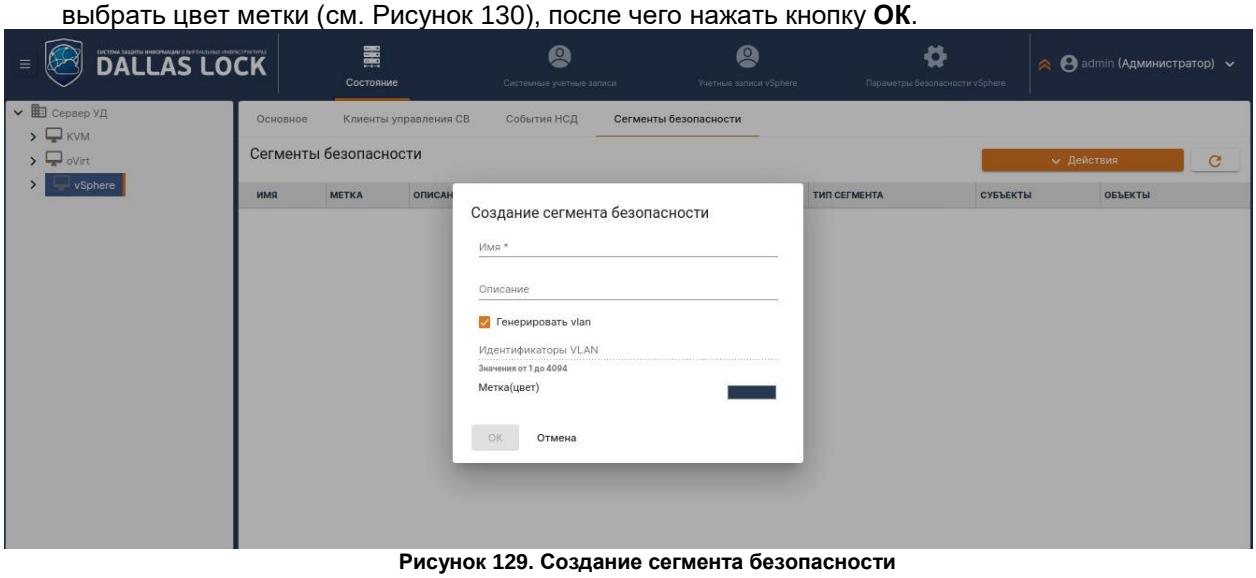

Рисунок 129. Создание сегмента безопасности

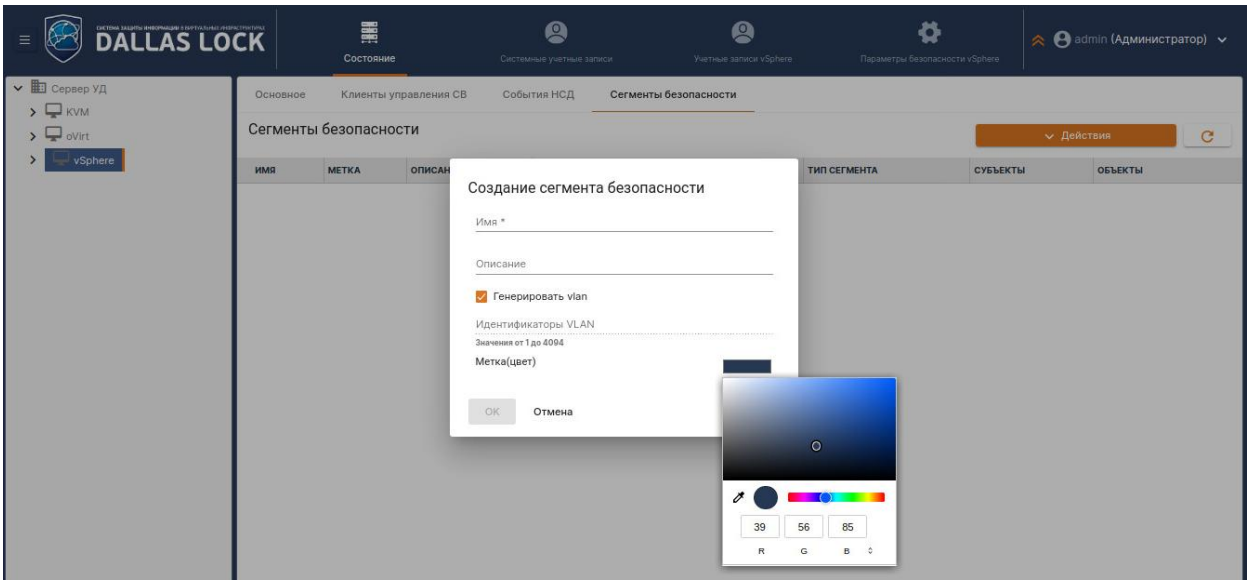

Рисунок 130. Выбор цвета метки

3. Изменения вступят в силу при следующей синхронизации (подробнее см. п. 3.5 «Синхронизация»).

5.4.1.2 Добавление объекта ВИ в сегмент безопасности

> **!** Добавление объекта ВИ в сегмент безопасности происходит только на уровне ВМ раздела vSphere.

Для добавления объекта ВИ в сегмент безопасности необходимо:

1. Перейти на уровень ВМ в разделе vSphere.

2. В блоке *Действия* нажать кнопку **Сегмент безопасности** (см. Рисунок 131).

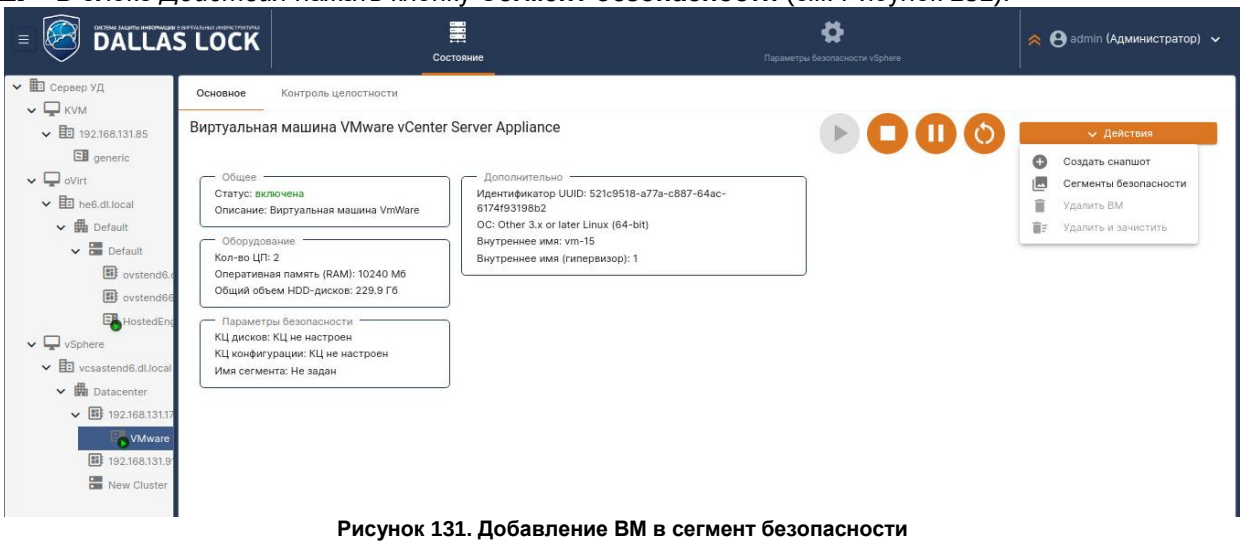

Рисунок 131. Добавление ВМ в сегмент безопасности

3. В появившемся окне выбрать нужный сегмент из выпадающего списка (см. Рисунок 132).

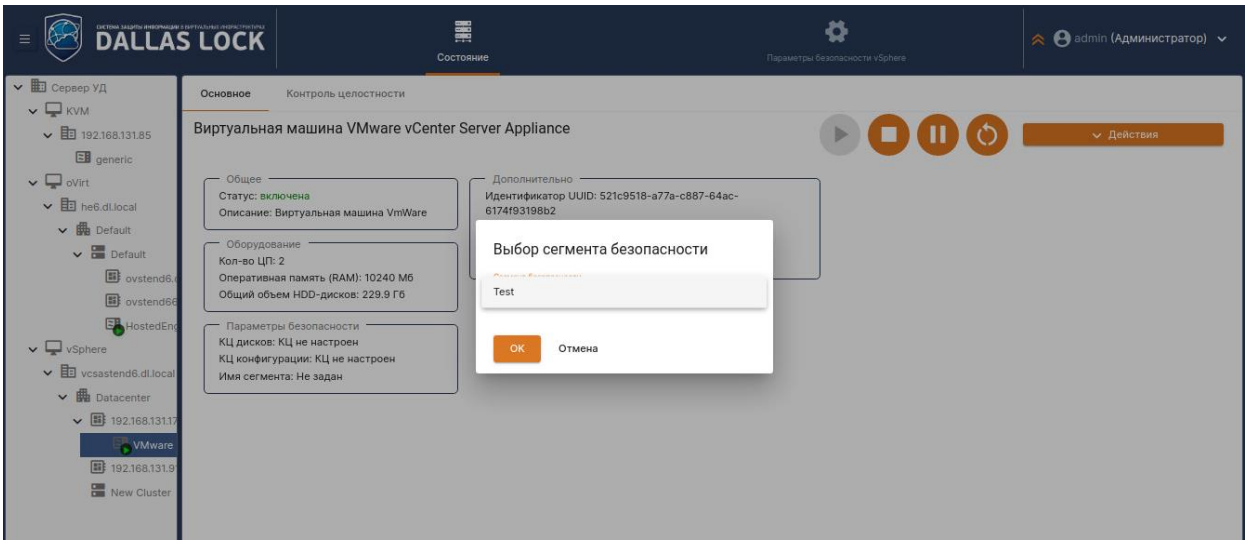

Рисунок 132. Выбор сегмента безопасности

4. Нажать кнопку **ОК** (см. Рисунок 133).

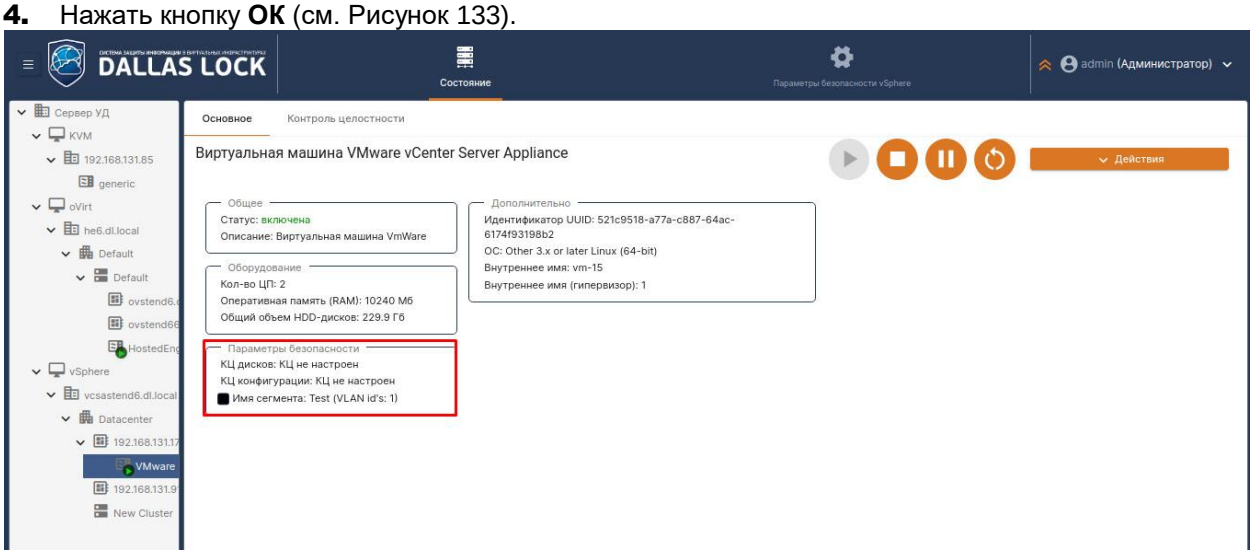

Рисунок 133. Результат добавления ВМ в сегмент безопасности

5. Изменения вступят в силу при следующей синхронизации (подробнее см. п. 3.5 «Синхронизация»).

5.4.1.3 Удаление объекта ВИ из сегмента безопасности

1. Порядок действий для удаления объекта ВИ из сегмента безопасности аналогичен п. 5.4.1.2, за исключением того, что в окне выбора сегмента безопасности в выпадающем списке необходимо выбрать пустой пункт (см. Рисунок 134).

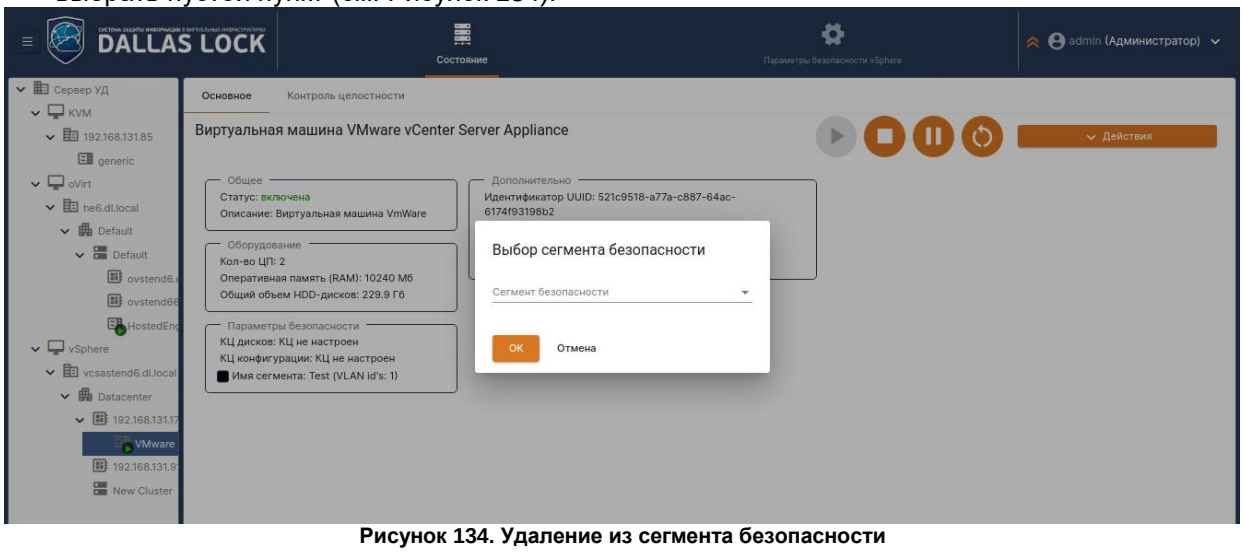

Рисунок 134. Удаление из сегмента безопасности

2. Нажать кнопку **ОК**.
3. Изменения вступят в силу при следующей синхронизации (подробнее см. п. 3.5 «Синхронизация»).

5.4.1.4 Редактирование сегмента безопасности

Для редактирования сегмента безопасности необходимо:

1. Открыть категорию **Состояние** на уровне группы vSphere → **Сегменты безопасности**.
2. ЛКМ выбрать в списке необходимый сегмент безопасности.
3. Нажать кнопку **Изменить**.
4. После внесения изменений нажать кнопку **ОК**.
5. Изменения вступят в силу при следующей синхронизации (подробнее см. п. 3.5 «Синхронизация»).

5.4.1.5 Удаление сегмента безопасности

Для удаления сегмента безопасности необходимо:

1. Открыть категорию **Состояние** на уровне группы vSphere → **Сегменты безопасности**.
2. ЛКМ выбрать в списке необходимый сегмент безопасности.
3. Нажать кнопку **Удалить**.
4. Изменения вступят в силу при следующей синхронизации (подробнее см. п. 3.5 «Синхронизация»).

6 ПОДСИСТЕМА КОНТРОЛЯ ЦЕЛОСТНОСТИ

СЗИ ВИ включает в свой состав подсистему обеспечения целостности. Она позволяет контролировать целостность файлов агентов **СЗИ ВИ**, файлов гипервизора, файлов дисков и конфигурации виртуальных машин, а также аппаратной конфигурации СВ и гипервизоров.

Основу механизмов контроля целостности представляет проверка соответствия контролируемого объекта эталонному образцу. Для этого используются контрольные суммы.

Процедура контроля целостности осуществляется следующим образом: после назначения дескриптора целостности при следующей проверке проверяется, было ли уже вычислено эталонное значение контрольной суммы параметра. Если оно еще не было вычислено, оно вычисляется и сохраняется. Если же оно уже было вычислено, то оно сравнивается с вычисляемым текущим значением контрольной суммы контролируемого параметра. Если хотя бы для одного из проверяемых параметров текущее значение параметра не совпало с эталонным значением, результат проверки считается отрицательным, а целостность контролируемых объектов – нарушенной.

Проверка целостности по умолчанию осуществляется при запуске ВМ и при проверке по команде администратора. Дополнительно можно задать проверку целостности по расписанию и по времени.

Для расчета контрольных сумм по содержимому объектов используются алгоритмы: CRC32, MD5. Алгоритм выбирается администратором при назначении контроля целостности.

Для изменения значений параметров контроля целостности и для изменения списка контролируемых объектов пользователю веб-консоли **ЦУ СЗИ ВИ** должна быть присвоена роль *Администратор*. Для просмотра установленнх значений пользователю должна быть присвоена роль *Аудитор*.

6.1 Контроль целостности файлов

События нарушения целостности сопровождаются записью в журнале **ЦУ СЗИ ВИ**, при этом в графах *Событие* и *Результат* отображается значение параметра контроля целостности.

В случае обнаружения события нарушения целостности, в интерфейсе запущенной веб-консоли будет отображено соответствующее событие сигнализации (см. п. 3.6 «Сигнализация об НСД»).

6.1.1 Настройка контроля целостности системных файлов для Сервера УД

Для системных файлов, аппаратного обеспечения и файлов ядра **СЗИ ВИ** контроль целостности включен по умолчанию и отключить его невозможно. Возможно только изменить алгоритм расчета КС, задать период или расписание массово на все файлы.

Краткий список файлов, для которых автоматически назначается КЦ на ТС с **ЦУ СЗИ ВИ**:

- бинарные исполняемые файлы (vicored);
- все файлы веба (директория /static);
- sh-скрипты;
- пакеты агентов DL.

Список файлов, находящихся под КЦ осуществляются **Сервер УД** → **Контроль целостности** (см. Рисунок 135):

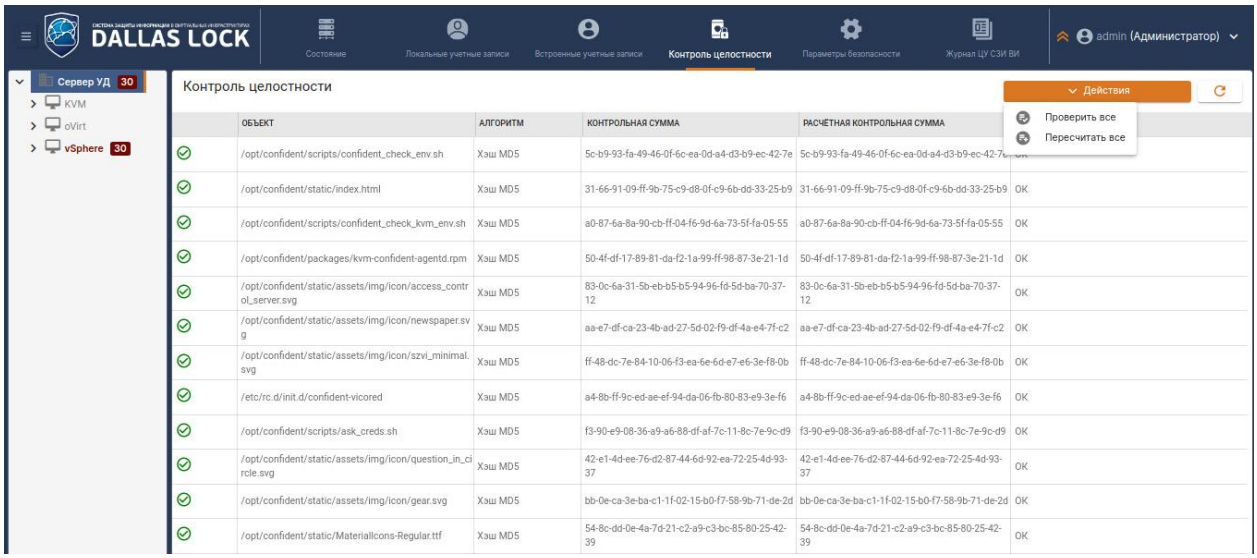

Рисунок 135. Список файлов, находящихся под КЦ

На данной вкладке доступно:

- просмотр списка всех системных файлов под КЦ;
- в меню *Действия*:
  - Проверить все − возможность ручной проверки файлов, до наступления периода или расписания, если таковые значения настроены.
  - Пересчитать все − при нажатии кнопки происходит пересчет контрольной суммы. Пересчет контрольной суммы позволяет принять текущее состояние файла за эталонное и соответственно снять нарушение КЦ, если такое событие было зафиксировано.

Настройки КЦ файлов Сервера УД осуществляются в **Меню → Параметры Сервера УД → Сервер УД** (см. Рисунок 136):

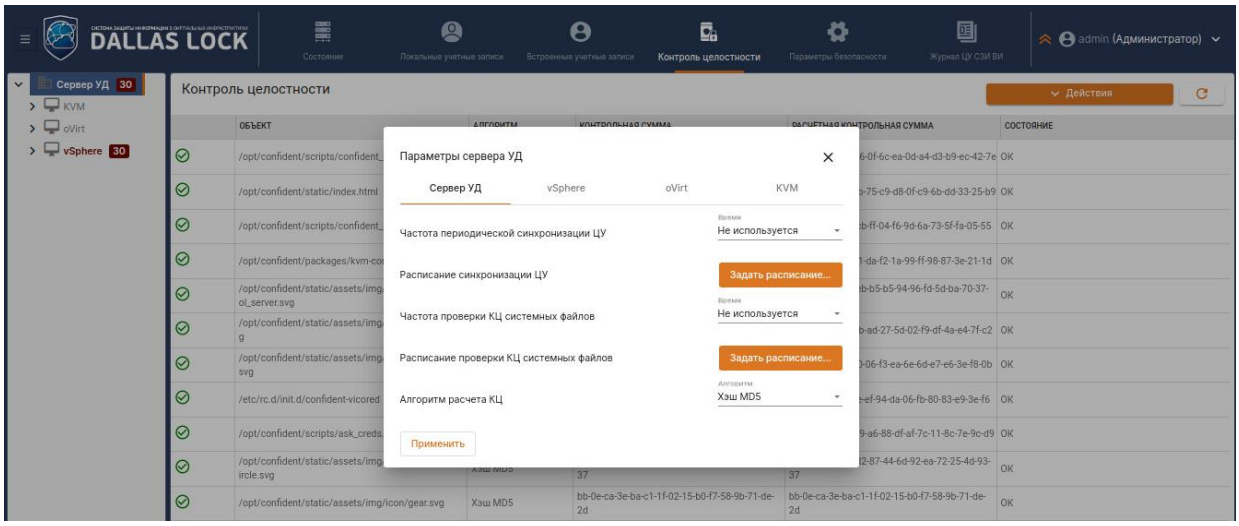

Рисунок 136. Настройка КЦ файлов Сервера УД

В данном окне осуществляется настройка частоты проверки синхронизации ЦУ и системных файлов (периодичность), расписание (см. Рисунок 137) и алгоритм расчета КС.

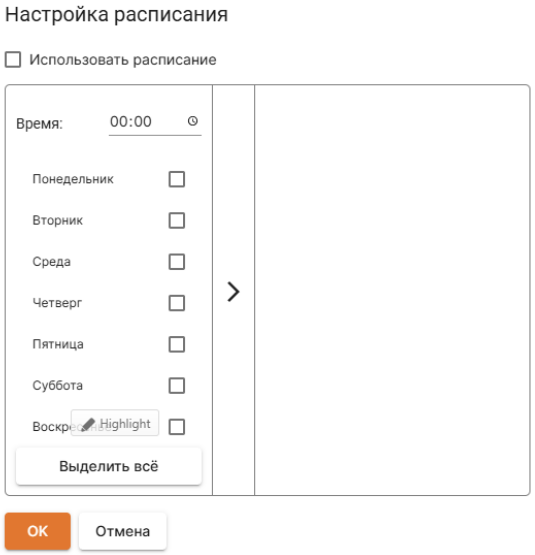

Рисунок 137. Настройка расписания КЦ

6.1.2 Массовая настройка КЦ системных файлов для vSphere/oVirt/KVM

Массовая настройка периода и расписания для всех объектов ВИ с типом *Системные файлы* доступна в **Меню** → **Параметры Сервера УД** → **vSphere/oVirt/KVM** (см. Рисунок 138, Рисунок 139 и Рисунок 140).

На каждой вкладке соответствующей группе объектов ВИ/платформе виртуализации настройка периода и расписания применяется для всех объектов в данной группе/платформе. Например, при задании периода/расписания проверки КЦ системных файлов на вкладке vSphere, данная настройка должна применяться на всех СВ vCSA и гипервизорах ESXi. Аналогично для oVirt (для всех Engine и Host) и KVM.

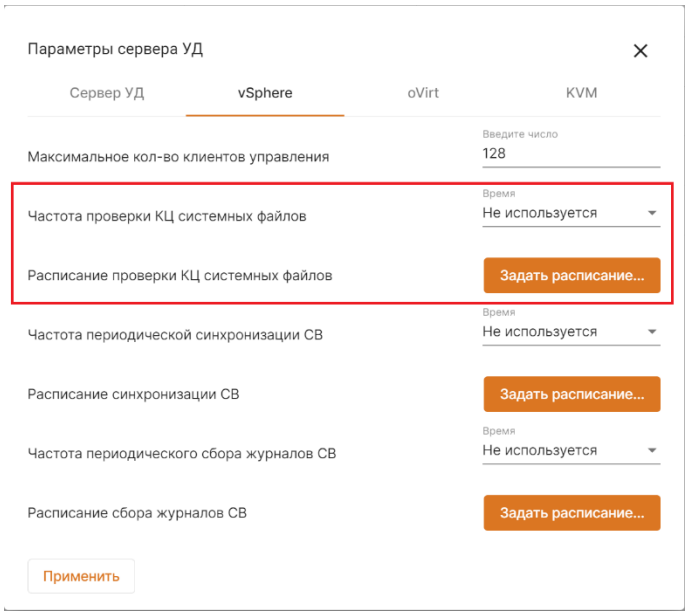

Рисунок 138. Массовая настройка КЦ для группы vSphere

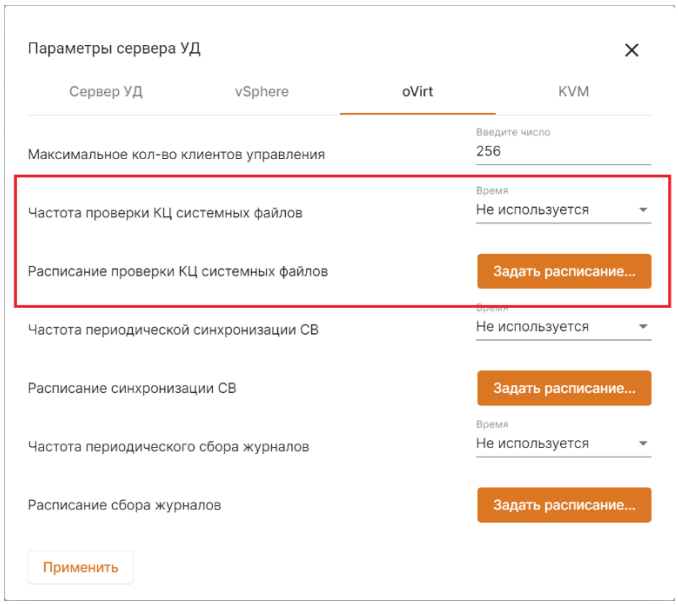

Рисунок 139. Массовая настройка КЦ для группы oVirt

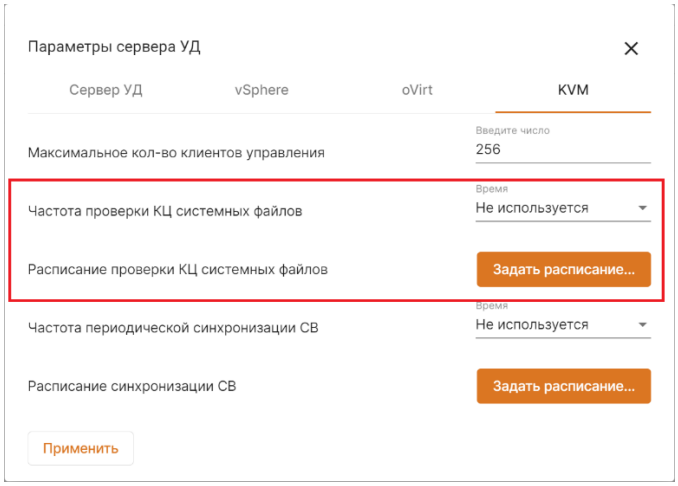

Рисунок 140. Массовая настройка КЦ для группы KVM

6.1.3 Точечная настройка контроля целостности системных файлов на СВ vSphere/vCSA

Просмотр списка системных файлов взятых под КЦ для СВ vSphere/vCSA происходит на уровне СВ в категории «Контроль целостности» (см. Рисунок 141).

Для файлов конфигурации ВМ с vCSA и файлов дисков ВМ vCSA КЦ возможно поставить только на выключенной ВМ. Настройка параметров КЦ в части ВМ описана в п. 6.2 «Настройка контроля целостности ВМ».

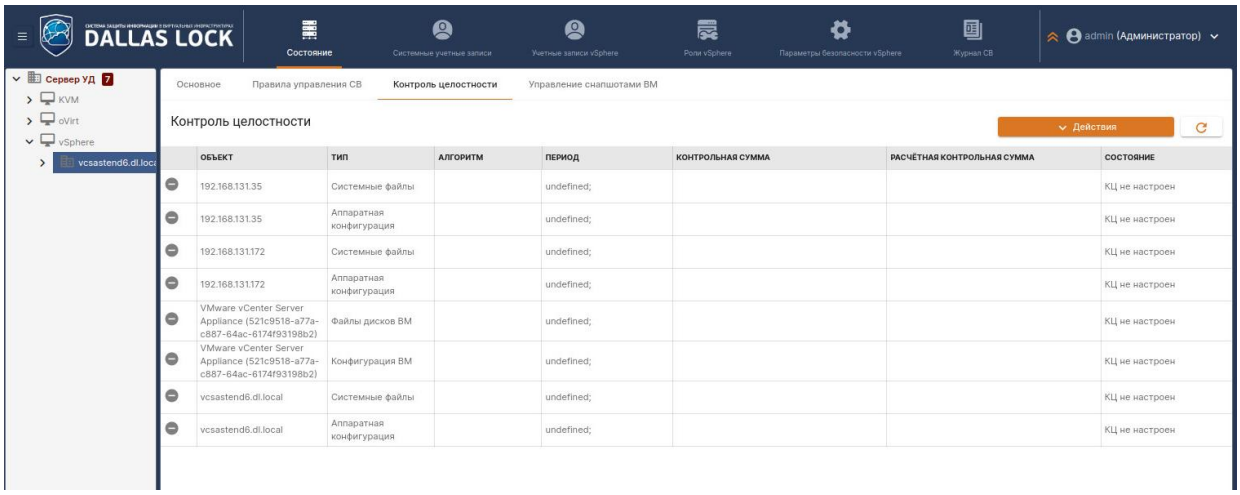

Рисунок 141. КЦ системных файлов и аппаратного обеспечения vSphere

Частота периодической проверки КЦ системных файлов гипервизора ESXi редактируется только для всех гипервизоров (см. п. 3.3.2 «Основные параметры группы СВ vSphere»).

6.1.4 Точечная настройка контроля целостности системных файлов гипервизора ESXi

Для системных файлов и аппаратного обеспечения гипервизора ESXi КЦ включен по умолчанию и отключить его невозможно, возможно только изменить алгоритм расчета КС.

Просмотр списка системных файлов взятых под КЦ для гипервизора ESXi происходит на уровне гипервизора в категории **Состояние** → **Контроль целостности** (см. Рисунок 142).

Настройка параметров КЦ в части ВМ описана в п. 6.2 «Настройка контроля целостности ВМ».

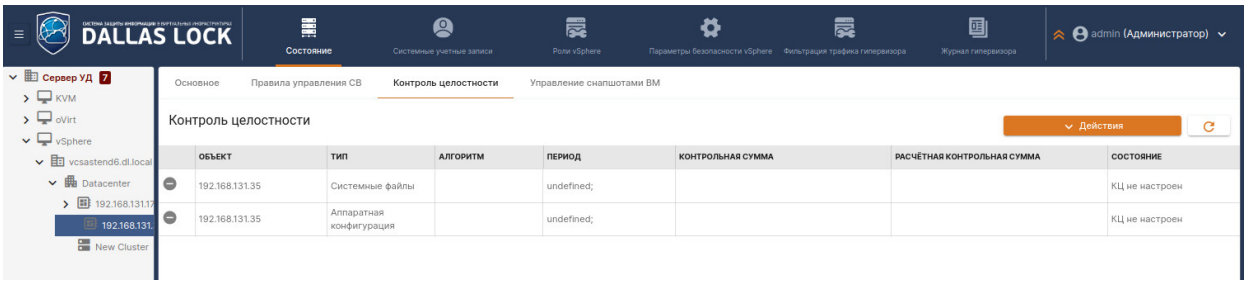

Рисунок 142. КЦ системных файлов ESXi

При подключении/отключении flash-накопителей предупреждение о нарушении КЦ на гипервизоре ESXi выводится при первой проверке КЦ и при последующих перезагрузках платформы.

Частота периодической проверки КЦ системных файлов гипервизора ESXi редактируется только для всех гипервизоров (см. п. 3.3.2 «Основные параметры группы СВ vSphere»).

6.1.5 Точечная настройка контроля целостности системных файлов на СВ oVirt/zVirt/HOSTVM/RedVirt

Для файлов конфигурации ВМ с Engine и файлов дисков ВМ Engine КЦ возможно поставить только на выключенной ВМ.

Просмотр списка системных файлов взятых под КЦ для СВ oVirt/zVirt/HOSTVM/RedVirt происходит на уровне СВ в категории **Состояние** → **Контроль целостности** (см. Рисунок 143).

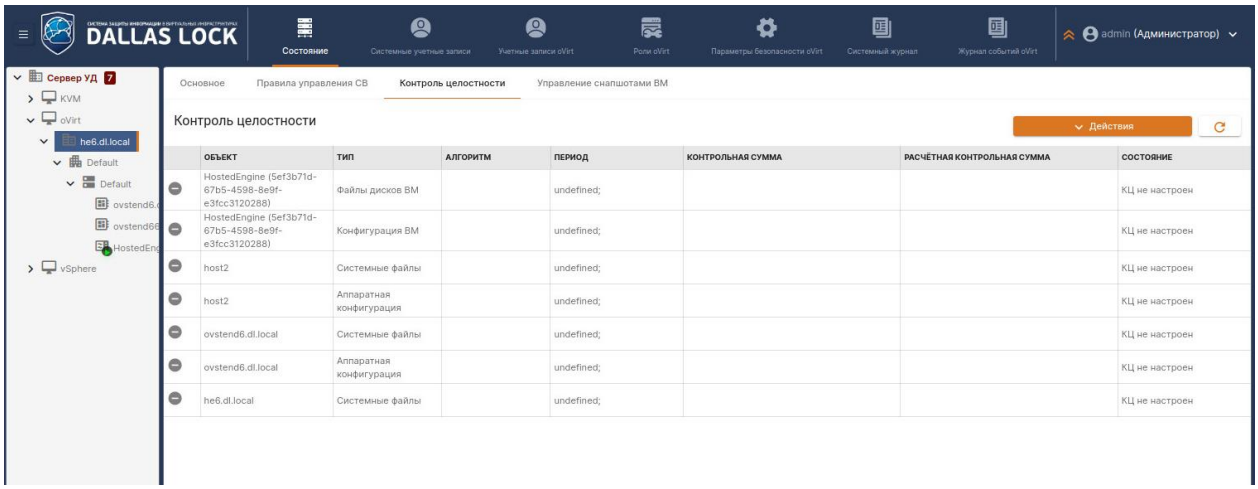

Рисунок 143. КЦ СВ oVirt

Настройка параметров КЦ в части ВМ описана в п. 6.2 «Настройка контроля целостности ВМ».

Частота периодической проверки КЦ системных файлов и аппаратного обеспечения СВ oVirt/zVirt/HOSTVM/RedVirt редактируется только для всех объектов группы KVM (см. п. 3.3.4 «Основные параметры группы KVM»).

6.1.6 Точечная настройка контроля целостности системных файлов гипервизора oVirt/zVirt/HOSTVM/RedVirt

Просмотр списка системных файлов взятых под КЦ для гипервизора oVirt/zVirt/HOSTVM/RedVirt происходит на уровне гипервизора в категории **Состояние** → **Контроль целостности** (см. Рисунок 144).

Настройка параметров КЦ в части ВМ описана в п. 6.2 «Настройка контроля целостности ВМ».

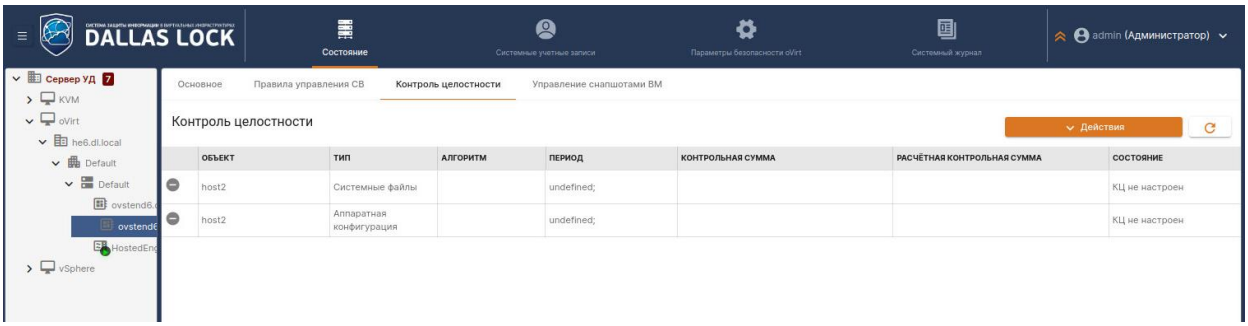

Рисунок 144. КЦ системных файлов гипервизора oVirt/zVirt/HOSTVM/RedVirt

Частота периодической проверки КЦ системных файлов и аппаратного обеспечения гипервизора oVirt/zVirt/HOSTVM/RedVirt редактируется только для всех объектов группы KVM (см. п. 3.3.4 «Основные параметры группы KVM»).

6.1.7 Настройка контроля целостности гипервизора KVM

Для системных файлов и аппаратного обеспечения гипервизора KVM КЦ включен по умолчанию и отключить его невозможно, возможно только изменить алгоритм расчета КС.

Просмотр списка системных файлов взятых под КЦ для гипервизора KVM происходит на уровне СВ в категории **Состояние** → **Контроль целостности** (см. Рисунок 145).

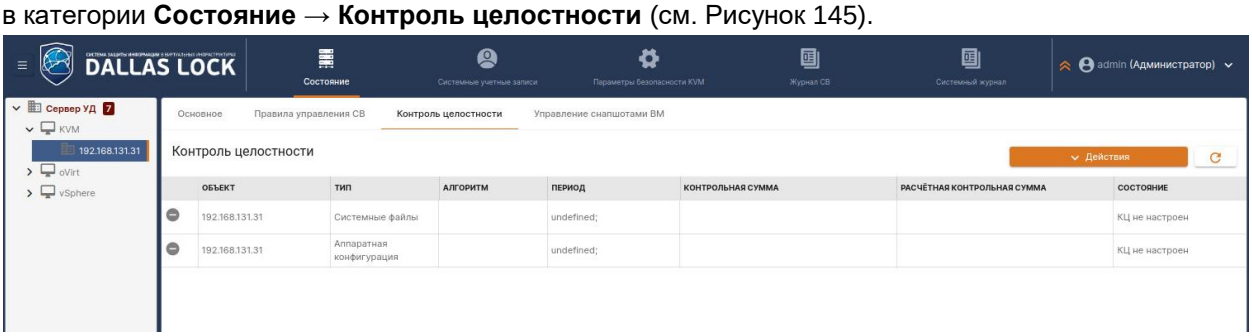

Рисунок 145. КЦ системных файлов гипервизора KVM

Частота периодической проверки КЦ системных файлов гипервизора KVM редактируется только для всех объектов группы KVM (см. п. 3.3.4 «Основные параметры группы KVM»).

Настройка параметров КЦ в части ВМ описана в п. 6.2 «Настройка контроля целостности ВМ».

6.2 Настройка контроля целостности ВМ

При выполнении миграции ВМ между хостами КЦ автоматически не пересчитывается и регистрируется событие НСД. Для исключения подобных ситуаций необходимо перед миграцией ВМ снять КЦ с данной ВМ, после завершения миграции поставить необходимые компоненты ВМ под КЦ.

КЦ на файлы дисков ВМ и конфигурацию ВМ можно поставить только на выключенной ВМ.

Для дисков ВМ для платформы vSphere реализован быстрый расчет КС. Расчет идет по ключевым параметрам. Не рекомендуется использовать для ВМ тип дисков Thick Provision Lazy Zeroed и Thick Provision Eager Zeroed.

6.2.1 Настройка контроля целостности конфигурации ВМ

Проверка КЦ конфигурации ВМ осуществляется периодически и при включении ВМ. Частота периодической проверки КЦ для конфигурации ВМ редактируется при настройке КЦ для конфигурации ВМ.

Для включения контроля целостности конфигурации ВМ необходимо:

1. Выбрать уровень Сервера виртуализации oVirt, vSphere, KVM либо выбрать уровень гипервизора или ВМ и открыть вкладку **Состояние** → **Контроль целостности**.
2. Выбрать из списка виртуальную машину.
3. Выбрать действие **Включить КЦ** (см. Рисунок 146).

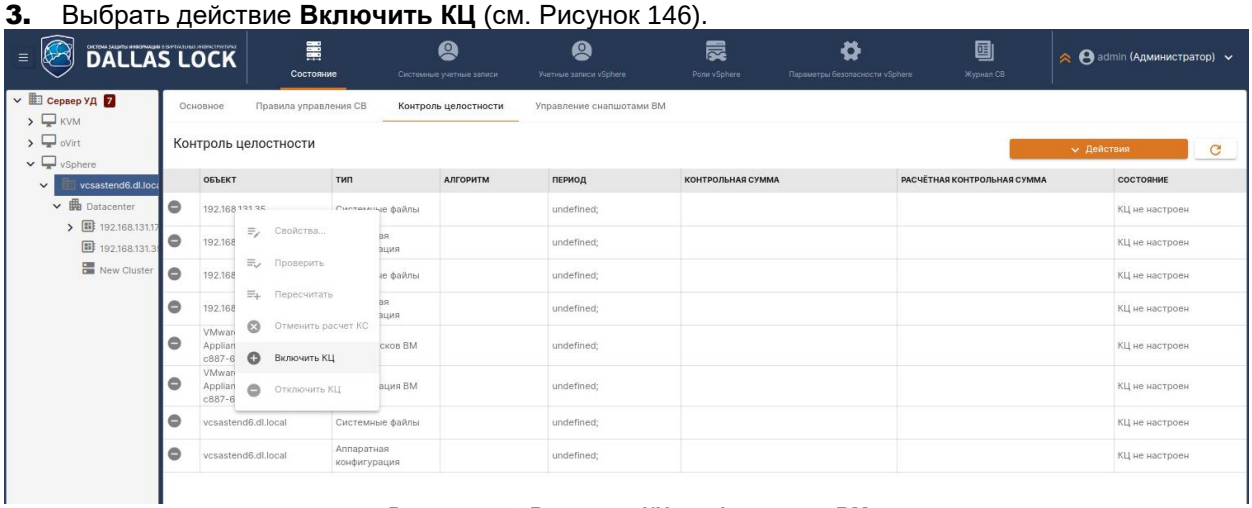

Рисунок 146. Включить КЦ конфигурации ВМ

4. Выбрать алгоритм расчета контрольной суммы (CRC32, Хэш MD5) (см. Рисунок 147).

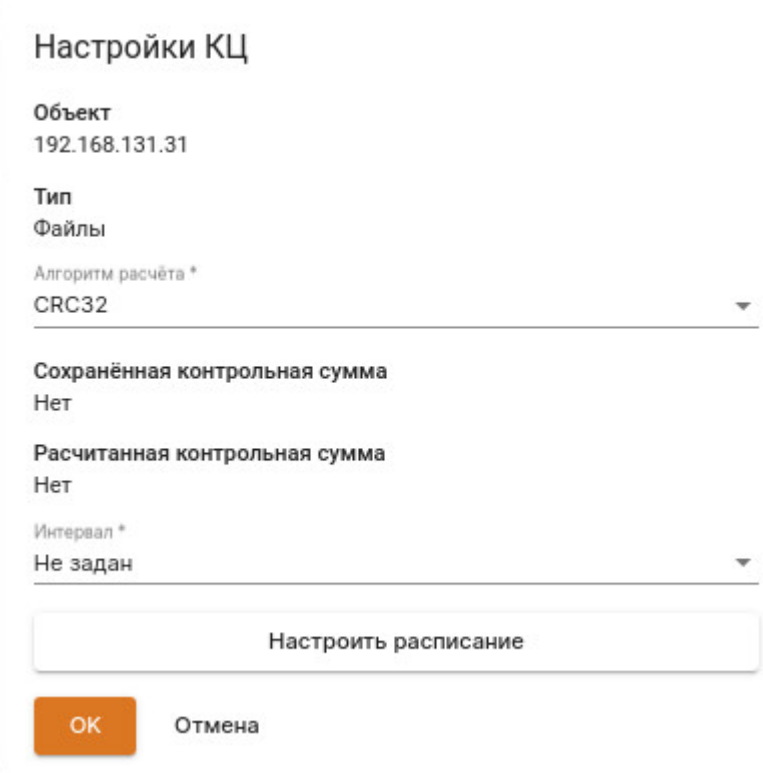

Рисунок 147. Настройка параметров КЦ для ВМ

5. Выбрать интервал расчета (периодичность проверки).
6. Настроить расписание.
7. Нажать кнопку **ОК**.
8. После завершения расчета КС, появится соответствующее информационное окно.

Для снятия КЦ необходимо выбрать объект с включенным КЦ, левой кнопкой мыши нажать по нему и затем нажать кнопку **Отключить КЦ**.

6.2.2 Настройка контроля целостности для образов дисков ВМ

Проверка КЦ образов дисков ВМ осуществляется периодически и при включении ВМ. Частота периодической проверки КЦ для образов дисков ВМ редактируется при настройке КЦ для образов дисков ВМ.

Расчет контрольных сумм образов дисков ВМ происходит только при выключенной ВМ.

Если требуется доверенная загрузка, перед запуском ВМ необходимо проверить КЦ файлов дисков данной ВМ. Проверка конфигурации будет произведена автоматически при запуске ВМ, если данный тип данных находится под КЦ.

Для включения контроля целостности для образов дисков ВМ необходимо:

1. Выбрать уровень Сервера виртуализации, либо выбрать уровень гипервизора или ВМ и открыть КЦ **Состояние** → **Контроль целостности**.
2. Выбрать из списка образ диска ВМ.
3. Выбрать действие **Включить КЦ**.
4. Выбрать алгоритм расчета контрольной суммы (CRC32, Хэш MD5).
5. Выбрать интервал расчета (периодичность проверки).
6. Настроить расписание.
7. Нажать кнопку **ОК**.
8. Появится предупреждающее окно, что выполняется расчет КС (см. Рисунок 148). Данное операция может занимать некоторое время в зависимости от объемов дисков ВМ.

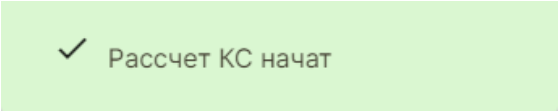

Рисунок 148. Предупреждение о расчете КС

9. После завершения расчета КС выберите **Обновить**. В случае успешного выполнения расчёта КС, в графе *Состояние* расчитываемого файла появится запись «*ОК*».

Для снятия КЦ необходимо выбрать объект с включенным КЦ и на панели действий нажать кнопку **Отключить КЦ**.

При постановке под КЦ ВМ без диска, диск всё равно будет отображаться в списке. «КЦ дисков» — это абстрактный объект, который выдается любой ВМ (как и «КЦ конфигурации») по умолчанию независимо от того, есть диски или нет.

6.2.3 Проверка целостности конфигураций, дисков ВМ

Если некоторый объект, на который назначена целостность, будет изменен или поврежден, то при нажатии на кнопку **Проверить все** (см. Рисунок 149), в списке объектов контроля целостности, значок выбранного объекта у которого нарушена целостность изменится на красный – .

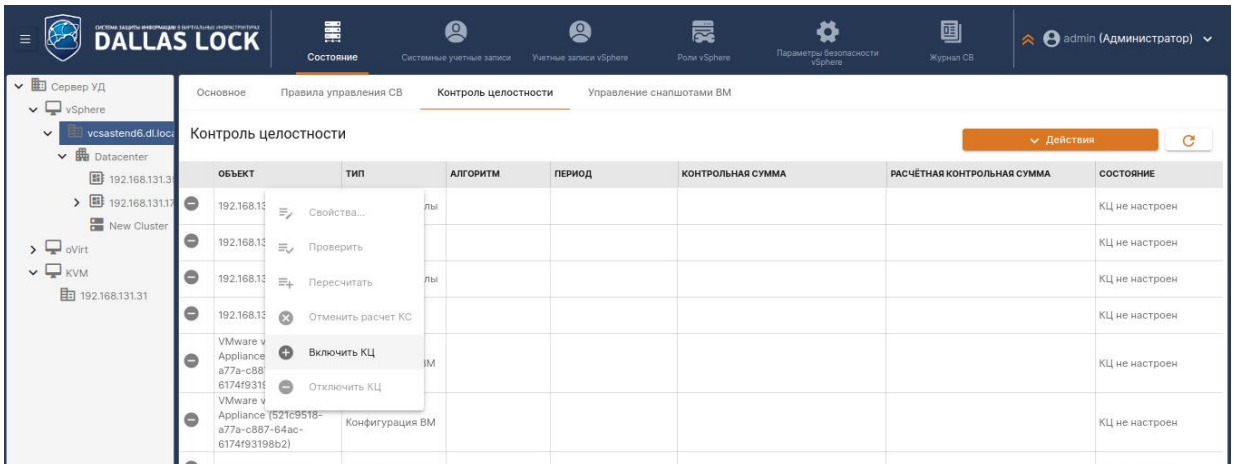

Рисунок 149. Контроль целостности конфигураций и дисков ВМ

При нажатии кнопки **Пересчитать** происходит пересчет контрольной суммы. Пересчет контрольной суммы позволяет принять текущее состояние файла за эталонное и соответственно снять нарушение КЦ.

Значения контрольных сумм для контролируемых объектов в Консоли появляются после команд проверки и пересчета контрольных сумм.

Подсчет контрольной суммы образа дисков ВМ производится с учетом всех используемых в работе ВМ жестких дисков. Вне зависимости от их количества, результатом будет одна контрольная сумма. Нарушение целостности одного из дисков повлечет за собой событие нарушения целостности образа дисков ВМ.

При совпадении факта изменения конфигурации ВМ с периодическим контролем целостности конфигурации ВМ, изменение конфигурации может быть заблокировано, о чем будет сообщено в журнале VMware. Повторное изменение конфигурации должно быть успешным.

7 ПОДСИСТЕМА ГАРАНТИРОВАННОЙ ОЧИСТКИ ПАМЯТИ

7.1 Очистка остаточной информации на объектах ВИ

Затирание производится записью маскирующей последовательности поверх освобождаемого пространства. Параметру **Количество циклов затирания** можно задать значение от одного до четырех циклов затирания. Чем большее число циклов затирания выбрано, тем надежнее происходит удаление информации. При этом следует учесть, что чем больше циклов затирания будет выбрано, тем больше времени эта процедура будет занимать.

7.1.1 Очистка остаточной информации из консоли на клиентах vSphere[10]

Для использования функции удалить и зачистить на vSphere 8.0 требуется ручная установка пакета: eraser.lib. Команда для установки пакета выглядит следующим образом:
esxcli software vib install -v /tmp/<имя пакета>.vib -f --no-sig-check.

Чтобы воспользоваться данной функцией необходимо на уровне группы vSphere в основном меню открыть вкладку *Параметры безопасности vSphere* и нажать кнопку **Очистка остаточной информации**. В рабочей области появится параметр **[Гипервизоры] Количество циклов затирания**. Данному параметру можно установить значение от одного до десяти циклов затирания. Чтобы изменить это количество, необходимо произвести клик по указанному параметру и в открывшемся окне выставить нужное значение (см. Рисунок 150). Затем нажать кнопку **ОК** и в категории *Действия* нажать кнопку **Сохранить**.

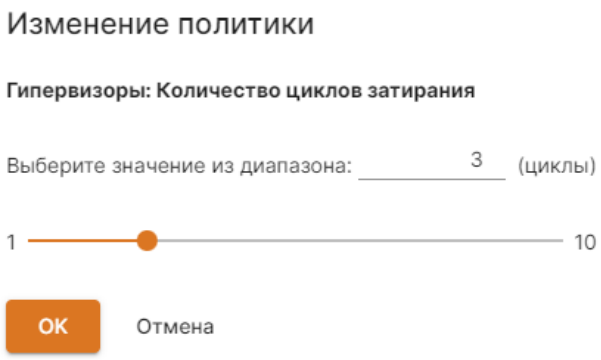

Рисунок 150. Установка количества циклов затирания

На уровне СВ и гипервизора также можно задать значение данного параметра на вкладке *Параметры безопасности vSphere*.

Для зачистки ВМ необходимо:

1. Перейти на уровень удаляемой ВМ и во вкладке *Состояние* в блоке *Действия* нажать кнопку **Удалить и зачистить**.
2. В появившемся диалоговом окне подтвердить удаление ВМ.

7.1.2 Очистка остаточной информации из консоли на гипервизорах KVM/oVirt/zVirt/HOSTVM/RedVirt

Чтобы воспользоваться данной функцей необходимо на уровне группы KVM или на уровне СВ KVM/oVirt/zVirt/HOSTVM/RedVirt (для индивидуальной настройки) в основном меню открыть вкладку *Параметры безопасности KVM* и нажать кнопку **Очистка остаточной информации**. (см. Рисунок 151) В рабочей области появится параметр **Количество циклов затирания**. Данному параметру можно установить значение от одного до десяти циклов затирания. Чтобы изменить это количество, необходимо произвести двойной клик по указанному параметру и в открывшемся окне выставить нужное значение (см. Рисунок 152). Затем нажать кнопку **Ок** и в категории *Действия* нажать кнопку **Сохранить**.

[10] Для vSphere 8.0 пакет требуется ставить руками (см. примечание в п. 7.1.1 «Очистка остаточной информации из консоли на клиентах vSphere»).

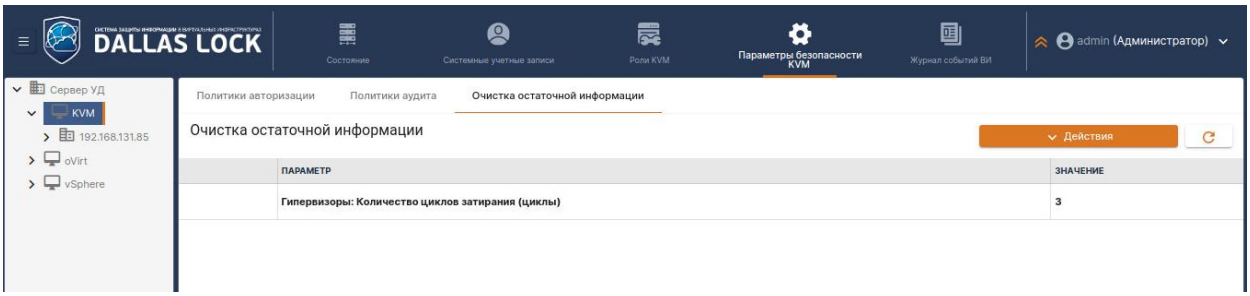

Рисунок 151. Очистка остаточной информации KVM

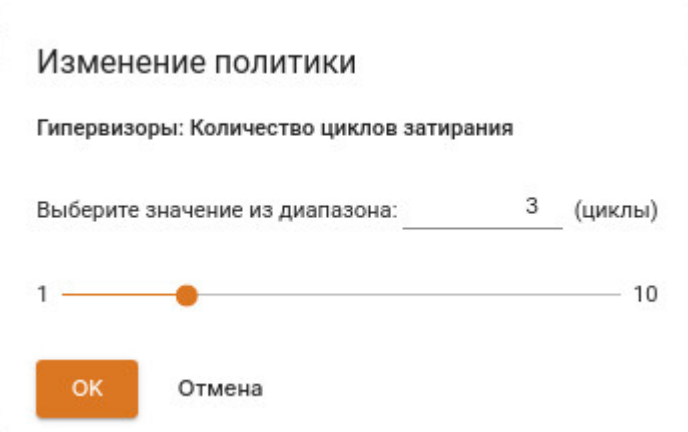

Рисунок 152. Установка количества циклов затирания для KVM

7.1.3 Удаление и зачистка виртуальной машины

Чтобы удалить и зачистить виртуальную машину, необходимо перейти в дерево, выбрать виртуальную машину, выбрать категорию **Состояние**, **Основное** → нажать на блок *Действия* → **Удалить и зачистить** (см. Рисунок 153). После этого появится окно, уведомляющее о ходе процесса удаления и зачистки.

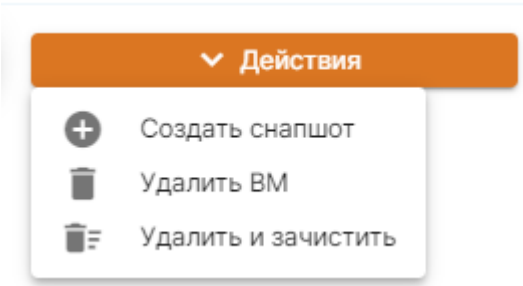

Рисунок 153. Удаление и зачистка виртуальной машины

Очистка информации с помощью утилиты Eraser

Eraser используется через ssh на стороне ESXi. Утилита поставляется в виде отдельного бинарного файла и в виде vib-пакета (для ESXi 7.0+).

Eraser – это утилита для зачистки конфигурации и образов дисков виртуальных машин, которая гарантирует предотвращение восстановления удаленных данных.

Для работы с утилитой необходимо получить доступ к интерфейсу командной строки гипервизора. Для этого существует несколько способов:

- локальная командная строка, доступная с локальной консоли гипервизора при нажатии комбинации клавиш **Alt+F1**;
- подключение через SSH;
- подключение через vSphere PowerCLI.

Данная утилита работает с именами, не содержащими кириллические символы.

Получив доступ к командной строке гипервизора, необходимо авторизоваться с правами администратора. Для работы с утилитой Eraser доступны следующие команды.

--recursive, -r
Рекурсивный обход директорий
--count, -c <число циклов>
Количество проходов очистки
--verbose, -v
Вывод информации о зачищаемом файле
--preserve, -p
Сохранить зачищенный файл
--verbose-extra, -vv
Дополнительный вывод информации о зачищаемом файле (включает --verbose)
--files, -f <список файлов>
Список зачищаемых файлов через запятую
--silent, -s
Тихий режим (без вывода информации, не работает с --verbose)

7.1.3.1 Пример зачистки ВМ

Рассмотрим пример зачистки ВМ используя локальную командную строку гипервизора. Для этого необходимо:

1. Получить доступ к локальной командной строке гипервизора используя комбинацию клавиш **Alt+F1**.
2. Ввести логин и пароль администратора гипервизора (см. Рисунок 154).

```
[root@PMV-szivi-esxi2:~] vmware -vl
VMware ESXi 7.0.3 build-23794027
VMware ESXi 7.0 Update 3
[root@PMV-szivi-esxi2:~]
```

Рисунок 154. Версия гипервизора

3. Перейти в каталог с виртуальными машинами используя команду «*cd *путь к каталогу**» (см. Рисунок 155). Для отображения объектов ФС в текущем каталоге возможно ввести команду «*ls –la*».

Утилита Eraser работает глобально из любого каталога, но рекомендуется перед удалением перейти в нужный каталог. Это позволит избежать ошибочной зачистки, т.к. после нее восстановление данных невозможно

```
[root@PMV-szivi-esxi2:~] ls -la /vmfs/volumes/datastore1\ \(1\)/
total 1474560
drwxr-xr-t    1 root     root          73728 Dec 12 08:07 .
drwxr-xr-x    1 root     root            512 Dec 12 08:21 ..
-r--------    1 root     root        1376256 Jul  9 12:17 .fbb.sf
-r--------    1 root     root      134807552 Jul  9 12:17 .fdc.sf
-r--------    1 root     root      268632064 Jul  9 12:17 .jbc.sf
-r--------    1 root     root       16908288 Jul  9 12:17 .pb2.sf
-r--------    1 root     root          65536 Jul  9 12:17 .pbc.sf
-r--------    1 root     root     1074331648 Jul  9 12:17 .sbc.sf
drwx------    1 root     root          69632 Jul  9 12:17 .sdd.sf
-r--------    1 root     root        7340032 Jul  9 12:17 .vh.sf
[root@PMV-szivi-esxi2:~]
```

Рисунок 155. Переход в каталог

4. Выполнить команду «*/eraser –f=*Имя каталога с ВМ* -r -v -c=2*» и дождаться зачистки (см. Рисунок 156).

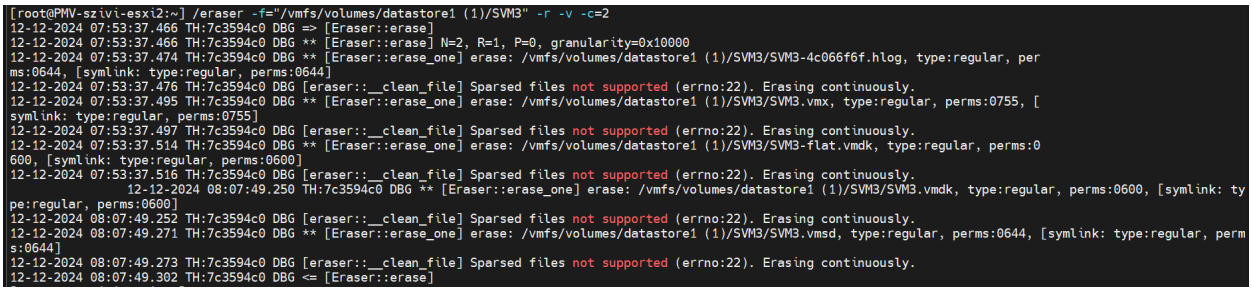

Рисунок 156. Процесс зачистки ВМ и результат

Необходимо соблюдать регистр (нижний или верхний) при вводе команды, иначе она не будет выполнена.

8 ПОДСИСТЕМА АУДИТА

8.1 Журналы событий

В **ЦУ СЗИ ВИ** регистрируются события и группируются, в зависимости от типов событий, подлежащих протоколированию, также задается степень детализации аудита и другие факторы. Для этого используются следующие журналы:

1. журнал ЦУ СЗИ ВИ,
2. журнал событий ВИ (для каждого СВ oVirt, KVM),
3. журнал сервера виртуализации (для каждого СВ vSphere, KVM),
4. журнал гипервизора (только для ESXi),
5. журнал событий oVirt/zVirt/HOSTVM/RedVirt (только для СВ oVirt/zVirt/HOSTVM/RedVirt),
6. системный журнал (только для СВ oVirt/zVirt/HOSTVM и гипервизоров KVM и oVirt/zVirt/HOSTVM/RedVirt).

В каждом журнале фиксируются дата, время, событие, результат и прочие параметры.

Каждый текущий журнал формируется в папке «/opt/confident/jrn».

На панели *Действия* расположены элементы управления журналом. При нажатии кнопки **Обновить** отображаемые данные журналов после применения к ним новых настроек будут обновлены. Чтобы собрать информацию, отображенную в журналах, нужно в блоке *Действия* нажать кнопку **Архивировать** (см. Рисунок 157).

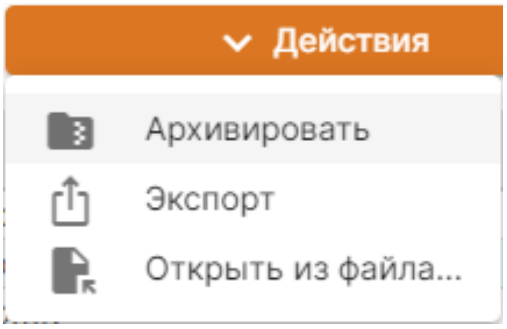

Рисунок 157. Кнопка «Архивировать»

После выбора архивации журнала, в окне журнала записи очищаются, и он начинает вестись заново. В журнал **ЦУ СЗИ ВИ** вносится соответствующая запись об операции архивации. Также, в случае, когда журнал переполняется (максимальный размер – 250000 записей, подробнее об настройке максимального количества записей в журналах в п. 4.4.1 «Настройка параметров безопасности»), он архивируется в файл со специальным расширением *.dlvj и помещается в папку «/opt/confident/jrn-archives/». При этом текущий журнал очищается и начинает вестись заново. В имени архивного файла с журналом записаны наименование журнала, имя/ip-адрес хоста, дата и время создания архива в формате дд.мм.гг и расширение файла. Для открытия такого файла, необходимо в блоке *Действия* нажать кнопку **Открыть из файла**, а затем, в открывшемся окне, выбрать файл журнала, нажав кнопку **Загрузить** (см. Рисунок 158).

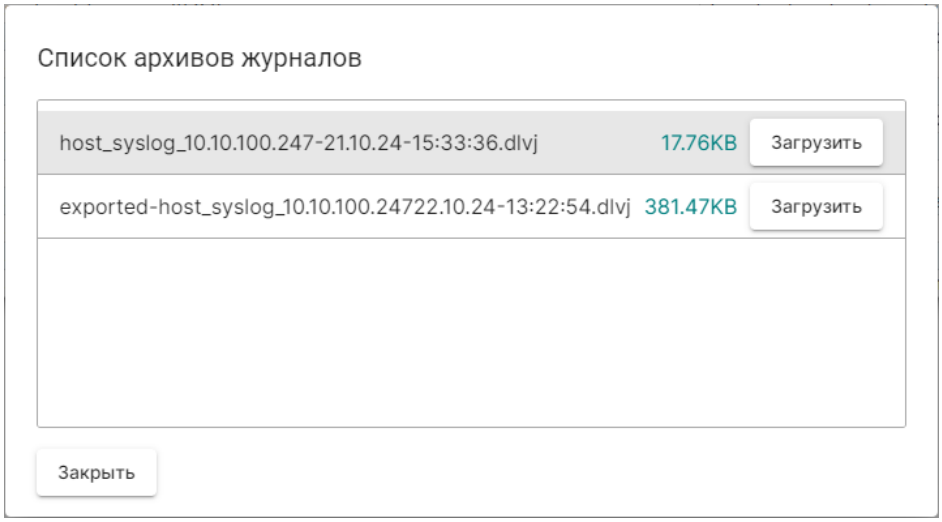

Рисунок 158. Окно со списком архивов

Чтобы вернуться к просмотру текущего журнала, можно перейти на любую другую вкладку и вновь

перейти к журналу. Кнопка **Экспорт** отвечает за сбор и конвертирование информации журналов в файлы с расширением .dlvj (с табуляцией или без), CSV, HTML или XML. Для осуществления данной функции нужно нажать кнопку **Экспорт**, указать имя файла и выбрать место для его хранения.

Для полного удаления журнала, необходимо открыть папку «/opt/confident/jrn» и удалить соответствующий файл.

8.1.1 Журнал ЦУ СЗИ ВИ

Журнал **ЦУ СЗИ ВИ** – это журнал, в который заносятся события, связанные непосредственно с работой **ЦУ СЗИ ВИ** (воспроизводится звуковой сигнал и выводится сообщение). Регистрируются такие события, например, как:

- Запуск службы Ядра ЦУ СЗИ ВИ;
- Остановка службы Ядра ЦУ СЗИ ВИ;
- Добавление СВ в СЗИ ВИ;
- Вывод СВ из СЗИ ВИ;
- Установка учетных данных;
- Удаление учетных данных;
- Вход пользователя в веб-Консоль;
- Выход пользователя из веб-Консоли;
- Синхронизация начата...;
- Подготовка данных для синхронизации...;
- Начало синхронизации этапа...;
- Завершение синхронизации этапа;
- Синхронизации этапа...;
- Синхронизация завершена;
- Изменение настроек веб-интерфейса;
- Активация файла-ключа;
- Загрузка и инициализация файлов-ключей;
- Файл-ключ активирован;
- Файл-ключ деактивирован;
- Файл-ключ добавлен в хранилище;
- Файл-ключ удален из хранилища;
- Изменение директории хранилища файлов-ключей;
- Выдача квоты лицензий CPU;
- Возврат квоты лицензий CPU;
- Активация демо-версии;
- Срок действия демо-версии истек;
- Изменены параметры сервера УД;
- Параметры сервера УД сброшены к значениям по умолчанию;
- Изменение значения порта веб-сервера;
- Установлены параметры веб-сервера по умолчанию;
- Применение конфигурации;
- Сохранение конфигурации;
- Сбор журналов;
- Архивация журналов;
- Экспорт журналов;
- Загрузка журнала из файла;
- Изменение периодичности сбора журналов;
- Изменение расписания сбора журналов;
- Изменена политика;
- Применена политика;
- Все политики пронаследованы;
- Исправление значений политики;
- Изменение правил МЭ;
- Добавление правил МЭ;
- Удаление правил МЭ;
- Активация правила МЭ;
- Деактивация правила МЭ;
- Добавление клиента управления;
- Удаление клиента управления;

- Запуск ВМ;
- Остановка ВМ;
- Пауза ВМ;
- Перезагрузка ВМ;
- Удаление ВМ;
- Удаление и зачистка ВМ;
- Создание снапшота ВМ;
- Включение автоматического создания снапшотов ВМ;
- Отключение автоматического создания снапшотов ВМ;
- Редактирование параметров создания снапшотов ВМ;
- Подключение уведомлений на Агент ВИ;
- Отключение уведомлений Агента ВИ;
- Установка агента;
- Начато удаление агента;
- Ввод в домен безопасности;
- Вывод из домена безопасности;
- Установка учетных данных на Агент ВИ;
- НСД-событие отмечено как прочитанное!;
- НСД-событие отмечено как непрочитанное!;
- НСД-события отмечены как прочитанные!;
- Возвращение событий НСД в состояние: «Не прочитано»;
- Очистка списка НСД-событий;
- Удаление события НСД;
- Внутренняя учетная запись: создание;
- Внутренняя учетная запись: удаление;
- Внутренняя учетная запись: изменение;
- Внутренняя учетная запись: смена пароля;
- Создание учетной записи суперадминистратора;
- Внутренняя учетная запись заблокирована;
- Внутренняя учетная запись разблокирована;
- Изменение пароля учетной записи;
- Создание пользователя виртуальной инфраструктуры;
- Удаление пользователя виртуальной инфраструктуры;
- Изменение пользователя виртуальной инфраструктуры;
- Создание группы виртуальной инфраструктуры;
- Удаление группы виртуальной инфраструктуры;
- Изменение группы виртуальной инфраструктуры;
- Создание пользователя в операционной системе;
- Удаление пользователя в операционной системе;
- Изменение пользователя в операционной системе;
- Создание группы;
- Удаление группы;
- Изменение группы;
- Создание учетной записи;
- Удаление учетной записи;
- Изменение учетной записи;
- Добавление доверенного клиента управления;
- Удаление доверенного клиента управления;
- Изменение доверенного клиента управления;
- Достигнуто предельное количество клиентов управления;
- Создание группы в операционной системе;
- Удаление группы в операционной системе;
- Изменение группы в операционной системе;
- Создание роли;
- Удаление роли;
- Изменение роли;
- Копирование роли;
- Назначение права пользователя;
- Удаление права пользователя;

- Изменение права пользователя;
- Копирование права пользователя;
- Постановка объекта под контроль целостности;
- Запуск расчёта контрольной суммы объекта;
- Завершение расчёта контрольной суммы объекта;
- Отмена расчёта контрольной суммы для объекта;
- Снятие объекта с контроля целостности;
- Изменение настроек контроля целостности;
- Начат пересчёт контрольной суммы для объекта;
- Завершен пересчёт контрольной суммы для объекта;
- Начата проверка контрольной суммы для объекта;
- Завершена проверка контрольной суммы для объекта;
- Ввод модуля СЗИ ВИ под управление ЕЦУ;
- Вывод модуля СЗИ ВИ из под управления ЕЦУ;
- Начата синхронизации с ЕЦУ;
- Завершена синхронизация с ЕЦУ;
- Начата синхронизация заданий;
- Завершена синхронизация заданий;
- Начата синхронизация политик с ЕЦУ;
- Завершена синхронизация политик с ЕЦУ;
- Начата синхронизация пользователей с ЕЦУ;
- Завершена синхронизация пользователей с ЕЦУ;
- Выполнение задания ЕЦУ: Получить отчет о конфигурации;
- Выполнение задания ЕЦУ: Сохранить конфигурацию;
- Выполнение задания ЕЦУ: Применить конфигурацию;
- Выполнение задания ЕЦУ: Проверить обновления;
- Отправка всех журналов на ЕЦУ;
- Сгенерирован отчет безопасности;
- Получение отчета пользователем;
- Применение шаблона(-ов) безопасности.

Просмотр журнала происходит на уровне **Сервер УД** на вкладке *Журнал ЦУ СЗИ ВИ* (см. Рисунок 159).

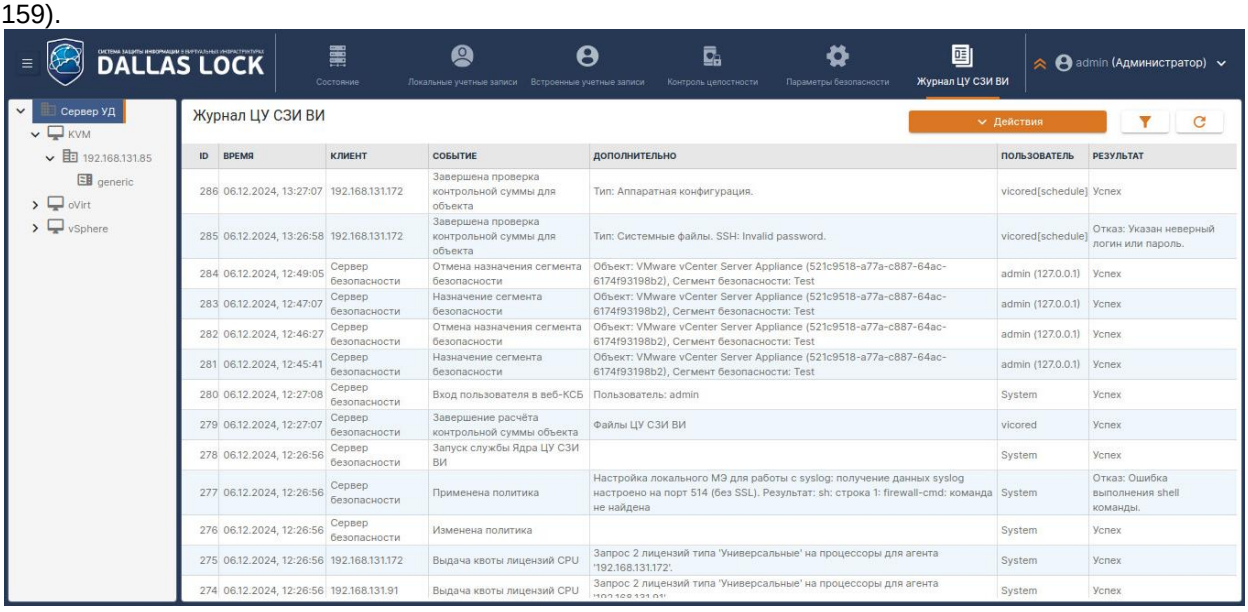

Рисунок 159. Журнал ЦУ СЗИ ВИ

Управление журналом описано в п. 8.1 «Журналы событий».

Управление фильтрацией журнала производится в категории **Фильтр**. Для этого нужно кликнуть на кнопку ▼ и выбрать **Настройка фильтра**, после чего установить необходимые параметры фильтрации и нажать **ОК** (см. Рисунок 160).

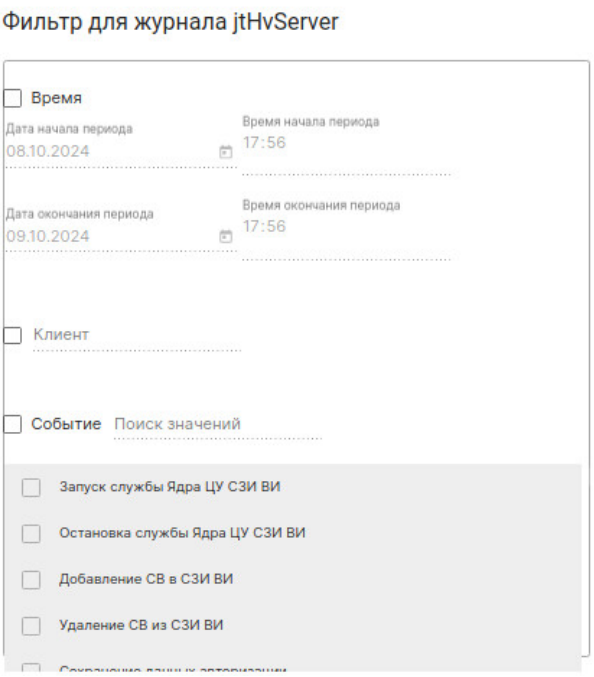

Рисунок 160. Отдельная форма записи журнала событий

Для задания параметров фильтра необходимо нажать на кнопку . В появившемся окне можно задать количество и тип записей, период времени, за который необходимо отобразить события, дополнительные параметры. Фильтр также можно инвертировать фильтр. После завершения настройки фильтра необходимо нажать кнопку **ОК**. Затем, чтобы применить настроенный фильтр, необходимо нажать кнопку **Активировать фильтр**. Для отмены фильтрации следует нажать на кнопку **Сбросить фильтр**.

В категории **Фильтр** также можно настроить группировку записей журнала по полям. Чтобы применить настройки группировки необходимо нажать на кнопку **Настроить группировку**, а потом **Активировать группировку**.

8.1.2 Журнал сервера виртуализации

Журнал сервера виртуализации – это журнал, который содержит информацию об изменениях состояния управляемых объектов на сервере виртуализации. События включают в себя действия системы и пользователей, которые происходят на объеках ВИ.

Просмотр журнала СВ происходит на уровне **Сервера виртуализации** на вкладке *Журнал СВ* (см. Рисунок 161).

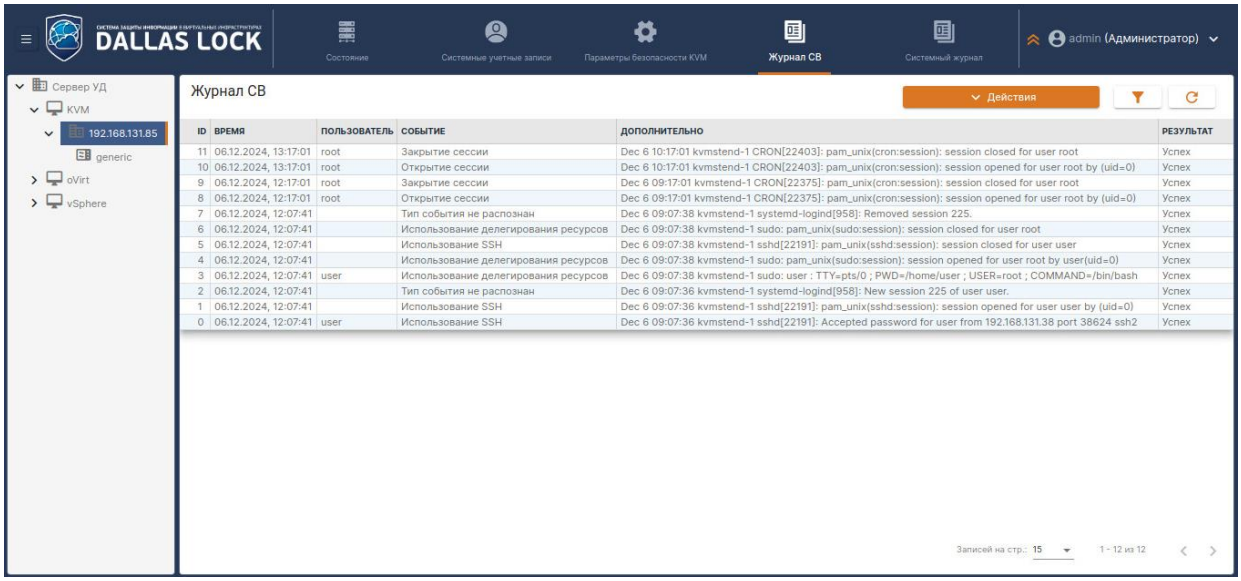

Рисунок 161. Журнал СВ

Формирование этого журнала происходит на момент команды сбора журнала путем нажатия кнопки **Собрать журнал** в блоке *Действия*, а также при настроенном периодическом сборе журналов в

параметрах **ЦУ СЗИ ВИ**.

В поле «Пользователь» журналов СВ vCSA могут быть указаны в том числе и VMware vCSA соответственно, даже если они не зарегистрированы в **СЗИ ВИ**.

Управление журналом описано в п. 8.1 «Журналы событий».

Для журналов серверов виртуализации возможно задать частоту и расписание периодического сбора журналов (см. п. 3.2.1.2 «Информационная панель групп ВИ»).

8.1.3 Журнал событий oVirt/zVirt/HOSTVM/RedVirt

Журнал событий oVirt/zVirt/HOSTVM/RedVirt – это журнал, который содержит информацию об изменениях состояния управляемых объектов на сервере виртуализации. События включают в себя действия системы и пользователей, которые происходят на объектах ВИ.

Просмотр журнала происходит на уровне Сервера виртуализации на вкладке *Журнал событий oVirt* (см. Рисунок 162).

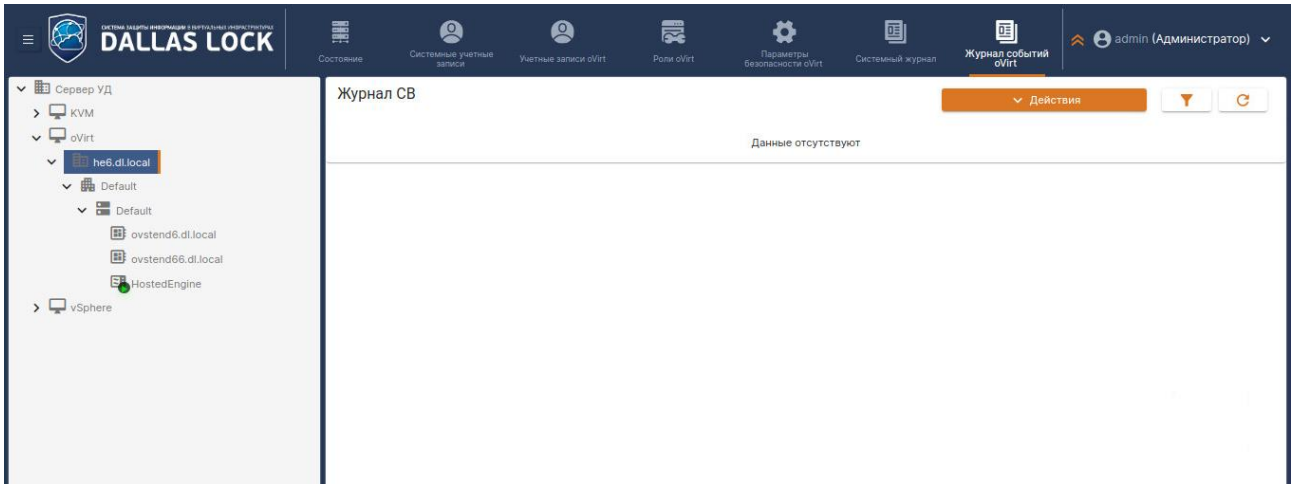

Рисунок 162. Журнал событий oVirt

Формирование этого журнала происходит на момент команды сбора журнала путем нажатия кнопки **Собрать журнал**, а также при настроенном периодическом сборе журналов в параметрах **ЦУ СЗИ ВИ**.

Фильтрация осуществляется по аналогии с фильтрацией журнала **ЦУ СЗИ ВИ** и описана в п. 8.1 настоящего документа.

8.1.4 Системный журнал (KVM/oVirt/zVirt/HOSTVM/RedVirt)

Системный журнал – в данный журнал содержит события системного журнала ОС СВ oVirt/zVirt/HOSTVM/RedVirt и гипервизоров KVM и oVirt/zVirt/HOSTVM/RedVirt.

Просмотр журнала происходит на уровне сервера виртуализации/гипервизора на вкладке *Системный журнал* (см. Рисунок 163).

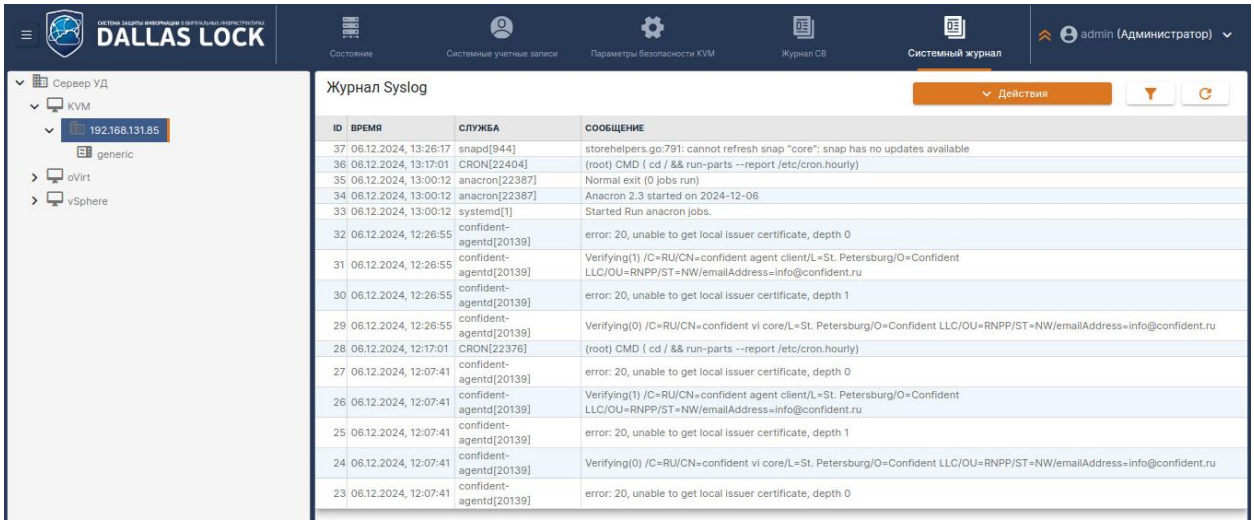

Рисунок 163. Системный журнал

Формирование этого журнала происходит в режиме реального времени. Для обновления информации необходимо нажать кнопку **Обновить**.

Для удобства просмотра журнала возможно использовать фильтры.

8.1.5 Журнал гипервизора ESXi

Журнал гипервизора – в данный журнал регистрируются события безопасности гипервизора ESXi. Журнал включает в себя системные события и действия ESXi. Для работы данного журнала должны быть настроены **Политики аудита**, например, для регистрации событий об аутентификации необходимо включить параметр «[vSphere] Агент ESXi» и сохранить изменения (см. п. 8.2.1 «Аудит гипервизоров ESXi»).

Просмотр журнала гипервизора происходит на уровне гипервизора на вкладке «Журнал гипервизора» (см. Рисунок 164).

Формирование этого журнала происходит в режиме реального времени. Для обновления информации необходимо нажать кнопку **Обновить** рядом с блоком «Действия».

Для удобства просмотра журнала возможно использовать фильтр.

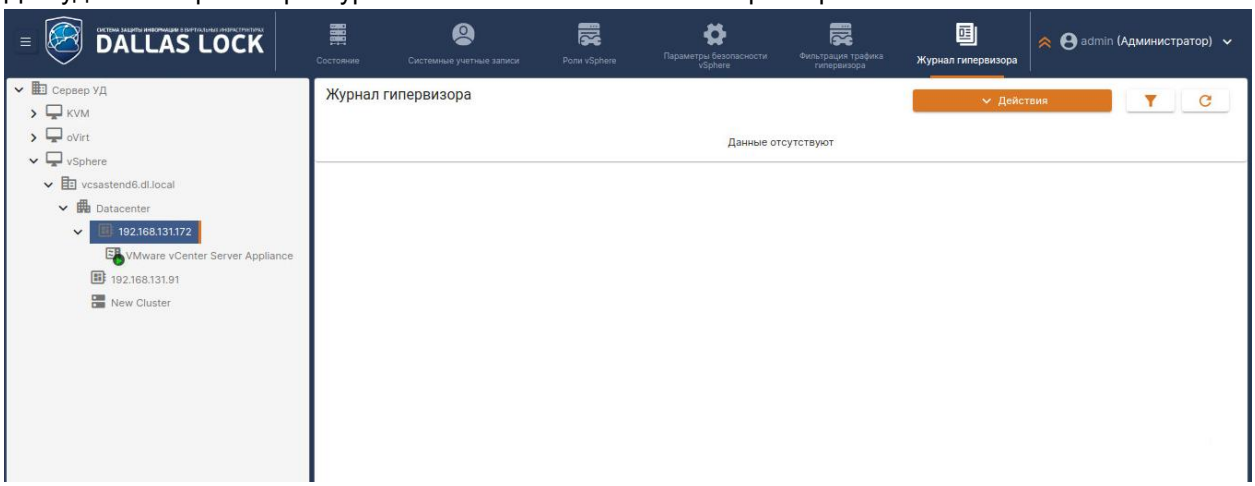

Рисунок 164. Журнал гипервизора

8.2 Аудит гипервизоров

8.2.1 Аудит гипервизоров ESXi

События безопасности регистрируются на всех гипервизорах, на которых установлен агент, после чего пересылаются на **ЦУ СЗИ ВИ**.

Просмотр и редактирование параметров аудита гипервизоров для гипервизоров vSphere происходит на уровне «vSphere» в категории **Параметры безопасности vSphere → Политики аудита** (см. Рисунок 165).

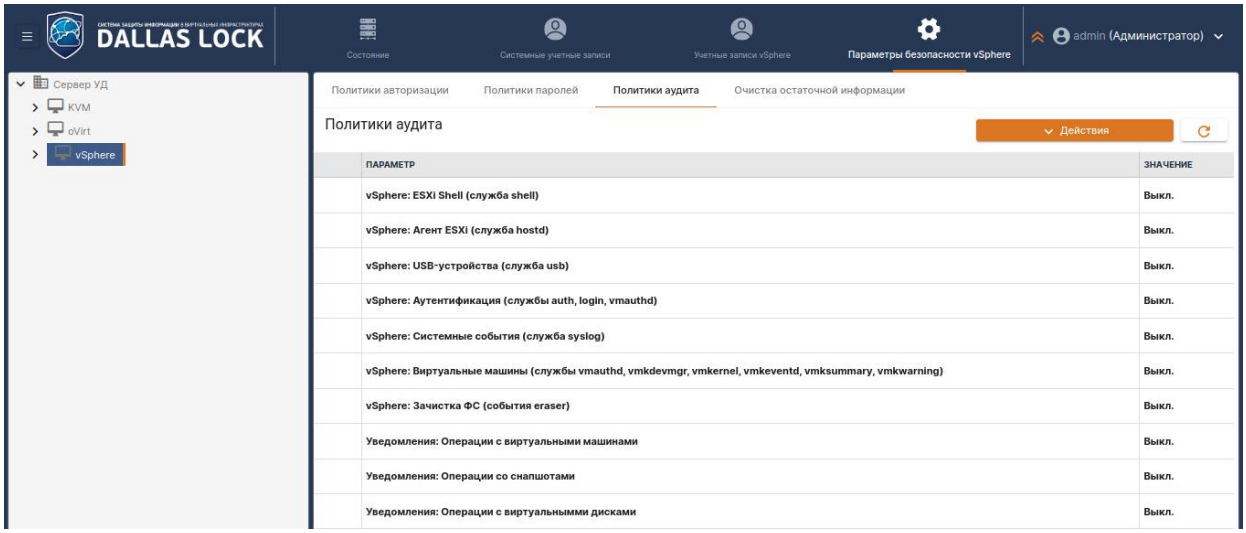

Рисунок 165. Аудит гипервизоров

В соответствии с настроенными параметрами информация регистрируется в журнале гипервизора (см. п. 8.1.5 «Журнал гипервизора ESXi»).

Доступны следующие параметры:

vSphere: ESXi Shell (служба shell)
Данный параметр позволяет включить регистрацию событий и записей всех введенных команд в ESXi Shell. По умолчанию значение данного параметра: **Выкл**..
vSphere: Агент ESXi (служба hostd)
Данный параметр позволяет включить регистрацию сведений о действиях агента, который управляет и конфигурирует гипервизор виртуальные машины, а также включить регистрацию событий аутентификации на гипервизоре. По умолчанию значение данного параметра: **Выкл**..
vSphere: USB-устройства (служба usb)
Данный параметр позволяет включить регистрацию событий, связанных с подключаемыми USB-устройствами к гипервизору. По умолчанию значение данного параметра: **Выкл**..
vSphere: Аутентификация (службы auth, login, vmauthd)
Данный параметр позволяет включить регистрацию событий, связанных с аутентификацией на гипервизоре. По умолчанию значение данного параметра: **Выкл**..
vSphere: Системные события (служба syslog)
Данный параметр позволяет включить регистрацию общих сообщений журнала (Syslog), которые могут быть использованы для устранения неполадок. По умолчанию значение данного параметра: **Выкл**..
vSphere: Виртуальные машины (службы vmauthd, vmkdevmgr, vmkernel, vmkeventd, vmksummary, vmkwarning)
Данный параметр позволяет включить регистрацию событий, связанных с виртуальными машинами и гипервизорами. По умолчанию значение данного параметра: **Выкл**..
vSphere: Зачистка ФС (служба eraser)
Данный параметр позволяет включить регистрацию событий, связанных с зачисткой файловой системы гипервизора. По умолчанию значение данного параметра: **Выкл**..
Уведомления: Операции с виртуальными машинами
По умолчанию значение данного параметра: **Выкл**..
Уведомления: Операции со снапшотами
Данный параметр позволяет включить регистрацию событий, связанных с созданием снапшотов. По умолчанию значение данного параметра: **Выкл**..
Уведомления: Операции с виртуальными дисками
Данный параметр позволяет включить регистрацию событий, связанных виртуальными дисками. По умолчанию значение данного параметра: **Выкл**..
Уведомления: Операции с объектами виртуальной сети
Данный параметр позволяет включить регистрацию событий, связанных с объектами виртуальной сети. По умолчанию значение данного параметра: **Выкл**..
Уведомления: Изменение общих настроек сервера виртуализации
Данный параметр позволяет включить регистрацию событий, связанных изменением настроек сервера виртуализации. По умолчанию значение данного параметра: **Выкл**..

8.2.2 Аудит гипервизоров KVM

Просмотр и редактирование параметров аудита гипервизоров для гипервизоров oVirt происходит на

уровне группы oVirt в категории **Параметры безопасности KVM** → **Политики аудита** (см. Рисунок 166).

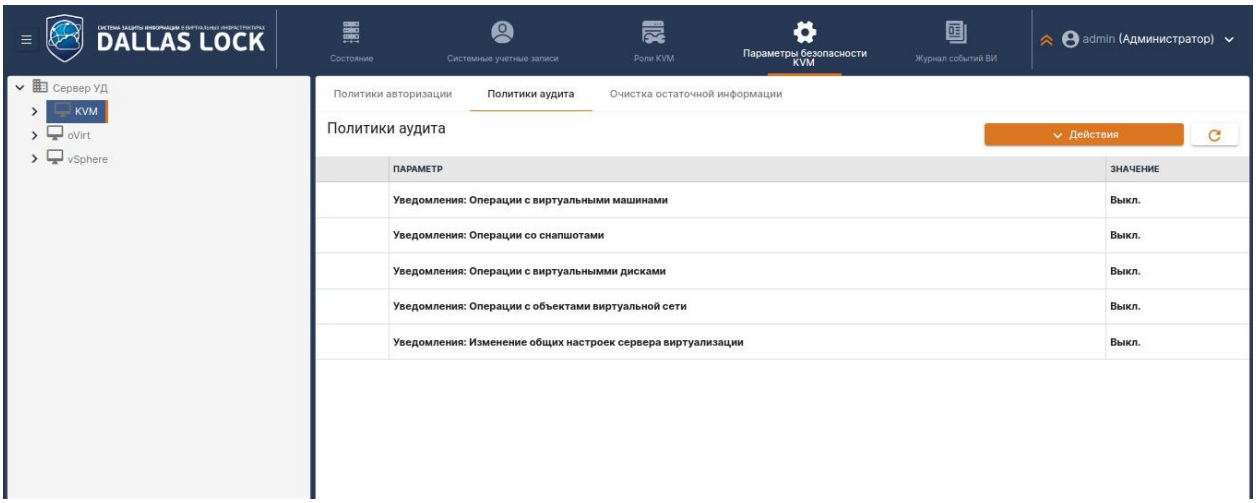

Рисунок 166. Аудит гипервизоров KVM

Доступны следующие параметры:

Уведомления: Операции с виртуальными машинами
Данный параметр позволяет включить регистрацию событий, связанных с виртуальными машинами. Параметр может принимать значение **Вкл** или **Выкл**.
Уведомления: Операции со снапшотами
Данный параметр позволяет включить регистрацию событий, связанных со снапшотами. Параметр может принимать значение **Вкл** или **Выкл**.
Уведомления: Операции с виртуальными дисками
Данный параметр позволяет включить регистрацию событий, связанных с виртуальными дисками. Параметр может принимать значение **Вкл** или **Выкл**.
Уведомления: Операции с объектами выртуальной сети
Данный параметр позволяет включить регистрацию событий, связанных с объектами виртуальной сети. Параметр может принимать значение **Вкл** или **Выкл**.
Уведомления: Изменение общих настроек сервера виртуализации
Данный параметр позволяет включить регистрацию событий, связанных с изменением общих настроек сервера виртуализации. Параметр может принимать значение **Вкл** или **Выкл**.

Чтобы изменить значение параметра, необходимо выбрать этот параметр в списке и вызвать окно изменения политики двойным щелчком мыши либо нажав кнопку **Редактировать** в блоке *Действия*. Выбрать значение и нажать кнопку **ОК** (см. Рисунок 167).

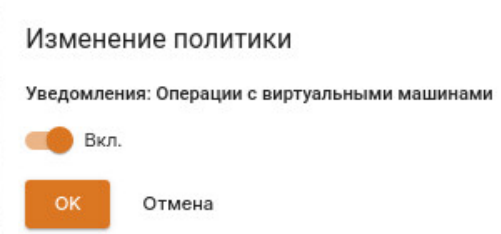

Рисунок 167. Изменение политики аудита KVM

После внесения всех изменений необходимо в блоке *Действия* нажать кнопку **Сохранить**.

Параметры, настроенные на уровне группы KVM, по умолчанию наследуются на уровне серверов виртуализации (подробнее см. п. 3.7 «Наследование настроек»).

Для редактирования параметров наследования необходимо перейти на уровень сервера виртуализации KVM на вкладку *Параметры безопасности KVM* и выбрать категорию **Политики**

аудита (см. Рисунок 168).

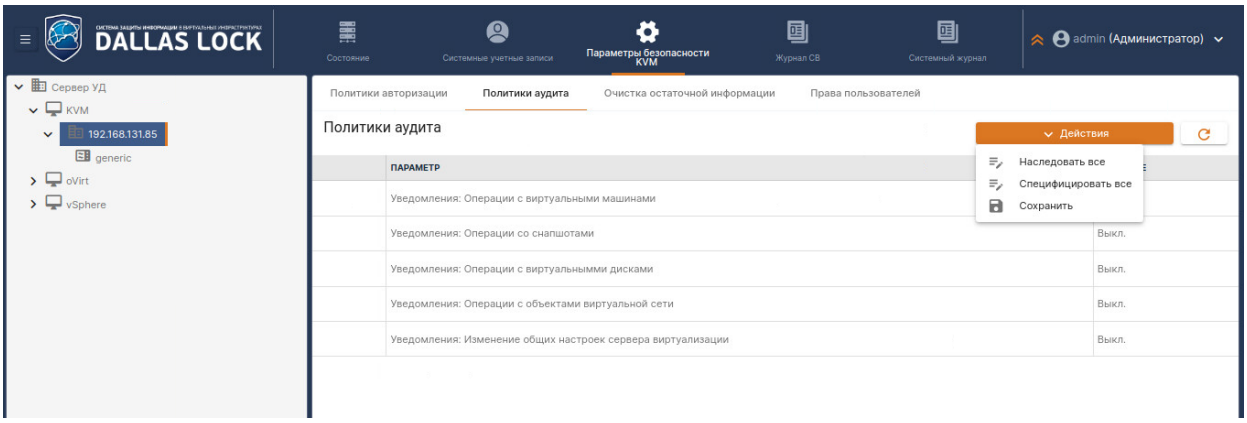

Рисунок 168. Настройка параметров аудита KVM на уровне СВ

Чтобы отменить наследование всех настроек параметров аудита гипервизоров группы KVM в блоке *Действия* необходимо нажать кнопку **Специфицировать все настройки**. Чтобы включить наследование всех настроек параметров аудита гипервизоров группы KVM в блоке *Действия* необходимо нажать кнопку **Наследовать все настройки**.

Для настройки конкретного параметра необходимо двойным щелчком мыши на нем вызвать окно редактирования параметров безопасности. Выбрать необходимое значение и нажать кнопку **ОК** (см. Рисунок 169).

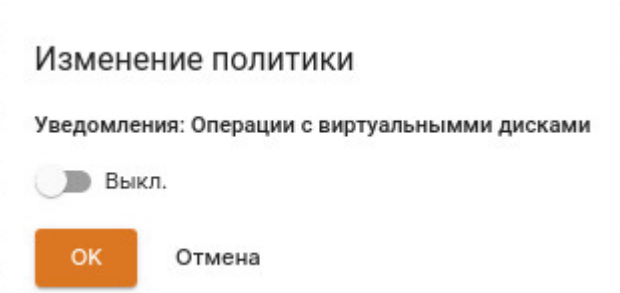

Рисунок 169. Редактирование параметров аудита KVM на уровне СВ

После внесения всех изменений необходимо в блоке *Действия* нажать кнопку **Сохранить**.

9 ЕДИНЫЙ ЦЕНТР УПРАВЛЕНИЯ DALLAS LOCK

Для реализации централизованного управления различными модулями на клиентах необходимо использовать Единый центр управления **Dallas Lock** (**ЕЦУ Dallas Lock**), управление которым осуществляется через пользовательский интерфейс — консоль **ЕЦУ**.

ЕЦУ Dallas Lock позволяет осуществлять централизованное управление такими модулями клиентов, как **СЗИ Dallas Lock 8.0** редакций «К» и «С» (включая модули МЭ и СОВ), **СЗИ НСД Dallas Lock Linux**, **СЗИ ВИ Dallas Lock** редакции «Стандартная» и «Расширенная», **СДЗ Dallas Lock** и **WAF Dallas Lock**.

При работе с модулями **СЗИ ВИ Dallas Lock** доступны следующие возможности:

- отображение информации о состоянии модуля;
- синхронизация политик/пользователей[11];
- управление пользователями и группами пользователей[11] на модуле;
- синхронизация и управление политиками безопасности;
- настройка неактивного режима работы модуля[12];
- управление заданиями на:
  - проверку обновлений;
  - получение конфигурации;
  - применение конфигурации;
  - получение отчета о параметрах безопасности **СЗИ ВИ**;
- сбор журналов модуля;
- открытие веб-интерфейса администрирования;
- отправка сигнализации об инцидентах безопасности.

Некоторые параметры безопасности могут быть настроены сразу для всего **ДБ**, некоторые — для отдельных клиентов.

9.1 Ввод СЗИ ВИ в ДБ ЕЦУ

Ввести модуль **СЗИ ВИ Dallas Lock** в Домен безопасности можно через веб-консоль **ЦУ СЗИ ВИ Dallas Lock**.

При вводе модуля **СЗИ ВИ Dallas Lock** в **ДБ** должен быть соблюден ряд условий:

1. в ЛВС должен быть работающий сервер **ЕЦУ**;
2. между модулем и сервером **ЕЦУ** должен быть свободный обмен пакетами по TCP/IP порту 1790

После ввода модуля **СЗИ ВИ Dallas Lock** под управление **ЕЦУ** значения параметров безопасности подлежат синхронизации со значениями политик **ЕЦУ** для базовой группы «Нераспределенные объекты».

Для ввода модуля в ДБ через веб-консоль **ЦУ СЗИ ВИ Dallas Lock** необходимо:

1. убедиться, что сервер **ЕЦУ** доступен по сети;
2. запустить ЦУ **СЗИ ВИ**;
3. выбрать в дополнительном меню пункт *Параметры ЕЦУ* (см. Рисунок 170);

[11] Для модулей **СЗИ ВИ ИК4**. Для **СЗИ ВИ ИК5** доступно управление встроенными учетными записями пользователей на модуле и синхронизация встроенных учетных записей пользователей.

[12] Для модулей **СЗИ ВИ ИК4**.

Рисунок 170. Параметры ЕЦУ

4. в появившемся окне **Параметры ЕЦУ** поставить флаг в поле *Под управлением ЕЦУ* и указать следующие данные (см. Рисунок 171):
   - DNS-имя или IP-адрес сервера **ЕЦУ**,
   - имя АРМ, в составе которого необходимо ввести модуль,
   - ключ доступа к **ДБ ЕЦУ**;

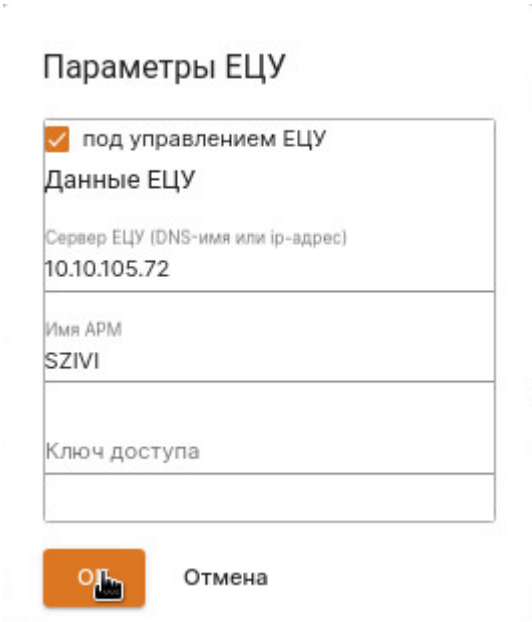

Рисунок 171. Окно «Параметры ЕЦУ»

5. нажать кнопку **ОК**, и будет инициировано создание АРМ и регистрация модуля в его составе.

Если процесс ввода модуля в ДБ прошел успешно, то через некоторое время появится соответствующие записи в журнале **ЦУ СЗИ ВИ** (см. Рисунок 172).

502	10.12.2024, 16:14:46	oVirt	Изменена политика	Политика 'Виртуальная машина: Проверять целостность при загрузке ОС'. Старое значение: Да, новое значение: Нет	ЕЦУ	Успех
501	10.12.2024, 16:14:46	oVirt	Изменена политика	Политика 'oVirt: Напоминать о смене пароля за'. Старое значение: 3 дн., новое значение: 1 дн.	ЕЦУ	Успех
500	10.12.2024, 16:14:46	oVirt	Изменена политика	Политика 'oVirt: Максимальный срок действия пароля'. Старое значение: 42 дн., новое значение: 180 дн.	ЕЦУ	Успех
499	10.12.2024, 16:14:46	oVirt	Изменена политика	Политика 'oVirt: Минимальная длина пароля'. Старое значение: 8, новое значение: 6	ЕЦУ	Успех
498	10.12.2024, 16:14:46	oVirt	Изменена политика	Политика 'Максимальное количество ошибок ввода пароля'. Старое значение: 3, новое значение: 5	ЕЦУ	Успех
497	10.12.2024, 16:14:46	KVM	Изменена политика	Всего изменено политик: 2	ЕЦУ	Успех
496	10.12.2024, 16:14:46	KVM	Изменена политика	Политика 'Виртуальная машина: Проверять целостность при загрузке ОС'. Старое значение: Да, новое значение: Нет	ЕЦУ	Успех
495	10.12.2024, 16:14:46	KVM	Изменена политика	Политика 'Максимальное количество ошибок ввода пароля'. Старое значение: 3, новое значение: 5	ЕЦУ	Успех
494	10.12.2024, 16:14:46	Сервер УД	Изменена политика	Всего изменено политик: 2	ЕЦУ	Успех
493	10.12.2024, 16:14:46	Сервер безопасности	Применена политика	Настройка локального МЭ для работы с syslog: получение данных syslog настроено на порт 514 (без SSL). Результат: sh: строка 1: firewall-cmd: команда не найдена	System	Отказ: Ошибка выполнения shell команды.
492	10.12.2024, 16:14:45	Сервер УД	Изменена политика	Политика 'Разрешена генерация пароля'. Старое значение: Да, новое значение: Нет	ЕЦУ	Успех
491	10.12.2024, 16:14:45	Сервер УД	Изменена политика	Политика 'Максимальное количество ошибок ввода пароля'. Старое значение: 3, новое значение: 5	ЕЦУ	Успех
490	10.12.2024, 16:14:45	Сервер безопасности	Начата синхронизация политик с ЕЦУ	10.10.105.47:17900	ЕЦУ (DESKTOP-1BGEAP2:17900)	Успех

Рисунок 172. Записи об успешной регистрации модуля в журнале ЦУ СЗИ ВИ

Если во время процесса ввода модуля **СЗИ ВИ Dallas Lock** в **ДБ** возникает ошибка, содержащая текст «*Ошибка регистрации в ЕЦУ! (Некорректные параметры вызова функции.)*», то необходимо выполнить следующие действия:

- в настройках **ЕЦУ** (см. «Инструкция по использованию ЕЦУ» - «Общие параметры работы») в параметре **Способ подключения к серверу** установить значение *Оба способа* и выбрать приоритет подключения по IP-адресам;
- подождать 30 секунд для применения новых значений;
- повторить попытку ввода модуля **СЗИ ВИ Dallas Lock** в **ДБ**.

После при необходимости можно установить значение по умолчанию для параметра **Способ подключения к серверу** (оба способа с приоритетом подключения по полным доменным именам), на управление уже зарегистрированными в **ДБ** модулями **СЗИ ВИ Dallas Lock** это не повлияет.

9.2 Вывод СЗИ ВИ из ДБ ЕЦУ

Вывести модуль **СЗИ ВИ Dallas Lock** из Домена безопасности можно следующими способами:

- с помощью консоли **ЕЦУ** (см. «Инструкция по использованию ЕЦУ» – «Настройка модуля»);
- через веб-консоль **ЦУ СЗИ ВИ Dallas Lock**.

Для вывода модуля через веб-консоль **ЦУ СЗИ ВИ Dallas Lock** необходимо:

1. запустить веб-консоль **СЗИ ВИ**, подключиться к Центру управления **СЗИ ВИ**;
2. выбрать в дополнительном меню пункт *Параметры ЕЦУ*;
3. в появившемся окне **Параметры ЕЦУ** убрать флаг в поле *Под управлением ЕЦУ* и нажать кнопку «ОК».
4. в появившемся диалоговом окне нажать кнопку **Да**, будет инициировано удаление АРМ из **ДБ ЕЦУ** (см. Рисунок 173);

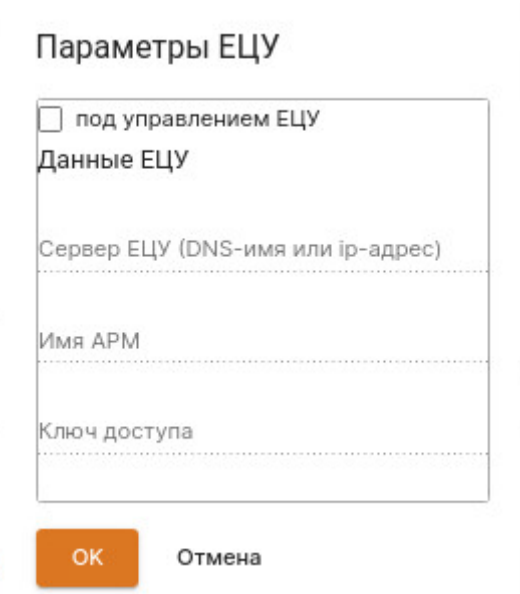

Рисунок 173. Вывод АРМ из-под управления сервера ЕЦУ

Если процесс вывода модуля из **ДБ** прошел успешно, то через некоторое время в журнале **ЦУ СЗИ ВИ** появится соответствующая запись (см. Рисунок 174).

520	10.12.2024, 16:19:36	Сервер безопасности	Вывод модуля СЗИ ВИ из под управления ЕЦУ	10.10.105.47:17900	admin (127.0.0.1)	Успех

Рисунок 174. Вывод модуля СЗИ ВИ из-под управления ЕЦУ

В консоли **ЕЦУ** удаленный модуль переместится в базовую группу *Удаленные объекты» дерева ДБ*.

10 ДОПОЛНИТЕЛЬНЫЕ ВОЗМОЖНОСТИ

10.1 Сохранение конфигурации ЦУ СЗИ ВИ

С помощью резервной копии файла конфигурации **СЗИ ВИ** позволяет быстро возобновить работу в случае сбоя или переустановки ЦУ **СЗИ ВИ**.

Сохранение и применение файла конфигурации **ЦУ СЗИ ВИ** осуществляется только на соответствующем **ЦУ СЗИ ВИ** с соответствующей версией, на котором данная конфигурация была сформирована. Использовать данный механизм для обновления **СЗИ ВИ** на более старшую версию не рекомендуется. Подробнее про обновление см. п. 2.9 «Обновление системы защиты».

Перед операциями сохранения или применения конфигурации необходимо отключить все фоновые операции по синхронизации, контрольной целостности (КЦ) и сбору журналов (кнопка дополнительного меню консоли – вкладка *Параметры сервера УД* и далее на всех вкладках (*Сервер УД*, *v Sphere*, *oVirt*, *KVM*), (подробнее см. п. 3.3 «Основные параметры»).

Для сохранения настроек **ЦУ СЗИ ВИ** необходимо открыть дополнительное меню Консоли и нажать кнопку **Сохранить конфигурацию** (см. Рисунок 175).

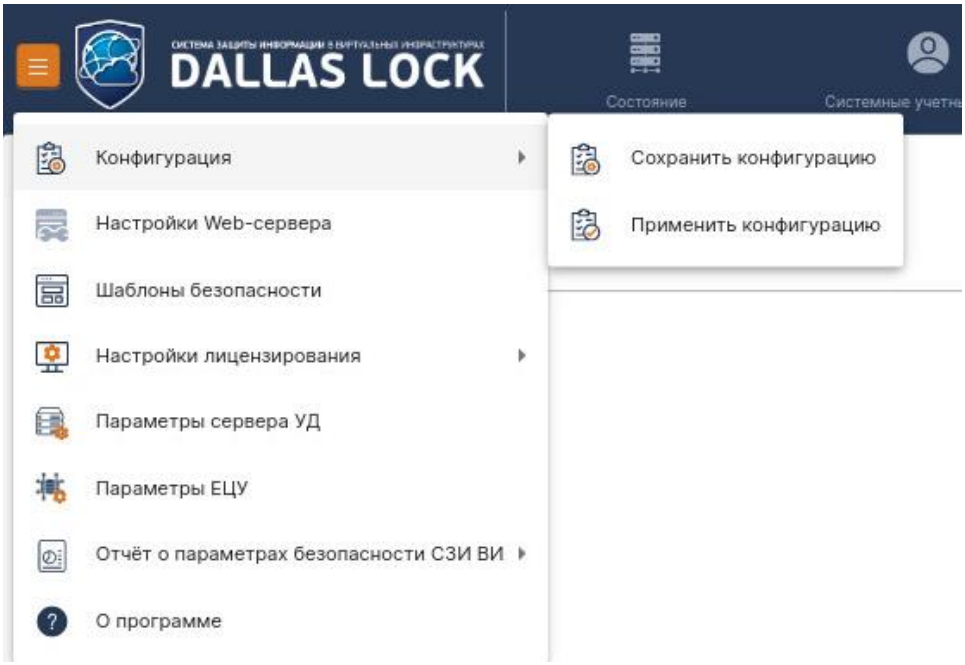

Рисунок 175. Меню Консоли

Появится окно **Начато сохранение конфигурации** (см. Рисунок 176), после его исчезновения файл конфигурации ЦУ **СЗИ ВИ** будет сформирован и сохранен. Сохраненный файл конфигурации будет иметь расширение *.bin.

Рисунок 176. Окно «Начато сохранение конфигурации»

Применяется данный файл конфигурации на уже установленный ЦУ **СЗИ ВИ** с помощью пункта *Применить конфигурацию* кнопки дополнительного меню Консоли.

Перед применением ранее сохраненной конфигурации необходимо отключить все фоновые операции по синхронизации, контрольной целостности (КЦ) и сбору журналов (кнопка дополнительного меню консоли – вкладка *Параметры сервера УД* и далее на всех вкладках (*Сервер УД*, *v Sphere*, *oVirt*, *KVM*), (подробнее см. п. 3.3 «Основные параметры»).
Данные процессы выполняемые обновременно с применением файла конфигурации могут нарушить процесс восстановления.

10.2 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).

10.2.1 Включение логов на агентах Linux (ESXi, vCSA, KVM/oVirt/zVirt/HOSTVM/RedVirt)

Для включения логов агента/Ядра нужно создать пустой файл в директории /tmp/ следующей командой в директории /tmp/

- *touch dlneedlog*.

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».

10.3 Настройки лицензирования

Для изменения параметров лицензии для Сервера УД необходимо открыть дополнительное меню Консоли и нажать кнопку **Настройки лицензирования…** и выбрать *Выбор файла-ключа* (см. Рисунок 177).

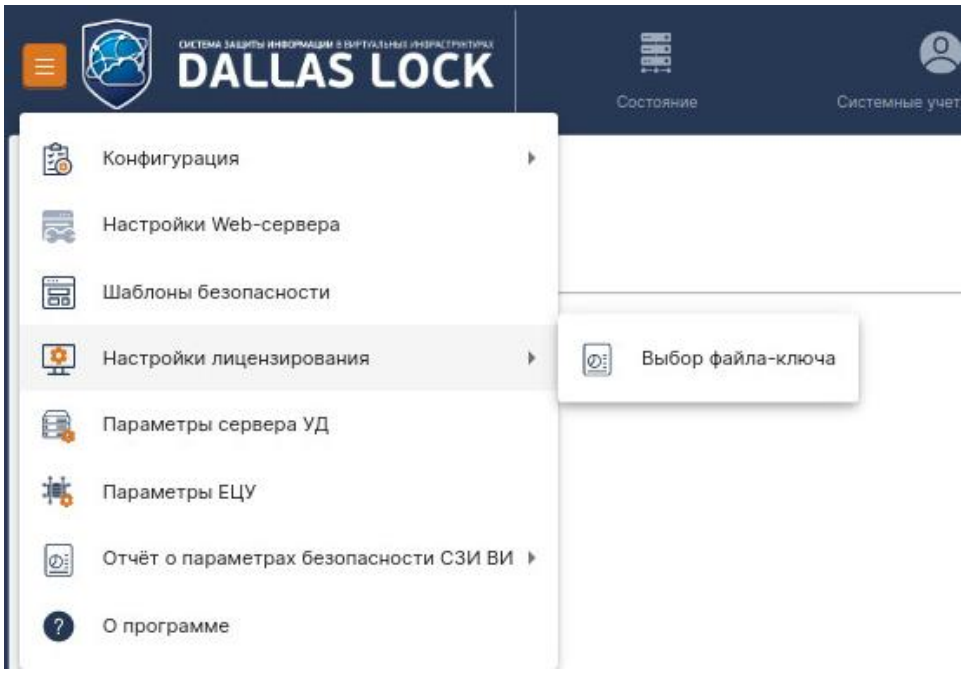

Рисунок 177. Настройки лицензирования

После чего выбрать свой файл-ключ и нажать **Применить** (см. Рисунок 178).

Рисунок 178. Настройка сервера лицензий для ЦУ СЗИ ВИ

10.4 Шаблоны безопасности

В **СЗИ ВИ Dallas Lock** реализована возможность применения шаблонов безопасности, содержащих в себе конкретные настройки для **СЗИ ВИ** под требования нормативных документов. После установки выставлены настройки по умолчанию. Для применения шаблона безопасности в дополнительном меню Консоли необходимо нажать на пункт **Шаблоны безопасности** (см. Рисунок 179).

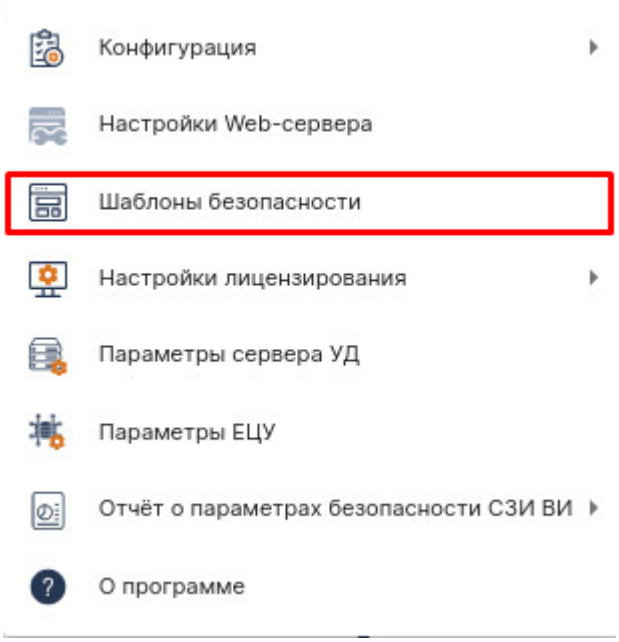

Рисунок 179. Шаблоны безопасности

В появившемся окне установить флаг в поле с необходимым шаблоном безопасности, нажать кнопку **Применить** (см. Рисунок 180). При этом можно выбрать сразу несколько пунктов – шаблоны могут складываться, в таком случае при разных значениях одинаковых параметров, устанавливается самое ограничивающее значение.

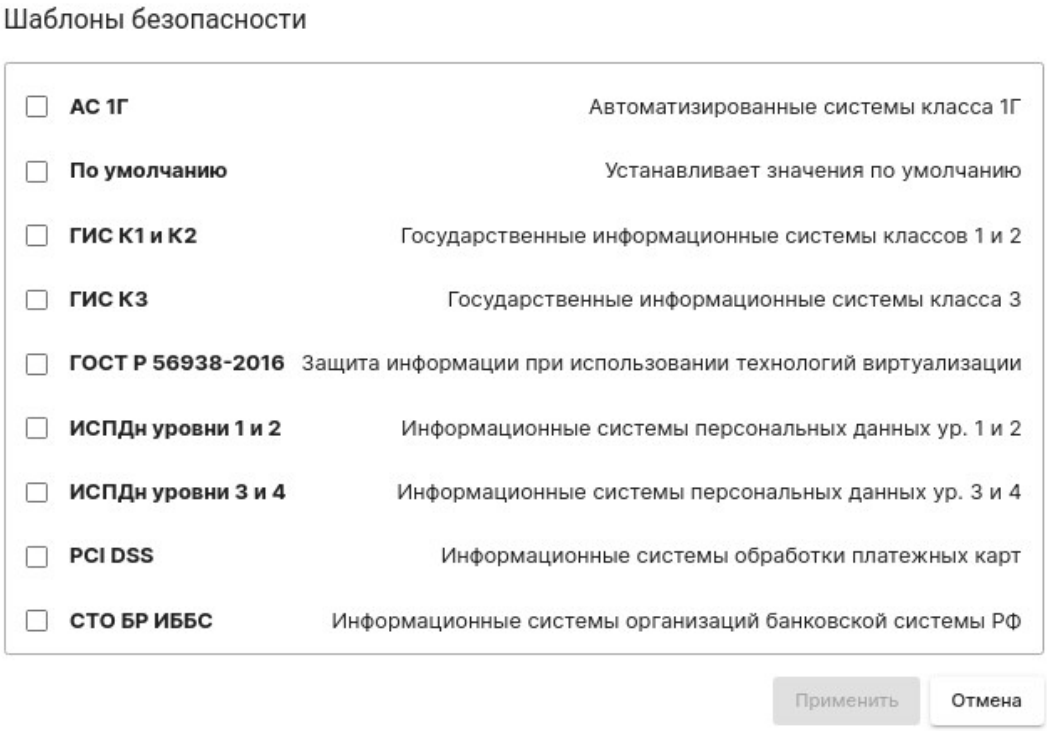

Рисунок 180. Выбор шаблонов безопасности

Результатом произведенных действий будут настройки, выставленные в соответствии с требованиями выбранной политики безопасности. Перечень настроек приведен в Приложение № 1.

10.5 Снапшоты

СЗИ ВИ Dallas Lock позволяет делать снимки состояния ВМ для платформ виртуализации vSphere и oVirt.

Для корректной установки **СЗИ Dallas Lock 8.0** на 32-х разрядную версию ОС Windows требуется не менее 2 ГБ оперативной памяти.

СЗИ ВИ не контролирует количество снапшотов и занимаемый ими объем хранилищ, поэтому при создании автоматического сценария создания снапшотов, необходимо контролировать их количество и занимаемую ими память хранилища.

Для платформы KVM, при создании снапшота для ВМ в выключенном состоянии, если используется диск с форматом «qcow2», то происходит изменение в его метаданных, что приводит к изменению КС. Если диск находится под КЦ, будет зафиксировано событие НСД при последующей проверке КС.
Для корректной работы рекомендуется учитывать эту особенность при планировании операций со снапшотами.

10.5.1 Ручное создание снапшота

Для создания снапшота необходимо:
Перейти на уровень ВМ и открыть категорию **Состояние** → нажать **Создать снапшот** в блоке *Действия*.

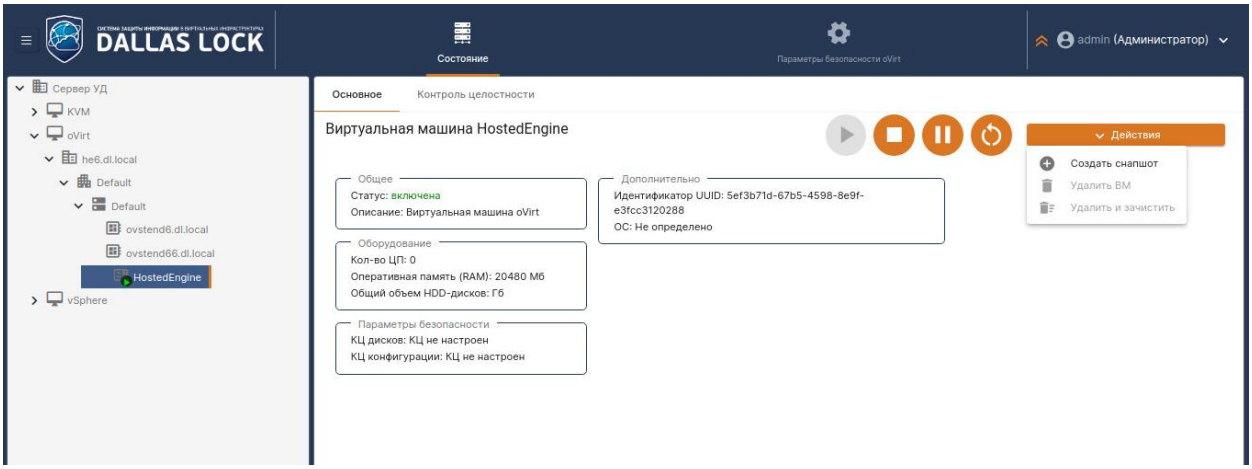

Рисунок 181. Ручное создание снапшота

При создании снапшота присваевается имя по умолчанию или заданное пользователем имя, дата и время создания.

10.5.2 Автоматическое снятие снапшотов

СЗИ ВИ Dallas Lock позволяет настроить автоматическое снятие снапшотов с заданной периодичностью и по расписанию.
Для настройки расписания снятия снапшотов необходимо:

1. Перейти на уровень СВ vSphere, oVirt или гипервизора ESXi и открыть категорию **Состояние** → **Управление снапшотами ВМ**.
2. Выбрать из списка виртуальную машину.
3. Нажать кнопку **Действия** и выбрать **Настроить расписание…**.
4. В появившемся окне задать необходимые параметры расписания снятия снапшотов, нажать стрелку и **ОК** (см. Рисунок 182).

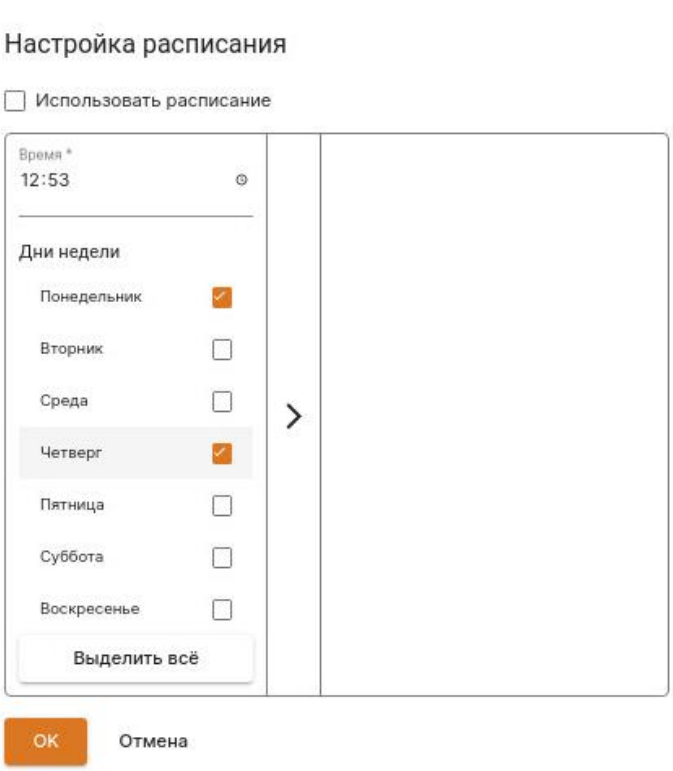

Рисунок 182. Настройка расписания

Для настройки периодичности снятия снапшотов необходимо:

1. Перейти на уровень СВ vSphere, oVirt или гипервизора ESXi и открыть категорию **Состояние → Управление снапшотами ВМ**.
2. Выбрать из списка виртуальную машину.
3. Нажать кнопку **Действия** и выбрать **Настроить периодичность**.
4. В появившемся окне выбрать необходимый интервал снятия снапшотов (см. Рисунок 183).

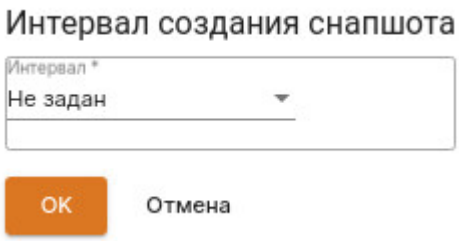

Рисунок 183. Настройка интервала создания снапшота

Для отключения всех настроенных параметров снятия снапшотов ВМ необходимо:

1. Перейти на уровень СВ vSphere, oVirt или гипервизора ESXi и открыть категорию **Состояние → Управление снапшотами ВМ**.
2. Нажать кнопку **Действия** и выбрать **Отключить все**.

10.6 Создание отчета о параметрах безопасности и назначенных правах

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* (см. Рисунок 184) и нажать **Сгенерировать**, после чего дождаться построения отчёта.

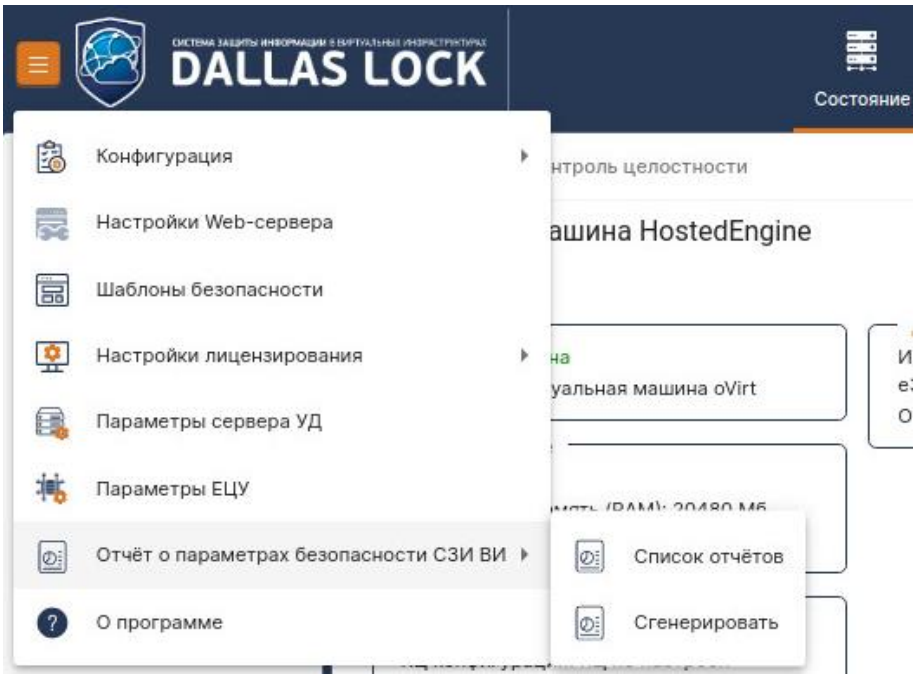

Рисунок 184. Окно создания отчета

Затем в пункте *Отчет о параметрах безопасности СЗИ ВИ* выбрать **Список отчётов** и, нажав на кнопку , стоящую напротив нужного отчёта 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»;
- «Номер системного блока».

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

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.

11 Приложение № 1

Параметры, настраиваемые в политиках безопасности

1. Шаблон: По умолчанию

1.1. Сервер УД

1.1.1. Политики авторизации

Параметр	Значение
Время блокировки учетной записи в случае ввода неправильных паролей (мин.), (1 – 300)	**15**
Максимальное количество ошибок ввода пароля (попытки) (1 – 10)	**5**
Включить синхронизацию времени по NTP	**Используется**

1.1.2. Политики паролей

Параметр	Значение
Максимальный срок действия пароля (1 – 180)	**42**
Минимальная длина пароля (симв.) (1 – 14)	**8**
Необходимо наличие спец. символов	**Нет**
Необходимо наличие цифр	**Нет**
Необходимо наличие строчных и прописных букв	**Нет**
Необходимо отсутствие цифры в первом и последнем символах	**Нет**
Разрешена генерация пароля	**Да**

1.1.3. Политики аудита

Параметр	Значение
Регистрация НСД: Ошибка выполнения задачи	**Вкл.**
Регистрация НСД: Доступ запрещен	**Вкл.**
Регистрация НСД: События входов	**Вкл.**
Регистрация НСД: Вход: Учетная запись заблокирована	**Вкл.**
Регистрация НСД: Вход: Доступ запрещен	**Вкл.**
Регистрация НСД: События нарушения контроля целостности ВМ	**Вкл.**
Регистрация НСД: Нарушение КЦ: Попытка запуска/клонирования ВМ с нарушенной целостностью	**Вкл.**
Регистрация НСД: Нарушение КЦ: Попытка запуска ВМ напрямую с гипервизора	**Вкл.**
Регистрация НСД: Нарушение КЦ: Системные файлы	**Вкл.**
Регистрация НСД: Нарушение КЦ: Прогр. апп. среда	**Вкл.**
Регистрация НСД: Нарушение КЦ: Файл был удален	**Вкл.**
Получение событий syslog	**Получение по UDP**
Порт для работы syslog по UDP	**514**
Порт для работы syslog по SLL	**1514**

1.2. СЗИ ВИ (vSphere)

1.2.1. Политики авторизации

Параметр	Значение
Время блокировки учетной записи в случае ввода неправильных паролей (мин.) (1 – 300)	**15**
Максимальное количество ошибок ввода пароля (1 – 10)	**5**
Включить синхронизацию времени по NTP	**Используется**
vSphere: запрет на работу через Web-клиент	**Нет**
vCSA: Время, в течение которого подсчитываются ошибки ввода пароля (минуты)	**1**

Параметр	Значение
vCSA: Разрешить локальный вход с консоли	**Да**
vCSA: Разрешить вход на Web-клиент VCSA Management Interface (VAMI)	**Да**
vCSA: Блокировать протокол SSH	**Нет**
ESXi: Период неиспользования (дни)	**1**
ESXi: Время, в течение которого допускается выполнить одну попытку ввода пароля (минуты)	**1**
ESXi: Количество попыток ввода нового пароля, удовлетворяющего текущим парольным политикам (попытки)	**3**
ESXi: Запретить возможность авторизации (Lockdown Mode)	**Не запрещать**
ESXi: Блокировать протокол SSH	**Нет**

1.2.2. Политики паролей

Параметр	Значение
vSphere: Максимальный срок действия пароля (1 – 180 дней)	**180**
vSphere: Минимальная длина пароля (симв.) (1 – 30)	**6**
ESXi: Напоминать о смене пароля за	**Не используется**
ESXi: Минимальное количество классов символов	**Не используется**
vCenter: Количество предыдущих паролей, которые пользователь не может использовать (шт.) (1 – 10)	**5**
vCenter: Максимальная длина пароля (симв.) (1 – 40)	**20**
vCenter: Максимально допустимое количество одинаковых символов, стоящих рядом (симв.) (1 – 5)	**3**
vCenter: Минимальное количество прописных букв (шт.) (1 – 9)	**Не используется**
vCenter: Минимальное количество символов алфавита (шт.) (1 – 15)	**Не используется**
vCenter: Минимальное количество специальных символов (шт.) (1 – 9)	**Не используется**
vCenter: Минимальное количество строчных букв (шт.) (1 – 9)	**Не используется**
vCenter: Минимальное количество цифр (шт.) (1 – 9)	**Не используется**

1.2.3. Политики аудита

Параметр	Значение
vSphere: ESXi Shell (служба shell)	**Выкл.**
vSphere: Агент ESXi (служба hostd)	**Выкл.**
vSphere: USB-устройства (служба usb)	**Выкл.**
vSphere: Аутентификация (службы auth, login, vmauthd)	**Выкл.**
vSphere: Системные события (служба syslog)	**Выкл.**
vSphere: Виртуальные машины (службы vmauthd, vmkdevmgr, vmkernel, vmkeventd, vmksummary, vmkwarning)	**Выкл.**
vSphere: Зачистка ФС (события eraser)	**Выкл.**
Уведомления: Операции с виртуальными машинами	**Выкл.**
Уведомления: Операции со снапшотами	**Выкл.**
Уведомления: Операции с виртуальными дисками	**Выкл.**
Уведомления: Операции с объектами виртуальной сети	**Выкл.**
Уведомления: Изменение общих настроек сервера виртуализации	**Выкл.**

1.2.4. Очистка остаточной информации

Параметр	Значение
Количество циклов затирания (циклы) (1 – 10)	**1**

1.3. СЗИ ВИ (oVirt)

1.3.1. Политики авторизации

Параметр	Значение
Максимальное количество ошибок ввода пароля	**5**
Время блокировки учетной записи в случае ввода неправильных паролей (минуты)	**15**
Включить синхронизацию времени по NTP	**Используется**
KVM: блокировать протокол SSH	**Да**
KVM: блокировать доступ к Cockpit Web Interface	**Да**

1.3.2. Политики паролей

Параметр	Значение
oVirt: Минимальная длина пароля (символы)	**8**
oVirt: Максимальный срок действия пароля (дни)	**42**
oVirt: Напоминать о смене пароля за (дни)	**Не используется**
oVirt: Минимальное количество прописных букв (штук)	**Не используется**
oVirt: Минимальное количество строчных букв (штук)	**Не используется**
oVirt: Минимальное количество специальных символов (штук)	**Не используется**
oVirt: Минимальное количество цифр (штук)	**Не используется**
oVirt: Количество предыдущих паролей, которые пользователь не может использовать (штук)	**5**

1.3.3. Политики аудита

Параметр	Значение
Уведомления: Операции с виртуальными машинами	**Выкл.**
Уведомления: Операции со снапшотами	**Выкл.**
Уведомления: Операции с виртуальнымми дисками	**Выкл.**

1.3.4. Очистка остаточной информации

Параметр	Значение
Количество циклов затирания (циклы) (1 – 10)	**1**

1.4. СЗИ ВИ (KVM)

1.4.1. Политики авторизации

Параметр	Значение
Максимальное количество ошибок ввода пароля (попытки)	**5**
Время блокировки учетной записи в случае ввода неправильных паролей (мин.) (1 – 300)	**15**
KVM: блокировать протокол SSH	**Да**
Включить синхронизацию времени по NTP	**Используется**
KVM: Блокировать доступ к Cockpit Web Interface	**Да**

1.4.2. Политики аудита

Параметр	Значение
Уведомления: Операции с виртуальными машинами	**Выкл.**
Уведомления: Операции со снапшотами	**Выкл.**
Уведомления: Операции с виртуальнымми дисками	**Выкл.**
Уведомления: Операции с объектами виртуальной сети	**Выкл.**
Уведомления: Изменение общих настроек сервера виртуализации	**Выкл.**

1.4.3. Очистка остаточной информации

Параметр	Значение
Гипервизоры: Количество циклов затирания	**1**

2. Шаблон: АС 1Г

2.1. Сервер УД

2.1.1. Политики авторизации

Параметр	Значение
Время блокировки учетной записи в случае ввода неправильных паролей (мин.), (1 – 300)	**15**
Максимальное количество ошибок ввода пароля (попытки) (1 – 10)	**5**
Включить синхронизацию времени по NTP	**Используется**

2.1.2. Политики паролей

Параметр	Значение
Встроенные УЗ. Максимальный срок действия пароля (1 – 180)	**42**
Встроенные УЗ. Минимальная длина пароля (симв.) (1 – 14)	**6**
Встроенные УЗ. Необходимо наличие спец. символов	**Нет**
Встроенные УЗ. Необходимо наличие цифр	**Да**
Встроенные УЗ. Необходимо наличие строчных и прописных букв	**Нет**
Встроенные УЗ. Необходимо отсутствие цифры в первом и последнем символах	**Нет**
Разрешена генерация пароля	**Да**

2.1.3. Политики аудита

Параметр	Значение
Регистрация НСД: Ошибка выполнения задачи	**Вкл.**
Регистрация НСД: Доступ запрещен	**Вкл.**
Регистрация НСД: События входов	**Вкл.**
Регистрация НСД: Вход: Учетная запись заблокирована	**Вкл.**
Регистрация НСД: Вход: Доступ запрещен	**Вкл.**
Регистрация НСД: События нарушения контроля целостности ВМ	**Вкл.**
Регистрация НСД: Нарушение КЦ: Попытка запуска/клонирования ВМ с нарушенной целостностью	**Вкл.**
Регистрация НСД: Нарушение КЦ: Попытка запуска ВМ напрямую с гипервизора	**Вкл.**
Регистрация НСД: Нарушение КЦ: Системные файлы	**Вкл.**
Регистрация НСД: Нарушение КЦ: Прогр. апп. среда	**Вкл.**
Регистрация НСД: Нарушение КЦ: Файл был удален	**Вкл.**
Получение событий syslog	**Получение по UDP**
Порт для работы syslog по UDP	**514**
Порт для работы syslog по SLL	**1514**

2.2. СЗИ ВИ (vSphere)

2.2.1. Политики авторизации

Параметр	Значение
Максимальное количество ошибок ввода пароля (попытки)	**5**
Время блокировки учетной записи в случае ввода неправильных паролей (минуты)	**15**
Включить синхронизацию времени по NTP	**Используется**
vSphere: Запрет на работу через Web-клиент	**Нет**
vCSA: Время, в течение которого подсчитываются ошибки ввода пароля (минуты)	**1**
vCSA: Разрешить локальный вход с консоли	**Да**
vCSA: Разрешить вход на Web-клиент VCSA Management Interface (VAMI)	**Да**

Параметр	Значение
vCSA: Блокировать протокол SSH	**Нет**
ESXi: Время, в течение которого допускается выполнить одну попытку ввода пароля (минуты)	**1**
ESXi: Период неиспользования (дни)	**1**
ESXi: Количество попыток ввода нового пароля, удовлетворяющего текущим парольным политикам (попытки)	**3**
ESXi: Запретить возможность авторизации (Lockdown Mode)	**Не запрещать**
ESXi: Блокировать протокол SSH	**нет**

2.2.2. Политики паролей

Параметр	Значение
vSphere: Максимальный срок действия пароля (1 – 180 дней)	**42**
vSphere: Минимальная длина пароля (симв.) (1 – 30)	**6**
vCenter: Максимальная длина пароля (символы)	**20**
vCenter: Количество предыдущих паролей, которые пользователь не может использовать (штук)	**5**
vCenter: Минимальное количество символов алфавита (штук)	**Не используется**
vCenter: Минимальное количество специальных символов (штук)	**Не используется**
vCenter: Минимальное количество прописных букв (штук)	**Не используется**
vCenter: Минимальное количество строчных букв (штук)	**Не используется**
vCenter: Минимальное количество цифр (штук)	**1**
vCenter: Максимально допустимое количество одинаковых символов, стоящих рядом (символы)	**3**
ESXi: Напоминать о смене пароля за (дни)	**Не используется**
ESXi: Минимальное количество классов символов (класс символов)	**Не используется**

2.2.3. Политики аудита

Параметр	Значение
vSphere: ESXi Shell (служба shell)	**Вкл.**
vSphere: Агент ESXi (служба hostd)	**Вкл.**
vSphere: USB-устройства (служба usb)	**Вкл.**
vSphere: Аутентификация (службы auth, login, vmauthd)	**Вкл.**
vSphere: Системные события (служба syslog)	**Вкл.**
vSphere: Виртуальные машины (службы vmauthd, vmkdevmgr, vmkernel, vmkeventd, vmksummary, vmkwarning)	**Вкл.**
vSphere: Зачистка ФС (события eraser)	**Вкл.**
Уведомления: Операции с виртуальными машинами	**Вкл.**
Уведомления: Операции со снапшотами	**Вкл.**
Уведомления: Операции с виртуальными дисками	**Вкл.**
Уведомления: Операции с объектами виртуальной сети	**Вкл.**
Уведомления: Изменение общих настроек сервера виртуализации	**Вкл.**

2.2.4. Очистка остаточной информации

Параметр	Значение
Количество циклов затирания (циклы) (1 – 10)	**1**

2.3. СЗИ ВИ (oVirt)

2.3.1. Политики авторизации

Параметр	Значение
Максимальное количество ошибок ввода пароля (попытки)	**5**
Время блокировки учетной записи в случае ввода неправильных паролей	**15**

Параметр	Значение
(минуты)	
Включить синхронизацию времени по NTP	**Используется**
KVM: блокировать протокол SSH	**Да**
KVM: блокировать доступ к Cockpit Web Interface	**Да**

2.3.2. Политики паролей

Параметр	Значение
oVirt: Минимальная длина пароля (символы)	**6**
oVirt: Максимальный срок действия пароля (дни)	**42**
oVirt: Напоминать о смене пароля за (дни)	**Не используется**
oVirt: Минимальное количество прописных букв (штук)	**Не используется**
oVirt: Минимальное количество строчных букв (штук)	**Не используется**
oVirt: Минимальное количество специальных символов (штук)	**Не используется**
oVirt: Минимальное количество цифр (штук)	**Не используется**
oVirt: Количество предыдущих паролей, которые пользователь не может использовать (штук)	**5**

2.3.3. Политики аудита

Параметр	Значение
Уведомления: Операции с виртуальными машинами	**Вкл.**
Уведомления: Операции со снапшотами	**Вкл.**
Уведомления: Операции с виртуальнымми дисками	**Вкл.**

2.3.4. Очистка остаточной информации

Параметр	Значение
Количество циклов затирания	**1**

2.4. СЗИ ВИ (KVM)

2.4.1. Политики авторизации

Параметр	Значение
Максимальное количество ошибок ввода пароля (попытки)	**5**
Время блокировки учетной записи в случае ввода неправильных паролей (минуты)	**15**
KVM: Блокировать протокол SSH	**Да**
Включить синхронизацию времени по NTP	**Используется**
KVM: Блокировать доступ к Cockpit Web Interface	**Да**
KVM: Блокировать запуск ВМ в пространстве пользователя	**Да**

2.4.2. Политики аудита

Параметр	Значение
Уведомления: Операции с виртуальными машинами	**Вкл.**
Уведомления: Операции со снапшотами	**Вкл.**
Уведомления: Операции с виртуальными дисками	**Вкл.**
Уведомления: Операции с объектами виртуальной сети	**Вкл.**
Уведомления: Изменение общих настроек сервера виртуализации	**Вкл.**

2.4.3. Очистка остаточной информации

Параметр	Значение
Количество циклов затирания	**1**

3. Шаблон: ГИС К1 и К2

3.1. Сервер УД

3.1.1. Политики авторизации

Параметр	Значение
Время блокировки учетной записи в случае ввода неправильных паролей (мин.), (1 – 300)	**15 мин**
Максимальное количество ошибок ввода пароля (попытки) (1 – 10)	**5**
Включить синхронизацию времени по NTP	**Используется**

3.1.2. Политики паролей

Параметр	Значение
Максимальный срок действия пароля (дней), (1 – 180)	**42 дн.**
Минимальная длина пароля (симв.) (1 – 14)	**6 симв.**
Необходимо наличие спец. символов	**Нет**
Необходимо наличие цифр	**Нет**
Необходимо наличие строчных и прописных букв	**Нет**
Необходимо отсутствие цифры в первом и последнем символах	**Нет**
Разрешена генерация пароля	**Да**

3.1.3. Политики аудита

Параметр	Значение
Регистрация НСД: Ошибка выполнения задачи	**Вкл.**
Регистрация НСД: Доступ запрещен	**Вкл.**
Регистрация НСД: События входов	**Вкл.**
Регистрация НСД: Вход: Учетная запись заблокирована	**Вкл.**
Регистрация НСД: Вход: Доступ запрещен	**Вкл.**
Регистрация НСД: События нарушения контроля целостности ВМ	**Вкл.**
Регистрация НСД: Нарушение КЦ: Попытка запуска/клонирования ВМ с нарушенной целостностью	**Вкл.**
Регистрация НСД: Нарушение КЦ: Попытка запуска ВМ напрямую с гипервизора	**Вкл.**
Регистрация НСД: Нарушение КЦ: Системные файлы	**Вкл.**
Регистрация НСД: Нарушение КЦ: Прогр. апп. среда	**Вкл.**
Регистрация НСД: Нарушение КЦ: Файл был удален	**Вкл.**
Получение событий syslog	**Получение по UDP**
Порт для работы syslog по UDP	**514**
Порт для работы syslog по SLL	**1514**

3.2. СЗИ ВИ (vSphere)

3.2.1. Политики авторизации

Параметр	Значение
Время блокировки учетной записи в случае ввода неправильных паролей (мин.) (1 – 300)	**15 мин.**
Максимальное количество ошибок ввода пароля (1 – 10)	**5**
vCSA: Блокировать протокол SSH	**Нет**
vCSA: Разрешить вход на Web-клиент VCSA Management Interface	**Да**
vCSA: Разрешить локальный вход с консоли	**Да**
vSphere: Запрет на работу через Web-клиент	**Нет**
ESXi: Блокировать протокол SSH	**Да**
ESXi: Время, в течение которого допускается выполнить одну попытку ввода пароля (минуты)	**1**
ESXi: Запретить возможность авторизации (Lockdown Mode)	**При удаленном подключении**
ESXi: Количество попыток ввода нового пароля, удовлетворяющего текущим парольным политикам (попытки) (1 – 10)	**3**

Параметр	Значение
ESXi: Период неиспользования	**1**
Включить синхронизацию времени по NTP	**Используется**
vCSA: Время, в течение которого подсчитываются ошибки ввода пароля (мин), (1 –300)	**1**

3.2.2. Политики паролей

Параметр	Значение
vSphere: Максимальный срок действия пароля (1 – 180)	**42 дн.**
vSphere: Минимальная длина пароля (симв.) (1 – 30)	**6**
ESXi: Напоминать о смене пароля за	**Не используется**
ESXi: Минимальное количество классов символов	**Не используется**
vCenter: Количество предыдущих паролей, которые пользователь не может использовать (шт.) (1 – 10)	**5**
vCenter: Максимальная длина пароля (симв.) (1 – 40)	**20**
vCenter: Максимально допустимое количество одинаковых символов, стоящих рядом (симв.) (1 – 5)	**3**
vCenter: Минимальное количество прописных букв (шт.) (1 – 9)	**Не используется**
vCenter: Минимальное количество символов алфавита (шт.) (1 – 15)	**Не используется**
vCenter: Минимальное количество специальных символов (шт.) (1 – 9)	**Не используется**
vCenter: Минимальное количество строчных букв (шт.) (1 – 9)	**Не используется**
vCenter: Минимальное количество цифр (шт.) (1 – 9)	**Не используется**

3.2.3. Политики аудита

Параметр	Значение
vSphere: Агент СВ vCenter	**Вкл.**
vSphere: ESXi Shell (служба shell)	**Вкл.**
vSphere: Агент ESXi (служба hostd)	**Вкл.**
vSphere: USB-устройства (служба usb)	**Вкл.**
vSphere: Аутентификация (службы auth, login, vmauthd)	**Вкл.**
vSphere: Системные события (служба syslog)	**Вкл.**
vSphere: Виртуальные машины (службы vmauthd, vmkdevmgr, vmkernel, vmkeventd, vmksummary, vmkwarning)	**Вкл.**
vSphere: Зачистка ФС (служба eraser)	**Вкл.**
Уведомления: Операции с виртуальными машинами	**Вкл.**
Уведомления: Операции со снапшотами	**Вкл.**
Уведомления: Операции с виртуальными дисками	**Вкл.**
Уведомления: Операции с объектами виртуальной сети	**Вкл.**
Уведомления: Изменение общих настроек сервера виртуализации	**Вкл.**

3.2.4. Очистка остаточной информации

Параметр	Значение
Количество циклов затирания (циклы) (1 – 10)	**1**

3.3. СЗИ ВИ (oVirt)

3.3.1. Политики авторизации

Параметр	Значение
Максимальное количество ошибок ввода пароля	**5**
Время блокировки учетной записи в случае ввода неправильных паролей	**15 мин.**
Включить синхронизацию времени по NTP	**Используется**
KVM: блокировать протокол SSH	**Да**

KVM: блокировать доступ к Cockpit Web Interface	**Да**

3.3.2. Политики паролей

Параметр	Значение
oVirt: Минимальная длина пароля (символы)	**6**
oVirt: Максимальный срок действия пароля (дни)	**42**
oVirt: Напоминать о смене пароля за	**Не используется**
oVirt: Минимальное количество прописных букв	**Не используется**
oVirt: Минимальное количество строчных букв	**Не используется**
oVirt: Минимальное количество специальных символов	**Не используется**
oVirt: Минимальное количество цифр	**Не используется**
oVirt: Количество предыдущих паролей, которые пользователь не может использовать	**Не используется**

3.3.3. Политики аудита

Параметр	Значение
Уведомления: Операции с виртуальными машинами	**Вкл.**
Уведомления: Операции со снапшотами	**Вкл.**
Уведомления: Операции с виртуальнымми дисками	**Вкл.**

3.3.4. Очистка остаточной информации

Параметр	Значение
Количество циклов затирания	**1**

3.4. СЗИ ВИ (KVM)

3.4.1. Политики авторизации

Параметр	Значение
Максимальное количество ошибок ввода пароля	**5**
Время блокировки учетной записи в случае ввода неправильных паролей (мин.) (1 – 300)	**15**
KVM: блокировать протокол SSH	**Да**
Включить синхронизацию времени по NTP	**Используется**
KVM: Блокировать доступ к Cockpit Web Interface	**Да**
KVM: Блокировать запуск ВМ в пространстве пользователя	**Да**

3.4.2. Политики аудита

Параметр	Значение
Уведомления: Операции с виртуальными машинами	**Вкл.**
Уведомления: Операции со снапшотами	**Вкл.**
Уведомления: Операции с виртуальнымми дисками	**Вкл.**
Уведомления: Операции с объектами виртуальной сети	**Вкл.**
Уведомления: Изменение общих настроек сервера виртуализации	**Вкл.**

3.4.3. Очистка остаточной информации

Параметр	Значение
Количество циклов затирания	**1**

4. Шаблон: ГИС К3

4.1. Сервер УД

4.1.1. Политики авторизации

Параметр	Значение
Время блокировки учетной записи в случае ввода неправильных паролей (мин.), (1 – 300)	**15**
Максимальное количество ошибок ввода пароля (попытки) (1 – 10)	**5**

Включить синхронизацию времени по NTP	**Используется**

4.1.2. Политики паролей

Параметр	Значение
Максимальный срок действия пароля (1 – 180)	**42**
Минимальная длина пароля (симв.) (1 – 14)	**6**
Необходимо наличие спец. символов	**Нет**
Необходимо наличие цифр	**Нет**
Необходимо наличие строчных и прописных букв	**Нет**
Необходимо отсутствие цифры в первом и последнем символах	**Нет**
Разрешена генерация пароля	**Да**

4.1.3. Политики аудита

Параметр	Значение
Регистрация НСД: Ошибка выполнения задачи	**Вкл.**
Регистрация НСД: Доступ запрещен	**Вкл.**
Регистрация НСД: События входов	**Вкл.**
Регистрация НСД: Вход: Учетная запись заблокирована	**Вкл.**
Регистрация НСД: Вход: Доступ запрещен	**Вкл.**
Регистрация НСД: События нарушения контроля целостности ВМ	**Вкл.**
Регистрация НСД: Нарушение КЦ: Попытка запуска/клонирования ВМ с нарушенной целостностью	**Вкл.**
Регистрация НСД: Нарушение КЦ: Попытка запуска ВМ напрямую с гипервизора	**Вкл.**
Регистрация НСД: Нарушение КЦ: Системные файлы	**Вкл.**
Регистрация НСД: Нарушение КЦ: Прогр. апп. среда	**Вкл.**
Регистрация НСД: Нарушение КЦ: Файл был удален	**Вкл.**
Получение событий syslog	**Получение по UDP**
Порт для работы syslog по UDP	**514**
Порт для работы syslog по SLL	**1514**

4.2. СЗИ ВИ (vSphere)

4.2.1. Политики авторизации

Параметр	Значение
Время блокировки учетной записи в случае ввода неправильных паролей (мин.) (1 – 300)	**15**
Максимальное количество ошибок ввода пароля (1 – 10)	**5**
vCSA: Блокировать протокол SSH	**Нет**
vCSA: Разрешить вход на Web-клиент VCSA Management Interface	**Да**
vCSA: Разрешить локальный вход с консоли	**Да**
vSphere: Запрет на работу через Web-клиент	**Нет**
ESXi: Блокировать протокол SSH	**Да**
ESXi: Время, в течение которого допускается выполнить одну попытку ввода пароля (минуты)	**1**
ESXi: Запретить возможность авторизации (Lockdown Mode)	**При удаленном подключении**
ESXi: Количество попыток ввода нового пароля, удовлетворяющего текущим парольным политикам (попытки) (1 – 10)	**3**
ESXi: Период неиспользования	**1**
Включить синхронизацию времени по NTP	**Используется**
vCSA: Время, в течение которого подсчитываются ошибки ввода пароля (мин), (1 –300)	**1**

4.2.2. Политики паролей

Параметр	Значение
vSphere: Максимальный срок действия пароля (1 – 180)	**42**
vSphere: Минимальная длина пароля (симв.) (1 – 30)	**6**
ESXi: Напоминать о смене пароля за (дни)	**Не используется**
ESXi: Минимальное количество классов символов	**Не используется**
vCenter: Количество предыдущих паролей, которые пользователь не может использовать (шт.) (1 – 10)	**5**
vCenter: Максимальная длина пароля (симв.) (1 – 40)	**20**
vCenter: Максимально допустимое количество одинаковых символов, стоящих рядом (симв.) (1 – 5)	**3**
vCenter: Минимальное количество прописных букв (шт.) (1 – 9)	**Не используется**
vCenter: Минимальное количество символов алфавита (шт.) (1 – 15)	**Не используется**
vCenter: Минимальное количество специальных символов (шт.) (1 – 9)	**Не используется**
vCenter: Минимальное количество строчных букв (шт.) (1 – 9)	**Не используется**
vCenter: Минимальное количество цифр (шт.) (1 – 9)	**Не используется**

4.2.3. Политики аудита

Параметр	Значение
vSphere: Агент СВ vCenter	**Вкл.**
vSphere: ESXi Shell (служба shell)	**Вкл.**
vSphere: Агент ESXi (служба hostd)	**Вкл.**
vSphere: USB-устройства (служба usb)	**Вкл.**
vSphere: Аутентификация (службы auth, login, vmauthd)	**Вкл.**
vSphere: Системные события (служба syslog)	**Вкл.**
vSphere: Виртуальные машины (службы vmauthd, vmkdevmgr, vmkernel, vmkeventd, vmksummary, vmkwarning)	**Вкл.**
vSphere: Зачистка ФС (служба eraser)	**Вкл.**
Уведомления: Операции с виртуальными машинами	**Вкл.**
Уведомления: Операции со снапшотами	**Вкл.**
Уведомления: Операции с виртуальными дисками	**Вкл.**
Уведомления: Операции с объектами виртуальной сети	**Вкл.**
Уведомления: Изменение общих настроек сервера виртуализации	**Вкл.**

4.2.4. Очистка остаточной информации

Параметр	Значение
Количество циклов затирания (циклы) (1 – 10)	**1**

4.3. СЗИ ВИ (oVirt)

4.3.1. Политики авторизации

Параметр	Значение
Максимальное количество ошибок ввода пароля	**5**
Время блокировки учетной записи в случае ввода неправильных паролей	**15**
Включить синхронизацию времени по NTP	**Используется**
KVM: блокировать протокол SSH	**Да**
KVM: блокировать доступ к Cockpit Web Interface	**Да**

4.3.2. Политики паролей

Параметр	Значение
oVirt: Минимальная длина пароля (символы)	**6**
oVirt: Максимальный срок действия пароля (дни)	**42**

Параметр	Значение
oVirt: Напоминать о смене пароля за (дни)	**Не используется**
oVirt: Минимальное количество прописных букв	**Не используется**
oVirt: Минимальное количество строчных букв	**Не используется**
oVirt: Минимальное количество специальных символов	**Не используется**
oVirt: Минимальное количество цифр	**Не используется**
oVirt: Количество предыдущих паролей, которые пользователь не может использовать	**5**

4.3.3. Политики аудита

Параметр	Значение
Уведомления: Операции с виртуальными машинами	**Вкл.**
Уведомления: Операции со снапшотами	**Вкл.**
Уведомления: Операции с виртуальнымми дисками	**Вкл.**

4.3.4. Очистка остаточной информации

Параметр	Значение
Количество циклов затирания	**1**

4.4. СЗИ ВИ (KVM)

4.4.1. Политики авторизации

Параметр	Значение
Максимальное количество ошибок ввода пароля	**5**
Время блокировки учетной записи в случае ввода неправильных паролей (мин.) (1 – 300)	**15**
KVM: блокировать протокол SSH	**Да**
Включить синхронизацию времени по NTP	**Используется**
KVM: Блокировать доступ к Cockpit Web Interface	**Да**
KVM: Блокировать запуск ВМ в пространстве пользователя	**Да**

4.4.2. Политики аудита

Параметр	Значение
Уведомления: Операции с виртуальными машинами	**Вкл.**
Уведомления: Операции со снапшотами	**Вкл.**
Уведомления: Операции с виртуальнымми дисками	**Вкл.**
Уведомления: Операции с объектами виртуальной сети	**Вкл.**
Уведомления: Изменение общих настроек сервера виртуализации	**Вкл.**

4.4.3. Очистка остаточной информации

Параметр	Значение
Количество циклов затирания	**1**

5. Шаблон: ГОСТ Р 56938-2016

5.1. Сервер УД

5.1.1. Политики авторизации

Параметр	Значение
Время блокировки учетной записи в случае ввода неправильных паролей (мин.), (1 – 300)	**15**
Максимальное количество ошибок ввода пароля (попытки) (1 – 10)	**5**
Включить синхронизацию времени по NTP	**Используется**

5.1.2. Политики паролей

Параметр	Значение
Максимальный срок действия пароля (1 – 180) (дни)	**42**

Параметр	Значение
Минимальная длина пароля (симв.) (1 – 14) (символы)	**6**
Необходимо наличие спец. символов	**Нет**
Необходимо наличие цифр	**Нет**
Необходимо наличие строчных и прописных букв	**Нет**
Необходимо отсутствие цифры в первом и последнем символах	**Нет**
Разрешена генерация пароля	**Да**

5.1.3. Политики аудита

Параметр	Значение
Регистрация НСД: Ошибка выполнения задачи	**Вкл.**
Регистрация НСД: Доступ запрещен	**Вкл.**
Регистрация НСД: События входов	**Вкл.**
Регистрация НСД: Вход: Учетная запись заблокирована	**Вкл.**
Регистрация НСД: Вход: Доступ запрещен	**Вкл.**
Регистрация НСД: События нарушения контроля целостности ВМ	**Вкл.**
Регистрация НСД: Нарушение КЦ: Попытка запуска/клонирования ВМ с нарушенной целостностью	**Вкл.**
Регистрация НСД: Нарушение КЦ: Попытка запуска ВМ напрямую с гипервизора	**Вкл.**
Регистрация НСД: Нарушение КЦ: Системные файлы	**Вкл.**
Регистрация НСД: Нарушение КЦ: Прогр. апп. среда	**Вкл.**
Регистрация НСД: Нарушение КЦ: Файл был удален	**Вкл.**
Получение событий syslog	**Получение по UDP**
Порт для работы syslog по UDP	**514**
Порт для работы syslog по SLL	**1514**

5.2. СЗИ ВИ (vSphere)

5.2.1. Политики авторизации

Параметр	Значение
Время блокировки учетной записи в случае ввода неправильных паролей (мин.) (1 – 300)	**15**
Максимальное количество ошибок ввода пароля (1 – 10)	**5**
vCSA: Блокировать протокол SSH	**Нет**
vCSA: Разрешить вход на Web-клиент VCSA Management Interface	**Да**
vCSA: Разрешить локальный вход с консоли	**Да**
vSphere: Запрет на работу через Web-клиент	**нет**
ESXi: Блокировать протокол SSH	**Да**
ESXi: Время, в течение которого допускается выполнить одну попытку ввода пароля (минуты)	**1**
ESXi: Запретить возможность авторизации (Lockdown Mode)	**При удаленном подключении**
ESXi: Количество попыток ввода нового пароля, удовлетворяющего текущим парольным политикам (попытки) (1 – 10)	**3**
ESXi: Период неиспользования	**1**
Включить синхронизацию времени по NTP	**Используется**
vCSA: Время, в течение которого подсчитываются ошибки ввода пароля (мин), (1 –300)	**1**

5.2.2. Политики паролей

Параметр	Значение
vSphere: Максимальный срок действия пароля (1 – 180)	**42**

Параметр	Значение
vSphere: Минимальная длина пароля (симв.) (1 – 30)	**6**
ESXi: Напоминать о смене пароля за	**Не используется**
ESXi: Минимальное количество классов символов	**Не используется**
vCenter: Количество предыдущих паролей, которые пользователь не может использовать (шт.) (1 – 10)	**5**
vCenter: Максимальная длина пароля (симв.) (1 – 40)	**20**
vCenter: Максимально допустимое количество одинаковых символов, стоящих рядом (симв.) (1 – 5)	**3**
vCenter: Минимальное количество прописных букв (шт.) (1 – 9)	**Не используется**
vCenter: Минимальное количество символов алфавита (шт.) (1 – 15)	**Не используется**
vCenter: Минимальное количество специальных символов (шт.) (1 – 9)	**Не используется**
vCenter: Минимальное количество строчных букв (шт.) (1 – 9)	**Не используется**
vCenter: Минимальное количество цифр (шт.) (1 – 9)	**Не используется**

5.2.3. Политики аудита

Параметр	Значение
vSphere: Агент CB vCenter	**Вкл.**
vSphere: ESXi Shell (служба shell)	**Вкл.**
vSphere: Агент ESXi (служба hostd)	**Вкл.**
vSphere: USB-устройства (служба usb)	**Вкл.**
vSphere: Аутентификация (службы auth, login, vmauthd)	**Вкл.**
vSphere: Системные события (служба syslog)	**Вкл.**
vSphere: Виртуальные машины (службы vmauthd, vmkdevmgr, vmkernel, vmkeventd, vmksummary, vmkwarning)	**Вкл.**
vSphere: Зачистка ФС (служба eraser)	**Вкл.**
Уведомления: Операции с виртуальными машинами	**Вкл.**
Уведомления: Операции со снапшотами	**Вкл.**
Уведомления: Операции с виртуальными дисками	**Вкл.**
Уведомления: Операции с объектами виртуальной сети	**Вкл.**
Уведомления: Изменение общих настроек сервера виртуализации	**Вкл.**

5.2.4. Очистка остаточной информации

Параметр	Значение
Количество циклов затирания (циклы) (1 – 10)	**1**

5.3. СЗИ ВИ (oVirt)

5.3.1. Политики авторизации

Параметр	Значение
Максимальное количество ошибок ввода пароля (попытки)	**5**
Время блокировки учетной записи в случае ввода неправильных паролей (минуты)	**15**
Включить синхронизацию времени по NTP	**Используется**
KVM: блокировать протокол SSH	**Да**
KVM: блокировать доступ к Cockpit Web Interface	**Да**

5.3.2. Политики паролей

Параметр	Значение
oVirt: Минимальная длина пароля (символы)	**6**
oVirt: Максимальный срок действия пароля (дни)	**42**
oVirt: Напоминать о смене пароля за (дни)	**Не используется**
oVirt: Минимальное количество прописных букв (штук)	**Не используется**

Параметр	Значение
oVirt: Минимальное количество строчных букв (штук)	**Не используется**
oVirt: Минимальное количество специальных символов (штук)	**Не используется**
oVirt: Минимальное количество цифр (штук)	**Не используется**
oVirt: Количество предыдущих паролей, которые пользователь не может использовать (штук)	**5**

5.3.3. Политики аудита

Параметр	Значение
Уведомления: Операции с виртуальными машинами	**Вкл.**
Уведомления: Операции со снапшотами	**Вкл.**
Уведомления: Операции с виртуальнымми дисками	**Вкл.**

5.3.4. Очистка остаточной информации

Параметр	Значение
Количество циклов затирания	**1**

5.4. СЗИ ВИ (KVM)

5.4.1. Политики авторизации

Параметр	Значение
Максимальное количество ошибок ввода пароля (попытки)	**5**
Время блокировки учетной записи в случае ввода неправильных паролей (мин.) (1 – 300)	**15**
KVM: блокировать протокол SSH	**Да**
Включить синхронизацию времени по NTP	**Используется**
KVM: Блокировать доступ к Cockpit Web Interface	**Да**
KVM: Блокировать запуск ВМ в пространстве пользователя	**Да**

5.4.2. Политики аудита

Параметр	Значение
Уведомления: Операции с виртуальными машинами	**Вкл.**
Уведомления: Операции со снапшотами	**Вкл.**
Уведомления: Операции с виртуальнымми дисками	**Вкл.**
Уведомления: Операции с объектами виртуальной сети	**Вкл.**
Уведомления: Изменение общих настроек сервера виртуализации	**Вкл.**

5.4.3. Очистка остаточной информации

Параметр	Значение
Количество циклов затирания	**1**

6. Шаблон: ИСПДн уровни 1 и 2

6.1. Сервер УД

6.1.1. Политики авторизации

Параметр	Значение
Время блокировки учетной записи в случае ввода неправильных паролей (мин.), (1 – 300)	**15**
Максимальное количество ошибок ввода пароля (попытки) (1 – 10)	**5**
Включить синхронизацию времени по NTP	**Используется**

6.1.2. Политики паролей

Параметр	Значение
Максимальный срок действия пароля (1 – 180)	**42**
Минимальная длина пароля (симв.) (1 – 14)	**6**
Необходимо наличие спец. символов	**Нет**

Необходимо наличие цифр	**Нет**
Необходимо наличие строчных и прописных букв	**Нет**
Необходимо отсутствие цифры в первом и последнем символах	**Нет**
Разрешена генерация пароля	**Да**

6.1.3. Политики аудита

Параметр	Значение
Регистрация НСД: Ошибка выполнения задачи	**Вкл.**
Регистрация НСД: Доступ запрещен	**Вкл.**
Регистрация НСД: События входов	**Вкл.**
Регистрация НСД: Вход: Учетная запись заблокирована	**Вкл.**
Регистрация НСД: Вход: Доступ запрещен	**Вкл.**
Регистрация НСД: События нарушения контроля целостности ВМ	**Вкл.**
Регистрация НСД: Нарушение КЦ: Попытка запуска/клонирования ВМ с нарушенной целостностью	**Вкл.**
Регистрация НСД: Нарушение КЦ: Попытка запуска ВМ напрямую с гипервизора	**Вкл.**
Регистрация НСД: Нарушение КЦ: Системные файлы	**Вкл.**
Регистрация НСД: Нарушение КЦ: Прогр. апп. среда	**Вкл.**
Регистрация НСД: Нарушение КЦ: Файл был удален	**Вкл.**
Получение событий syslog	**Получение по UDP**
Порт для работы syslog по UDP	**514**
Порт для работы syslog по SLL	**1514**

6.2. СЗИ ВИ (vSphere)

6.2.1. Политики авторизации

Параметр	Значение
Время блокировки учетной записи в случае ввода неправильных паролей (мин.) (1 – 300)	**15**
Максимальное количество ошибок ввода пароля (1 – 10)	**5**
vCSA: Блокировать протокол SSH	**Нет**
vCSA: Разрешить вход на Web-клиент VCSA Management Interface	**Да**
vCSA: Разрешить локальный вход с консоли	**Да**
vSphere: Запрет на работу через Web-клиент	**Нет**
ESXi: Блокировать протокол SSH	**Да**
ESXi: Время, в течение которого допускается выполнить одну попытку ввода пароля (минуты)	**1**
ESXi: Запретить возможность авторизации (Lockdown Mode)	**При удаленном подключении**
ESXi: Количество попыток ввода нового пароля, удовлетворяющего текущим парольным политикам (попытки) (1 – 10)	**3**
ESXi: Период неиспользования	**1**
Включить синхронизацию времени по NTP	**Используется**
vCSA: Время, в течение которого подсчитываются ошибки ввода пароля (мин), (1 –300)	**1**

6.2.2. Политики паролей

Параметр	Значение
vSphere: Максимальный срок действия пароля (1 – 180)	**42**
vSphere: Минимальная длина пароля (симв.) (1 – 30)	**6**
ESXi: Напоминать о смене пароля за (дни)	**Не используется**
ESXi: Минимальное количество классов символов (класс символов)	**Не используется**

Параметр	Значение
vCenter: Количество предыдущих паролей, которые пользователь не может использовать (шт.) (1 – 10)	**5**
vCenter: Максимальная длина пароля (симв.) (1 – 40)	**20**
vCenter: Максимально допустимое количество одинаковых символов, стоящих рядом (симв.) (1 – 5)	**3**
vCenter: Минимальное количество прописных букв (шт.) (1 – 9)	**Не используется**
vCenter: Минимальное количество символов алфавита (шт.) (1 – 15)	**Не используется**
vCenter: Минимальное количество специальных символов (шт.) (1 – 9)	**Не используется**
vCenter: Минимальное количество строчных букв (шт.) (1 – 9)	**Не используется**
vCenter: Минимальное количество цифр (шт.) (1 – 9)	**Не используется**

6.2.3. Политики аудита

Параметр	Значение
vSphere: Агент CB vCenter	**Вкл.**
vSphere: ESXi Shell (служба shell)	**Вкл.**
vSphere: Агент ESXi (служба hostd)	**Вкл.**
vSphere: USB-устройства (служба usb)	**Вкл.**
vSphere: Аутентификация (службы auth, login, vmauthd)	**Вкл.**
vSphere: Системные события (служба syslog)	**Вкл.**
vSphere: Виртуальные машины (службы vmauthd, vmkdevmgr, vmkernel, vmkeventd, vmksummary, vmkwarning)	**Вкл.**
vSphere: Зачистка ФС (служба eraser)	**Вкл.**
Уведомления: Операции с виртуальными машинами	**Вкл.**
Уведомления: Операции со снапшотами	**Вкл.**
Уведомления: Операции с виртуальными дисками	**Вкл.**
Уведомления: Операции с объектами виртуальной сети	**Вкл.**
Уведомления: Изменение общих настроек сервера виртуализации	**Вкл.**

6.2.4. Очистка остаточной информации

Параметр	Значение
Количество циклов затирания (циклы) (1 – 10)	**1**

6.3. СЗИ ВИ (oVirt)

6.3.1. Политики авторизации

Параметр	Значение
Максимальное количество ошибок ввода пароля	**5**
Время блокировки учетной записи в случае ввода неправильных паролей	**15**
Включить синхронизацию времени по NTP	**Используется**
KVM: блокировать протокол SSH	**Да**
KVM: блокировать доступ к Cockpit Web Interface	**Да**

6.3.2. Политики паролей

Параметр	Значение
oVirt: Минимальная длина пароля (символы)	**6**
oVirt: Максимальный срок действия пароля (дни)	**42**
oVirt: Напоминать о смене пароля за (дни)	**Не используется**
oVirt: Минимальное количество прописных букв	**Не используется**
oVirt: Минимальное количество строчных букв	**Не используется**
oVirt: Минимальное количество специальных символов	**Не используется**
oVirt: Минимальное количество цифр	**Не используется**

oVirt: Количество предыдущих паролей, которые пользователь не может использовать	**5**

6.3.3. Политики аудита

Параметр	Значение
Уведомления: Операции с виртуальными машинами	**Вкл.**
Уведомления: Операции со снапшотами	**Вкл.**
Уведомления: Операции с виртуальнымми дисками	**Вкл.**

6.3.4. Очистка остаточной информации

Параметр	Значение
Количество циклов затирания (циклы)	**1**

6.4. СЗИ ВИ (KVM)

6.4.1. Политики авторизации

Параметр	Значение
Максимальное количество ошибок ввода пароля	**5**
Время блокировки учетной записи в случае ввода неправильных паролей (мин.) (1 – 300)	**15**
KVM: блокировать протокол SSH	**Да**
Включить синхронизацию времени по NTP	**Используется**
KVM: Блокировать доступ к Cockpit Web Interface	**Да**
KVM: Блокировать запуск ВМ в пространстве пользователя	**Да**

6.4.2. Политики аудита

Параметр	Значение
Уведомления: Операции с виртуальными машинами	**Вкл.**
Уведомления: Операции со снапшотами	**Вкл.**
Уведомления: Операции с виртуальнымми дисками	**Вкл.**
Уведомления: Операции с объектами виртуальной сети	**Вкл.**
Уведомления: Изменение общих настроек сервера виртуализации	**Вкл.**

6.4.3. Очистка остаточной информации

Параметр	Значение
Количество циклов затирания (циклы)	**1**

7. Шаблон: ИСПДн уровни 3 и 4

7.1. Сервер УД

7.1.1. Политики авторизации

Параметр	Значение
Время блокировки учетной записи в случае ввода неправильных паролей (мин.), (1 – 300)	**15**
Максимальное количество ошибок ввода пароля (попытки) (1 – 10)	**5**
Включить синхронизацию времени по NTP	**Используется**

7.1.2. Политики паролей

Параметр	Значение
Максимальный срок действия пароля (1 – 180) (дни)	**42**
Минимальная длина пароля (симв.) (1 – 14) (символы)	**6**
Необходимо наличие спец. символов	**Нет**
Необходимо наличие цифр	**Нет**
Необходимо наличие строчных и прописных букв	**Нет**
Необходимо отсутствие цифры в первом и последнем символах	**Нет**
Разрешена генерация пароля	**Да**

7.1.3. Политики аудита

Параметр	Значение
Регистрация НСД: Ошибка выполнения задачи	**Вкл.**
Регистрация НСД: Доступ запрещен	**Вкл.**
Регистрация НСД: События входов	**Вкл.**
Регистрация НСД: Вход: Учетная запись заблокирована	**Вкл.**
Регистрация НСД: Вход: Доступ запрещен	**Вкл.**
Регистрация НСД: События нарушения контроля целостности ВМ	**Вкл.**
Регистрация НСД: Нарушение КЦ: Попытка запуска/клонирования ВМ с нарушенной целостностью	**Вкл.**
Регистрация НСД: Нарушение КЦ: Попытка запуска ВМ напрямую с гипервизора	**Вкл.**
Регистрация НСД: Нарушение КЦ: Системные файлы	**Вкл.**
Регистрация НСД: Нарушение КЦ: Прогр. апп. среда	**Вкл.**
Регистрация НСД: Нарушение КЦ: Файл был удален	**Вкл.**
Получение событий syslog	**Получение по UDP**
Порт для работы syslog по UDP	**514**
Порт для работы syslog по SLL	**1514**

7.2. СЗИ ВИ (vSphere)

7.2.1. Политики авторизации

Параметр	Значение
Время блокировки учетной записи в случае ввода неправильных паролей (мин.) (1 – 300)	**15**
Максимальное количество ошибок ввода пароля (1 – 10)	**5**
vCSA: Блокировать протокол SSH	**Нет**
vCSA: Разрешить вход на Web-клиент VCSA Management Interface	**Да**
vCSA: Разрешить локальный вход с консоли	**Да**
vSphere: Запрет на работу через Web-клиент	**Нет**
ESXi: Блокировать протокол SSH	**Да**
ESXi: Время, в течение которого допускается выполнить одну попытку ввода пароля (минуты)	**1**
ESXi: Запретить возможность авторизации (Lockdown Mode)	**При удаленном подключении**
ESXi: Количество попыток ввода нового пароля, удовлетворяющего текущим парольным политикам (попытки) (1 – 10)	**3**
ESXi: Период неиспользования	**1**
Включить синхронизацию времени по NTP	**Используется**
vCSA: Время, в течение которого подсчитываются ошибки ввода пароля (мин), (1 –300)	**1**

7.2.2. Политики паролей

Параметр	Значение
vSphere: Максимальный срок действия пароля (1 – 180) (дни)	**42**
vSphere: Минимальная длина пароля (симв.) (1 – 30)	**6**
ESXi: Напоминать о смене пароля за (дни)	**Не используется**
ESXi: Минимальное количество классов символов (класс символов)	**Не используется**
vCenter: Количество предыдущих паролей, которые пользователь не может использовать (шт.) (1 – 10)	**5**
vCenter: Максимальная длина пароля (симв.) (1 – 40)	**20**
vCenter: Максимально допустимое количество одинаковых символов, стоящих рядом (симв.) (1 – 5)	**3**

vCenter: Минимальное количество прописных букв (шт.) (1 – 9)	**Не используется**
vCenter: Минимальное количество символов алфавита (шт.) (1 – 15)	**Не используется**
vCenter: Минимальное количество специальных символов (шт.) (1 – 9)	**Не используется**
vCenter: Минимальное количество строчных букв (шт.) (1 – 9)	**Не используется**
vCenter: Минимальное количество цифр (шт.) (1 – 9)	**Не используется**

7.2.3. Политики аудита

Параметр	Значение
vSphere: Агент СВ vCenter	**Вкл.**
vSphere: ESXi Shell (служба shell)	**Вкл.**
vSphere: Агент ESXi (служба hostd)	**Вкл.**
vSphere: USB-устройства (служба usb)	**Вкл.**
vSphere: Аутентификация (службы auth, login, vmauthd)	**Вкл.**
vSphere: Системные события (служба syslog)	**Вкл.**
vSphere: Виртуальные машины (службы vmauthd, vmkdevmgr, vmkernel, vmkeventd, vmksummary, vmkwarning)	**Вкл.**
vSphere: Зачистка ФС (служба eraser)	**Вкл.**
Уведомления: Операции с виртуальными машинами	**Вкл.**
Уведомления: Операции со снапшотами	**Вкл.**
Уведомления: Операции с виртуальными дисками	**Вкл.**
Уведомления: Операции с объектами виртуальной сети	**Вкл.**
Уведомления: Изменение общих настроек сервера виртуализации	**Вкл.**

7.2.4. Очистка остаточной информации

Параметр	Значение
Количество циклов затирания (циклы) (1 – 10)	**1**

7.3. СЗИ ВИ (oVirt)

7.3.1. Политики авторизации

Параметр	Значение
Максимальное количество ошибок ввода пароля (попытки)	**5**
Время блокировки учетной записи в случае ввода неправильных паролей (минуты)	**15**
Включить синхронизацию времени по NTP	**Используется**
KVM: Блокировать протокол SSH	**Да**
KVM: Блокировать доступ к Cockpit Web Interface	**Да**

7.3.2. Политики паролей

Параметр	Значение
oVirt: Минимальная длина пароля	**6**
oVirt: Максимальный срок действия пароля	**42**
oVirt: Напоминать о смене пароля за	**Не используется**
oVirt: Минимальное количество прописных букв	**Не используется**
oVirt: Минимальное количество строчных букв	**Не используется**
oVirt: Минимальное количество специальных символов	**Не используется**
oVirt: Минимальное количество цифр	**Не используется**
oVirt: Количество предыдущих паролей, которые пользователь не может использовать	**5**

7.3.3. Политики аудита

Параметр	Значение
Уведомления: Операции с виртуальными машинами	**Вкл.**

Уведомления: Операции со снапшотами	**Вкл.**
Уведомления: Операции с виртуальнымми дисками	**Вкл.**

7.3.4. Очистка остаточной информации

Параметр	Значение
Количество циклов затирания (циклы)	**1**

7.4. СЗИ ВИ (KVM)

7.4.1. Политики авторизации

Параметр	Значение
Максимальное количество ошибок ввода пароля	**5**
Время блокировки учетной записи в случае ввода неправильных паролей (мин.) (1 – 300)	**15**
KVM: блокировать протокол SSH	**Да**
Включить синхронизацию времени по NTP	**Используется**
KVM: Блокировать доступ к Cockpit Web Interface	**Да**
KVM: Блокировать запуск ВМ в пространстве пользователя	**Да**

7.4.2. Политики аудита

Параметр	Значение
Уведомления: Операции с виртуальными машинами	**Вкл.**
Уведомления: Операции со снапшотами	**Вкл.**
Уведомления: Операции с виртуальнымми дисками	**Вкл.**
Уведомления: Операции с объектами виртуальной сети	**Вкл.**
Уведомления: Изменение общих настроек сервера виртуализации	**Вкл.**

7.4.3. Очистка остаточной информации

Параметр	Значение
Количество циклов затирания (циклы)	**1**

7.5. Шаблон: PCI DSS

7.6. Сервер УД

7.6.1. Политики авторизации

Параметр	Значение
Время блокировки учетной записи в случае ввода неправильных паролей (мин.), (1 – 300)	**30**
Максимальное количество ошибок ввода пароля (попытки) (1 – 10)	**5**
Включить синхронизацию времени по NTP	**Используется**

7.6.2. Политики паролей

Параметр	Значение
Максимальный срок действия пароля (1 – 180) (дни)	**90**
Минимальная длина пароля (симв.) (1 – 14)	**7**
Необходимо наличие спец. символов	**Нет**
Необходимо наличие цифр	**Да**
Необходимо наличие строчных и прописных букв	**Да**
Необходимо отсутствие цифры в первом и последнем символах	**Нет**
Разрешена генерация пароля	**Да**

7.6.3. Политики аудита

Параметр	Значение
Регистрация НСД: Ошибка выполнения задачи	**Вкл.**
Регистрация НСД: Доступ запрещен	**Вкл.**

Параметр	Значение
Регистрация НСД: События входов	**Вкл.**
Регистрация НСД: Вход: Учетная запись заблокирована	**Вкл.**
Регистрация НСД: Вход: Доступ запрещен	**Вкл.**
Регистрация НСД: События нарушения контроля целостности ВМ	**Вкл.**
Регистрация НСД: Нарушение КЦ: Попытка запуска/клонирования ВМ с нарушенной целостностью	**Вкл.**
Регистрация НСД: Нарушение КЦ: Попытка запуска ВМ напрямую с гипервизора	**Вкл.**
Регистрация НСД: Нарушение КЦ: Системные файлы	**Вкл.**
Регистрация НСД: Нарушение КЦ: Прогр. апп. среда	**Вкл.**
Регистрация НСД: Нарушение КЦ: Файл был удален	**Вкл.**
Получение событий syslog	**Получение по UDP**
Порт для работы syslog по UDP	**514**
Порт для работы syslog по SLL	**1514**

7.7. СЗИ ВИ (vSphere)

7.7.1. Политики авторизации

Параметр	Значение
Время блокировки учетной записи в случае ввода неправильных паролей (мин.) (1 – 300)	**30**
Максимальное количество ошибок ввода пароля (1 – 10)	**5**
vCSA: Блокировать протокол SSH	**Нет**
vCSA: Разрешить вход на Web-клиент VCSA Management Interface	**Да**
vCSA: Разрешить локальный вход с консоли	**Да**
vSphere: Запрет на работу через Web-клиент	**Нет**
ESXi: Блокировать протокол SSH	**Да**
ESXi: Время, в течение которого допускается выполнить одну попытку ввода пароля (минуты)	**1**
ESXi: Запретить возможность авторизации (Lockdown Mode)	**При удаленном подключении**
ESXi: Количество попыток ввода нового пароля, удовлетворяющего текущим парольным политикам (попытки) (1 – 10)	**3**
ESXi: Период неиспользования	**1**
Включить синхронизацию времени по NTP	**Да**
vCSA: Время, в течение которого подсчитываются ошибки ввода пароля (мин), (1 –300)	**1**

7.7.2. Политики паролей

Параметр	Значение
vSphere: Максимальный срок действия пароля (1 – 180) (дни)	**90**
vSphere: Минимальная длина пароля (симв.) (1 – 30)	**7**
ESXi: Напоминать о смене пароля за	**5**
ESXi: Минимальное количество классов символов	**3**
vCenter: Количество предыдущих паролей, которые пользователь не может использовать (шт.) (1 – 10)	**5**
vCenter: Максимальная длина пароля (симв.) (1 – 40)	**20**
vCenter: Максимально допустимое количество одинаковых символов, стоящих рядом (симв.) (1 – 5)	**3**
vCenter: Минимальное количество прописных букв (шт.) (1 – 9)	**1**
vCenter: Минимальное количество символов алфавита (шт.) (1 – 15)	**Не используется**
vCenter: Минимальное количество специальных символов (шт.) (1 – 9)	**Не используется**

vCenter: Минимальное количество строчных букв (шт.) (1 – 9)	**1**
vCenter: Минимальное количество цифр (шт.) (1 – 9)	**1**

7.7.3. Политики аудита

Параметр	Значение
vSphere: Агент CB vCenter	**Вкл.**
vSphere: ESXi Shell (служба shell)	**Вкл.**
vSphere: Агент ESXi (служба hostd)	**Вкл.**
vSphere: USB-устройства (служба usb)	**Вкл.**
vSphere: Аутентификация (службы auth, login, vmauthd)	**Вкл.**
vSphere: Системные события (служба syslog)	**Вкл.**
vSphere: Виртуальные машины (службы vmauthd, vmkdevmgr, vmkernel, vmkeventd, vmksummary, vmkwarning)	**Вкл.**
vSphere: Зачистка ФС (служба eraser)	**Вкл.**
Уведомления: Операции с виртуальными машинами	**Вкл.**
Уведомления: Операции со снапшотами	**Вкл.**
Уведомления: Операции с виртуальными дисками	**Вкл.**
Уведомления: Операции с объектами виртуальной сети	**Вкл.**
Уведомления: Изменение общих настроек сервера виртуализации	**Вкл.**

7.7.4. Очистка остаточной информации

Параметр	Значение
Количество циклов затирания (циклы) (1 – 10)	**1**

7.8. СЗИ ВИ (oVirt)

7.8.1. Политики авторизации

Параметр	Значение
Максимальное количество ошибок ввода пароля	**5**
Время блокировки учетной записи в случае ввода неправильных паролей (мин.)	**30**
Включить синхронизацию времени по NTP	**Используется**
KVM: блокировать протокол SSH	**Да**
KVM: блокировать доступ к Cockpit Web Interface	**Да**

7.8.2. Политики паролей

Параметр	Значение
oVirt: Минимальная длина пароля (символы)	**7**
oVirt: Максимальный срок действия пароля (дни)	**90**
oVirt: Напоминать о смене пароля за	**5**
oVirt: Минимальное количество прописных букв	**Не используется**
oVirt: Минимальное количество строчных букв	**Не используется**
oVirt: Минимальное количество специальных символов	**Не используется**
oVirt: Минимальное количество цифр	**Не используется**
oVirt: Количество предыдущих паролей, которые пользователь не может использовать	**5**

7.8.3. Политики аудита

Параметр	Значение
Уведомления: Операции с виртуальными машинами	**Вкл.**
Уведомления: Операции со снапшотами	**Вкл.**
Уведомления: Операции с виртуальнымми дисками	**Вкл.**

7.8.4. Очистка остаточной информации

Параметр	Значение
Количество циклов затирания (циклы)	**1**

7.9. СЗИ ВИ (KVM)

7.9.1. Политики авторизации

Параметр	Значение
Максимальное количество ошибок ввода пароля	**5**
Время блокировки учетной записи в случае ввода неправильных паролей (мин.) (1 – 300)	**30**
KVM: блокировать протокол SSH	**Да**
Включить синхронизацию времени по NTP	**Используется**
KVM: Блокировать доступ к Cockpit Web Interface	**Да**
KVM: Блокировать запуск ВМ в пространстве пользователя	**Да**

7.9.2. Политики аудита

Параметр	Значение
Уведомления: Операции с виртуальными машинами	**Вкл.**
Уведомления: Операции со снапшотами	**Вкл.**
Уведомления: Операции с виртуальнымми дисками	**Вкл.**
Уведомления: Операции с объектами виртуальной сети	**Вкл.**
Уведомления: Изменение общих настроек сервера виртуализации	**Вкл.**

7.9.3. Очистка остаточной информации

Параметр	Значение
Количество циклов затирания (циклы)	**1**

8. Шаблон: СТО БР ИББС

8.1. Сервер УД

8.1.1. Политики авторизации

Параметр	Значение
Время блокировки учетной записи в случае ввода неправильных паролей (мин.), (1 – 300)	**30**
Максимальное количество ошибок ввода пароля (попытки) (1 – 10)	**5**
Включить синхронизацию времени по NTP	**Используется**

8.1.2. Политики паролей

Параметр	Значение
Максимальный срок действия пароля (1 – 180)	**30**
Минимальная длина пароля (симв.) (1 – 14)	**7**
Необходимо наличие спец. символов	**Нет**
Необходимо наличие цифр	**Да**
Необходимо наличие строчных и прописных букв	**Да**
Необходимо отсутствие цифры в первом и последнем символах	**Нет**
Разрешена генерация пароля	**Да**

8.1.3. Политики аудита

Параметр	Значение
Регистрация НСД: Ошибка выполнения задачи	**Вкл.**
Регистрация НСД: Доступ запрещен	**Вкл.**
Регистрация НСД: События входов	**Вкл.**
Регистрация НСД: Вход: Учетная запись заблокирована	**Вкл.**
Регистрация НСД: Вход: Доступ запрещен	**Вкл.**
Регистрация НСД: События нарушения контроля целостности ВМ	**Вкл.**

Параметр	Значение
Регистрация НСД: Нарушение КЦ: Попытка запуска/клонирования ВМ с нарушенной целостностью	**Вкл.**
Регистрация НСД: Нарушение КЦ: Попытка запуска ВМ напрямую с гипервизора	**Вкл.**
Регистрация НСД: Нарушение КЦ: Системные файлы	**Вкл.**
Регистрация НСД: Нарушение КЦ: Прогр. апп. среда	**Вкл.**
Регистрация НСД: Нарушение КЦ: Файл был удален	**Вкл.**
Получение событий syslog	**Получение по UDP**
Порт для работы syslog по UDP	**514**
Порт для работы syslog по SLL	**1514**

8.2. СЗИ ВИ (vSphere)

8.2.1. Политики авторизации

Параметр	Значение
Время блокировки учетной записи в случае ввода неправильных паролей (мин.) (1 – 300)	**30**
Максимальное количество ошибок ввода пароля (1 – 10)	**5**
vCSA: Блокировать протокол SSH	**Нет**
vCSA: Разрешить вход на Web-клиент VCSA Management Interface	**Да**
vCSA: Разрешить локальный вход с консоли	**Да**
vSphere: Запрет на работу через Web-клиент	**Нет**
ESXi: Блокировать протокол SSH	**Да**
ESXi: Время, в течение которого допускается выполнить одну попытку ввода пароля (минуты)	**1**
ESXi: Запретить возможность авторизации (Lockdown Mode)	**При удаленном подключении**
ESXi: Количество попыток ввода нового пароля, удовлетворяющего текущим парольным политикам (попытки) (1 – 10)	**3**
ESXi: Период неиспользования	**1**
Включить синхронизацию времени по NTP	**Используется**
vCSA: Время, в течение которого подсчитываются ошибки ввода пароля (мин), (1 –300)	**1**

8.2.2. Политики паролей

Параметр	Значение
vSphere: Максимальный срок действия пароля (1 – 180) (дни)	**30**
vSphere: Минимальная длина пароля (симв.) (1 – 30)	**7**
ESXi: Напоминать о смене пароля за	**5**
ESXi: Минимальное количество классов символов	**3**
vCenter: Количество предыдущих паролей, которые пользователь не может использовать (шт.) (1 – 10)	**5**
vCenter: Максимальная длина пароля (симв.) (1 – 40)	**20**
vCenter: Максимально допустимое количество одинаковых символов, стоящих рядом (симв.) (1 – 5)	**3**
vCenter: Минимальное количество прописных букв (шт.) (1 – 9)	**1**
vCenter: Минимальное количество символов алфавита (шт.) (1 – 15)	**Не используется**
vCenter: Минимальное количество специальных символов (шт.) (1 – 9)	**Не используется**
vCenter: Минимальное количество строчных букв (шт.) (1 – 9)	**1**
vCenter: Минимальное количество цифр (шт.) (1 – 9)	**1**

8.2.3. Политики аудита

Параметр	Значение
vSphere: Агент СВ vCenter	**Вкл.**
vSphere: ESXi Shell (служба shell)	**Вкл.**
vSphere: Агент ESXi (служба hostd)	**Вкл.**
vSphere: USB-устройства (служба usb)	**Вкл.**
vSphere: Аутентификация (службы auth, login, vmauthd)	**Вкл.**
vSphere: Системные события (служба syslog)	**Вкл.**
vSphere: Виртуальные машины (службы vmauthd, vmkdevmgr, vmkernel, vmkeventd, vmksummary, vmkwarning)	**Вкл.**
vSphere: Зачистка ФС (служба eraser)	**Вкл.**
Уведомления: Операции с виртуальными машинами	**Вкл.**
Уведомления: Операции со снапшотами	**Вкл.**
Уведомления: Операции с виртуальными дисками	**Вкл.**
Уведомления: Операции с объектами виртуальной сети	**Вкл.**
Уведомления: Изменение общих настроек сервера виртуализации	**Вкл.**

8.2.4. Очистка остаточной информации

Параметр	Значение
Количество циклов затирания (циклы) (1 – 10)	**1**

8.3. СЗИ ВИ (oVirt)

8.3.1. Политики авторизации

Параметр	Значение
Максимальное количество ошибок ввода пароля (попытки)	**5**
Время блокировки учетной записи в случае ввода неправильных паролей (мин.)	**30**
Включить синхронизацию времени по NTP	**Используется**
KVM: блокировать протокол SSH	**Да**
KVM: блокировать доступ к Cockpit Web Interface	**Да**

8.3.2. Политики паролей

Параметр	Значение
oVirt: Минимальная длина пароля (символы)	**7**
oVirt: Максимальный срок действия пароля (дни)	**30**
oVirt: Напоминать о смене пароля за	**5**
oVirt: Минимальное количество прописных букв	**Не используется**
oVirt: Минимальное количество строчных букв	**Не используется**
oVirt: Минимальное количество специальных символов	**Не используется**
oVirt: Минимальное количество цифр	**Не используется**
oVirt: Количество предыдущих паролей, которые пользователь не может использовать	**5**

8.3.3. Политики аудита

Параметр	Значение
Уведомления: Операции с виртуальными машинами	**Вкл.**
Уведомления: Операции со снапшотами	**Вкл.**
Уведомления: Операции с виртуальнымми дисками	**Вкл.**

8.3.4. Очистка остаточной информации

Параметр	Значение
Количество циклов затирания (циклы)	**1**

8.4. СЗИ ВИ (KVM)

8.4.1. Политики авторизации

Параметр	Значение
Максимальное количество ошибок ввода пароля (попытки)	**5**
Время блокировки учетной записи в случае ввода неправильных паролей (мин.) (1 – 300)	**30**
KVM: блокировать протокол SSH	**Да**
Включить синхронизацию времени по NTP	**Используется**
KVM: Блокировать доступ к Cockpit Web Interface	**Да**
KVM: Блокировать запуск ВМ в пространстве пользователя	**Да**

8.4.2. Политики аудита

Параметр	Значение
Уведомления: Операции с виртуальными машинами	**Вкл.**
Уведомления: Операции со снапшотами	**Вкл.**
Уведомления: Операции с виртуальнымми дисками	**Вкл.**
Уведомления: Операции с объектами виртуальной сети	**Вкл.**
Уведомления: Изменение общих настроек сервера виртуализации	**Вкл.**

8.4.3. Очистка остаточной информации

Параметр	Значение
Количество циклов затирания (циклы)	**1**