KeyStack SE

Руководство пользователя

Содержание

Сокращения

ОО	–	Объект оценки
ПО	–	Программное обеспечение
СУБД	–	Система управления базами данных
ФСТЭК России	–	Федеральная служба по техническому и экспортному контролю России
LCM	–	(англ. Life-Cycle Manager), Система управления инсталляциями (экземплярами) ПО «KeyStack SE»
BMC	–	(англ. Baseboard Management Controller), Контроллер управления материнской платой сервера

1. ВВЕДЕНИЕ

Идентификация документа

Наименование документа	Программное обеспечение «Облачная платформа KeyStack SE v.1». Руководство пользователя
Версия документа	Версия 1.0
Обозначение документа	1087746411378.62.01.29.000.001 34
Идентификация ОО	Программное обеспечение «Облачная платформа KeyStack SE v.1». (ПО «KeyStack SE»)
Уровень доверия	ПО «KeyStack SE» соответствует 4 уровню доверия, в соответствии с Требованиями по безопасности информации, устанавливающими уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий, утвержденными приказом ФСТЭК России от 2 июня 2020 г. № 76

2. НАЗНАЧЕНИЕ И УСЛОВИЯ ПРИМЕНЕНИЯ ПО «KeyStack SE»

2.1 Назначение и описание функций безопасности

Основным назначением программного обеспечения «Облачная платформа KeyStack SE v.1» (далее – ПО «KeyStack SE», Платформа) является создание гибкой, масштабируемой и безопасной инфраструктуры виртуализации с автоматизированными процессами развертывания и управления.

ПО «KeyStack SE» представляет собой совокупность функциональных подсистем, обеспечивающих выполнение функций по виртуализации вычислительных ресурсов, созданию и управлению виртуальными машинами, мониторингу состояния инфраструктуры и осуществляющих централизованное управление средой виртуализации.

ПО «KeyStack SE» реализует следующие меры защиты согласно требованиям документа «Требования по безопасности информации к средствам виртуализации» (введен в действие приказом ФСТЭК России № 187 от октября 2022 г.):

1) функционирование в среде хостовой операционной системы, соответствующей 4 классу защиты и 4 уровню доверия;
2) реализация следующих функций безопасности:
   - доверенная загрузка виртуальных машин;
   - контроль целостности;
   - регистрация событий безопасности;
   - ролевой метод управления доступом;
   - резервное копирование;
   - ограничение программной среды;
   - управление потоками информации;
   - защита памяти;
   - идентификация и аутентификация пользователей;
   - централизованное управление образами виртуальных машин и виртуальными машинами.

2.2 Среда функционирования

ПО «KeyStack SE» функционирует в среде, которая сконфигурирована и контролируется администраторами в соответствии с эксплуатационной документацией.

Платформа использует для управления инфраструктурой узлы нескольких типов:

LCM (Seed node) — главный узел управления сервисной инфраструктурой Платформы. На нем хранится кодовая база основных компонентов Платформы и основная конфигурация узлов остальных типов. С этого узла начинается развертывание Платформы и управление ее жизненным циклом.

Controller — узел с управляющими модулями вычислительных ресурсов, сетевых агентов и вспомогательными службами. В некоторых случаях может совмещать роль узла Network.

Compute — узел с гипервизором KVM, управляет виртуальными машинами (ВМ) основной инфраструктуры. Для обеспечения сетевой связности ВМ используется агент сетевой службы.

Storage — узел с дисками блочных хранилищ. Блочные хранилища используются для организации индивидуального и/или совместного дискового пространства для ВМ.

Network — узел с компонентами программно-определяемых сетей.

Характеристики аппаратного элемента вычислительной инфраструктуры (сервера) ПО «KeyStack SE» приведены в Таблице 1.

Таблица 1 – Характеристики аппаратного элемента вычислительной инфраструктуры (сервера) ПО «KeyStack SE»

№ п/п	Название характеристик	Назначение серверов			
		Сервер вычислительных ресурсов (Controller-сервер)	**Сервер гипервизора KVM[1] (Compute-сервер)**	**Сервер сетевых служб (Network-сервер)[2]**	**Сервер управления сервисной инфраструктурой (LCM-сервер)**
1	Архитектура CPU	x86_64	x86_64	x86_64	x86_64
2	Количество CPU	2	2	2	2
3	Количество ядер одного CPU без учёта мультипоточности.	12	12	8	12
4	Объём RAM, Гб	64	64	32	128
5	Системные диски	2x 480GB, Enterprise SSD MixUse (RAID1)	2x 480GB, Enterprise SSD MixUse (RAID1)	2x 480GB, Enterprise SSD MixUse (RAID1)	2x 480GB, Enterprise SSD MixUse (RAID1)
6	Диски для данных	2x 1.9TB, Enterprise SSD MixUse (RAID1)	не требуется	не требуется	2x 3.8TB, Enterprise SSD MixUse (RAID1)
7	Количество портов 10/25 Gbps Ethernet	4	4	6	2
8	Количество портов FC SAN (HBA)	2	2	0	0

2.3 Требования к программному обеспечению

ПО «KeyStack SE» функционирует в среде, которая сконфигурирована и контролируется администратором в соответствии с эксплуатационной документацией.

Система обеспечивает функционирование на базе следующего общего программного обеспечения, указанного в таблице 2.

Таблица 2 – Программная среда функционирования ПО «KeyStack SE»

[1]При росте количества серверов гипервизоров KVM требования к серверам пересматриваются в сторону увеличения.

[2]Опционально. В ряде случае данную роль совмещает в себе сервер вычислительных ресурсов (Controller-сервер).

№	Назначение сервера	Элемент среды функционирования	Наименование
1	Сервер управления сервисной инфраструктурой (LCM-сервер)	ОС	Platform V SberLinux OS Server (Сертификат ФСТЭК России №4884 от 04.12.2024, действителен до 04.12.2029)
		Компонент ОС	Podman (входит в состав сертифицированного образа Platform V SberLinux OS Server)
		СУБД	Platform V Pangolin (Сертификат ФСТЭК России №4491 от 15.12.2021, действителен до 15.12.2026)
2	Сервер гипервизора KVM (Compute-сервер)	ОС	Platform V SberLinux OS Server (Сертификат ФСТЭК России №4884 от 04.12.2024, действителен до 04.12.2029)
		Компонент ОС	Podman (входит в состав сертифицированного образа Platform V SberLinux OS Server)
3	Сервер сетевых служб (Network-сервер)	ОС	Platform V SberLinux OS Server (Сертификат ФСТЭК России №4884 от 04.12.2024, действителен до 04.12.2029)
		Компонент ОС	Podman (входит в состав сертифицированного образа Platform V SberLinux OS Server)
4	Сервер вычислительных ресурсов (Controller-сервер)	ОС	Platform V SberLinux OS Server (Сертификат ФСТЭК России №4884 от 04.12.2024, действителен до 04.12.2029)
		Компонент ОС	Podman (входит в состав сертифицированного образа Platform V SberLinux OS Server)

3. ДЕЙСТВИЯ ПО ПРИЕМКЕ

Приемка поставленного ПО «KeyStack SE» осуществляется в соответствии с указаниями, содержащимися в документе «Программное обеспечение «Облачная платформа KeyStack SE v.1». Технические условия», 1087746411378.62.01.29.000.001 ТУ.

4. ДЕЙСТВИЯ ПО БЕЗОПАСНОЙ УСТАНОВКЕ

4.1 Указания по эксплуатации

Персонал, ответственный за функционирование ОО, должен обеспечивать надлежащее функционирование ОО в соответствии с документами:

- Программное обеспечение «Облачная платформа KeyStack SE v.1». Руководство пользователя (1087746411378.62.01.29.000.001 34);
- Программное обеспечение «Облачная платформа KeyStack SE v.1». Руководство администратора (1087746411378.62.01.29.000.001 91);
- Программное обеспечение «Облачная платформа KeyStack SE v.1». Формуляр (1087746411378.62.01.29.000.001 ФО).

4.2 Процесс инициализации

Перед процессом инициализации производится инсталляция ПО «KeyStack SE». Инсталляция ПО «KeyStack SE» происходит следующим образом:

- Подготовка инфраструктуры, которая включает в себя создание узлов всех типов, согласно аппаратным и программным требованиям;
- Установка основных компонентов Платформы, которая включает в себя:
  - Установку дистрибутива ПО «KeyStack SE» на LCM-узле;
  - Подготовка BMC-узлов инфраструктуры;
  - Создание регионов;
- Настройка сетевой связности.
- Ручной запуск пайплайнов.
- Подключение и настройка служебных сервисов.
- Проверка работоспособности Платформы.

Компонент (логическая сущность) Life-Cycle Manager (LCM) предназначен для управления и развертывания инсталляций (экземпляров) ПО «KeyStack SE» и выполняет такие функции, как:

- установка операционной системы и конфигурации физических серверов для добавления в инсталляцию;
- автоматизация процессов доставки сервисов и их конфигураций на целевые узлы облачной платформы;
- хранение исходных кодов некоторых компонентов;
- запуск пайплайнов (последовательности этапов управления инсталляцией), который производится только аутентифицированными пользователями среды функционирования с соответствующими правами доступа в этой среде (сертифицированной операционной системе); запуск резервного копирования на узле LCM.

Инициализация ПО «KeyStack SE» происходит следующим образом:

- инициализация элементов аппаратной платформы и передача управления операционной системе;
- загрузка ОС Platform V SberLinux OS Server 9.0 (Сертификат ФСТЭК России №4884 от 04.12.2024, действителен до 04.12.2029);
- загрузка системы контейнеризации Podman;
- запуск модулей ПО «KeyStack SE» с учетом проверок по контролю целостности конфигурационных файлов в среде контейнеризации;
- запуск программных сервисов ПО «KeyStack SE».

Действия, проводимые при инсталляции ПО «KeyStack SE», а также при

инициализации ПО «KeyStack SE» подлежат журналированию.

Для безопасного процесса инициализации ПО «KeyStack SE» выполняются следующие требования и ограничения:

- установка, конфигурирование и управление ПО «KeyStack SE» осуществляются в соответствии с эксплуатационной документацией;
- обеспечено наличие ответственных лиц – администратора среды функционирования (операционной системы), а также администратора средства виртуализации, которые осуществляют установку и первоначальную настройку ПО «KeyStack SE»;
- обеспечена физическая сохранность серверной платформы с установленным ПО «KeyStack SE» и исключение возможности физического доступа к ней посторонних лиц;
- обеспечивается предотвращение несанкционированного доступа к идентификаторам и паролям пользователей ПО «KeyStack SE» путем интеграции KeyStone с сертифицированными продуктами, использующими протоколы OpenID, OAuth;
- в процессе загрузки ПО «KeyStack SE» осуществляется проверка целостности конфигурационных файлов;
- выделение отдельного пользовательского сегмента от сегмента управления и ограничение доступа к сегменту управления;
- в сертифицированных средах функционирования, используемых для ПО «KeyStack SE», регулярно применяются все обновления безопасности.

5. РЕЖИМЫ РАБОТЫ ПО «KeyStack SE»

ПО «KeyStack SE» функционирует в следующих режимах:

- штатный режим регулярной работы, при котором обеспечивается выполнение задач в объеме функций, предусмотренных техническим заданием и обеспечиваемый регулярной загрузкой данных из источников;
- сервисный режим, необходимый для проведения обслуживания, реконфигурации и пополнения технических и программных средств ПО «KeyStack SE» новыми компонентами;
- аварийный режим работы.

В штатном режиме функционирования ПО «KeyStack SE» обеспечивает следующий режим работы: доступность функций системы, составляющая не менее 95% в год.

В сервисном режиме ПО «KeyStack SE» обеспечивает возможность проведения следующих работ:

- техническое обслуживание;
- модернизацию программного комплекса;
- устранение аварийных ситуаций.

ПО «KeyStack SE» переходит в аварийный режим при возникновении нештатной ситуации и невозможности штатной работы. В случае перехода ПО «KeyStack SE» в аварийный режим, администратору необходимо перевести ПО «KeyStack SE» в сервисный режим в соответствии с инструкциями, изложенными в руководстве Администратора системы.

Регламентные работы должны производиться с учётом требований о доступности ПО «KeyStack SE».

Функционирование ПО «KeyStack SE» при отказах и сбоях серверного общесистемного и специального программного обеспечения, в том числе структурных узлов ПО «KeyStack SE», не предусматривается.

6. ПОДГОТОВКА К РАБОТЕ

6.1 Проверка соответствия требованиям

Перед началом эксплуатации ПО необходимо проверить его соответствие требованиям к комплектности, упаковке и маркировке, отраженным в документе «Программное обеспечение «Облачная платформа KeyStack SE v.1». Формуляр», 1087746411378.62.01.29.000.001 ФО в зависимости от вариантов исполнения ПО.

При проверке комплектности проводится проверка целостности и качества записи дистрибутива программного обеспечения ПО на оптическом носителе информации посредством подсчета контрольной суммы дистрибутива и сравнения их с контрольной суммой, отраженной в документе «Программное обеспечение «Облачная платформа KeyStack SE v.1». Формуляр», 1087746411378.62.01.29.000.001 ФО. Необходимо произвести резервное копирование конфигурации ПО (не менее 2-х копий) для обновления (при необходимости) и проверки целостности ПО.

6.2 Подготовка ПО «KeyStack SE» к работе

6.2.1 Подключение к Порталу самообслуживания

Подключение к Порталу самообслуживания производится с помощью веб-браузера. Для доступа к интерфейсам управления Портала самообслуживания могут использоваться браузеры актуальных версий:

- Google Chrome 72 и выше;
- Mozilla Firefox 63 и выше.

При запросе логина и пароля необходимо ввести учетные данные.

Главная страница интерфейса управления имеет тематическое боковое меню (далее в тексте — левое меню), с помощью которого выполняется переход к различным разделам интерфейса управления Платформы.

6.2.2 Подключение к интерфейсу управления Openstack CLI

Интерфейс управления OpenStack CLI позволяет выполнять команды OpenStack в интерфейсе командной строки. OpenStack CLI может быть установлен на узел LCM или любой другой внешний узел.

Для установки и настройки OpenStack CLI обратитесь к инструкции: Подключение к интерфейсу командной строки OpenStack.

Для получения справки по командам OpenStack CLI обратитесь к документации OpenStack: https://docs.openstack.org/ocata/user-guide/cli-cheat-sheet.html.

Подключение к интерфейсу командной строки OpenStack

Для выполнения команд OpenStack необходимо подключение к интерфейсу командной строки (OpenStack CLI). Для управления сервисом DRS используется интерфейс командной строки drsclient. Эти клиенты уже входят в поставку LCM-узла KeyStack, но их также можно установить на рабочее место администратора. Ниже приведен порядок установки интерфейсов командной строки для различных ОС.

Установка клиентов CLI под Linux

Установка выполняется с помощью менеджера пакетов Python **pip**. Чтобы установить необходимые пакеты, выполните команды:

$ sudo pip install drsclient

$ sudo pip install python-cinderclient

$ sudo pip install python-novaclient

$ sudo pip install python-openstackclient

Получение файла **openrc**

Для подключения к CLI необходимо загрузить исходный файл OpenStack RC**.** Этот файл устанавливает переменные окружения, необходимые для подключения и авторизации клиента OpenStack CLI. Файл openrc можно получить разными способами.

Получение файла openrc из Портала администратора

Файл openrc, полученный таким способом, не содержит пароль пользователя. Его необходимо ввести при применении файла.

1. Откройте интерфейс Портала администратора (AdminUI) и авторизуйтесь пользователем admin**.**
2. Нажмите кнопку **Скачать OpenStack RC-файл** на странице Status Page**.**

Получение файла openrc из Vault

При получении файла openrc этим способом в нём явно указывается пароль пользователя admin. Будьте осторожны при обращении с файлом.

Зайдите на LCM-узел через SSH.

Выполните команду экспорта файла openrc:

podman exec -ti vault vault read secret_v2/data/deployments/<ks-lcm.cloud.itkey.com>/<имя региона>/openrc -format=json | jq -r '.data.data.value' > openrc-<имя региона>.sh

Применение файла openrc

Если вы используете собственный сертификат CA, убедитесь, что цепочка CA-сертификатов chain-cert.pem сохранена в директории /installer/data/ca/cert/ сервиса Vault.

В импортированный файл добавьте строку:
export OS_CACERT=/installer/data/ca/cert/chain-ca.pem

Скопируйте файл openrc на компьютер с установленным клиентом OpenStack CLI.

Выполните команду для вашего файла для установки переменных окружения:
$ source admin-openrc.sh

Проверка работоспособности OpenStack CLI

Для проверки корректности настроек выполните команду, которая возвращает список виртуальных машин:

$ openstack server list

Полный список команд и другая справочная информация по OpenStack CLI: https://docs.openstack.org/python-openstackclient/latest/index.html

Перечень команд доступных утилите и совместимых с ОО:

access rule delete Delete access rule(s)
access rule list List access rules
access rule show Display access rule details
access token create Create an access token
address group create Create a new Address Group
address group delete Delete address group(s)
address group list List address groups

address group set Set address group properties
address group show Display address group details
address group unset Unset address group properties
address scope create Create a new Address Scope
address scope delete Delete address scope(s)
address scope list List address scopes
address scope set Set address scope properties
address scope show Display address scope details
aggregate add host Add host to aggregate
aggregate cache image Request image caching for aggregate
aggregate create Create a new aggregate
aggregate delete Delete existing aggregate(s)
aggregate list List all aggregates
aggregate remove host Remove host from aggregate
aggregate set Set aggregate properties
aggregate show Display aggregate details
aggregate unset Unset aggregate properties
application credential create Create new application credential
application credential delete Delete application credentials(s)
application credential list List application credentials
application credential show Display application credential details
availability zone list List availability zones and their status
bgp dragent add speaker Add a BGP speaker to a dynamic routing agent (python-neutronclient)
bgp dragent list List dynamic routing agents (python-neutronclient)
bgp dragent remove speaker Removes a BGP speaker from a dynamic routing agent (python-neutronclient)
bgp peer create Create a BGP peer (python-neutronclient)
bgp peer delete Delete a BGP peer (python-neutronclient)
bgp peer list List BGP peers (python-neutronclient)
bgp peer set Update a BGP peer (python-neutronclient)
bgp peer show Show information for a BGP peer (python-neutronclient)
bgp speaker add network Add a network to a BGP speaker (python-neutronclient)
bgp speaker add peer Add a peer to a BGP speaker (python-neutronclient)
bgp speaker create Create a BGP speaker (python-neutronclient)
bgp speaker delete Delete a BGP speaker (python-neutronclient)
bgp speaker list List BGP speakers (python-neutronclient)
bgp speaker list advertised routes List routes advertised (python-neutronclient)
bgp speaker remove network Remove a network from a BGP speaker (python-neutronclient)
bgp speaker remove peer Remove a peer from a BGP speaker (python-neutronclient)
bgp speaker set Set BGP speaker properties (python-neutronclient)
bgp speaker show Show a BGP speaker (python-neutronclient)
bgpvpn create Create BGP VPN resource (python-neutronclient)
bgpvpn delete Delete BGP VPN resource(s) (python-neutronclient)
bgpvpn list List BGP VPN resources (python-neutronclient)
bgpvpn network association create Create a BGP VPN network association (python-neutronclient)
bgpvpn network association delete Delete a BGP VPN network association(s) for a given BGP VPN (python-neutronclient)
bgpvpn network association list List BGP VPN network associations for a given BGP VPN (python-neutronclient)
bgpvpn network association show Show information of a given BGP VPN network association (python-neutronclient)
bgpvpn port association create Create a BGP VPN port association (python-neutronclient)
bgpvpn port association delete Delete a BGP VPN port association(s) for a given BGP VPN (python-neutronclient)

bgpvpn port association list List BGP VPN port associations for a given BGP VPN (python-neutronclient)
bgpvpn port association set Set BGP VPN port association properties (python-neutronclient)
bgpvpn port association show Show information of a given BGP VPN port association (python-neutronclient)
bgpvpn port association unset Unset BGP VPN port association properties (python-neutronclient)
bgpvpn router association create Create a BGP VPN router association (python-neutronclient)
bgpvpn router association delete Delete a BGP VPN router association(s) for a given BGP VPN (python-neutronclient)
bgpvpn router association list List BGP VPN router associations for a given BGP VPN (python-neutronclient)
bgpvpn router association set Set BGP VPN router association properties (python-neutronclient)
bgpvpn router association show Show information of a given BGP VPN router association (python-neutronclient)
bgpvpn router association unset Unset BGP VPN router association properties (python-neutronclient)
bgpvpn set Set BGP VPN properties (python-neutronclient)
bgpvpn show Show information of a given BGP VPN (python-neutronclient)
bgpvpn unset Unset BGP VPN properties (python-neutronclient)
block storage cleanup Do block storage cleanup
block storage cluster list List block storage clusters
block storage cluster set Set block storage cluster properties
block storage cluster show Show detailed information for a block storage cluster
block storage log level list List log levels of block storage service
block storage log level set Set log level of block storage service
block storage resource filter list List block storage resource filters
block storage resource filter show Show filters for a block storage resource type
block storage snapshot manageable list List manageable snapshots
block storage volume manageable list List manageable volumes
cached image clear Clear all images from cache, queue or both
cached image delete Delete image(s) from cache
cached image list Get Cache State
cached image queue Queue image(s) for caching
catalog list List services in the service catalog
catalog show Display service catalog details
command list List recognized commands by group
complete print bash completion command (cliff)
compute agent create Create compute agent
compute agent delete Delete compute agent(s)
compute agent list List compute agents
compute agent set Set compute agent properties
compute service delete Delete compute service(s)
compute service list List compute services
compute service set Set compute service properties
configuration show Display configuration details
consistency group add volume Add volume(s) to consistency group
consistency group create Create new consistency group
consistency group delete Delete consistency group(s)
consistency group list List consistency groups
consistency group remove volume Remove volume(s) from consistency group
consistency group set Set consistency group properties
consistency group show Display consistency group details
consistency group snapshot create Create new consistency group snapshot
consistency group snapshot delete Delete consistency group snapshot(s)
consistency group snapshot list List consistency group snapshots

consistency group snapshot show Display consistency group snapshot details
console log show Show server's console output
console url show Show server's remote console URL
consumer create Create new consumer
consumer delete Delete consumer(s)
consumer list List consumers
consumer set Set consumer properties
consumer show Display consumer details
container create Create new container
container delete Delete container
container list List containers
container save Save container contents locally
container set Set container properties
container show Display container details
container unset Unset container properties
credential create Create new credential
credential delete Delete credential(s)
credential list List credentials
credential set Set credential properties
credential show Display credential details
default security group rule create Add a new security group rule to the default security group template
default security group rule delete Remove security group rule(s) from the default security group template
default security group rule list List security group rules used for new default security groups
default security group rule show Show a security group rule used for new default security groups
domain create Create new domain
domain delete Delete domain(s)
domain list List domains
domain set Set domain properties
domain show Display domain details
ec2 credentials create Create EC2 credentials
ec2 credentials delete Delete EC2 credentials
ec2 credentials list List EC2 credentials
ec2 credentials show Display EC2 credentials details
endpoint add project Associate a project to an endpoint
endpoint create Create new endpoint
endpoint delete Delete endpoint(s)
endpoint group add project Add a project to an endpoint group
endpoint group create Create new endpoint group
endpoint group delete Delete endpoint group(s)
endpoint group list List endpoint groups
endpoint group remove project Remove project from endpoint group
endpoint group set Set endpoint group properties
endpoint group show Display endpoint group details
endpoint list List endpoints
endpoint remove project Dissociate a project from an endpoint
endpoint set Set endpoint properties
endpoint show Display endpoint details
extension list List API extensions
extension show Show API extension
federation domain list List accessible domains
federation project list List accessible projects
federation protocol create Create new federation protocol
federation protocol delete Delete federation protocol(s)

federation protocol list List federation protocols
federation protocol set Set federation protocol properties
federation protocol show Display federation protocol details
firewall group create Create a new firewall group (python-neutronclient)
firewall group delete Delete firewall group(s) (python-neutronclient)
firewall group list List firewall groups (python-neutronclient)
firewall group policy add rule Insert a rule into a given firewall policy (python-neutronclient)
firewall group policy create Create a new firewall policy (python-neutronclient)
firewall group policy delete Delete firewall policy(s) (python-neutronclient)
firewall group policy list List firewall policies (python-neutronclient)
firewall group policy remove rule Remove a rule from a given firewall policy (python-neutronclient)
firewall group policy set Set firewall policy properties (python-neutronclient)
firewall group policy show Display firewall policy details (python-neutronclient)
firewall group policy unset Unset firewall policy properties (python-neutronclient)
firewall group rule create Create a new firewall rule (python-neutronclient)
firewall group rule delete Delete firewall rule(s) (python-neutronclient)
firewall group rule list List firewall rules that belong to a given tenant (python-neutronclient)
firewall group rule set Set firewall rule properties (python-neutronclient)
firewall group rule show Display firewall rule details (python-neutronclient)
firewall group rule unset Unset firewall rule properties (python-neutronclient)
firewall group set Set firewall group properties (python-neutronclient)
firewall group show Display firewall group details (python-neutronclient)
firewall group unset Unset firewall group properties (python-neutronclient)
flavor create Create new flavor
flavor delete Delete flavor(s)
flavor list List flavors
flavor set Set flavor properties
flavor show Display flavor details
flavor unset Unset flavor properties
floating ip create Create floating IP
floating ip delete Delete floating IP(s)
floating ip list List floating IP(s)
floating ip pool list List pools of floating IP addresses
floating ip port forwarding create Create floating IP port forwarding
floating ip port forwarding delete Delete floating IP port forwarding
floating ip port forwarding list List floating IP port forwarding
floating ip port forwarding set Set floating IP Port Forwarding Properties
floating ip port forwarding show Display floating IP Port Forwarding details
floating ip set Set floating IP Properties
floating ip show Display floating IP details
floating ip unset Unset floating IP Properties
group add user Add user to group
group contains user Check user membership in group
group create Create new group
group delete Delete group(s)
group list List groups
group remove user Remove user from group
group set Set group properties
group show Display group details
help print detailed help for another command (cliff)
host list DEPRECATED: List hosts
host set Set host properties
host show DEPRECATED: Display host details
hypervisor list List hypervisors
hypervisor show Display hypervisor details

hypervisor stats show Display hypervisor stats details
identity provider create Create new identity provider
identity provider delete Delete identity provider(s)
identity provider list List identity providers
identity provider set Set identity provider properties
identity provider show Display identity provider details
image add project Associate project with image
image create Create/upload an image
image delete Delete image(s)
image import Initiate the image import process
image import info Show available import methods
image list List available images
image member get Show a particular project associated with image
image member list List projects associated with image
image metadef namespace create Create a metadef namespace
image metadef namespace delete Delete metadef namespace
image metadef namespace list List metadef namespaces
image metadef namespace set Set metadef namespace properties
image metadef namespace show Show a metadef namespace
image metadef object create Create a metadef object
image metadef object delete Delete metadata definitions object(s)
image metadef object list List metadef objects inside a specific namespace
image metadef object show Show a particular metadef object
image metadef object update Update a metadef object
image metadef property create Create a metadef property
image metadef property delete Delete metadef propert(ies)
image metadef property list List metadef properties
image metadef property set Update metadef namespace property
image metadef property show Show a particular metadef property
image metadef resource type list List metadef resource types
image remove project Disassociate project with image
image save Save an image locally
image set Set image properties
image show Display image details
image stage Upload data for a specific image to staging
image stores list Get available backends (only valid with Multi-Backend support)
image task list List tasks
image task show Display task details
image unset Unset image tags and properties
implied role create Creates an association between prior and implied roles
implied role delete Deletes an association between prior and implied roles
implied role list List implied roles
ip availability list List IP availability for network
ip availability show Show network IP availability details
keypair create Create new public or private key for server ssh access
keypair delete Delete public or private key(s)
keypair list List key fingerprints
keypair show Display key details
limit create Create a limit
limit delete Delete a limit
limit list List limits
limit set Update information about a limit
limit show Display limit details
limits show Show compute and block storage limits
local ip association create Create Local IP Association
local ip association delete Delete Local IP association(s)

local ip association list List Local IP Associations
local ip create Create Local IP
local ip delete Delete local IP(s)
local ip list List local IPs
local ip set Set local ip properties
local ip show Display local IP details
mapping create Create new mapping
mapping delete Delete mapping(s)
mapping list List mappings
mapping set Set mapping properties
mapping show Display mapping details
module list List module versions
network agent add network Add network to an agent
network agent add router Add router to an agent
network agent delete Delete network agent(s)
network agent list List network agents
network agent remove network Remove network from an agent
network agent remove router Remove router from an agent
network agent set Set network agent properties
network agent show Display network agent details
network auto allocated topology create Create the auto allocated topology for project
network auto allocated topology delete Delete auto allocated topology for project
network create Create new network
network delete Delete network(s)
network flavor add profile Add a service profile to a network flavor
network flavor create Create new network flavor
network flavor delete Delete network flavors
network flavor list List network flavors
network flavor profile create Create new network flavor profile
network flavor profile delete Delete network flavor profile
network flavor profile list List network flavor profile(s)
network flavor profile set Set network flavor profile properties
network flavor profile show Display network flavor profile details
network flavor remove profile Remove service profile from network flavor
network flavor set Set network flavor properties
network flavor show Display network flavor details
network l3 conntrack helper create Create a new L3 conntrack helper
network l3 conntrack helper delete Delete L3 conntrack helper
network l3 conntrack helper list List L3 conntrack helpers
network l3 conntrack helper set Set L3 conntrack helper properties
network l3 conntrack helper show Display L3 conntrack helper details
network list List networks
network log create Create a new network log (python-neutronclient)
network log delete Delete network log(s) (python-neutronclient)
network log list List network logs (python-neutronclient)
network log set Set network log properties (python-neutronclient)
network log show Display network log details (python-neutronclient)
network loggable resources list List supported loggable resources (python-neutronclient)
network meter create Create network meter
network meter delete Delete network meter
network meter list List network meters
network meter rule create Create a new meter rule
network meter rule delete Delete meter rule(s)
network meter rule list List meter rules
network meter rule show Display meter rules details
network meter show Show network meter

network onboard subnets Onboard network subnets into a subnet pool (python-neutronclient)
network qos policy create Create a QoS policy
network qos policy delete Delete Qos Policy(s)
network qos policy list List QoS policies
network qos policy set Set QoS policy properties
network qos policy show Display QoS policy details
network qos rule create Create new Network QoS rule
network qos rule delete Delete Network QoS rule
network qos rule list List Network QoS rules
network qos rule set Set Network QoS rule properties
network qos rule show Display Network QoS rule details
network qos rule type list List QoS rule types
network qos rule type show Show details about supported QoS rule type
network rbac create Create network RBAC policy
network rbac delete Delete network RBAC policy(s)
network rbac list List network RBAC policies
network rbac set Set network RBAC policy properties
network rbac show Display network RBAC policy details
network segment create Create new network segment
network segment delete Delete network segment(s)
network segment list List network segments
network segment range create Create new network segment range
network segment range delete Delete network segment range(s)
network segment range list List network segment ranges
network segment range set Set network segment range properties
network segment range show Display network segment range details
network segment set Set network segment properties
network segment show Display network segment details
network service provider list List Service Providers
network set Set network properties
network show Show network details
network subport list List all subports for a given network trunk
network trunk create Create a network trunk for a given project
network trunk delete Delete a given network trunk
network trunk list List all network trunks
network trunk set Set network trunk properties
network trunk show Show information of a given network trunk
network trunk unset Unset subports from a given network trunk
network unset Unset network properties
object create Upload object to container
object delete Delete object from container
object list List objects
object save Save object locally
object set Set object properties
object show Display object details
object store account set Set account properties
object store account show Display account details
object store account unset Unset account properties
object unset Unset object properties
policy create Create new policy
policy delete Delete policy(s)
policy list List policies
policy set Set policy properties
policy show Display policy details
port create Create a new port
port delete Delete port(s)

port list List ports
port set Set port properties
port show Display port details
port unset Unset port properties
project cleanup Clean resources associated with a project
project create Create new project
project delete Delete project(s)
project list List projects
project set Set project properties
project show Display project details
quota delete Delete configured quota for a project and revert to defaults
quota list List quotas for all projects with non-default quota values or list detailed quota information for requested project
quota set Set quotas for project or class
quota show Show quotas for project or class
region create Create new region
region delete Delete region(s)
region list List regions
region set Set region properties
region show Display region details
registered limit create Create a registered limit
registered limit delete Delete a registered limit
registered limit list List registered limits
registered limit set Update information about a registered limit
registered limit show Display registered limit details
request token authorize Authorize a request token
request token create Create a request token
role add Adds a role assignment to a user or group on the system, a domain, or a project
role assignment list List role assignments
role create Create new role
role delete Delete role(s)
role list List roles
role remove Removes a role assignment from system/domain/project : user/group
role set Set role properties
role show Display role details
router add port Add a port to a router
router add route Add extra static routes to a router's routing table
router add subnet Add a subnet to a router
router create Create a new router
router delete Delete router(s)
router list List routers
router ndp proxy create Create NDP proxy
router ndp proxy delete Delete NDP proxy
router ndp proxy list List NDP proxies
router ndp proxy set Set NDP proxy properties
router ndp proxy show Display NDP proxy details
router remove port Remove a port from a router
router remove route Remove extra static routes from a router's routing table
router remove subnet Remove a subnet from a router
router set Set router properties
router show Display router details
router unset Unset router properties
security group create Create a new security group
security group delete Delete security group(s)
security group list List security groups
security group rule create Create a new security group rule

security group rule delete Delete security group rule(s)
security group rule list List security group rules
security group rule show Display security group rule details
security group set Set security group properties
security group show Display security group details
security group unset Unset security group properties
server add fixed ip Add fixed IP address to server
server add floating ip Add floating IP address to server
server add network Add network to server
server add port Add port to server
server add security group Add security group to server
server add volume Add volume to server
server backup create Create a server backup image
server create Create a new server
server delete Delete server(s)
server dump create Create a dump file in server(s)
server evacuate Evacuate a server to a different host
server event list List recent events of a server
server event show Show server event details
server group create Create a new server group
server group delete Delete existing server group(s)
server group list List all server groups
server group show Display server group details
server image create Create a new server disk image from an existing server
server list List servers
server lock Lock server(s)
server migrate Migrate server to different host
server migrate confirm DEPRECATED: Use 'server migration confirm' instead
server migrate revert DEPRECATED: Use 'server migration revert' instead
server migration abort Cancel an ongoing live migration
server migration confirm Confirm server migration
server migration force complete Force an ongoing live migration to complete
server migration list List server migrations
server migration revert Revert server migration
server migration show Show an in-progress live migration for a given server
server pause Pause server(s)
server reboot Perform a hard or soft server reboot
server rebuild Rebuild server
server remove fixed ip Remove fixed IP address from server
server remove floating ip Remove floating IP address from server
server remove network Remove all ports of a network from server
server remove port Remove port from server
server remove security group Remove security group from server
server remove volume Remove volume from server
server rescue Put server in rescue mode
server resize Scale server to a new flavor
server resize confirm Confirm server resize
server resize revert Revert server resize
server restore Restore server(s)
server resume Resume server(s)
server set Set server properties
server shelve Shelve and optionally offload server(s)
server show Show server details
server ssh SSH to server
server start Start server(s)
server stop Stop server(s)

server suspend Suspend server(s)
server unlock Unlock server(s)
server unpause Unpause server(s)
server unrescue Restore server from rescue mode
server unset Unset server properties and tags
server unshelve Unshelve server(s)
server volume list List all the volumes attached to a server
server volume set Update a volume attachment on the server
server volume update DEPRECATED: Use 'server volume set' instead
service create Create new service
service delete Delete service(s)
service list List services
service provider create Create new service provider
service provider delete Delete service provider(s)
service provider list List service providers
service provider set Set service provider properties
service provider show Display service provider details
service set Set service properties
service show Display service details
sfc flow classifier create Create a flow classifier (python-neutronclient)
sfc flow classifier delete Delete a given flow classifier (python-neutronclient)
sfc flow classifier list List flow classifiers (python-neutronclient)
sfc flow classifier set Set flow classifier properties (python-neutronclient)
sfc flow classifier show Display flow classifier details (python-neutronclient)
sfc port chain create Create a port chain (python-neutronclient)
sfc port chain delete Delete a given port chain (python-neutronclient)
sfc port chain list List port chains (python-neutronclient)
sfc port chain set Set port chain properties (python-neutronclient)
sfc port chain show Display port chain details (python-neutronclient)
sfc port chain unset Unset port chain properties (python-neutronclient)
sfc port pair create Create a port pair (python-neutronclient)
sfc port pair delete Delete a given port pair (python-neutronclient)
sfc port pair group create Create a port pair group (python-neutronclient)
sfc port pair group delete Delete a given port pair group (python-neutronclient)
sfc port pair group list List port pair group (python-neutronclient)
sfc port pair group set Set port pair group properties (python-neutronclient)
sfc port pair group show Display port pair group details (python-neutronclient)
sfc port pair group unset Unset port pairs from port pair group (python-neutronclient)
sfc port pair list List port pairs (python-neutronclient)
sfc port pair set Set port pair properties (python-neutronclient)
sfc port pair show Display port pair details (python-neutronclient)
sfc service graph create Create a service graph (python-neutronclient)
sfc service graph delete Delete a given service graph (python-neutronclient)
sfc service graph list List service graphs (python-neutronclient)
sfc service graph set Set service graph properties (python-neutronclient)
sfc service graph show Show information of a given service graph (python-neutronclient)
subnet create Create a subnet
subnet delete Delete subnet(s)
subnet list List subnets
subnet pool create Create subnet pool
subnet pool delete Delete subnet pool(s)
subnet pool list List subnet pools
subnet pool set Set subnet pool properties
subnet pool show Display subnet pool details
subnet pool unset Unset subnet pool properties
subnet set Set subnet properties

subnet show Display subnet details
subnet unset Unset subnet properties
token issue Issue new token
token revoke Revoke existing token
trust create Create new trust
trust delete Delete trust(s)
trust list List trusts
trust show Display trust details
usage list List resource usage per project
usage show Show resource usage for a single project
user create Create new user
user delete Delete user(s)
user list List users
user password set Change current user password
user set Set user properties
user show Display user details
versions show Show available versions of services
volume attachment complete Complete an attachment for a volume
volume attachment create Create an attachment for a volume
volume attachment delete Delete an attachment for a volume
volume attachment list Lists all volume attachments
volume attachment set Update an attachment for a volume
volume attachment show Show detailed information for a volume attachment
volume backend capability show Show capability command
volume backend pool list List pool command
volume backup create Create new volume backup
volume backup delete Delete volume backup(s)
volume backup list List volume backups
volume backup record export Export volume backup details
volume backup record import Import volume backup details
volume backup restore Restore volume backup
volume backup set Set volume backup properties
volume backup show Display volume backup details
volume backup unset Unset volume backup properties
volume create Create new volume
volume delete Delete volume(s)
volume group create Create a volume group
volume group delete Delete a volume group
volume group failover Failover replication for a volume group
volume group list Lists all volume groups
volume group set Update a volume group
volume group show Show detailed information for a volume group
volume group snapshot create Create a volume group snapshot
volume group snapshot delete Delete a volume group snapshot
volume group snapshot list Lists all volume group snapshot
volume group snapshot show Show detailed information for a volume group snapshot
volume group type create Create a volume group type
volume group type delete Delete a volume group type
volume group type list Lists all volume group types
volume group type set Update a volume group type
volume group type show Show detailed information for a volume group type
volume host set Set volume host properties
volume list List volumes
volume message delete Delete a volume failure message
volume message list List volume failure messages
volume message show Show a volume failure message

volume migrate Migrate volume to a new host
volume qos associate Associate a QoS specification to a volume type
volume qos create Create new QoS specification
volume qos delete Delete QoS specification
volume qos disassociate Disassociate a QoS specification from a volume type
volume qos list List QoS specifications
volume qos set Set QoS specification properties
volume qos show Display QoS specification details
volume qos unset Unset QoS specification properties
volume revert Revert a volume to a snapshot
volume service list List service command
volume service set Set volume service properties
volume set Set volume properties
volume show Display volume details
volume snapshot create Create new volume snapshot
volume snapshot delete Delete volume snapshot(s)
volume snapshot list List volume snapshots
volume snapshot set Set volume snapshot properties
volume snapshot show Display volume snapshot details
volume snapshot unset Unset volume snapshot properties
volume summary Show a summary of all volumes in this deployment
volume transfer request accept Accept volume transfer request
volume transfer request create Create volume transfer request
volume transfer request delete Delete volume transfer request(s)
volume transfer request list Lists all volume transfer requests
volume transfer request show Show volume transfer request details
volume type create Create new volume type
volume type delete Delete volume type(s)
volume type list List volume types
volume type set Set volume type properties
volume type show Display volume type details
volume type unset Unset volume type properties
volume unset Unset volume properties
vpn endpoint group create Create an endpoint group (python-neutronclient)
vpn endpoint group delete Delete endpoint group(s) (python-neutronclient)
vpn endpoint group list List endpoint groups that belong to a given project (python-neutronclient)
vpn endpoint group set Set endpoint group properties (python-neutronclient)
vpn endpoint group show Display endpoint group details (python-neutronclient)
vpn ike policy create Create an IKE policy (python-neutronclient)
vpn ike policy delete Delete IKE policy (policies) (python-neutronclient)
vpn ike policy list List IKE policies that belong to a given project (python-neutronclient)
vpn ike policy set Set IKE policy properties (python-neutronclient)
vpn ike policy show Display IKE policy details (python-neutronclient)
vpn ipsec policy create Create an IPsec policy (python-neutronclient)
vpn ipsec policy delete Delete IPsec policy(policies) (python-neutronclient)
vpn ipsec policy list List IPsec policies that belong to a given project (python-neutronclient)
vpn ipsec policy set Set IPsec policy properties (python-neutronclient)
vpn ipsec policy show Display IPsec policy details (python-neutronclient)
vpn ipsec site connection create Create an IPsec site connection (python-neutronclient)
vpn ipsec site connection delete Delete IPsec site connection(s) (python-neutronclient)
vpn ipsec site connection list List IPsec site connections that belong to a given project (python-neutronclient)
vpn ipsec site connection set Set IPsec site connection properties (python-neutronclient)
vpn ipsec site connection show Show information of a given IPsec site connection (python-neutronclient)

vpn service create Create an VPN service (python-neutronclient)
vpn service delete Delete VPN service(s) (python-neutronclient)
vpn service list List VPN services that belong to a given project (python-neutronclient)
vpn service set Set VPN service properties (python-neutronclient)
vpn service show Display VPN service details (python-neutronclient)

7. ПРИНЦИНЫ БЕЗОПАСНОЙ РАБОТЫ ПО «KeyStack SE»

7.1 Защита ПО «KeyStack SE» от несанкционированного доступа

Обеспечение собственной защиты ПО «KeyStack SE» от несанкционированного доступа осуществляется за счет:

- наличия ответственного лица (администратора среды функционирования – операционной системы), отвечающего за установку компонентов логической сущности LCM, а также их настройку. Идентификация и аутентификация указанных при настройке компонентов LCM осуществляется с помощью 2FA на основе индивидуального сертификата;
- настройка компонентов LCM должна осуществляться в соответствии с эксплуатационной документацией (руководством администратора ПО «KeyStack SE»);
- обеспечения физической сохранности аппаратной платформы с установленным ПО «KeyStack SE» и исключением возможности доступа к ней посторонних лиц;
- выделением необходимых сетевых сегментов для работы с ПО «KeyStack SE»;
- обеспечения предотвращения несанкционированного доступа к идентификаторам и паролям привилегированных пользователей (администраторов);
- разделения полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование ПО «KeyStack SE»;
- осуществления доступа к объектам доступа ПО «KeyStack SE» с учетом минимально необходимых прав и привилегий;
- предоставления прав и привилегий по доступу к функциям безопасности (параметрам настройки) ПО «KeyStack SE» исключительно администратору средства виртуализации, наделенному полномочиями в соответствии с требованиями к функциям безопасности;
- параметры и настройки ПО «KeyStack SE» хранятся на уровне файловой системы и базы данных, эти ресурсы недоступны пользователям ПО «KeyStack SE» через предоставляемые для них программные интерфейсы. Доступ к ним имеет только лицо, ответственное за установку и настройку компонентов LCM (который производит установку и настройку ПО, администратора среды функционирования – операционной системы);
- пересмотра перечня событий безопасности, подлежащих регистрации, не менее чем один раз в год, а также по результатам контроля (мониторинга) за обеспечением уровня защищенности информации, содержащейся в ПО «KeyStack SE»;
- обеспечения срока хранения информации о зарегистрированных событиях безопасности не менее трех месяцев, если иное не установлено требованиями законодательства Российской Федерации, при этом осуществляется хранение записей о выявленных событиях безопасности и записей системных журналов, которые послужили основанием для регистрации события безопасности;
- в процессе функционирования ПО «KeyStack SE» с заданной периодичность осуществляется контроль целостности исполняемых файлов и конфигурации ПО;
- ПО «KeyStack SE» должен контролировать целостность исполняемых файлов и параметров настройки средства виртуализации с использованием программной среды (Platform V SberLinux OS Server 9.0).
- определения в ПО «KeyStack SE» источника надежных меток времени (с использованием функции NTP в операционной системе).

- пересмотра перечня событий безопасности, подлежащих регистрации, не менее чем один раз в год, а также по результатам контроля (мониторинга) за обеспечением уровня защищенности информации, содержащейся в ПО «KeyStack SE»;
- обеспечения срока хранения информации о зарегистрированных событиях безопасности не менее трех месяцев, если иное не установлено требованиями законодательства Российской Федерации, при этом осуществляется хранение записей о выявленных событиях безопасности и записей системных журналов, которые послужили основанием для регистрации события безопасности;
- в процессе функционирования ПО «KeyStack SE» с заданной периодичность осуществляется контроль целостности исполняемых файлов и конфигурации ПО;
- ПО «KeyStack SE» должен контролировать целостность исполняемых и конфигурационных файлов средства виртуализации с использованием программной среды (ОС Platform V SberLinux OS Server 9.0).
- определения в ПО «KeyStack SE» источника надежных меток времени (с использованием функции NTP в операционной системе);

8. ОПИСАНИЕ ОПЕРАЦИЙ

8.1 Интерфейсы Портала Администрирования

8.1.1 Идентификация и аутентификация пользователей

8.1.1.1 Интерфейс идентификации и аутентификации пользователя

На Рисунке 1.1 приведён интерфейс ПО «KeyStack SE», назначением которого является реализация требований безопасности, связанных с идентификацией и аутентификацией пользователей. Интерфейс представлен в GUI и используется для идентификации и аутентификации пользователей в ПО «KeyStack SE».

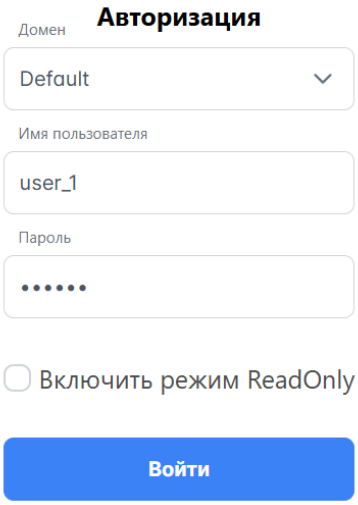

Рисунок 1.1

Интерфейс идентификации и аутентификации пользователя реализует следующие требования по безопасности информации:

– Идентификация и аутентификация пользователей в ПО «KeyStack SE» осуществляется с учетом требований разделов 4 – 7 ГОСТ Р 58833–2020 «Защита информации. Идентификация и аутентификация. Общие положения».

– ПО «KeyStack SE» должно осуществлять аутентификацию пользователей при предъявлении идентификатора и пароля пользователя.

– Защита пароля пользователя ПО «KeyStack SE» должна обеспечиваться при его вводе за счет отображения вводимых символов условными знаками.

– Пароль пользователя ПО «KeyStack SE» должен содержать не менее 8 символов при алфавите пароля не менее 70 символов. Максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки – 4.

– При попытке ввода неправильного значения идентификатора или пароля пользователя должно выводиться сообщение с приглашением ввести правильный идентификатор и пароль еще раз.

Интерфейс позволяет выполнять следующие действия:

– идентификация пользователя;

– аутентификация пользователя.

В интерфейсе предусмотрены действия, не влияющие на выполнение требований безопасности к ПО «KeyStack SE»:

– просматривать информацию о списке доступных доменов;

– включать режим ReadOnly.

При вызове указанного интерфейса предусмотрены следующие ошибки безопасности:

– ERROR: Failed to log in. User with the <имя пользователя> name was not found or does not exist;

– ERROR: Failed to log in. The request you have made requires authentication.

Параметры, используемые интерфейсом идентификации и аутентификации пользователя:

– имя пользователя;

– домен;

– пароль.

Способ использования интерфейса:

– ввод данных в графический пользовательский интерфейс.

Адреса обработки запроса:

“POST /api/login” – URL, находящийся на модуле Adminui-backend, вызывающем API Openstack, используется для реализации ФБ (функции безопасности)

“POST /v3/auth/tokens” – API Openstack модуля KeyStone (Аутентификация и управление токенами)

8.1.1.2 Интерфейс изменения пароля пользователя

На Рисунке 1.2 приведён интерфейс ПО «KeyStack SE», назначением которого является реализация требований безопасности, связанных с аутентификацией пользователей. Интерфейс представлен в GUI и используется для изменения пароля пользователей в ПО «KeyStack SE».

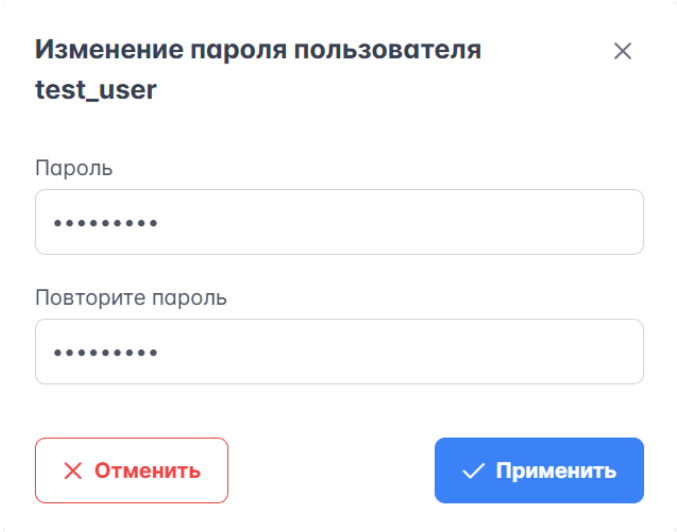

Рисунок 1.2

Интерфейс изменения пароля пользователя реализует следующие требования по безопасности информации:

– ПО «KeyStack SE» должно обеспечивать возможность смены установленного администратором ПО «KeyStack SE» пароля пользователя ПО «KeyStack SE» после его первичной аутентификации.

– Защита пароля пользователя ПО «KeyStack SE» должна обеспечиваться при его вводе за счет отображения вводимых символов условными знаками.

– Пароль пользователя ПО «KeyStack SE» должен содержать не менее 8 символов при алфавите пароля не менее 70 символов. Максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки – 4.

– ПО «KeyStack SE» должно обеспечивать:

- хранение аутентификационной информации пользователя ПО «KeyStack SE» в защищенном формате или в защищенном хранилище;

- взаимную идентификацию и аутентификацию пользователей и ПО «KeyStack SE» при удаленном доступе с использованием сетей связи общего пользования.

Интерфейс позволяет выполнять следующие действия:

- изменять пароль пользователя.

Действий, не влияющих на выполнение требований безопасности к ПО «KeyStack SE», в интерфейсе не предусмотрено.

При вызове указанного интерфейса предусмотрены следующие ошибки безопасности:

- ERROR: You need a valid user and password to access this content.

Параметры, используемые интерфейсом изменения пароля пользователя:

- новый пароль.

Способ использования интерфейса:

- ввод данных в графический пользовательский интерфейс.

Адреса обработки запроса:

“PUT /api/fstek1/users” – URL, находящийся на модуле Adminui-backend, вызывающем API Openstack, используется для реализации ФБ (функции безопасности)

“POST /v3/users/{user_id}/password” – API Openstack модуля KeyStone (Пользователи)

8.1.2 Управление доступом

8.1.2.1 Интерфейсы управления ролями

8.1.2.1.1 Интерфейс смены роли

На Рисунке 1.3 приведён интерфейс ПО «KeyStack SE», назначением которого является реализация требований безопасности, связанных с реализацией ролевой модели управления доступом. Интерфейс представлен в GUI и используется для смены роли пользователя в ПО «KeyStack SE».

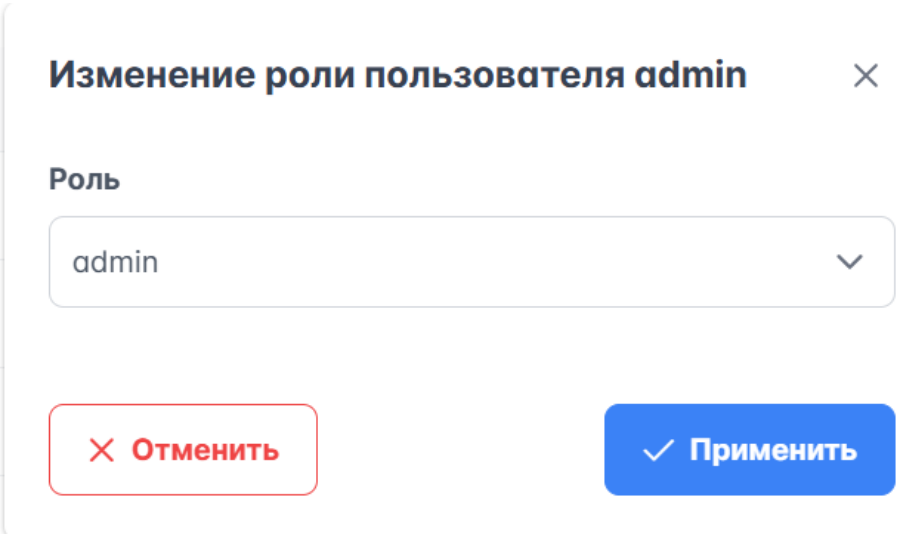

Рисунок 1.3

Интерфейс смены роли реализует следующие требования по безопасности информации:

– В ПО «KeyStack SE» должен быть реализован ролевой метод управления доступом с ролями пользователей: разработчик виртуальной машины, администратор безопасности ПО «KeyStack SE», администратор ПО «KeyStack SE», администратор виртуальной машины.

Интерфейс позволяет выполнять следующие действия:

– сменить роль пользователю.

В интерфейсе не предусмотрены действия, не влияющие на выполнение требований безопасности к ПО «KeyStack SE».

При вызове указанного интерфейса не предусмотрены ошибки безопасности:

Параметры, используемые интерфейсом смены роли:

– наименование роли.

Способ использования интерфейса:

– выбор значения из списка в графическом пользовательском интерфейсе.

Адреса обработки запроса:

“PUT /api/fstek2/users/{идентификатор пользователя}” – URL, находящийся на модуле Adminui-backend, вызывающем API Openstack, используется для реализации ФБ (функции безопасности)

“PUT /v3/projects/{project_id}/users/{user_id}/roles/{role_id}” – API Openstack модуля KeyStone (Роли)

8.1.2.2 Интерфейсы управления пользователями

8.1.2.2.1 Интерфейс просмотра списка пользователей

На Рисунке 1.4 приведён интерфейс ПО «KeyStack SE», назначением которого является реализация требований безопасности, связанных с просмотром списка пользователей. Интерфейс представлен в GUI и используется для просмотра списка пользователей в ПО «KeyStack SE».

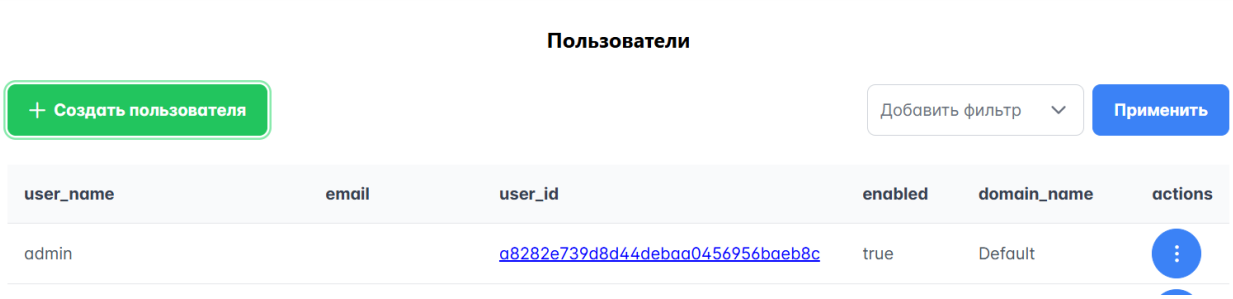

Рисунок 1.4

Интерфейс просмотра списка пользователей реализует следующие требования по безопасности информации:

– ПО «KeyStack SE» должно обеспечивать невозможность установления одинаковых идентификаторов и паролей для разных пользователей.

– ПО «KeyStack SE» должно обеспечивать:

- хранение аутентификационной информации пользователя ПО «KeyStack SE» в защищенном формате или в защищенном хранилище;
- взаимную идентификацию и аутентификацию пользователей и ПО «KeyStack SE» при удаленном доступе с использованием сетей связи общего пользования.

Интерфейс позволяет выполнять следующие действия:

– просматривать аутентификационную информацию;

– переходить к интерфейсам просмотра параметров, редактирования пользователя, изменения пароля и смены роли.

В интерфейсе предусмотрены действия, не влияющие на выполнение требований безопасности к ПО «KeyStack SE»:

– фильтрация списка пользователей.

При вызове указанного интерфейса не предусмотрены ошибки безопасности.

Параметры, используемые интерфейсом просмотра списка пользователей:

– наименование пользователя;

– электронная почта пользователя;

– идентификатор пользователя;

– статус пользователя;

– имя домена, к которому относится пользователь.

Способ использования интерфейса:

– просмотр списка пользователей.

Адреса обработки запроса:

“GET /api/fstek2/users” – URL, находящийся на модуле Adminui-backend, вызывающем API Openstack, используется для реализации ФБ (функции безопасности)

“DELETE /v3/users/{user_id}” – API Openstack модуля KeyStone (Пользователи)

8.1.2.2.2 Интерфейс просмотра параметров пользователя

На Рисунке 1.5 приведён интерфейс ПО «KeyStack SE», назначением которого является реализация требований безопасности, связанных с просмотром параметров пользователя. Интерфейс представлен в GUI и используется для просмотра параметров пользователя в ПО «KeyStack SE».

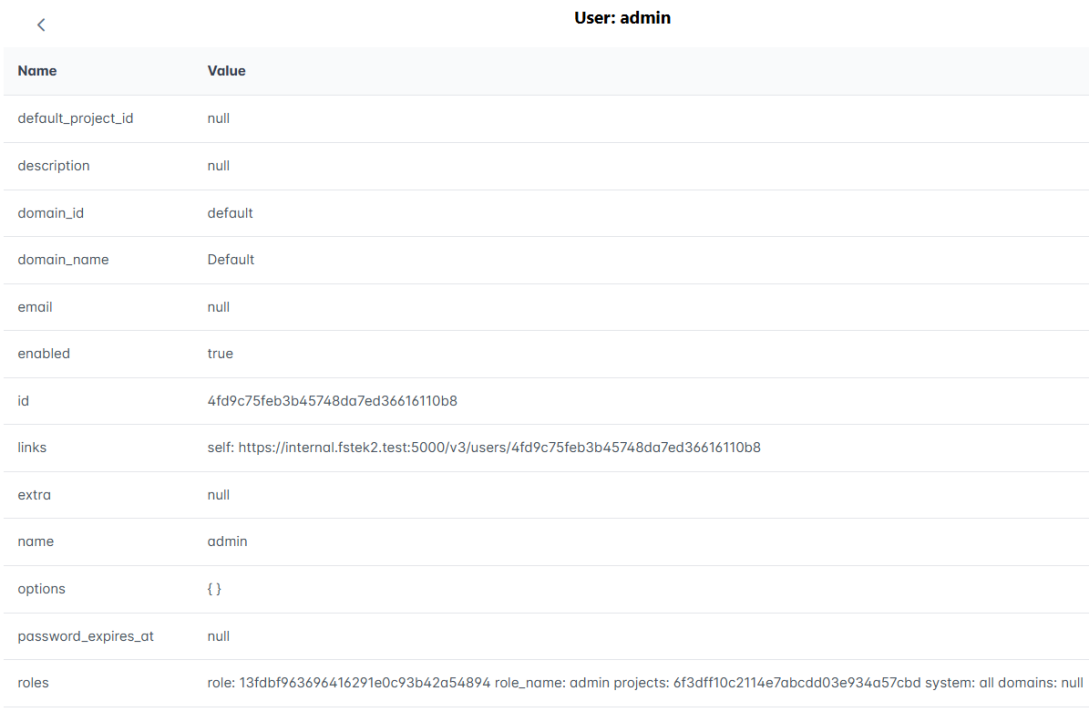

Рисунок 1.5

Интерфейс просмотра параметров пользователя реализует следующие требования по безопасности информации:

– ПО «KeyStack SE» должно обеспечивать невозможность установления одинаковых идентификаторов и паролей для разных пользователей.

– ПО «KeyStack SE» должно обеспечивать:

- хранение аутентификационной информации пользователя ПО «KeyStack SE» в защищенном формате или в защищенном хранилище;
- взаимную идентификацию и аутентификацию пользователей и ПО «KeyStack SE» при удаленном доступе с использованием сетей связи общего пользования.

Интерфейс позволяет выполнять следующие действия:

– просматривать параметры пользователя.

Действий, не влияющих на выполнение требований безопасности к ПО «KeyStack SE», в интерфейсе не предусмотрено.

При вызове указанного интерфейса не предусмотрены ошибки безопасности.

Параметры, используемые интерфейсом просмотра списка пользователей:

– идентификатор проекта по умолчанию, к которому относится пользователь;
– описание пользователя;
– идентфикатор домена, к которому относится пользователь;
– имя домена, к которому относится пользователь;
– электронная почта пользователя;
– статус пользователя;
– идентификатор пользователя;
– ссылка на пользователя;
– экстра параметры пользователя;
– наименование пользователя;
– опции пользователя;
– дата и время истечения срока пароля;
– роли пользователя.

Способ использования интерфейса:

– просмотр таблицы через графический пользовательский интерфейс.

Адрес обработки запроса:

“GET /api/fstek2/users/{идентификатор пользователя}”

8.1.2.2.3 Интерфейс создания пользователя

На Рисунке 1.6 приведён интерфейс ПО «KeyStack SE», назначением которого является реализация требований безопасности, связанных с управлением пользователями. Интерфейс представлен в GUI и используется для создания пользователей в ПО «KeyStack SE».

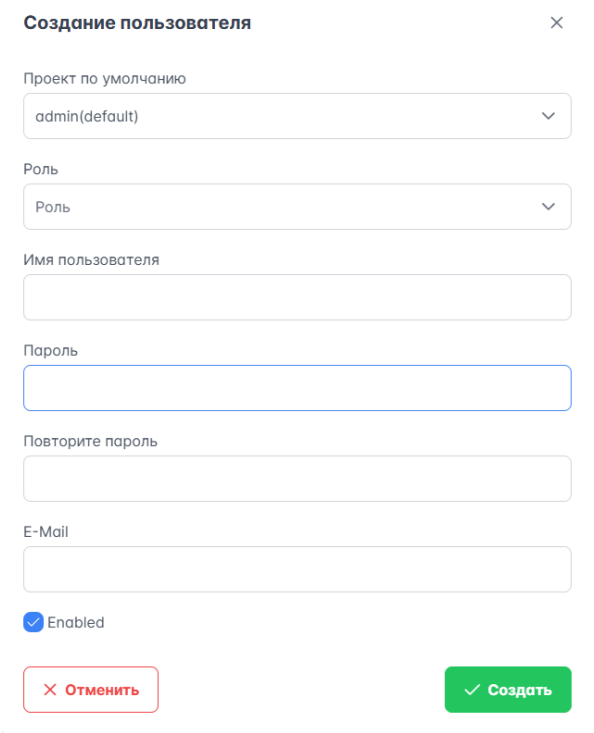

Рисунок 1.6

Интерфейс создания пользователя реализует следующие требования по безопасности информации:

– Первичная идентификация пользователей ПО «KeyStack SE» должна осуществляться администратором ПО «KeyStack SE».

– Идентификация и аутентификация пользователей в ПО «KeyStack SE» осуществляется с учетом требований разделов 4 – 7 ГОСТ Р 58833–2020 «Защита информации. Идентификация и аутентификация. Общие положения».

– Пароль пользователя для первичной аутентификации должен устанавливаться администратором ПО «KeyStack SE».

– ПО «KeyStack SE» должно обеспечивать невозможность установления одинаковых идентификаторов и паролей для разных пользователей.

– Защита пароля пользователя ПО «KeyStack SE» должна обеспечиваться при его вводе за счет отображения вводимых символов условными знаками.

– Пароль пользователя ПО «KeyStack SE» должен содержать не менее 8 символов при алфавите пароля не менее 70 символов. Максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки – 4.

– В случае неуспешной идентификации и аутентификации пользователей в ПО «KeyStack SE» их доступ должен быть заблокирован.

– При исчерпании установленного максимального количества неуспешных попыток ввода неправильного пароля учетная запись пользователя ПО «KeyStack SE» должна быть заблокирована с возможностью разблокировки администратором ПО «KeyStack SE» или с возможностью автоматической разблокировки по истечении временного интервала, устанавливаемого администратором ПО «KeyStack SE».

– ПО «KeyStack SE» должно обеспечивать:

- хранение аутентификационной информации пользователя ПО «KeyStack SE» в защищенном формате или в защищенном хранилище;
- взаимную идентификацию и аутентификацию пользователей и ПО «KeyStack SE» при удаленном доступе с использованием сетей связи общего пользования.

Интерфейс позволяет выполнять следующие действия:

– создавать пользователя.

В интерфейсе предусмотрены действия, не влияющие на выполнение требований безопасности к ПО «KeyStack SE»:

– просматривать информацию о списке доступных проекто и ролей.

При вызове указанного интерфейса предусмотрены следующие ошибки безопасности:

– ERROR: Введите имя.

Параметры, используемые интерфейсом создания пользователя:

– имя пользователя;

– пароль;

– электронная почта;

– имя проекта;

– имя роли;

– статус пользователя.

Способ использования интерфейса:

– ввод данных в графический пользовательский интерфейс.

Адреса обработки запроса:

“POST /api/fstek1/users” – URL, находящийся на модуле Adminui-backend, вызывающем API Openstack, используется для реализации ФБ (функции безопасности)

“POST //v3/users” – API Openstack модуля KeyStone (Пользователи)

8.1.2.2.4 Интерфейс редактирования пользователя

На Рисунке 1.7 приведён интерфейс ПО «KeyStack SE», назначением которого является реализация требований безопасности, связанных с редактированием пользователя. Интерфейс представлен в GUI и используется для редактирования пользователей в ПО «KeyStack SE».

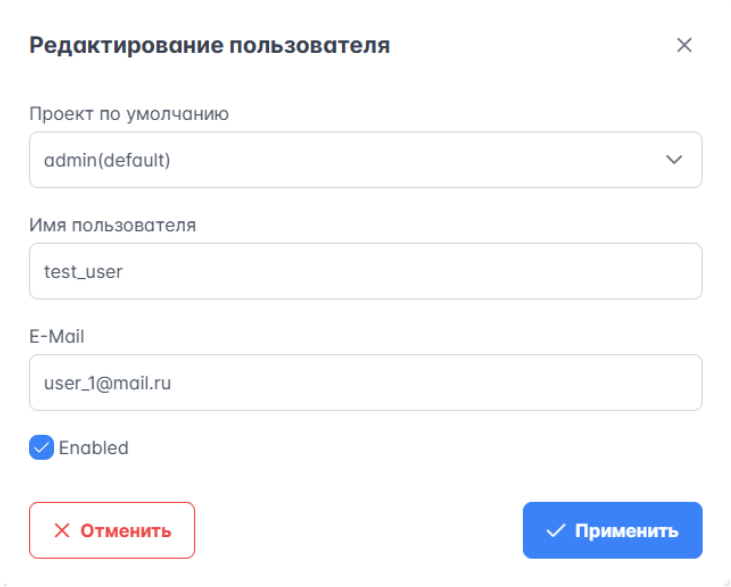

Рисунок 1.7

Интерфейс редактирования пользователя реализует следующие требования по безопасности информации:

– ПО «KeyStack SE» должно обеспечивать невозможность установления одинаковых идентификаторов и паролей для разных пользователей.

– ПО «KeyStack SE» должно обеспечивать:

- хранение аутентификационной информации пользователя ПО «KeyStack SE» в защищенном формате или в защищенном хранилище;
- взаимную идентификацию и аутентификацию пользователей и ПО «KeyStack SE» при удаленном доступе с использованием сетей связи общего пользования.

– При исчерпании установленного максимального количества неуспешных попыток ввода неправильного пароля учетная запись пользователя ПО «KeyStack SE» должна быть заблокирована с возможностью разблокировки администратором ПО «KeyStack SE» или с возможностью автоматической разблокировки по истечении временного интервала, устанавливаемого администратором ПО «KeyStack SE».

Интерфейс позволяет выполнять следующие действия:

– просматривать и редактировать аутентификационную информацию;

– блокировать и разблокировать пользователя.

В интерфейсе предусмотрены действия, не влияющие на выполнение требований безопасности к ПО «KeyStack SE»:

– просматривать список доступных проектов.

При вызове указанного интерфейса не предусмотрены ошибки безопасности.

Параметры, используемые интерфейсом редактирования пользователя:

– имя пользователя;

– электронная почта;

– принадлежность к проекту;

– статус.

Способ использования интерфейса:

– ввод данных в графический пользовательский интерфейс.

Адреса обработки запроса:

“PUT /api/fstek2/users/” – URL, находящийся на модуле Adminui-backend, вызывающем API Openstack, используется для реализации ФБ (функции безопасности)

“PATCH /v3/users/{user_id}” – API Openstack модуля KeyStone (Пользователи)

8.1.3 Централизованное управление образами виртуальных машин и виртуальными машинами

8.1.3.1 Интерфейсы управления образами виртуальных машин

8.1.3.1.1 Интерфейс загрузки образа

На Рисунке 1.8 приведён интерфейс ПО «KeyStack SE», назначением которого является реализация требований безопасности, связанных централизованным управлением образами виртуальных машин. Интерфейс представлен в GUI и используется для загрузки образа в ПО «KeyStack SE».

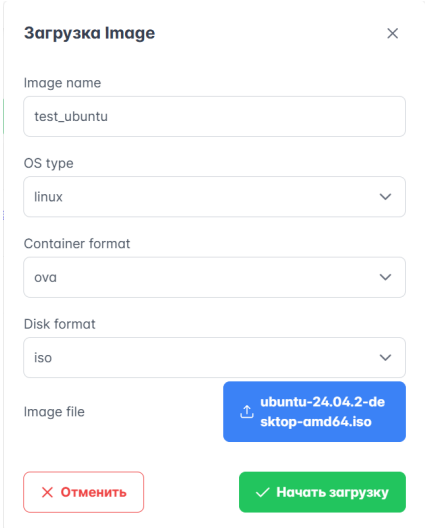

Рисунок 1.8

Интерфейс загрузки образа реализует следующие требования по безопасности информации:

– ПО «KeyStack SE» должно:

- создавать, модифицировать, хранить, получать и удалять образы виртуальных машин в информационной (автоматизированной) системе;
- обеспечивать управление размещением и перемещением виртуальных машин и их образов с возможностью сохранения их конфигурации и настроек.

Интерфейс позволяет выполнять следующие действия:

– загружать образ;

– настраивать параметры образа.

В интерфейсе не предусмотрены действия, не влияющие на выполнение требований безопасности к ПО «KeyStack SE»:

При вызове указанного интерфейса предусмотрены следующие ошибки безопасности:

– ERROR: Обязательное поле;

– ERROR: The provided image file has an incorrect extension.

Параметры, используемые интерфейсом загрузки образа:

– имя образа;

– тип ОС;

– формат контейнера;

– формат диска;

– файл с образом.

Способ использования интерфейса:

– ввод данных в графический пользовательский интерфейс.

Адреса обработки запроса:

“POST /api/fstek1/images” – URL, находящийся на модуле Adminui-backend, вызывающем API Openstack, используется для реализации ФБ (функции безопасности)

“POST /v2/images” – API Openstack модуля Glance (Образы)

8.1.3.1.2 Интерфейс обновления образа

На Рисунке 1.9 приведён интерфейс ПО «KeyStack SE», назначением которого является реализация требований безопасности, связанных централизованным управлением

образами виртуальных машин. Интерфейс представлен в GUI и используется для обновления образа в ПО «KeyStack SE».

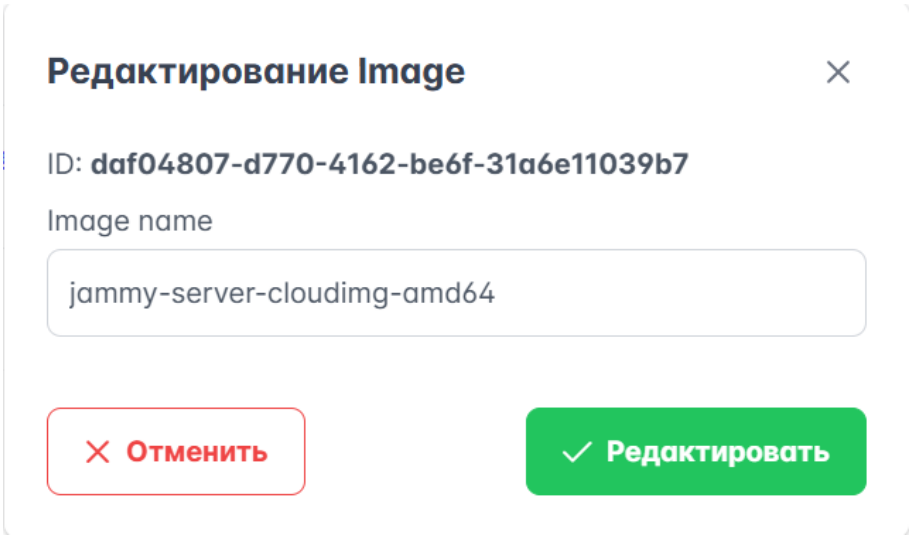

Рисунок 1.9

Интерфейс обновления образа реализует следующие требования по безопасности информации:

– ПО «KeyStack SE» должно:

  - создавать, модифицировать, хранить, получать и удалять образы виртуальных машин в информационной (автоматизированной) системе;
  - обеспечивать управление размещением и перемещением виртуальных машин и их образов с возможностью сохранения их конфигурации и настроек.

Интерфейс позволяет выполнять следующие действия:

– редактировать наименование образа.

В интерфейсе предусмотрены действия, не влияющие на выполнение требований безопасности к ПО «KeyStack SE»:

– просматривать информацию об образе.

При вызове указанного интерфейса предусмотрены следующие ошибки безопасности:

– ERROR: Обязательное поле.

Параметры, используемые интерфейсом обновления образа:

– идентификатор образа;

– имя образа.

Способ использования интерфейса:

– ввод данных в графический пользовательский интерфейс.

Адреса обработки запроса:

“PUT /api/fstek1/images” – URL, находящийся на модуле Adminui-backend, вызывающем API Openstack, используется для реализации ФБ (функции безопасности)

“PATCH /v2/images/{image_id}” – API Openstack модуля Glance (Образы)

8.1.3.1.3 Интерфейс удаления образа

На Рисунке 1.10 приведён интерфейс ПО «KeyStack SE», назначением которого является реализация требований безопасности, связанных централизованным управлением образами виртуальных машин. Интерфейс представлен в GUI и используется для удаления образа в ПО «KeyStack SE».

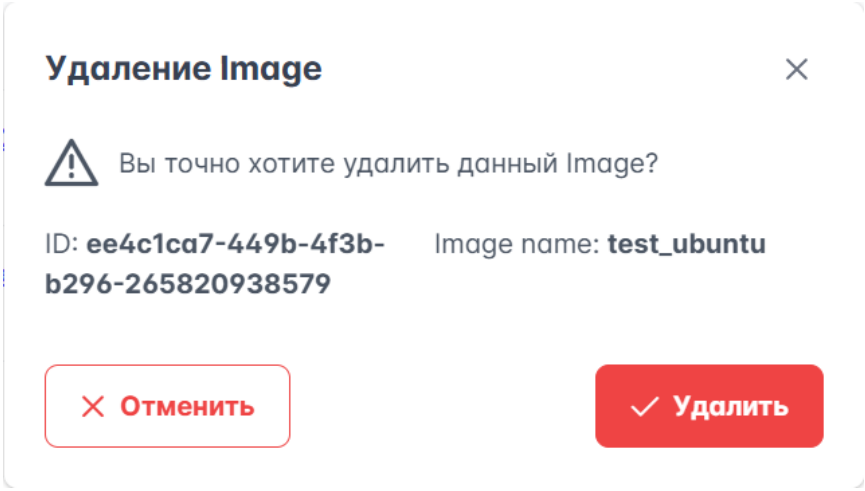

Рисунок 1.10

Интерфейс удаления образа реализует следующие требования по безопасности информации:

– ПО «KeyStack SE» должно:

- создавать, модифицировать, хранить, получать и удалять образы виртуальных машин в информационной (автоматизированной) системе;
- обеспечивать управление размещением и перемещением виртуальных машин и их образов с возможностью сохранения их конфигурации и настроек.

Интерфейс позволяет выполнять следующие действия:

– удалять образ.

В интерфейсе предусмотрены действия, не влияющие на выполнение требований безопасности к ПО «KeyStack SE»:

– просматривать информацию об образе.

При вызове указанного интерфейса не предусмотрены ошибки безопасности.

Параметры, используемые интерфейсом удаления образа:

– идентификатор образа;

– имя образа.

Способ использования интерфейса:

– использование ui элементов (кнопок) в графическом пользовательском интерфейсе.

Адреса обработки запроса:

“DELETE /api/fstek1/images” – URL, находящийся на модуле Adminui-backend, вызывающем API Openstack, используется для реализации ФБ (функции безопасности)

“DELETE /images/{id}” – API Openstack модуля Nova (Образы)

8.1.3.1.4 Интерфейс просмотра списка образов

На Рисунке 1.11 приведён интерфейс ПО «KeyStack SE», назначением которого является реализация требований безопасности, связанных централизованным управлением образами виртуальных машин. Интерфейс представлен в GUI и используется для просмотра списка образов в ПО «KeyStack SE».

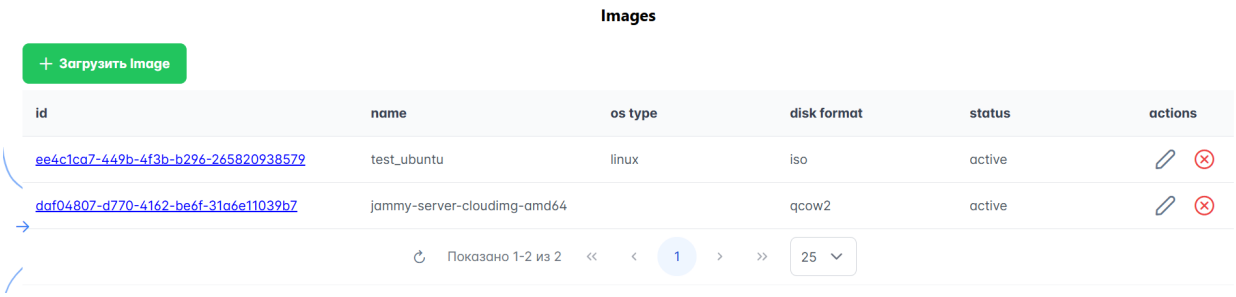

Рисунок 1.11

Интерфейс просмотра списка образов реализует следующие требования по безопасности информации:

– ПО «KeyStack SE» должно:

- создавать, модифицировать, хранить, получать и удалять образы виртуальных машин в информационной (автоматизированной) системе;
- обеспечивать управление размещением и перемещением виртуальных машин и их образов с возможностью сохранения их конфигурации и настроек.

Интерфейс позволяет выполнять следующие действия:

– просматривать информацию об образах;

– переходить к интерфейсам загрузки, удаления и обновления образа.

В интерфейсе не предусмотрены действия, не влияющие на выполнение требований безопасности к ПО «KeyStack SE»

При вызове указанного интерфейса не предусмотрены ошибки безопасности.

Параметры, используемые интерфейсом просмотра списка образов:

– идентификатор образа;

– наименование образа;

– тип ОС образа;

– формат диска;

– статус образа.

Способ использования интерфейса:

– использование ui элементов (кнопок и списков) в графическом пользовательском интерфейсе.

Адрес обработки запроса:

“GET /api/fstek1/images”

8.1.3.2 Интерфейсы управления виртуальными машинами

8.1.3.2.1 Интерфейс просмотра списка виртуальных машин

На Рисунке 1.12 приведён интерфейс ПО «KeyStack SE», назначением которого является реализация требований безопасности, связанных централизованным управлением виртуальными машинами. Интерфейс представлен в GUI и используется для просмотра списка виртуальных машин в ПО «KeyStack SE».

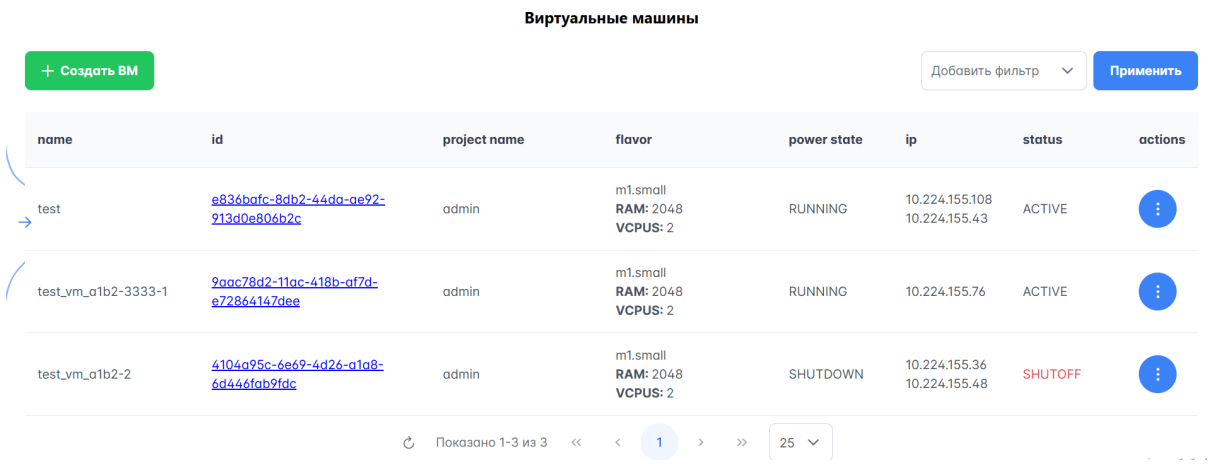

Рисунок 1.12

Интерфейс просмотра списка виртуальных машин реализует следующие требования по безопасности информации:

– ПО «KeyStack SE» должно:

- создавать, модифицировать, хранить, получать и удалять образы виртуальных машин в информационной (автоматизированной) системе;
- обеспечивать управление размещением и перемещением виртуальных машин и их образов с возможностью сохранения их конфигурации и настроек.

Интерфейс позволяет выполнять следующие действия:

– просматривать параметры виртуальных машин;

– переходить к интерфейсам создания, удаления, изменения и просмотра параметров виртуальной машины.

В интерфейсе предусмотрены действия, не влияющие на выполнение требований безопасности к ПО «KeyStack SE»:

– фильтрация списка.

При вызове указанного интерфейса не предусмотрены ошибки безопасности.

Параметры, используемые интерфейсом просмотра списка виртуальных машин:

– наименование виртуальной машины;

– идентификатор виртуальной машины;

– наименование проекта;

– тип инстанса (шаблон);

– состояние питания;

– ip адресса;

– статус;

– фильтр.

Способ использования интерфейса:

– использование ui элементов (кнопок и списков) в графическом пользовательском интерфейсе.

Адрес обработки запроса:

“GET /api/fstek1/servers”

8.1.3.2.2 Интерфейс просмотра параметров виртуальной машины

На Рисунках 1.13-1.20 приведён интерфейс ПО «KeyStack SE», назначением которого является реализация требований безопасности, связанных централизованным управлением виртуальными машинами. Интерфейс представлен в GUI и используется для просмотра параметров виртуальной машины в ПО «KeyStack SE».

Instance: new_instance

Status | Stats | Logs | Volumes | Ports

Name	Value
accessIPv4	""
accessIPv6	""
addresses	pub_net: addr: 10.224.155.46 OS-EXT-IPS-MAC:mac_addr: fa:16:3e:41:80:79 OS-EXT-IPS:type: fixed version: 4
config_drive	""
created	2025-05-23T10:49:15Z
description	null
flavor	disk: 5 ephemeral: 0 extra_specs: original_name: Test ram: 1024 swap: 0 vcpus: 2
host_status	UP
hostId	e0e67f7fd711198d83b7fee2c91ea64d0f36e476386989f80421809d

Рисунок 1.13

id	47aec22b-8454-4068-8fa0-cde721d40bff
image	""
key_name	null
links	href: https://internal.fstek2.test:8774/v2.1/servers/47aec22b-8454-4068-8fa0-cde721d40bff rel: self href: https://internal.fstek2.test:8774/servers/47aec22b-8454-4068-8fa0-cde721d40bff rel: bookmark
locked_reason	null
locked	false
metadata	{ }
name	new_instance
OS-DCF:diskConfig	AUTO
OS-EXT-AZ:availability_zone	nova
OS-EXT-SRV-ATTR:host	comp01-fstek2
OS-EXT-SRV-ATTR:hostname	new-instance
OS-EXT-SRV-ATTR:hypervisor_hostname	comp01-fstek2
OS-EXT-SRV-ATTR:instance_name	instance-00000017
OS-EXT-SRV-ATTR:kernel_id	""
OS-EXT-SRV-ATTR:launch_index	0

Рисунок 1.14

OS-EXT-SRV-ATTR:ramdisk_id	""
OS-EXT-SRV-ATTR:reservation_id	r-avxsah0n
OS-EXT-SRV-ATTR:root_device_name	/dev/vda
OS-EXT-SRV-ATTR:user_data	null
OS-EXT-STS:power_state	1
OS-EXT-STS:task_state	null
OS-EXT-STS:vm_state	active
os-extended-volumes:volumes_attached	delete_on_termination: false id: 323fffb9-e534-4f20-b482-e39ee2bb626c name: size: 5 delete_on_termination: false id: 97bfdf99-a4e3-43c5-b1e6-4850ed172e91 name: New_disk size: 1
OS-SRV-USG:launched_at	2025-05-23T10:50:15.000000
OS-SRV-USG:terminated_at	null
pinned_availability_zone	nova
progress	0
project_name	admin
security_groups	name: default

Рисунок 1.15

server_groups	[ ]
status	ACTIVE
tags	[ ]
tenant_id	6f3dff10c2114e7abcdd03e934a57cbd
trusted_image_certificates	null
updated	2025-05-23T11:16:15Z
user_id	4fd9c75feb3b45748da7ed36616110b8

Security Group Name	from_port	to_port	ip_protocol	ip_range
default	null	null	null	null
	null	null	null	null

Рисунок 1.16

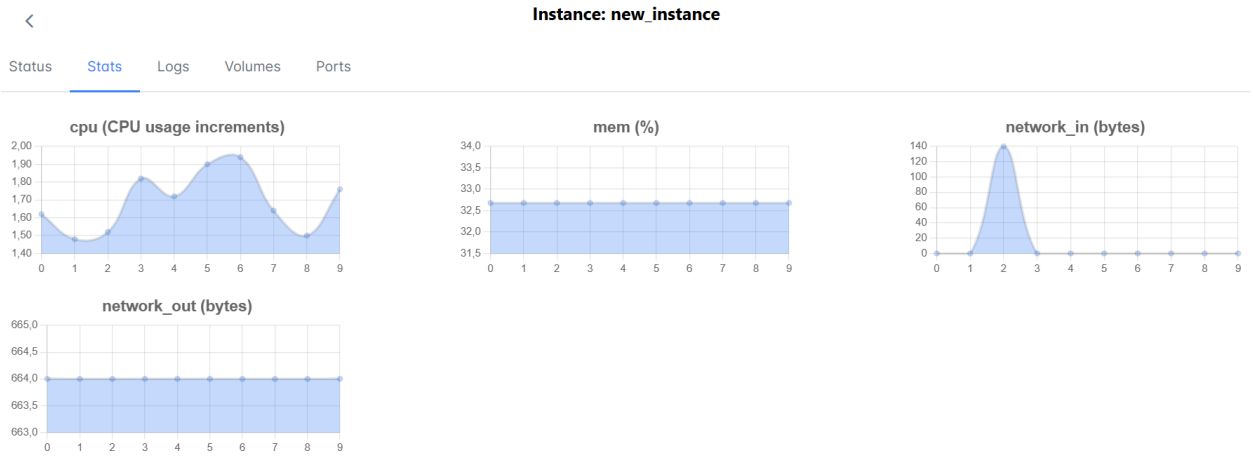

Рисунок 1.17

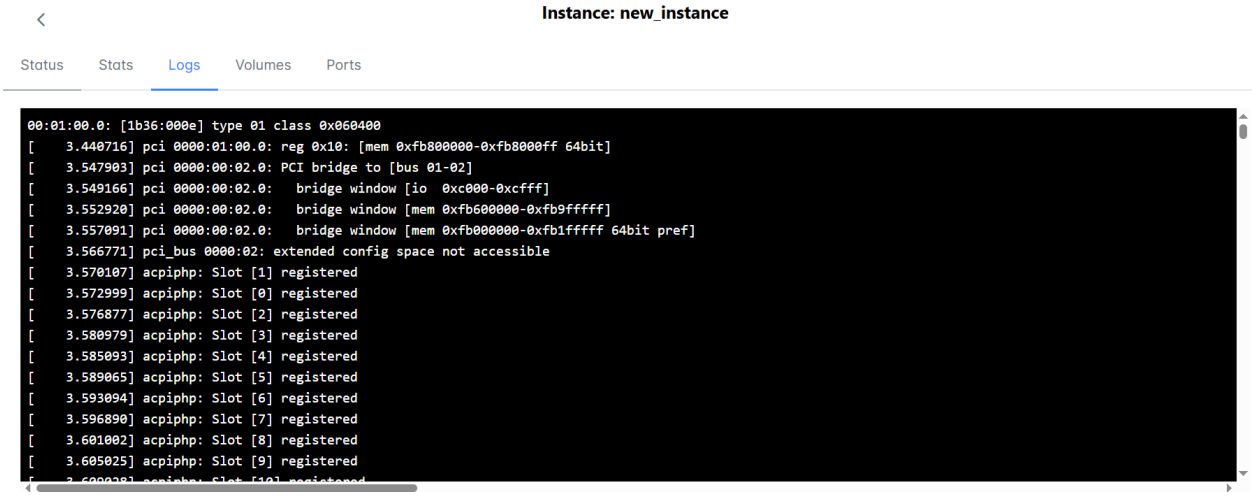

Рисунок 1.18

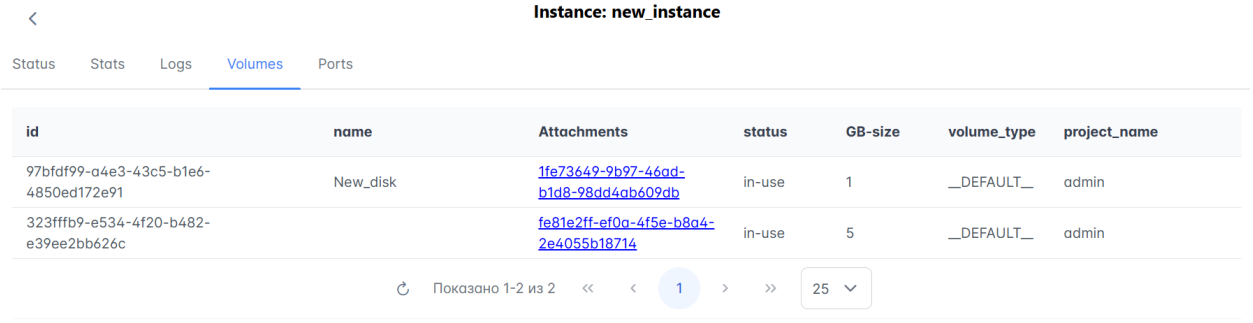

Рисунок 1.19

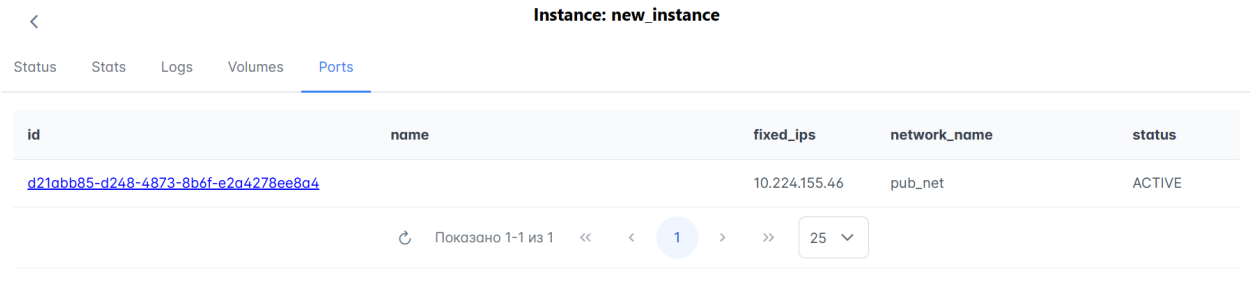

Рисунок 1.20

Интерфейс просмотра параметров виртуальной машины реализует следующие требования по безопасности информации:

– ПО «KeyStack SE» должно:

  - создавать, модифицировать, хранить, получать и удалять образы виртуальных машин в информационной (автоматизированной) системе;
  - обеспечивать управление размещением и перемещением виртуальных машин и их образов с возможностью сохранения их конфигурации и настроек.

Интерфейс позволяет выполнять следующие действия:

- просматривать информацию о параметрах виртуальной машины;
- переходить к просмотру параметров тома и порта;

В интерфейсе не предусмотрены действия, не влияющие на выполнение требований безопасности к ПО «KeyStack SE».

При вызове указанного интерфейса не предусмотрены ошибки безопасности.

Параметры, используемые интерфейсом просмотра списка виртуальных машин:

- список разрешенных ipv4 адрессов;
- список разрешенных ipv6 адрессов;
- адресса;
- конфигурационные диски;
- дата и время создания;
- описание;
- тип инстанса (шаблон);
- статус хоста;
- идентификатор хоста;
- образ;
- наименование ключа;
- ссылка на виртуальную машину;
- причина блокировки;
- статус блокировки;
- метаданные;
- наименование;
- настройка диска;
- зона доступности;
- хост;

– имя хоста;
– наименование гипервизора;
– имя инстанса;
– идентификатор ядра;
– индекс запуска;
– идентификатор диска оперативной памяти;
– идентификатор резервирования;
– имя корневого устройства;
– данные пользователя;
– состояние питания;
– состояние задачи;
– состояние виртуальной машины;
– присоединенные тома;
– дата и время запуска;
– дата и время завершения работы;
– закрепленная зона доступности;
– прогресс;
– наименование проекта;
– группы безопасности;
– группы серверов;
– статус;
– тэги;
– идентификатор организации;
– доверенные сертификаты образа;
– дата и время изменений;
– идентификатор пользователя;
– параметры групп безопасности;
– графики использования ресурсов (ЦПУ, память, входящий и исходящий сетевой трафик);
– параметры присоединенных томов;
– параметры используемых портов.

Способ использования интерфейса:

– просмотр таблиц, графиков и консоли через графический пользовательский интерфейс.

Адрес обработки запроса:

“GET /api/fstek2/servers/{идентификатор виртуальной машины}”

8.1.3.2.3 Интерфейс создания виртуальной машины

На Рисунках 1.21-1.22 приведён интерфейс ПО «KeyStack SE», назначением которого является реализация требований безопасности, связанных централизованным управлением виртуальными машинами. Интерфейс представлен в GUI и используется для создания виртуальной машины в ПО «KeyStack SE».

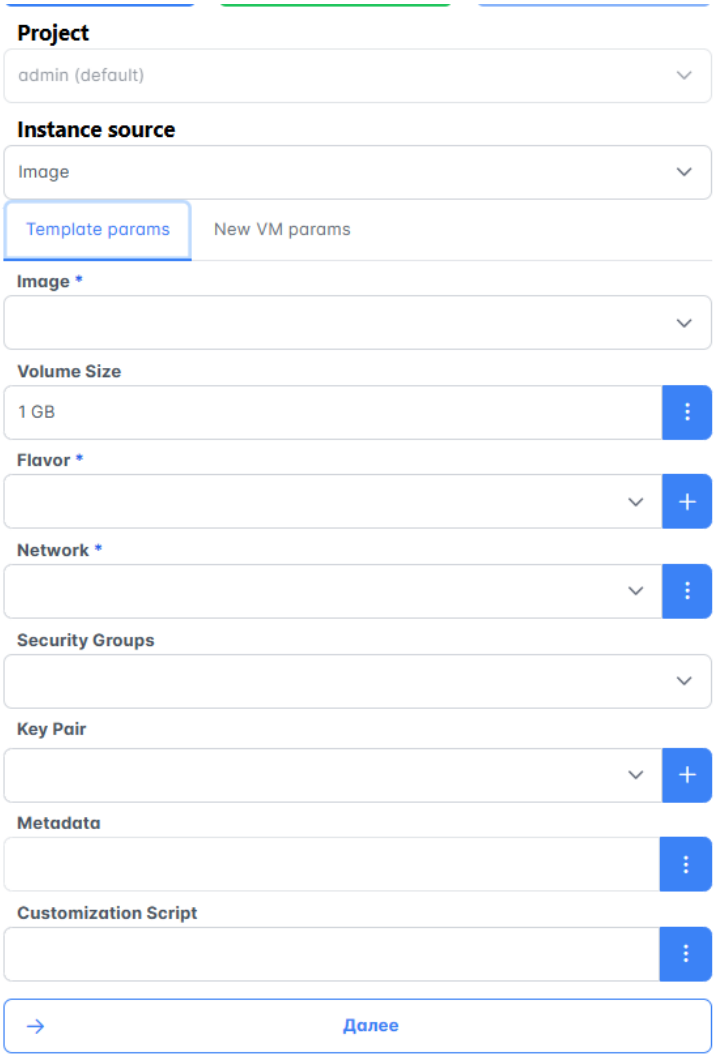

Рисунок 1.21

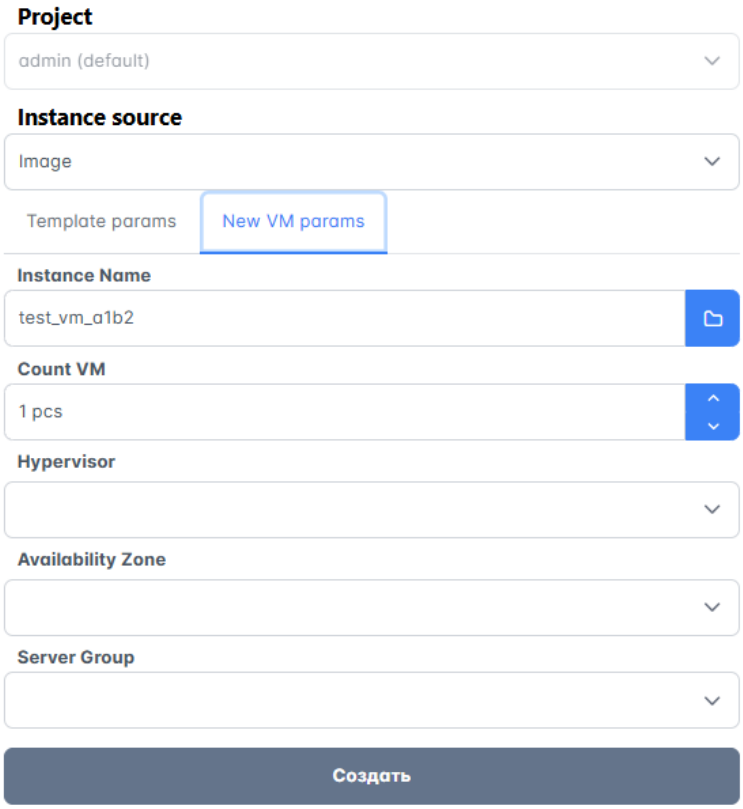

Рисунок 1.22

Интерфейс создания виртуальной машины реализует следующие требования по безопасности информации:

– ПО «KeyStack SE» должно:

- создавать, модифицировать, хранить, получать и удалять образы виртуальных машин в информационной (автоматизированной) системе;
- обеспечивать управление размещением и перемещением виртуальных машин и их образов с возможностью сохранения их конфигурации и настроек.

Интерфейс позволяет выполнять следующие действия:

– создавать виртуальную машину.

В интерфейсе предусмотрены действия, не влияющие на выполнение требований безопасности к ПО «KeyStack SE»:

– просматривать информацию о списке доступных проектов и параметров виртуальной машины;

При вызове указанного интерфейса предусмотрены следующие ошибки безопасности:

– ERROR: Не заполнены необходимые поля.

Параметры, используемые интерфейсом создания виртуальной машины:

- наименование проекта;
- источник экземпляра;
- наименование образа;
- объем тома;
- аппаратная конфигурация для сервера;
- сеть;
- группы безопасности;
- пары ключей;
- метаданные;
- скрипт настройки;
- имя экземпляра;
- количество виртуальных машин;
- гипервизор;
- зона доступности;
- группа серверов.

Способ использования интерфейса:

- ввод данных в графический пользовательский интерфейс.

Адреса обработки запроса:

“POST /api/fstek1/servers” – URL, находящийся на модуле Adminui-backend, вызывающем API Openstack, используется для реализации ФБ (функции безопасности)

“POST /servers” – API Openstack модуля Nova (Серверы)

8.1.3.2.4 Интерфейс изменения виртуальной машины

На Рисунке 1.23 приведён интерфейс ПО «KeyStack SE», назначением которого является реализация требований безопасности, связанных централизованным управлением виртуальными машинами. Интерфейс представлен в GUI и используется для изменения виртуальной машины в ПО «KeyStack SE».

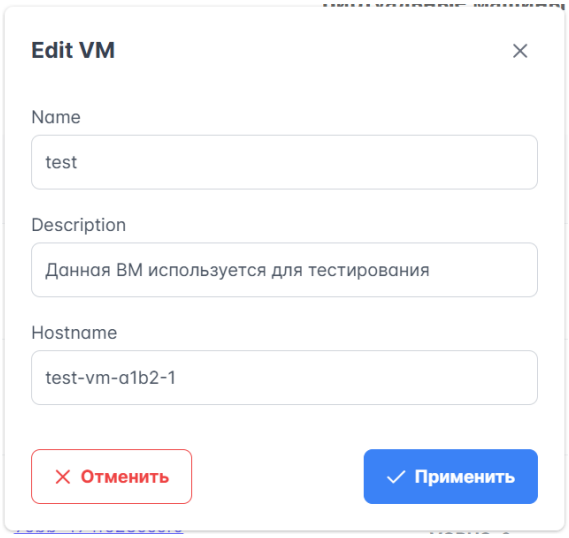

Рисунок 1.23

Интерфейс изменения виртуальной машины реализует следующие требования по безопасности информации:

– ПО «KeyStack SE» должно:

- создавать, модифицировать, хранить, получать и удалять образы виртуальных машин в информационной (автоматизированной) системе;
- обеспечивать управление размещением и перемещением виртуальных машин и их образов с возможностью сохранения их конфигурации и настроек.

Интерфейс позволяет выполнять следующие действия:

– изменять параметры виртуальной машины.

В интерфейсе предусмотрены действия, не влияющие на выполнение требований безопасности к ПО «KeyStack SE»:

– изменять описание виртуальной машины.

При вызове указанного интерфейса предусмотрены следующие ошибки безопасности:

– ERROR: Введите имя.

Параметры, используемые интерфейсом изменения виртуальной машины:

– имя виртуальной машины;

– описание;

– имя хоста.

Способ использования интерфейса:

– ввод данных в графический пользовательский интерфейс.

Адреса обработки запроса:

“PUT /api/fstek1/servers” – URL, находящийся на модуле Adminui-backend, вызывающем API Openstack, используется для реализации ФБ (функции безопасности)

“ PUT /servers/{id}” – API Openstack модуля Nova (Серверы)

8.1.3.2.5 Интерфейс удаления виртуальной машины

На Рисунке 1.24 приведён интерфейс ПО «KeyStack SE», назначением которого является реализация требований безопасности, связанных централизованным управлением виртуальными машинами. Интерфейс представлен в GUI и используется для удаления виртуальной машины в ПО «KeyStack SE».

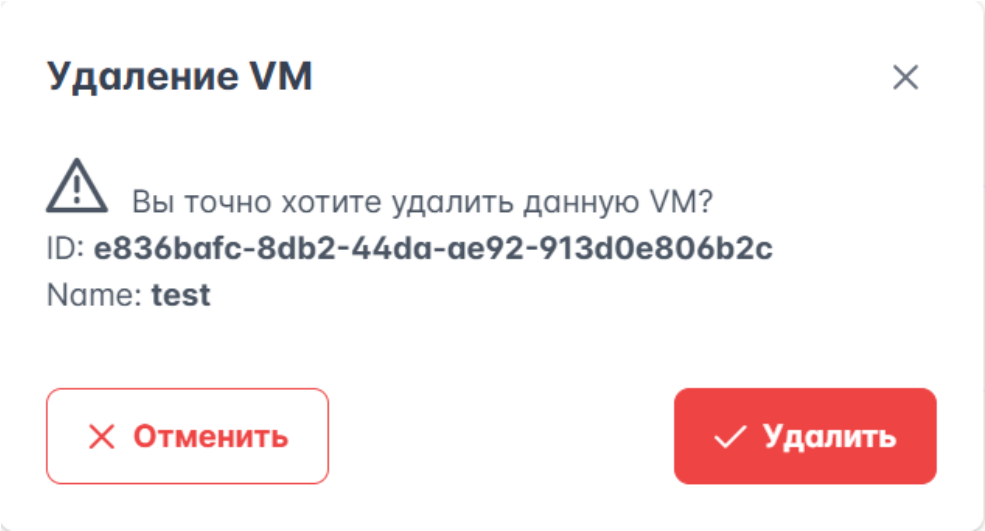

Рисунок 1.24

Интерфейс удаления виртуальной машины реализует следующие требования по безопасности информации:

– ПО «KeyStack SE» должно:

- создавать, модифицировать, хранить, получать и удалять образы виртуальных машин в информационной (автоматизированной) системе;
- обеспечивать управление размещением и перемещением виртуальных машин и их образов с возможностью сохранения их конфигурации и настроек.

Интерфейс позволяет выполнять следующие действия:

– удалять виртуальную машину.

В интерфейсе предусмотрены действия, не влияющие на выполнение требований безопасности к ПО «KeyStack SE»:

– просматривать ифнормацию о параметрах виртуальной машины.

При вызове указанного интерфейса не предусмотрены ошибки безопасности.

Параметры, используемые интерфейсом удаления виртуальной машины:

– id виртуальной машины;

– имя виртуальной машины.

Способ использования интерфейса:

– использование ui элементов (кнопок) в графическом пользовательском интерфейсе.

Адреса обработки запроса:

“DELETE /api/fstek1/servers” – URL, находящийся на модуле Adminui-backend, вызывающем API Openstack, используется для реализации ФБ (функции безопасности)

“DELETE /servers/{id}” – API Openstack модуля Nova (Серверы)

8.1.3.2.6 Интерфейс оперативной миграции виртуальной машины

На Рисунке 1.25 приведён интерфейс ПО «KeyStack SE», назначением которого является реализация требований безопасности, связанных централизованным управлением виртуальными машинами. Интерфейс представлен в GUI и используется для оперативной миграции виртуальной машины в ПО «KeyStack SE».

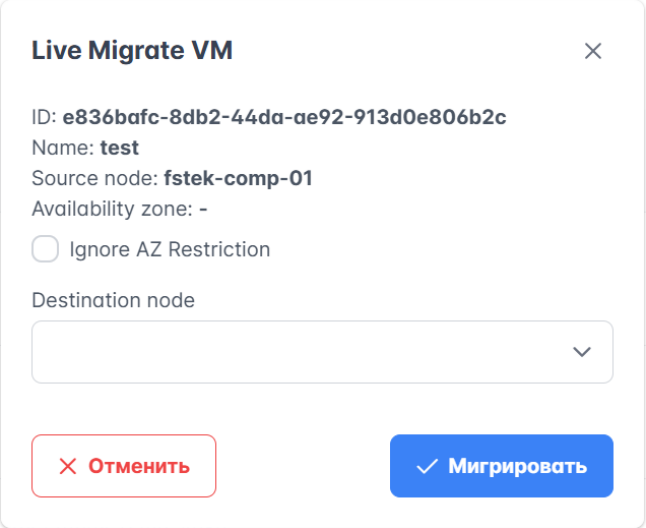

Рисунок 1.25

Интерфейс оперативной миграции виртуальной машины реализует следующие требования по безопасности информации:

– ПО «KeyStack SE» должно:

- создавать, модифицировать, хранить, получать и удалять образы виртуальных машин в информационной (автоматизированной) системе;

- обеспечивать управление размещением и перемещением виртуальных машин и их образов с возможностью сохранения их конфигурации и настроек.

Интерфейс позволяет выполнять следующие действия:

- проводить миграцию (перемещение) виртуальной машины.

В интерфейсе предусмотрены действия, не влияющие на выполнение требований безопасности к ПО «KeyStack SE»:

- просматривать параметры виртуальной машины;
- просматривать параметры миграции.

При вызове указанного интерфейса предусмотрены следующие ошибки безопасности:

- ERROR: Source и Destination гипервизоры совпадают.

Параметры, используемые интерфейсом оперативной миграции виртуальной машины:

- идентификатор виртуальной машины;
- наименование виртуальной машины;
- узел-источник;
- зона доступности;
- узел назначения (конечная нода);
- игнорирование ограничения az.

Способ использования интерфейса:

- использование ui элементов (кнопок и списков) в графическом пользовательском интерфейсе.

Адрес обработки запроса:

“POST /servers/{id}/action”

8.1.4 Управление потоками информации

8.1.4.1 Интерфейс просмотра списка групп безопасности

На Рисунке 1.26 приведён интерфейс ПО «KeyStack SE», назначением которого является реализация требований безопасности, связанных с управлением потоками информации. Интерфейс представлен в GUI и используется для просмотра списка групп безопасности в ПО «KeyStack SE».

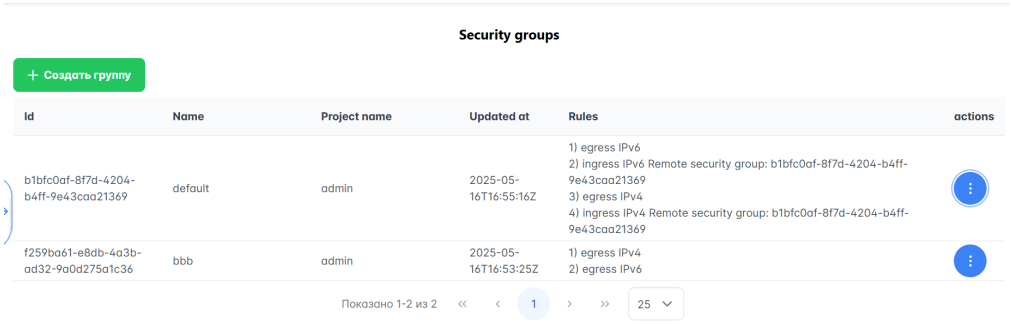

Рисунок 1.26

Интерфейс просмотра списка групп безопасности реализует следующие требования по безопасности информации:

– ПО «KeyStack SE» должно обеспечивать управление потоками информации между виртуальными машинами и информационными (автоматизированными) системами на канальном и сетевом уровнях самостоятельно или с применением сертифицированных средств управления потоками информации (коммутаторов, маршрутизаторов) и (или) межсетевых экранов, а также контроль взаимодействия виртуальных машин между собой.

Интерфейс позволяет выполнять следующие действия:

– просматривать список групп безопасности;

– переходить к интерфейсам создания и удаления групп безопасности.

В интерфейсе предусмотрены действия, не влияющие на выполнение требований безопасности к ПО «KeyStack SE»:

– просматривать параметры группы безопасности.

При вызове указанного интерфейса не предусмотрены ошибки безопасности.

Параметры, используемые интерфейсом просмотра списка групп безопасности:

– идентификатор группы безопасности;

– наименование группы безопасности;

– наименование проекта;

– дата и время обновления группы безопасности;

– правила группы безопасности.

Способ использования интерфейса:

– использование ui элементов (списков) в графическом пользовательском интерфейсе.

Адрес обработки запроса:

“GET /api/fstek2/security_groups”

8.1.4.2 Интерфейс создания группы безопасности

На Рисунке 1.27 приведён интерфейс ПО «KeyStack SE», назначением которого является реализация требований безопасности, связанных с управлением потоками информации. Интерфейс представлен в GUI и используется для создания групп безопасности в ПО «KeyStack SE».

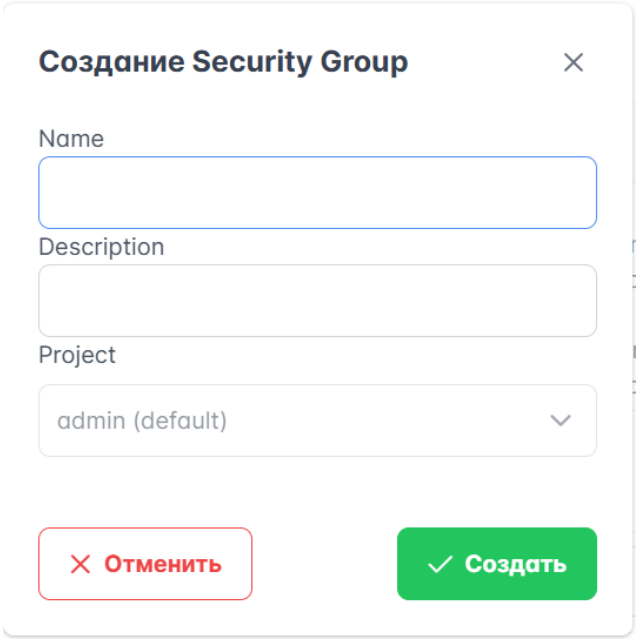

Рисунок 1.27

Интерфейс создания группы безопасности реализует следующие требования по безопасности информации:

– ПО «KeyStack SE» должно обеспечивать управление потоками информации между виртуальными машинами и информационными (автоматизированными) системами на канальном и сетевом уровнях самостоятельно или с применением сертифицированных средств управления потоками информации (коммутаторов, маршрутизаторов) и (или) межсетевых экранов, а также контроль взаимодействия виртуальных машин между собой.

Интерфейс позволяет выполнять следующие действия:

– создавать группы безопасности.

В интерфейсе предусмотрены действия, не влияющие на выполнение требований безопасности к ПО «KeyStack SE»:

– добавлять описание к группам безопасности;

– просматривать список доступных проектов.

При вызове указанного интерфейса не предусмотрены ошибки безопасности.

Параметры, используемые интерфейсом создания группы безопасности:

– наименование группы безопасности;

– описание;

– идентификатор проекта.

Способ использования интерфейса:

– использование ui элементов (кнопок и полей ввода) в графическом пользовательском интерфейсе.

Адреса обработки запроса:

“POST /api/fstek2/security_groups” – URL, находящийся на модуле Adminui-backend, вызывающем API Openstack, используется для реализации ФБ (функции безопасности)

“POST /os-security-groups” – API Openstack модуля Nova (Группы безопасности)

8.1.4.3 Интерфейс просмотра списка правил безопасности

На Рисунке 1.28 приведён интерфейс ПО «KeyStack SE», назначением которого является реализация требований безопасности, связанных с управлением потоками информации. Интерфейс представлен в GUI и используется для просмотра списка правил безопасности в ПО «KeyStack SE».

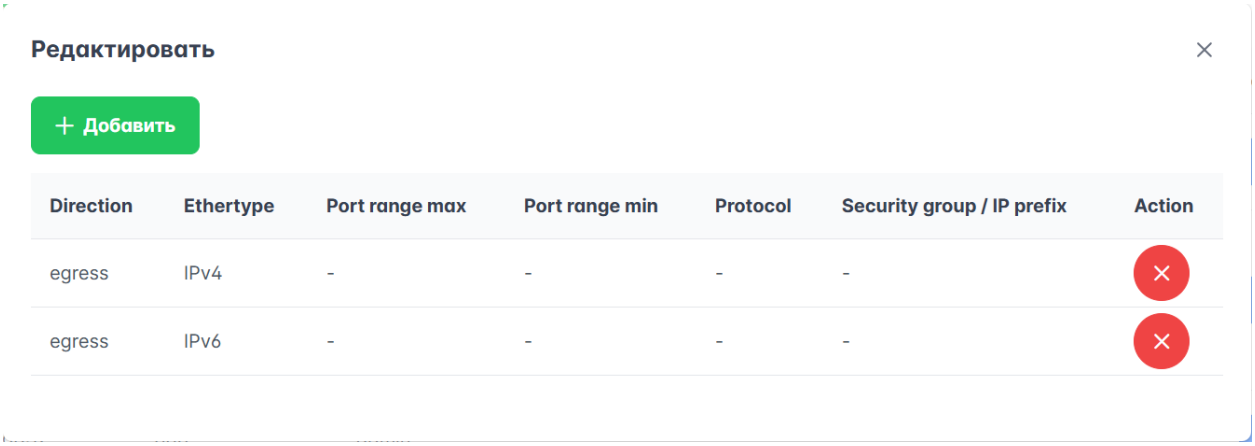

Рисунок 1.28

Интерфейс просмотра списка правил безопасности реализует следующие требования по безопасности информации:

– ПО «KeyStack SE» должно обеспечивать управление потоками информации между виртуальными машинами и информационными (автоматизированными) системами на канальном и сетевом уровнях самостоятельно или с применением сертифицированных средств управления потоками информации (коммутаторов, маршрутизаторов) и (или) межсетевых экранов, а также контроль взаимодействия виртуальных машин между собой.

Интерфейс позволяет выполнять следующие действия:

– просматривать список правил безопасности;

– переходить к интерфейсам добавления и удаления правил безопасности.

В интерфейсе не предусмотрены действия, не влияющие на выполнение требований безопасности к ПО «KeyStack SE».

При вызове указанного интерфейса не предусмотрены ошибки безопасности.

Параметры, используемые интерфейсом просмотра списка правил безопасности:

– направление трафика;

– тип интернет протокола;

– вид сетевого протокола;

– минимальное значение в диапазоне портов;

– максимальное значение в диапазоне портов;

– группа безопасности;

– ip-префикс.

Способ использования интерфейса:

– использование ui элементов (список) в графическом пользовательском интерфейсе.

Адрес обработки запроса:

“GET /api/fstek2/security_groups”

8.1.4.4 Интерфейс создания правил безопасности

На Рисунках 1.29-1.30 приведён интерфейс ПО «KeyStack SE», назначением которого является реализация требований безопасности, связанных с управлением потоками информации. Интерфейс представлен в GUI и используется для создания правил безопасности в ПО «KeyStack SE».

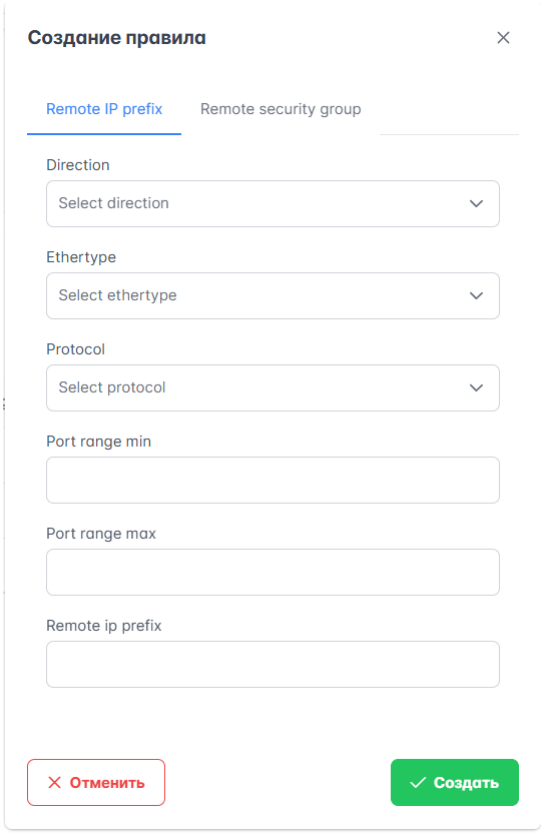

Рисунок 1.29

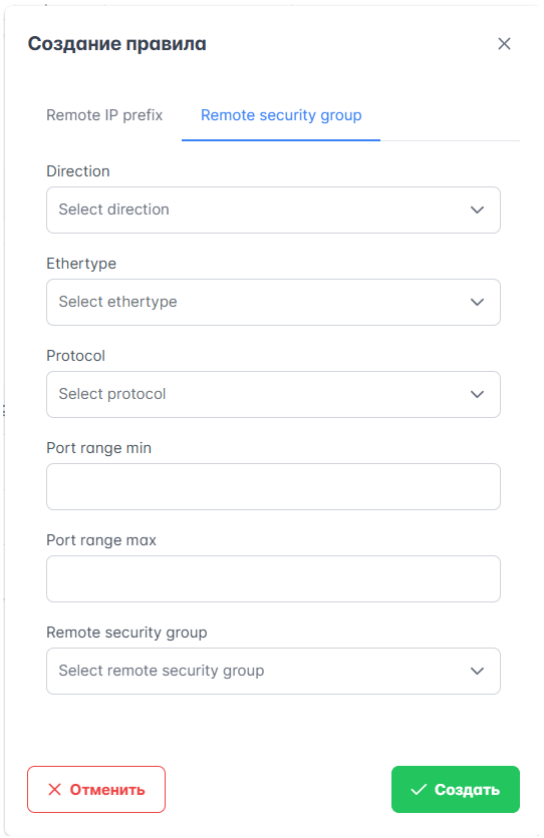

Рисунок 1.30

Интерфейс добавления правил безопасности реализует следующие требования по безопасности информации:

– ПО «KeyStack SE» должно обеспечивать управление потоками информации между виртуальными машинами и информационными (автоматизированными) системами на канальном и сетевом уровнях самостоятельно или с применением сертифицированных средств управления потоками информации (коммутаторов, маршрутизаторов) и (или) межсетевых экранов, а также контроль взаимодействия виртуальных машин между собой.

Интерфейс позволяет выполнять следующие действия:

– создать правило безопасности.

В интерфейсе не предусмотрены действия, не влияющие на выполнение требований безопасности к ПО «KeyStack SE».

При вызове указанного интерфейса предусмотрены следующие ошибки безопасности:

– ERROR: Must also specify protocol if port range is given.

Параметры, используемые интерфейсом создания правил безопасности:

– направление трафика;

– тип интернет протокола;

– вид сетевого протокола;

– минимальное значение в диапазоне портов;

– максимальное значение в диапазоне портов;

– группа удаленной безопасности;

– удаленный ip-префикс.

Способ использования интерфейса:

– использование ui элементов (полей ввода и списков) в графическом пользовательском интерфейсе.

Адреса обработки запроса:

“POST /api/fstek2/security/group/rules” – URL, находящийся на модуле Adminui-backend, вызывающем API Openstack, используется для реализации ФБ (функции безопасности)

“POST /os-security-group-rules” – API Openstack модуля Nova (Правила для группы безопасности)

8.1.4.5 Интерфейс удаления правил безопасности

На Рисунке 1.31 приведён интерфейс ПО «KeyStack SE», назначением которого является реализация требований безопасности, связанных с управлением потоками

информации. Интерфейс представлен в GUI и используется для удаления правил безопасности в ПО «KeyStack SE».

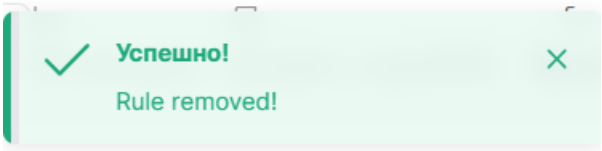

Рисунок 1.31

Интерфейс удаления правил безопасности реализует следующие требования по безопасности информации:

– ПО «KeyStack SE» должно обеспечивать управление потоками информации между виртуальными машинами и информационными (автоматизированными) системами на канальном и сетевом уровнях самостоятельно или с применением сертифицированных средств управления потоками информации (коммутаторов, маршрутизаторов) и (или) межсетевых экранов, а также контроль взаимодействия виртуальных машин между собой.

Интерфейс позволяет выполнять следующие действия:

– удалить правило безопасности.

В интерфейсе не предусмотрены действия, не влияющие на выполнение требований безопасности к ПО «KeyStack SE».

При вызове указанного интерфейса не предусмотрены ошибки безопасности.

Параметры интерфейсом удаления правил безопасности не используются.

Способ использования интерфейса:

– использование ui элементов (кнопок) в графическом пользовательском интерфейсе.

Адреса обработки запроса:

“DELETE /api/fstek2/security/group/rules/{идентификатор правила безопасности}” – URL, находящийся на модуле Adminui-backend, вызывающем API Openstack, используется для реализации ФБ (функции безопасности)

“DELETE /os-security-group-rules/{id}” – API Openstack модуля Nova (Правила для группы безопасности)

8.1.4.6 Интерфейс удаления группы безопасности

На Рисунке 1.32 приведён интерфейс ПО «KeyStack SE», назначением которого является реализация требований безопасности, связанных с управлением потоками

информации. Интерфейс представлен в GUI и используется для удаления группы безопасности в ПО «KeyStack SE».

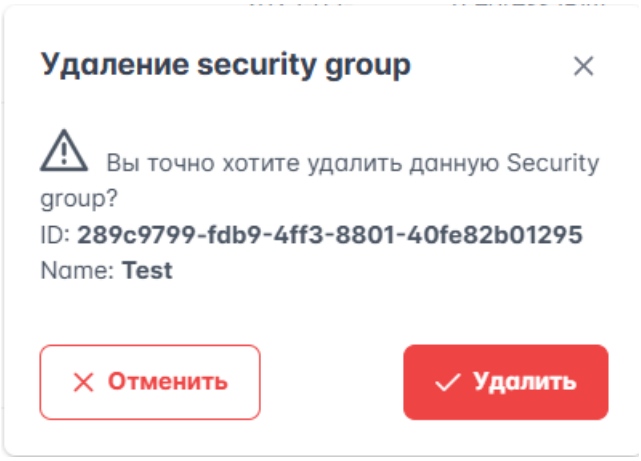

Рисунок 1.32

Интерфейс удаления группы безопасности реализует следующие требования по безопасности информации:

– ПО «KeyStack SE» должно обеспечивать управление потоками информации между виртуальными машинами и информационными (автоматизированными) системами на канальном и сетевом уровнях самостоятельно или с применением сертифицированных средств управления потоками информации (коммутаторов, маршрутизаторов) и (или) межсетевых экранов, а также контроль взаимодействия виртуальных машин между собой.

Интерфейс позволяет выполнять следующие действия:

– удалить группу безопасности.

В интерфейсе не предусмотрены действия, не влияющие на выполнение требований безопасности к ПО «KeyStack SE».

При вызове указанного интерфейса не предусмотрены ошибки безопасности.

Параметры, используемые интерфейсом удаления группы безопасности:

– идентификатор группы безопасности;

– наименование группы безопасности.

Способ использования интерфейса:

– использование ui элементов (кнопок) в графическом пользовательском интерфейсе.

Адреса обработки запроса:

“DELETE /api/fstek2/security_groups/{идентификатор группы безопасности}” – URL, находящийся на модуле Adminui-backend, вызывающем API Openstack, используется для реализации ФБ (функции безопасности)

“DELETE /v2.0/security-groups/{id}” – API Openstack модуля Neutron (Группы безопасности)

8.1.5 Интерфейсы Портала Администрирования, не влияющие на функции безопасности

8.1.5.1.1 Интерфейс просмотра списка миграций виртуальных машин

На Рисунке 1.33 приведён интерфейс ПО «KeyStack SE», который представлен в GUI и используется для просмотра списка миграций виртуальных машин в ПО «KeyStack SE».

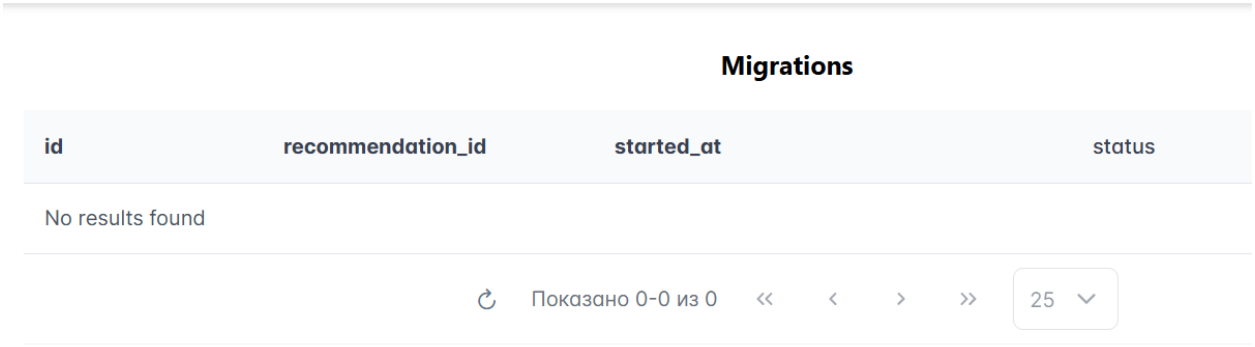

Рисунок 1.33

Интерфейс позволяет выполнять следующие действия:

– просматривать список миграций виртуальных машин.

Параметры, используемые интерфейсом просмотра списка миграций виртуальных машин:

– идентификатор миграции;

– предпочтительный идентфиикатор виртуальной машины после миграции;

– дата начала миграции;

– статус миграции.

Способ использования интерфейса:

– использование ui элементов (списков) в графическом пользовательском интерфейсе.

Адрес обработки запроса:

“GET /api/fstek2/drs/migrations”

8.1.5.2 Интерфейс управления питанием виртуальной машины

На Рисунке 1.34 приведён интерфейс управления питанием виртуальной машины. Интерфейс представлен в GUI и используется для управления питанием виртуальной машины в ПО «KeyStack SE».

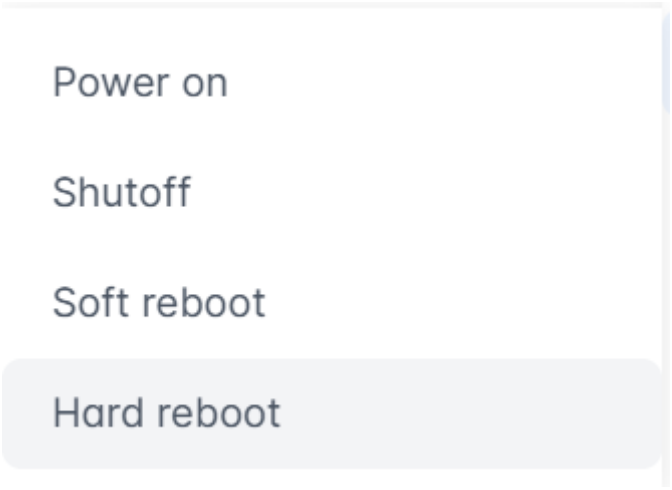

Рисунок 1.34

Интерфейс позволяет выполнять следующие действия:

– выключить виртуальную машину;

– запустить виртуальную машину;

– перезагрузить виртуальную машину.

Параметры интерфейсом управления питанием виртуальной машины не используются.

Способ использования интерфейса:

– использование ui элементов (кнопок) в графическом пользовательском интерфейсе.

Адрес обработки запроса:

“POST /api/fstek2/servers/{идентификатор виртуальной машины}”

8.1.5.3 Интерфейс управления томами виртуальной машины

На Рисунке 1.35 приведён интерфейс управления томами виртуальной машины. Интерфейс представлен в GUI и используется для управления томами виртуальной машины в ПО «KeyStack SE».

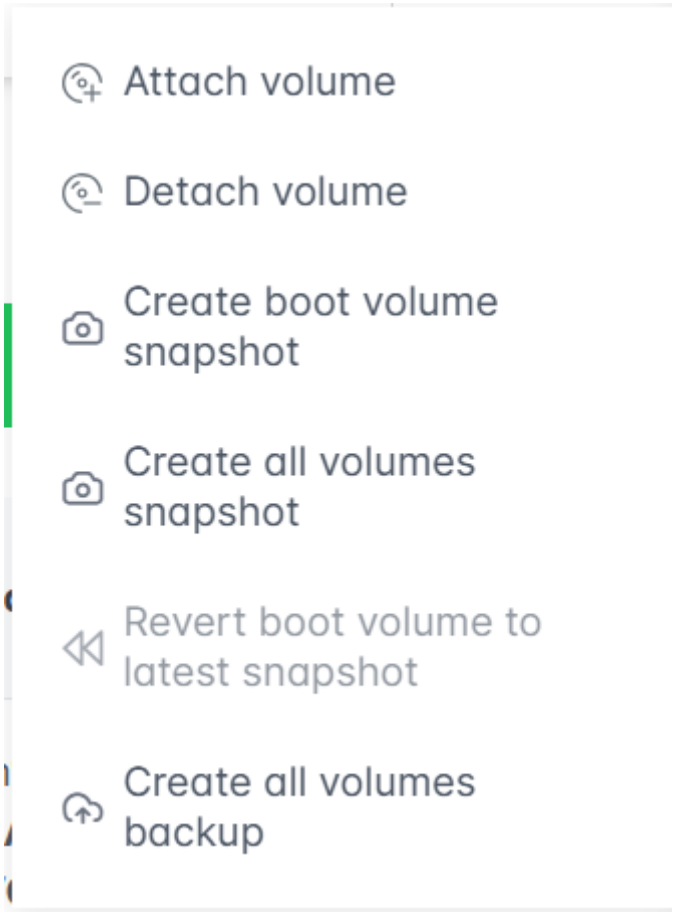

Рисунок 1.35

Интерфейс позволяет выполнять следующие действия:

– присоединить том;
– отсоединить том;
– сделать снапшот тома;
– сделать снапшот всех томов;
– восстановить том по последнему снапшоту;
– сделать бэкап всех томов.

Параметры интерфейсом управления томами виртуальной машины не используются.

Способ использования интерфейса:

– использование ui элементов (кнопок) в графическом пользовательском интерфейсе.

Адрес обработки запроса:

“POST /api/fstek2/servers/{идентификатор виртуальной машины}”

8.1.5.4 Интерфейс управления шаблонами конфигурации (флейворами) виртуальной машины

На Рисунке 1.36 приведён интерфейс управления шаблонами конфигурации виртуальной машины. Интерфейс представлен в GUI и используется для управления шаблонами конфигурации виртуальной машины в ПО «KeyStack SE».

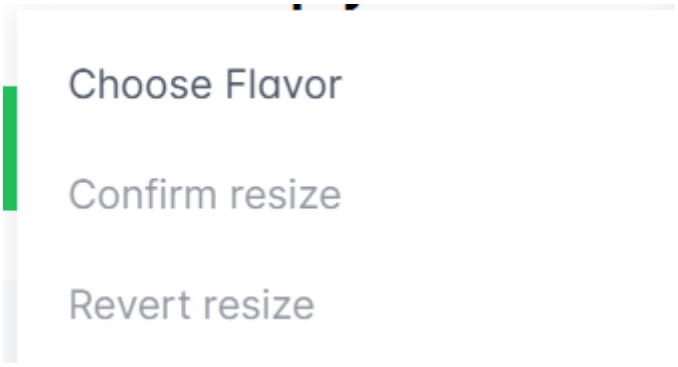

Рисунок 1.36

Интерфейс позволяет выполнять следующие действия:

– сменить шаблон конфигурации (флейвор);
– подтвердить смену шаблона конфигурации;
– вернуться к прежнему шаблону конфигурации.

Параметры интерфейсом управления шаблонами конфигрурации виртуальной машины не используются.

Способ использования интерфейса:

– использование ui элементов (кнопок) в графическом пользовательском интерфейсе.

Адрес обработки запроса:

“POST /api/fstek2/servers/{идентификатор виртуальной машины}”

8.1.5.5 Интерфейс просмотра консоли виртуальной машины

На Рисунке 1.37 приведён интерфейс просмотра консоли виртуальной машины. Интерфейс представлен в GUI и используется для просмотра консоли виртуальной машины в ПО «KeyStack SE».

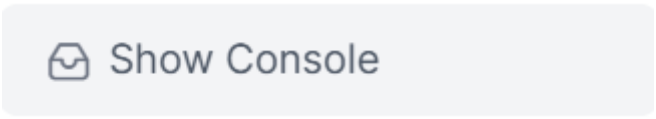

Рисунок 1.37

Интерфейс позволяет выполнять следующие действия:

– просмотреть консоль виртуальной машины.

Параметры интерфейсом просмотра консоли виртуальной машины не используются.

Способ использования интерфейса:

– использование ui элементов (кнопок) в графическом пользовательском интерфейсе.

Адрес обработки запроса:

“GET /admin/virtual-machines/{идентификатор виртуальной машины}”

8.1.5.6 Интерфейс возвращения в исходное состояние виртуальной машины

На Рисунке 1.38 приведён интерфейс возвращения в исходное состояние виртуальной машины. Интерфейс представлен в GUI и используется для возвращения в исходное состояние виртуальной машины в ПО «KeyStack SE».

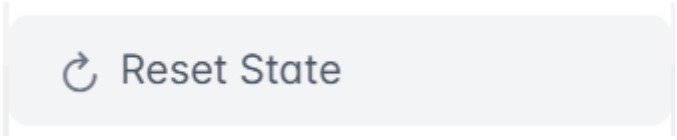

Рисунок 1.38

Интерфейс позволяет выполнять следующие действия:

– вернуть виртуальную машину в исходное состояние.

Параметры интерфейсом возвращения в исходное состояние виртуальной машины не используются.

Способ использования интерфейса:

– использование ui элементов (кнопок) в графическом пользовательском интерфейсе.

Адрес обработки запроса:

“GET /api/fstek2/servers/{идентификатор виртуальной машины}”

8.1.5.7 Интерфейс смены группы серверов виртуальной машины

На Рисунке 1.39 приведён интерфейс смены группы серверов виртуальной машины. Интерфейс представлен в GUI и используется для смены группы серверов виртуальной машины в ПО «KeyStack SE».

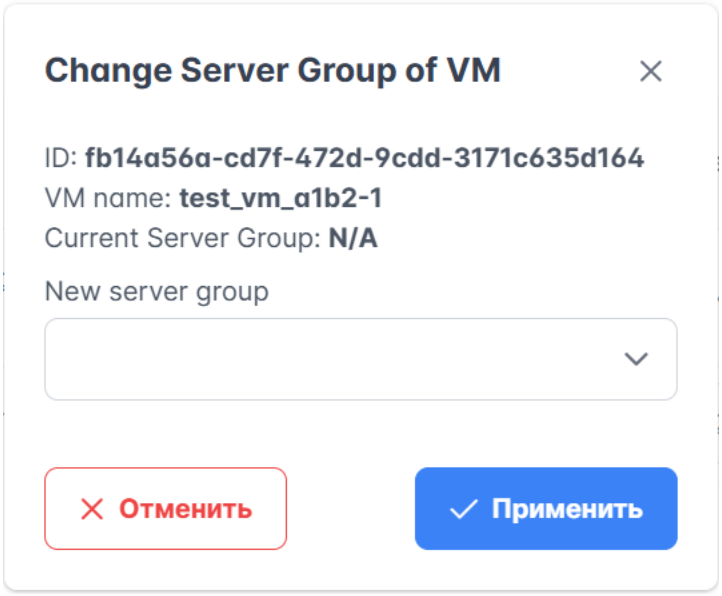

Рисунок 1.39

Интерфейс позволяет выполнять следующие действия:

– сменить группу серверов виртуальной машины.

Параметры, используемые интерфейсом смены группы серверов виртуальной машины:

– наименование новой группы серверов.

Способ использования интерфейса:

– использование ui элементов (кнопок и списка) в графическом пользовательском интерфейсе.

Адрес обработки запроса:

“PUT /api/fstek2/servers/{идентификатор виртуальной машины}”

8.1.5.8 Интерфейс смены папки виртуальной машины

На Рисунке 1.40 приведён интерфейс смены папки виртуальной машины. Интерфейс представлен в GUI и используется для смены папки виртуальной машины в ПО «KeyStack SE».

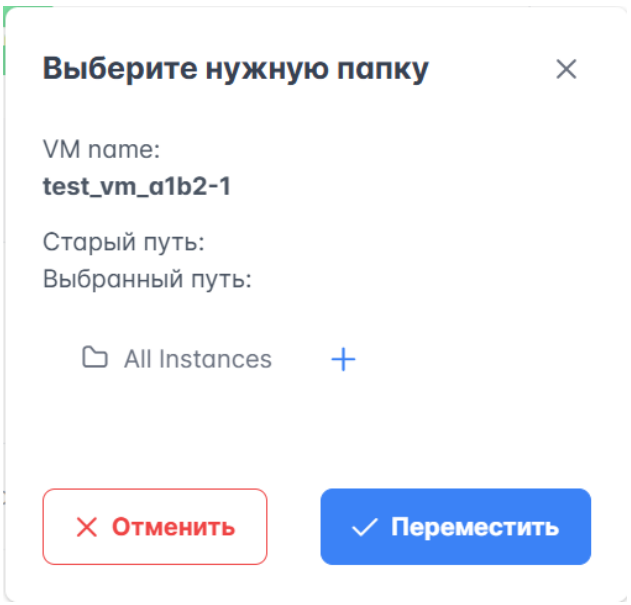

Рисунок 1.40

Интерфейс позволяет выполнять следующие действия:

– сменить папку виртуальной машины.

Параметры, используемые интерфейсом смены папки виртуальной машины:

– наименование новой папки виртуальных машин.

Способ использования интерфейса:

– использование ui элементов (кнопок и списка) в графическом пользовательском интерфейсе.

Адрес обработки запроса:

“PUT /api/fstek2/servers/{идентификатор виртуальной машины}/tags”

8.1.5.9 Интерфейс присоединение интерфейса к виртуальной машине

На Рисунке 1.41 приведён интерфейс присоеднинение интерфейса к виртуальной машине. Интерфейс представлен в GUI и используется для присоединение интерфейса к виртуальной машине в ПО «KeyStack SE».

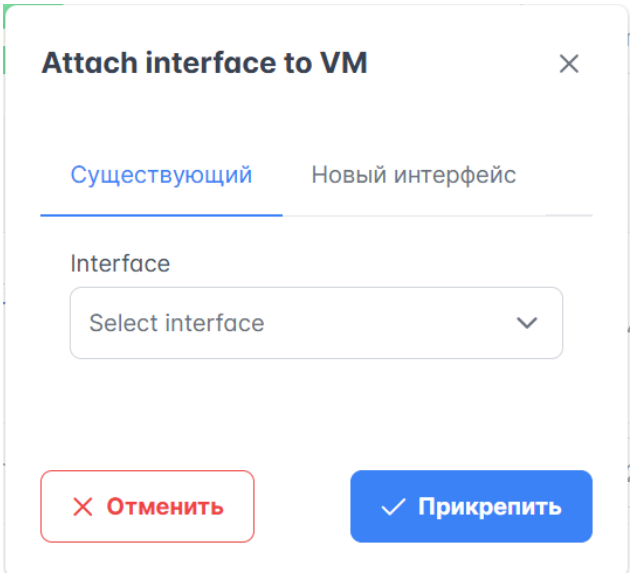

Рисунок 1.41

Интерфейс позволяет выполнять следующие действия:

– присоединить интерфейс к виртуальной машине.

Параметры, используемые интерфейсом присоединения интерфейса к виртуальной машине:

– наименование интерфейса.

Способ использования интерфейса:

– использование ui элементов (кнопок и списка) в графическом пользовательском интерфейсе.

Адрес обработки запроса:

“POST /api/fstek2/servers/{идентификатор виртуальной машины}/interfaces”

8.1.5.10 Интерфейс добавления нового интерфейса к виртуальной машине

На Рисунке 1.42 приведён интерфейс добавления нового интерфейса к виртуальной машине. Интерфейс представлен в GUI и используется для добавления нового интерфейса к виртуальной машине в ПО «KeyStack SE».

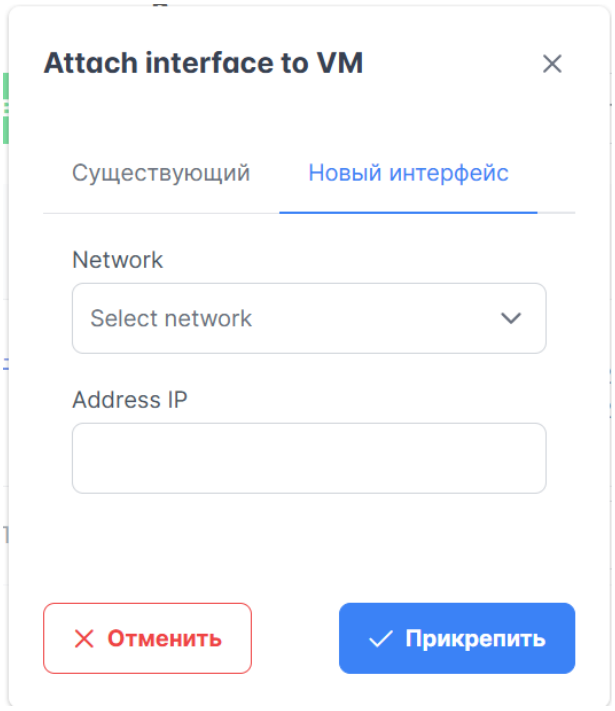

Рисунок 1.42

Интерфейс позволяет выполнять следующие действия:

– добавить новый интерфейс к виртуальной машине.

Параметры, используемые интерфейсом добавления нового интерфейса к виртуальной машине:

– сеть;

– ip адрес.

Способ использования интерфейса:

– использование ui элементов (кнопок и списка) в графическом пользовательском интерфейсе.

Адрес обработки запроса:

“POST /api/fstek2/servers/{идентификатор виртуальной машины}/interfaces”

8.1.5.11 Интерфейс отсоединения интерфейса к виртуальной машине

На Рисунке 1.43 приведён интерфейс отсоединения интерфейса от виртуальной машины. Интерфейс представлен в GUI и используется для отсоединения интерфейса от виртуальной машины в ПО «KeyStack SE».

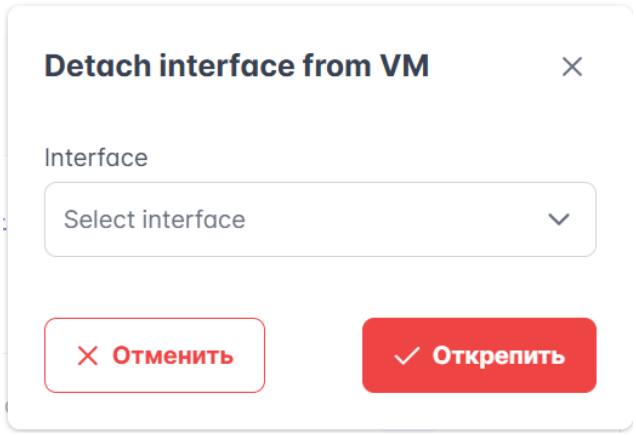

Рисунок 1.43

Интерфейс позволяет выполнять следующие действия:

– присоединить интерфейс к виртуальной машине.

Параметры, используемые интерфейсом отсоединения интерфейса от виртуальной машины:

– наименование интерфейса.

Способ использования интерфейса:

– использование ui элементов (кнопок и списка) в графическом пользовательском интерфейсе.

Адрес обработки запроса:

“DELETE /api/fstek2/servers/{идентификатор виртуальной машины}/interfaces/{идентификатор интерфейса}”

8.1.5.12 Интерфейс подключения через аварийную виртуальную машину к виртуальной машине

На Рисунке 1.44 приведён интерфейс подключения через аварийную виртуальную машину к виртуальной машине. Интерфейс представлен в GUI и используется для подключения через аварийную виртуальную машину к виртуальной машине в ПО «KeyStack SE».

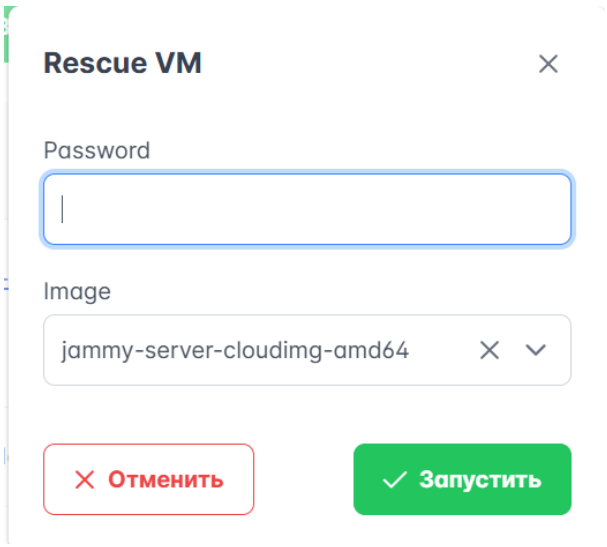

Рисунок 1.44

Интерфейс позволяет выполнять следующие действия:

– подключаться через аварийную виртуальную машину к виртуальной машине.

Параметры, используемые интерфейсом подключения через аварийную виртуальную машину к виртуальной машине:

– образ виртуальной машины;

– пароль.

Способ использования интерфейса:

– использование ui элементов (кнопок и списка) в графическом пользовательском интерфейсе.

Адрес обработки запроса:

“POST /api/fstek2/servers/{идентификатор виртуальной машины}/rescue

8.2 Интерфейс аутентификации пользователя GitLab

На Рисунке 1.45 приведён интерфейс модуля GitLab, назначением которого является реализация требований безопасности, связанных с идентификацией и аутентификацией пользователей. Интерфейс представлен в GUI и используется для аутентификации пользователей в ПО «KeyStack SE».

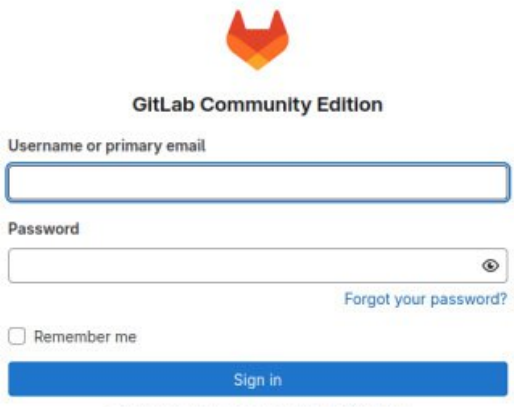

Рисунок 1.45

Интерфейс идентификации и аутентификации пользователя реализует следующие требования по безопасности информации:

– При попытке ввода неправильного значения идентификатора или пароля пользователя должно выводиться сообщение с приглашением ввести правильный идентификатор и пароль еще раз.

Интерфейс позволяет выполнять следующие действия:

– аутентификация пользователя.

В интерфейсе не предусмотрены действия, не влияющие на выполнение требований безопасности к ПО «KeyStack SE».

Параметры, используемые интерфейсом аутентификации пользователя:

– имя пользователя или email;

– пароль.

Способ использования интерфейса:

– ввод данных в графический пользовательский интерфейс.

8.3 Интерфейс аутентификации пользователя Hashicorp vault (Vault)

На Рисунке 1.46 приведён интерфейс модуля Hashicorp vault (Vault), назначением которого является реализация требований безопасности, связанных с идентификацией и аутентификацией пользователей. Интерфейс представлен в GUI и используется для аутентификации пользователей в ПО «KeyStack SE».

Рисунок 1.46

Интерфейс идентификации и аутентификации пользователя реализует следующие требования по безопасности информации:

– При попытке ввода неправильного значения идентификатора или пароля пользователя должно выводиться сообщение с приглашением ввести правильный идентификатор и пароль еще раз.

Интерфейс позволяет выполнять следующие действия:

– аутентификация пользователя.

В интерфейсе не предусмотрены действия, не влияющие на выполнение требований безопасности к ПО «KeyStack SE».

Параметры, используемые интерфейсом аутентификации пользователя:

– имя пользователя или email;

– пароль.

Способ использования интерфейса:

– ввод данных в графический пользовательский интерфейс.

8.4 Интерфейс аутентификации пользователя Grafana

На Рисунке 1.48 приведён интерфейс модуля Grafana, назначением которого является реализация требований безопасности, связанных с идентификацией и аутентификацией пользователей. Интерфейс представлен в GUI и используется для аутентификации пользователей в ПО «KeyStack SE».

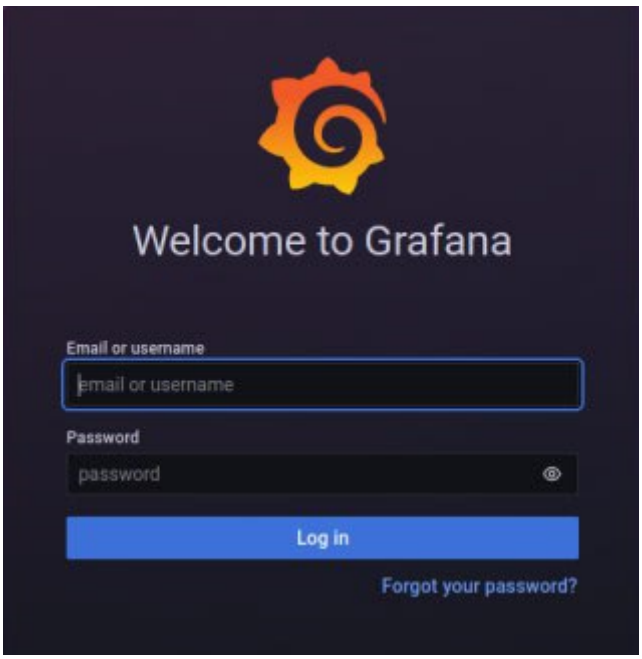

Рисунок 1.48

Интерфейс идентификации и аутентификации пользователя реализует следующие требования по безопасности информации:

- При попытке ввода неправильного значения идентификатора или пароля пользователя должно выводиться сообщение с приглашением ввести правильный идентификатор и пароль еще раз.

Интерфейс позволяет выполнять следующие действия:

- аутентификация пользователя.

В интерфейсе не предусмотрены действия, не влияющие на выполнение требований безопасности к ПО «KeyStack SE».

Параметры, используемые интерфейсом аутентификации пользователя:

- имя пользователя или email;
- пароль.

Способ использования интерфейса:

– ввод данных в графический пользовательский интерфейс.

8.5 Интерфейс аутентификации пользователя NetBox

На Рисунке 1.49 приведён интерфейс модуля NetBox, назначением которого является реализация требований безопасности, связанных с идентификацией и аутентификацией пользователей. Интерфейс представлен в GUI и используется для аутентификации пользователей в ПО «KeyStack SE».

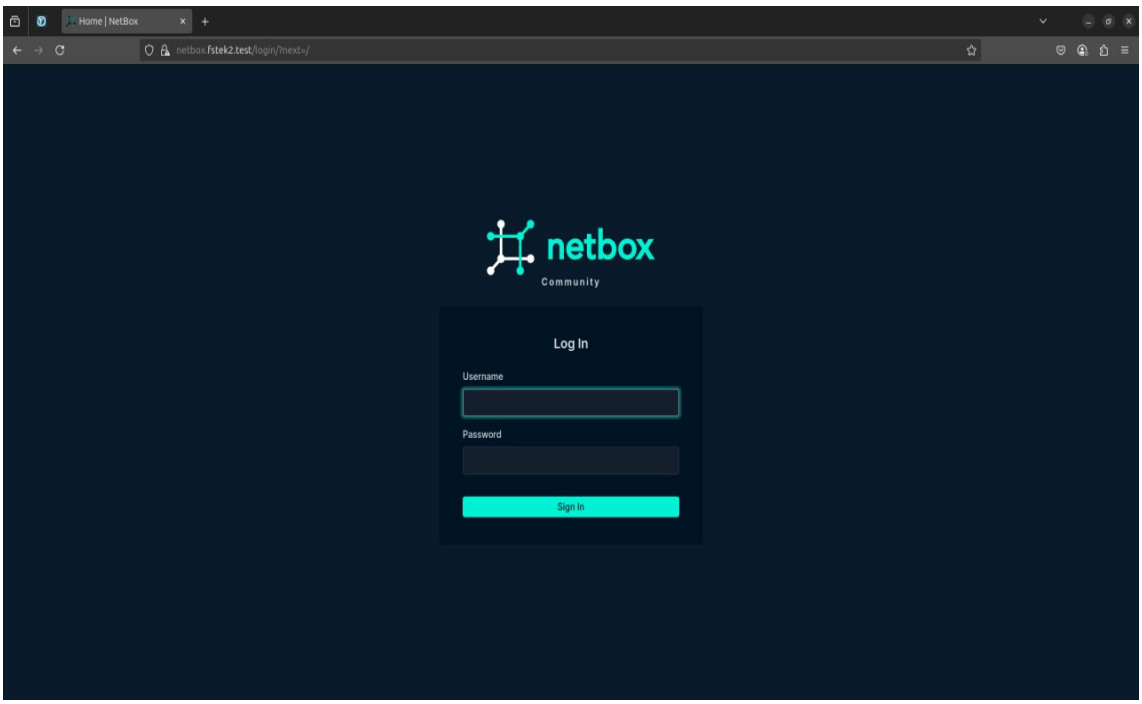

Рисунок 1.49

Интерфейс идентификации и аутентификации пользователя реализует следующие требования по безопасности информации:

– При попытке ввода неправильного значения идентификатора или пароля пользователя должно выводиться сообщение с приглашением ввести правильный идентификатор и пароль еще раз.

Интерфейс позволяет выполнять следующие действия:

– аутентификация пользователя.

В интерфейсе не предусмотрены действия, не влияющие на выполнение требований безопасности к ПО «KeyStack SE».

Параметры, используемые интерфейсом аутентификации пользователя:

– имя пользователя или email;

– пароль.

Способ использования интерфейса:

– ввод данных в графический пользовательский интерфейс.

8.6 Интерфейсы ПО «OpenSearch Dashboards», не влияющие на функции безопасности

8.6.1 Интерфейс просмотра списка пользовательских приложений

На Рисунке 1.50 приведён интерфейс ПО «OpenSearch Dashboards», который представлен в GUI и используется для просмотра списка пользовательских приложений в ПО «OpenSearch Dashboards».

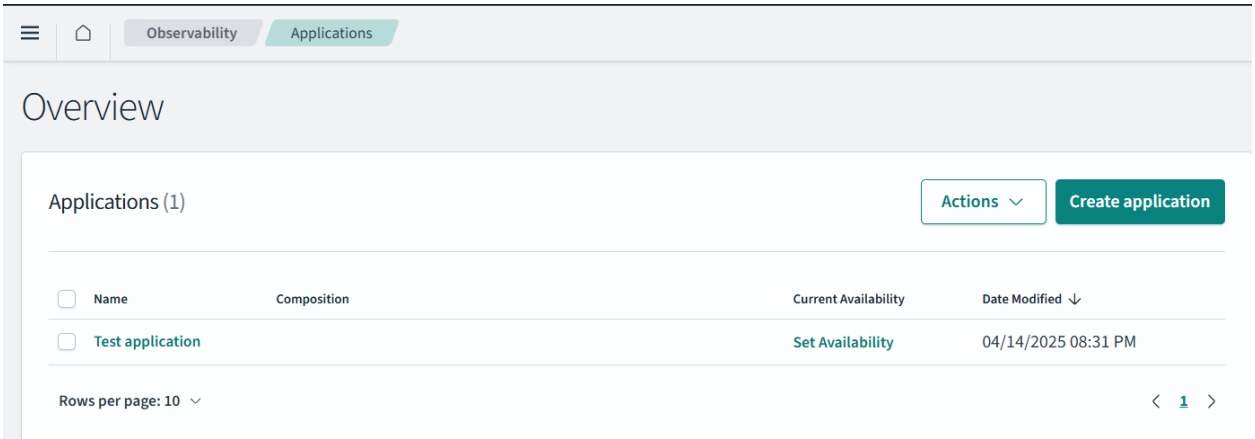

Рисунок 1.50

Интерфейс позволяет выполнять следующие действия:

– просматривать список пользовательских приложений;

– переходить к интерфейсам создания, переименования и удаления пользовательского приложения;

– просматривать параметры пользовательских приложений.

Параметры, используемые интерфейсом просмотра списка пользовательских приложений:

– наименование пользовательского приложения;

– состав пользовательского приложения;

– текущая доступность;

– дата и время изменения.

Способ использования интерфейса:

– использование ui элементов (кнопок и списков) в графическом пользовательском интерфейсе.

Адрес обработки запроса:

“GET /api/observability/application/”

8.6.2 Интерфейс создания пользовательского приложения

На Рисунке 1.51 приведён интерфейс ПО «OpenSearch Dashboards», который представлен в GUI и используется для создания пользовательского приложения в ПО «OpenSearch Dashboards».

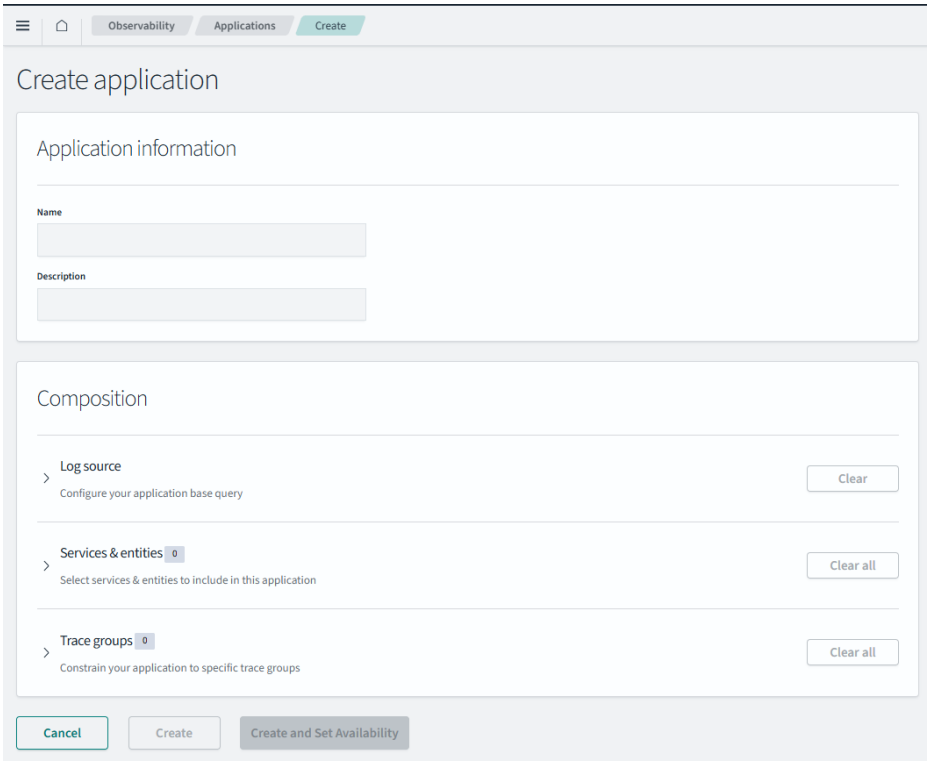

Рисунок 1.51

Интерфейс позволяет выполнять следующие действия:

– создавать пользовательское приложение, чтобы объединить события журналов с данными трассировки и метрик в единое представление об общем состоянии системы;

– создавать структуру пользовательского приложения;

– указывать описание пользовательских приложений.

Параметры, используемые интерфейсом создания пользовательского приложения:

– наименование;

– описание;

– состав.

Способ использования интерфейса:

– ввод данных в графический пользовательский интерфейс, использование ui элементов (кнопок).

Адрес обработки запроса:

“POST /api/observability/application/”

8.6.3 Интерфейс переименования пользовательского приложения

На Рисунке 1.52 приведён интерфейс ПО «OpenSearch Dashboards», который представлен в GUI и используется для переименования пользовательского приложения в ПО «OpenSearch Dashboards».

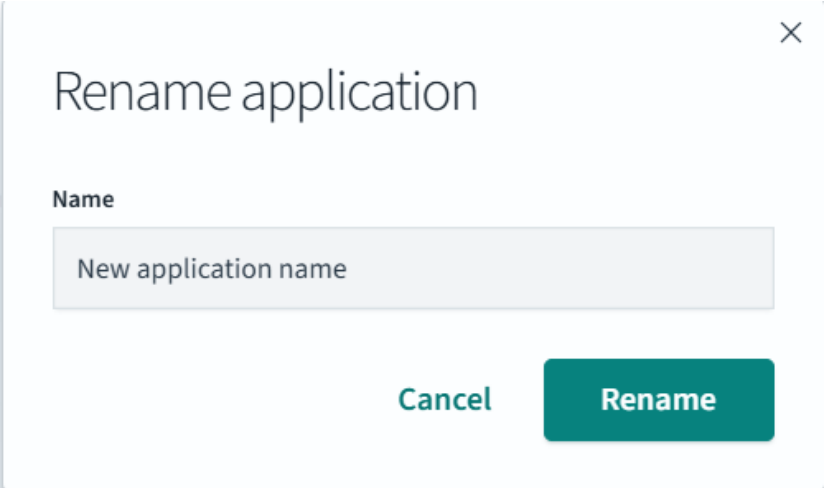

Рисунок 1.52

Интерфейс позволяет выполнять следующие действия:

– переименовывать пользовательское приложение.

Параметры, используемые интерфейсом переименования пользовательского приложения:

– наименование.

Способ использования интерфейса:

– ввод данных в графический пользовательский интерфейс, использование ui элементов (кнопок).

Адрес обработки запроса:

“PUT /api/observability/application/rename”

8.6.4 Интерфейс удаления пользовательского приложения

На Рисунке 1.53 приведён интерфейс ПО «OpenSearch Dashboards», который представлен в GUI и используется для удаления пользовательского приложения в ПО «OpenSearch Dashboards».

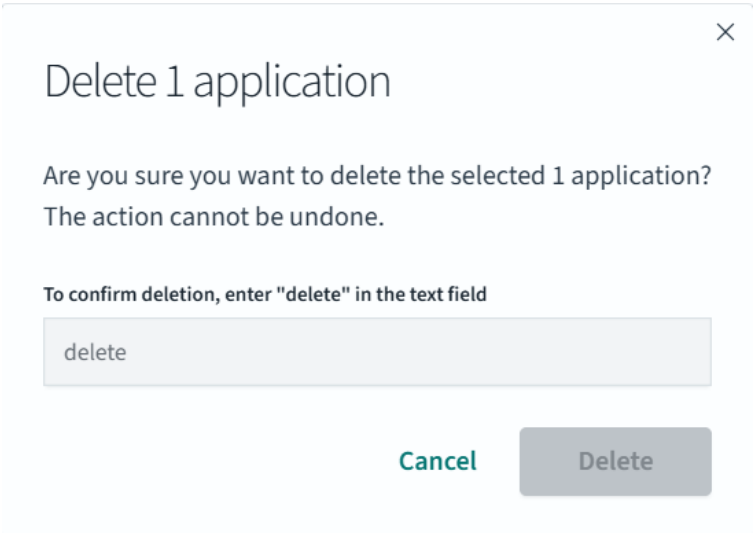

Рисунок 1.53

Интерфейс позволяет выполнять следующие действия:

– удалять пользовательское приложение.

Параметры, используемые интерфейсом удаления пользовательского приложения:

– слово для подтверждения удаления.

Способ использования интерфейса:

– ввод данных в графический пользовательский интерфейс, использование ui элементов (кнопок).

Адрес обработки запроса:

“DELETE /api/observability/application/{id приложения}”

8.6.5 Интерфейс сохранения выборки данных событий безопасности

На Рисунке 1.54 приведён интерфейс ПО «OpenSearch Dashboards», который представлен в GUI и используется для сохранения выборки данных событий безопасности в ПО «OpenSearch Dashboards».

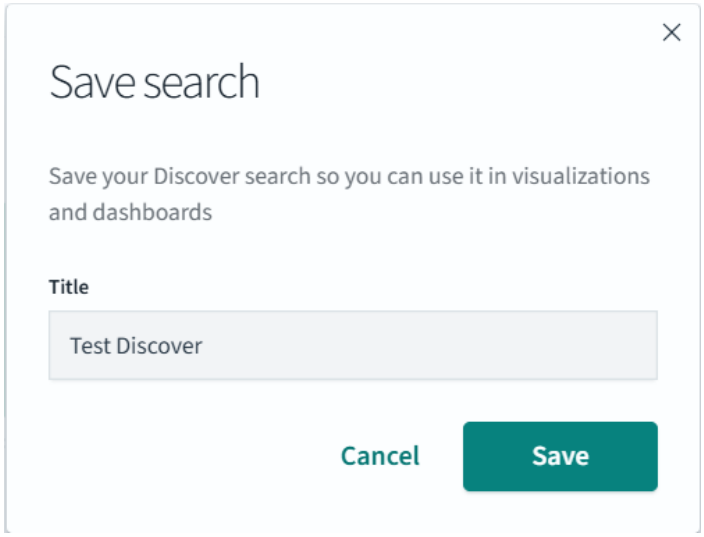

Рисунок 1.54

Интерфейс позволяет выполнять следующие действия:

– сохранять выборку данных событий безопасности.

Параметры, используемые интерфейсом выборки данных событий безопасности:

– наименование выборки данных событий безопасности.

Способ использования интерфейса:

– использование ui элементов (кнопок) в графическом пользовательском интерфейсе.

Адрес обработки запроса:

“POST /api/saved_objects/search?overwrite=true”

8.6.6 Интерфейс просмотра списка логов для визуализации

На Рисунке 1.55 приведён интерфейс ПО «OpenSearch Dashboards», который представлен в GUI и используется для просмотра списка логов для визуализации в ПО «OpenSearch Dashboards».

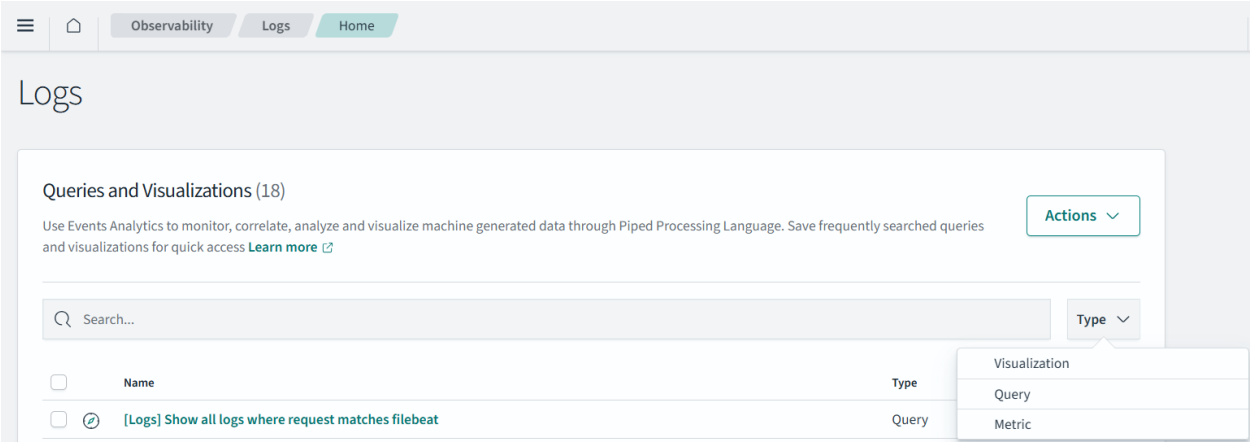

Рисунок 1.55

Интерфейс позволяет выполнять следующие действия:

– просматривать список логов для визуализации;

– переходить к интерфейсам удаления истории логов и их обзора.

– поиск по наименованию;

– фильтрация списка.

Параметры, используемые интерфейсом просмотра списка логов для визуализации:

– наименование;

– тип.

Способ использования интерфейса:

– ввод данных в графический пользовательский интерфейс, использование ui элементов (кнопок и списков)

Адрес обработки запроса:

“GET /api/observability/event_analytics/saved_objects?{параметры}”

8.6.7 Интерфейс удаления истории логов

На Рисунке 1.56 приведён интерфейс ПО «OpenSearch Dashboards», который представлен в GUI и используется для удаления истории логов в ПО «OpenSearch Dashboards».

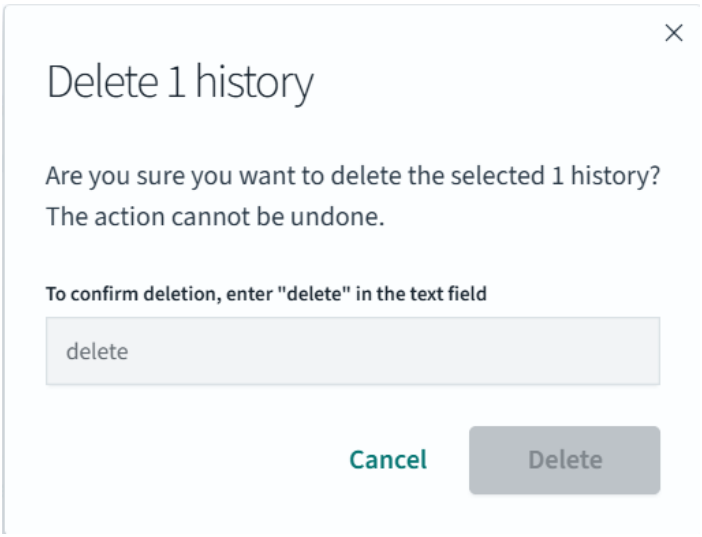

Рисунок 1.56

Интерфейс позволяет выполнять следующие действия:

– удалять историю логов.

Параметры, используемые интерфейсом удаления истории логов:

– слово для подтверждения удаления.

Способ использования интерфейса:

– ввод данных в графический пользовательский интерфейс, использование ui элементов (кнопок)

Адрес обработки запроса:

“DELETE /api/observability/event_analytics/saved_objects/{id истории логов}”

8.6.8 Интерфейс обзора логов

На Рисунке 1.57 приведён интерфейс ПО «OpenSearch Dashboards», который представлен в GUI и используется для обзора логов в ПО «OpenSearch Dashboards».

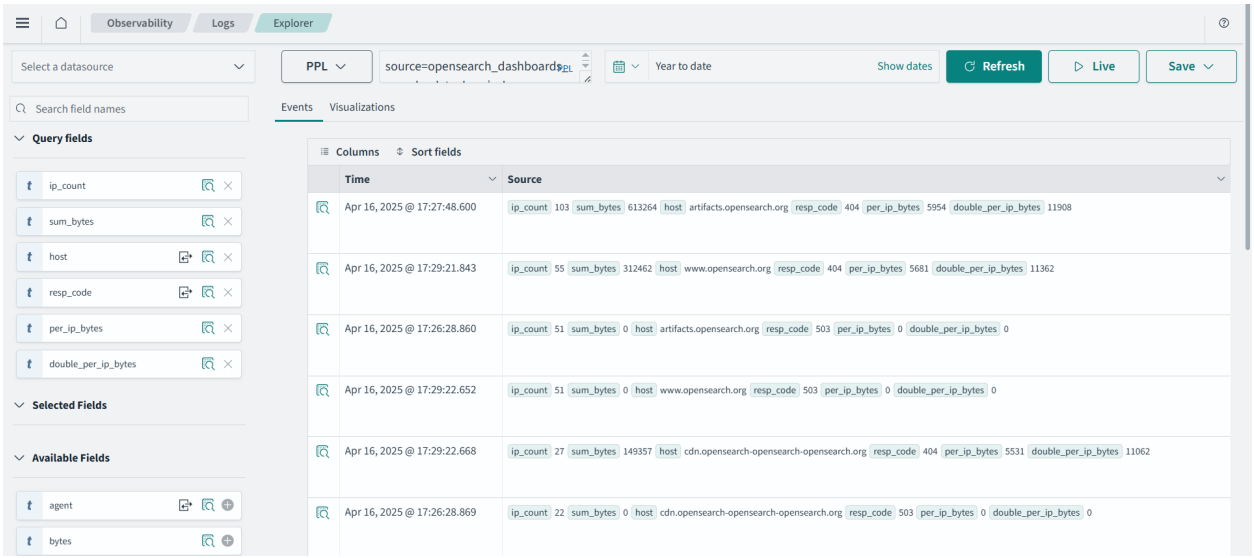

Рисунок 1.57

Интерфейс позволяет выполнять следующие действия:

– обозревать логи;

– визуализировать логи;

– сохранять логи;

– просматривать логи в режиме реального времени.

– фильтрация логов.

Параметры, используемые интерфейсом обзора логов:

– запрос;

– диапазон дат;

– дата и время событий;

– источник событий.

Способ использования интерфейса:

– ввод данных в графический пользовательский интерфейс, использование ui элементов (кнопок)

Адрес обработки запроса:

“GET /api/observability/event_analytics/saved_objects?objectId={id истории логов}”

8.7 Интерфейс идентификации и аутентификации пользователя Opensearch Dashboards

На Рисунке 1.58 приведён интерфейс ПО «OpenSearch Dashboards», назначением которого является реализация требований безопасности, связанных с идентификацией и аутентификацией пользователей. Интерфейс представлен в GUI и используется для идентификации и аутентификации пользователей в ПО «OpenSearch Dashboards».

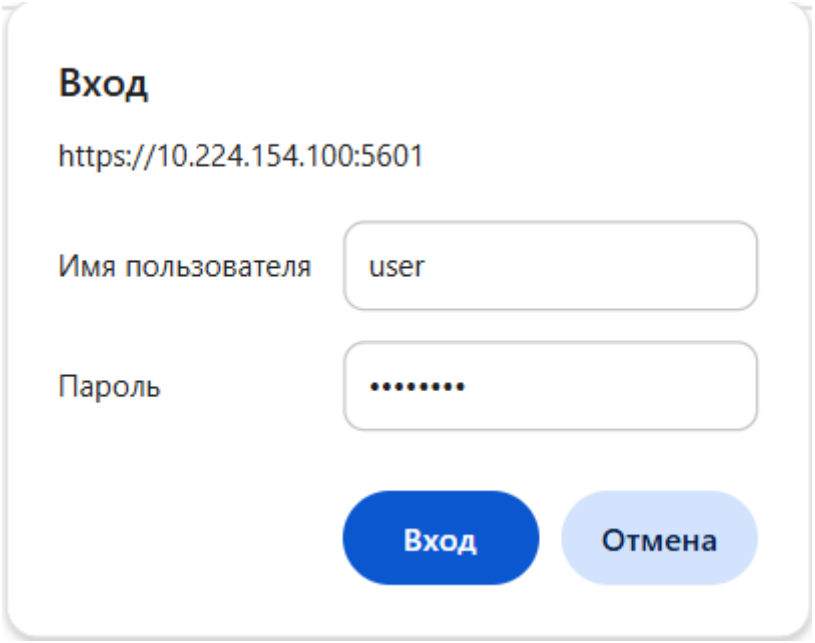

Рисунок 1.58

Интерфейс идентификации и аутентификации пользователя реализует следующие требования по безопасности информации:

– При попытке ввода неправильного значения идентификатора или пароля пользователя должно выводиться сообщение с приглашением ввести правильный идентификатор и пароль еще раз.

Интерфейс позволяет выполнять следующие действия:

– идентификация пользователя;

– аутентификация пользователя.

В интерфейсе не предусмотрены действия, не влияющие на выполнение требований безопасности к ПО «KeyStack SE».

При вызове указанного интерфейса не предусмотрены ошибки безопасности.

Параметры, используемые интерфейсом идентификации и аутентификации пользователя:

– имя пользователя;

– пароль.

Способ использования интерфейса:

– ввод данных в графический пользовательский интерфейс.

Адрес обработки запроса:

“GET / ”

8.8 Интерфейсы регистрация событий безопасности ПО «OpenSearch Dashboards»

8.8.1 Интерфейс выборки данных событий безопасности

На Рисунке 1.59 приведён интерфейс ПО «OpenSearch Dashboards», назначением которого является реализация требований безопасности, связанных регистрацией событий безопасности. Интерфейс представлен в GUI и используется для выборки данных событий безопасности в ПО «KeyStack SE».

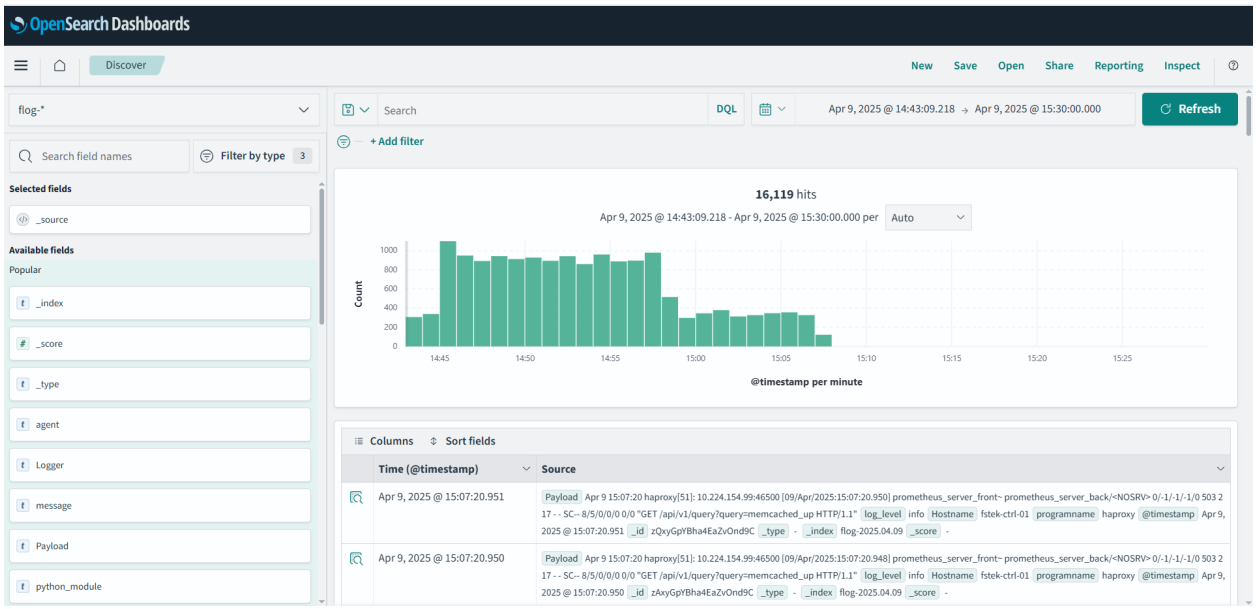

Рисунок 1.59

Интерфейс выборки данных событий безопасности реализует следующие требования по безопасности информации:

– ПО «KeyStack SE» должно:

- обеспечивать регистрацию событий безопасности, связанных с функционированием ПО «KeyStack SE»;
- оповещать администратора безопасности ПО «KeyStack SE» о событиях безопасности;
- выполнять действия, являющиеся реакцией на события безопасности самостоятельно или с применением сертифицированных средств защиты информации;
- осуществлять сбор и хранение записей в журнале событий безопасности, которые позволяют определить, когда и какие действия происходили;

- обеспечивать чтение записей о событиях безопасности, формирование отчетов с учетом заданных критериев отбора, выгрузку (экспорт) данных из журнала событий безопасности ПО «KeyStack SE».

– Регистрация событий безопасности в ПО «KeyStack SE» должна осуществляться с учетом разделов 3 - 6 ГОСТ Р 59548-2022 «Защита информации. Регистрация событий безопасности. Требования к регистрируемой информации».

– Для каждой функции безопасности в ПО «KeyStack SE» должен быть определен перечень событий, необходимых для регистрации и учета.

– Для регистрируемых событий безопасности в каждой записи журнала событий безопасности должны регистрироваться:

- номер (уникальный идентификатор) события, дата, время, тип события безопасности;
- описание события безопасности, включающее сведения о его важности.

– Записи журнала событий безопасности должны представляться в структурированном виде и содержать время события безопасности, взятое из аппаратной платформы или хостовой операционной системы.

– Регистрации подлежат, как минимум, следующие события безопасности:

- успешные и неуспешные попытки аутентификации пользователей ПО «KeyStack SE»;
- доступ пользователей ПО «KeyStack SE» к виртуальным машинам;
- создание и удаление виртуальных машин;
- запуск и остановка ПО «KeyStack SE» с указанием причины остановки;
- запуск и остановка виртуальных машин с указанием причины остановки;
- изменение ролевой модели;
- изменение конфигурации ПО «KeyStack SE»;
- изменение конфигураций виртуальных машин;
- факты нарушения целостности объектов контроля.

Интерфейс позволяет выполнять следующие действия:

– просматривать данные событий безопасности;

– обновлять выборку данных событи безопасности.

В интерфейсе предусмотрены действия, не влияющие на выполнение требований безопасности к ПО «KeyStack SE»:

– фильтрация данных событий безопасности по типу и временному диапазону;

– поиск данных событий безопасности.

При вызове указанного интерфейса не предусмотрены ошибки безопасности.

Параметры, используемые интерфейсом выборки данных событий безопасности:

– временная метка;

– источник события безопасности.

Способ использования интерфейса:

– использование ui элементов (кнопок, списков и календаря) в графическом пользовательском интерфейсе.

Адрес обработки запроса:

“POST /internal/search/opensearch”

8.8.2 Интерфейс загрузки выборки данных событий безопасности

На Рисунке 1.60 приведён интерфейс ПО «OpenSearch Dashboards», назначением которого является реализация требований безопасности, связанных регистрацией событий безопасности. Интерфейс представлен в GUI и используется для загрузки выборки данных событий безопасности в ПО «OpenSearch Dashboards».

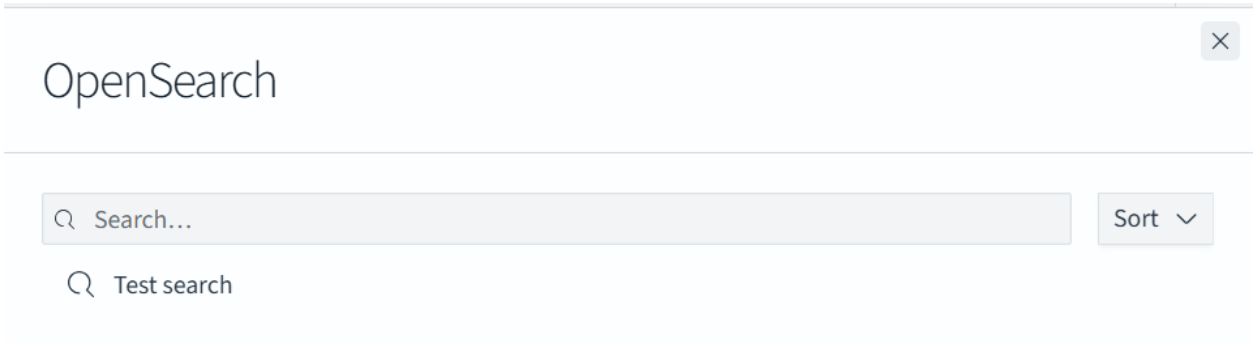

Рисунок 1.60

Интерфейс загрузки выборки данных событий безопасности реализует следующие требования по безопасности информации:

– ПО «KeyStack SE» должно:

- обеспечивать регистрацию событий безопасности, связанных с функционированием ПО «KeyStack SE»;
- оповещать администратора безопасности ПО «KeyStack SE» о событиях безопасности;
- выполнять действия, являющиеся реакцией на события безопасности самостоятельно или с применением сертифицированных средств защиты информации;

- осуществлять сбор и хранение записей в журнале событий безопасности, которые позволяют определить, когда и какие действия происходили;
- обеспечивать чтение записей о событиях безопасности, формирование отчетов с учетом заданных критериев отбора, выгрузку (экспорт) данных из журнала событий безопасности ПО «KeyStack SE».

– Регистрация событий безопасности в ПО «KeyStack SE» должна осуществляться с учетом разделов 3 - 6 ГОСТ Р 59548-2022 «Защита информации. Регистрация событий безопасности. Требования к регистрируемой информации».

– Для каждой функции безопасности в ПО «KeyStack SE» должен быть определен перечень событий, необходимых для регистрации и учета.

– Для регистрируемых событий безопасности в каждой записи журнала событий безопасности должны регистрироваться:

- номер (уникальный идентификатор) события, дата, время, тип события безопасности;
- описание события безопасности, включающее сведения о его важности.

– Записи журнала событий безопасности должны представляться в структурированном виде и содержать время события безопасности, взятое из аппаратной платформы или хостовой операционной системы.

– Регистрации подлежат, как минимум, следующие события безопасности:

- успешные и неуспешные попытки аутентификации пользователей ПО «KeyStack SE»;
- доступ пользователей ПО «KeyStack SE» к виртуальным машинам;
- создание и удаление виртуальных машин;
- запуск и остановка ПО «KeyStack SE» с указанием причины остановки;
- запуск и остановка виртуальных машин с указанием причины остановки;
- изменение ролевой модели;
- изменение конфигурации ПО «KeyStack SE»;
- изменение конфигураций виртуальных машин;
- факты нарушения целостности объектов контроля.

Интерфейс позволяет выполнять следующие действия:

– загружать выборку данных событий безопасности.

В интерфейсе предусмотрены действия, не влияющие на выполнение требований безопасности к ПО «KeyStack SE»:

– фильтрация списка;

– поиск по наименованию.

При вызове указанного интерфейса не предусмотрены ошибки безопасности.

Параметры, используемые интерфейсом выборки данных событий безопасности:

– наименование выборки данных событий безопасности;

– сортировка выборки данных событий безопасности.

Способ использования интерфейса:

– использование ui элементов (поиска и кнопок) в графическом пользовательском интерфейсе.

Адрес обработки запроса:

“POST /api/saved_objects/_bulk_get”

8.8.3 Интерфейс формирования отчета по выборке данных событий безопасности

На Рисунке 1.61 приведён интерфейс ПО «OpenSearch Dashboards», назначением которого является реализация требований безопасности, связанных регистрацией событий безопасности. Интерфейс представлен в GUI и используется для формирования отчета по выборке данных событий безопасности в ПО «OpenSearch Dashboards».

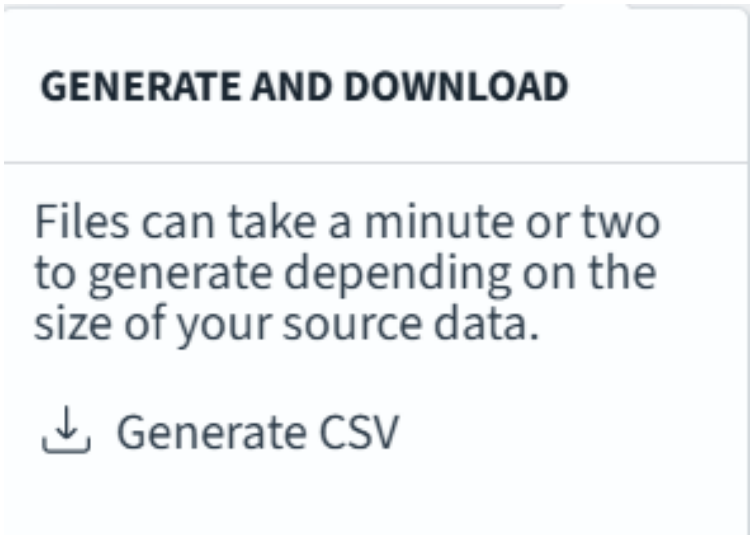

Рисунок 1.61

Интерфейс формирования отчета по выборке данных событий безопасности реализует следующие требования по безопасности информации:

– ПО «KeyStack SE» должно:

- обеспечивать регистрацию событий безопасности, связанных с функционированием ПО «KeyStack SE»;
- оповещать администратора безопасности ПО «KeyStack SE» о событиях безопасности;
- выполнять действия, являющиеся реакцией на события безопасности самостоятельно или с применением сертифицированных средств защиты информации;
- осуществлять сбор и хранение записей в журнале событий безопасности, которые позволяют определить, когда и какие действия происходили;
- обеспечивать чтение записей о событиях безопасности, формирование отчетов с учетом заданных критериев отбора, выгрузку (экспорт) данных из журнала событий безопасности ПО «KeyStack SE».

– Регистрация событий безопасности в ПО «KeyStack SE» должна осуществляться с учетом разделов 3 - 6 ГОСТ Р 59548-2022 «Защита информации. Регистрация событий безопасности. Требования к регистрируемой информации».

– Для каждой функции безопасности в ПО «KeyStack SE» должен быть определен перечень событий, необходимых для регистрации и учета.

– Для регистрируемых событий безопасности в каждой записи журнала событий безопасности должны регистрироваться:

- номер (уникальный идентификатор) события, дата, время, тип события безопасности;
- описание события безопасности, включающее сведения о его важности.

– Записи журнала событий безопасности должны представляться в структурированном виде и содержать время события безопасности, взятое из аппаратной платформы или хостовой операционной системы.

– Регистрации подлежат, как минимум, следующие события безопасности:

- успешные и неуспешные попытки аутентификации пользователей ПО «KeyStack SE»;
- доступ пользователей ПО «KeyStack SE» к виртуальным машинам;
- создание и удаление виртуальных машин;
- запуск и остановка ПО «KeyStack SE» с указанием причины остановки;
- запуск и остановка виртуальных машин с указанием причины остановки;

- изменение ролевой модели;
- изменение конфигурации ПО «KeyStack SE»;
- изменение конфигураций виртуальных машин;
- факты нарушения целостности объектов контроля.

Интерфейс позволяет выполнять следующие действия:

– формировать отчет по выборке данных событий безопасности.

Действий, не влияющих на выполнение требований безопасности к ПО «KeyStack SE», в интерфейсе не предусмотрено.

При вызове указанного интерфейса не предусмотрены ошибки безопасности.

Параметры интерфейсом формирования отчета по выборке данных событий безопасности не используются.

Способ использования интерфейса:

– использование ui элементов (кнопок) в графическом пользовательском интерфейсе.

Адрес обработки запроса:

“POST /api/reporting/generateReport?{параметры отчета}”

8.8.4 Интерфейс просмотра списка отчетов

На Рисунке 1.62 приведён интерфейс ПО «OpenSearch Dashboards», назначением которого является реализация требований безопасности, связанных регистрацией событий безопасности. Интерфейс представлен в GUI и используется для просмотра списка отчетов в ПО «OpenSearch Dashboards».

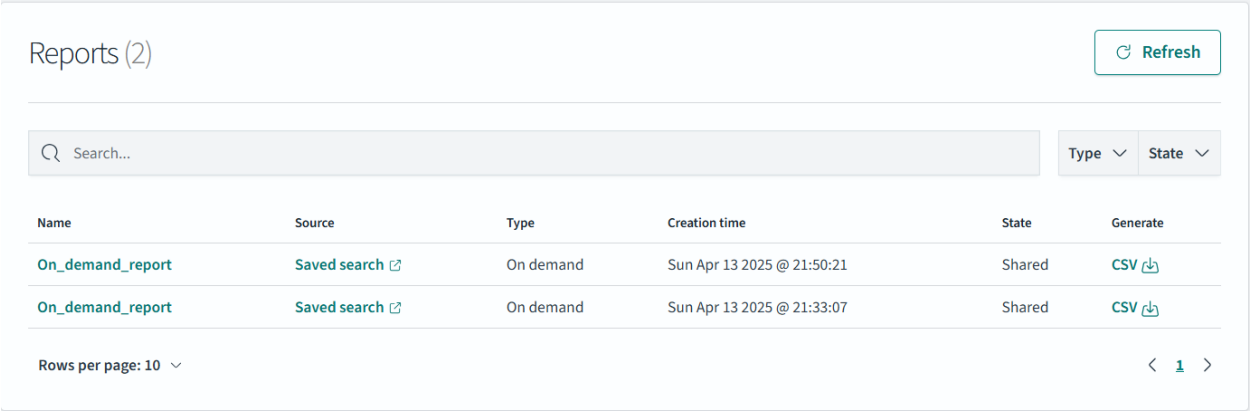

Рисунок 1.62

Интерфейс просмотра списка отчетов реализует следующие требования по безопасности информации:

– ПО «KeyStack SE» должно:

- обеспечивать регистрацию событий безопасности, связанных с функционированием ПО «KeyStack SE»;
- оповещать администратора безопасности ПО «KeyStack SE» о событиях безопасности;
- выполнять действия, являющиеся реакцией на события безопасности самостоятельно или с применением сертифицированных средств защиты информации;
- осуществлять сбор и хранение записей в журнале событий безопасности, которые позволяют определить, когда и какие действия происходили;
- обеспечивать чтение записей о событиях безопасности, формирование отчетов с учетом заданных критериев отбора, выгрузку (экспорт) данных из журнала событий безопасности ПО «KeyStack SE».

– Регистрация событий безопасности в ПО «KeyStack SE» должна осуществляться с учетом разделов 3 - 6 ГОСТ Р 59548-2022 «Защита информации. Регистрация событий безопасности. Требования к регистрируемой информации».

– Для каждой функции безопасности в ПО «KeyStack SE» должен быть определен перечень событий, необходимых для регистрации и учета.

– Для регистрируемых событий безопасности в каждой записи журнала событий безопасности должны регистрироваться:

- номер (уникальный идентификатор) события, дата, время, тип события безопасности;
- описание события безопасности, включающее сведения о его важности.

– Записи журнала событий безопасности должны представляться в структурированном виде и содержать время события безопасности, взятое из аппаратной платформы или хостовой операционной системы.

– Регистрации подлежат, как минимум, следующие события безопасности:

- успешные и неуспешные попытки аутентификации пользователей ПО «KeyStack SE»;
- доступ пользователей ПО «KeyStack SE» к виртуальным машинам;
- создание и удаление виртуальных машин;
- запуск и остановка ПО «KeyStack SE» с указанием причины остановки;
- запуск и остановка виртуальных машин с указанием причины остановки;

- изменение ролевой модели;
- изменение конфигурации ПО «KeyStack SE»;
- изменение конфигураций виртуальных машин;
- факты нарушения целостности объектов контроля.

Интерфейс позволяет выполнять следующие действия:

- просматривать список отчетов по выборке данных событий безопасности;
- скачивать отчеты по выборке данных событий безопасности;
- переходить к интерфейсам выборки данных событий безопасности и формирования отчета по выборке данных событий безопасности;
- обновлять список отчетов.

В интерфейсе предусмотрены действия, не влияющие на выполнение требований безопасности к ПО «KeyStack SE»:

- просматривать параметры отчетов;
- фильрация списка;
- поиск по наименованию.

При вызове указанного интерфейса не предусмотрены ошибки безопасности.

Параметры, используемые интерфейсом просмотра списка отчетов:

- наименование отчета;
- сортировка списка отчетов;
- источник отчета;
- тип отчета;
- дата и время создания отчета;
- состояние отчета.

Способ использования интерфейса:

- использование ui элементов (поиска и кнопок) в графическом пользовательском интерфейсе.

Адрес обработки запроса:

“GET /api/reporting/reports”

8.8.5 Интерфейс просмотра списка оповещений от триггеров

На Рисунке 1.63 приведён интерфейс ПО «OpenSearch Dashboards», назначением которого является реализация требований безопасности, связанных регистрацией событий безопасности. Интерфейс представлен в GUI и используется для просмотра списка оповещений от триггеров в ПО «OpenSearch Dashboards».

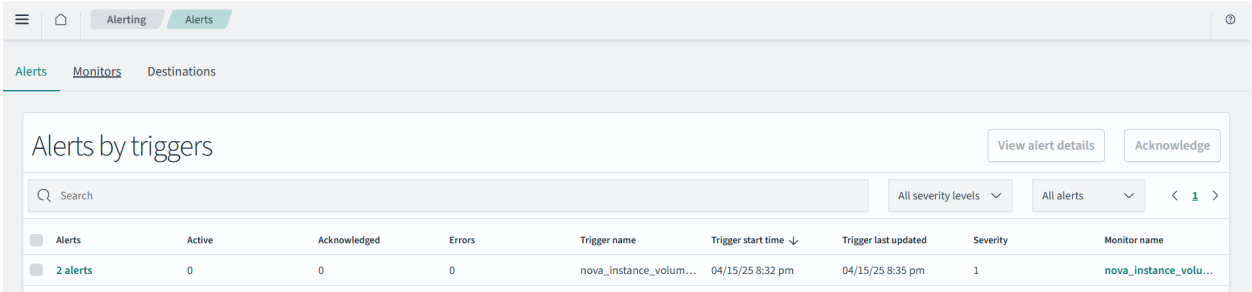

Рисунок 1.63

Интерфейс просмотра списка оповещений от триггеров реализует следующие требования по безопасности информации:

– ПО «KeyStack SE» должно:

- обеспечивать регистрацию событий безопасности, связанных с функционированием ПО «KeyStack SE»;
- оповещать администратора безопасности ПО «KeyStack SE» о событиях безопасности;
- выполнять действия, являющиеся реакцией на события безопасности самостоятельно или с применением сертифицированных средств защиты информации;
- осуществлять сбор и хранение записей в журнале событий безопасности, которые позволяют определить, когда и какие действия происходили;
- обеспечивать чтение записей о событиях безопасности, формирование отчетов с учетом заданных критериев отбора, выгрузку (экспорт) данных из журнала событий безопасности ПО «KeyStack SE».

– Регистрация событий безопасности в ПО «KeyStack SE» должна осуществляться с учетом разделов 3 - 6 ГОСТ Р 59548-2022 «Защита информации. Регистрация событий безопасности. Требования к регистрируемой информации».

– Для каждой функции безопасности в ПО «KeyStack SE» должен быть определен перечень событий, необходимых для регистрации и учета.

– Для регистрируемых событий безопасности в каждой записи журнала событий безопасности должны регистрироваться:

- номер (уникальный идентификатор) события, дата, время, тип события безопасности;
- описание события безопасности, включающее сведения о его важности.

– Записи журнала событий безопасности должны представляться в структурированном виде и содержать время события безопасности, взятое из аппаратной платформы или хостовой операционной системы.

– Регистрации подлежат, как минимум, следующие события безопасности:

- успешные и неуспешные попытки аутентификации пользователей ПО «KeyStack SE»;
- доступ пользователей ПО «KeyStack SE» к виртуальным машинам;
- создание и удаление виртуальных машин;
- запуск и остановка ПО «KeyStack SE» с указанием причины остановки;
- запуск и остановка виртуальных машин с указанием причины остановки;
- изменение ролевой модели;
- изменение конфигурации ПО «KeyStack SE»;
- изменение конфигураций виртуальных машин;
- факты нарушения целостности объектов контроля.

Интерфейс позволяет выполнять следующие действия:

– просматривать список оповещений от триггеров;

– переходить к интерфейсам просмотра оповещения и монитора.

В интерфейсе предусмотрены действия, не влияющие на выполнение требований безопасности к ПО «KeyStack SE»:

– просматривать параметры триггеров;

– фильтрация списка;

– поиск по наименованию.

При вызове указанного интерфейса не предусмотрены ошибки безопасности.

Параметры, используемые интерфейсом просмотра списка оповещений от триггеров:

– количество оповещений;

– наименование триггера;

– количество активных (не подтвержденных) оповещений;

– количество подтвержденных оповещений;

– количество возникших ошибок при работе триггера;

– дата и время начала работы триггера;

– дата и время иизменений состояния триггера;

– уровень строгости срабатывания триггера;

– наименование монитора.

Способ использования интерфейса:

– ввод данных в графический пользовательский интерфейс, использование ui элементов (кнопок и списков)

Адрес обработки запроса:

“GET /api/alerting/alerts?{параметры}”

8.8.6 Интерфейс просмотра оповещений

На Рисунке 1.64 приведён интерфейс ПО «OpenSearch Dashboards», назначением которого является реализация требований безопасности, связанных регистрацией событий безопасности. Интерфейс представлен в GUI и используется для просмотра оповещений в ПО «OpenSearch Dashboards».

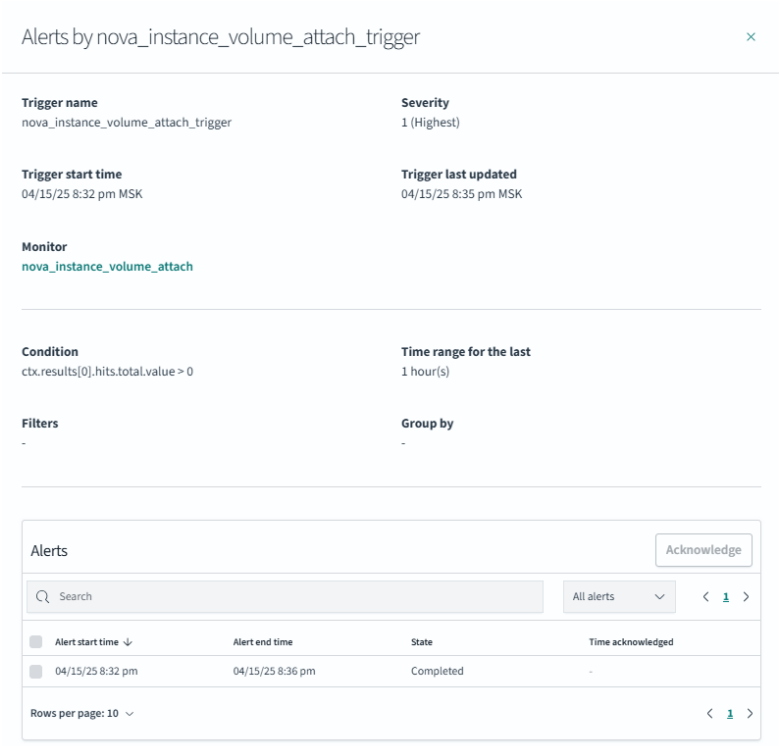

Рисунок 1.64

Интерфейс просмотра оповещений реализует следующие требования по безопасности информации:

– ПО «KeyStack SE» должно:

- обеспечивать регистрацию событий безопасности, связанных с функционированием ПО «KeyStack SE»;
- оповещать администратора безопасности ПО «KeyStack SE» о событиях безопасности;

- выполнять действия, являющиеся реакцией на события безопасности самостоятельно или с применением сертифицированных средств защиты информации;
- осуществлять сбор и хранение записей в журнале событий безопасности, которые позволяют определить, когда и какие действия происходили;
- обеспечивать чтение записей о событиях безопасности, формирование отчетов с учетом заданных критериев отбора, выгрузку (экспорт) данных из журнала событий безопасности ПО «KeyStack SE».

– Регистрация событий безопасности в ПО «KeyStack SE» должна осуществляться с учетом разделов 3 - 6 ГОСТ Р 59548-2022 «Защита информации. Регистрация событий безопасности. Требования к регистрируемой информации».

– Для каждой функции безопасности в ПО «KeyStack SE» должен быть определен перечень событий, необходимых для регистрации и учета.

– Для регистрируемых событий безопасности в каждой записи журнала событий безопасности должны регистрироваться:

- номер (уникальный идентификатор) события, дата, время, тип события безопасности;
- описание события безопасности, включающее сведения о его важности.

– Записи журнала событий безопасности должны представляться в структурированном виде и содержать время события безопасности, взятое из аппаратной платформы или хостовой операционной системы.

– Регистрации подлежат, как минимум, следующие события безопасности:

- успешные и неуспешные попытки аутентификации пользователей ПО «KeyStack SE»;
- доступ пользователей ПО «KeyStack SE» к виртуальным машинам;
- создание и удаление виртуальных машин;
- запуск и остановка ПО «KeyStack SE» с указанием причины остановки;
- запуск и остановка виртуальных машин с указанием причины остановки;
- изменение ролевой модели;
- изменение конфигурации ПО «KeyStack SE»;
- изменение конфигураций виртуальных машин;
- факты нарушения целостности объектов контроля.

Интерфейс позволяет выполнять следующие действия:

– просматривать содержимое оповещений.

В интерфейсе предусмотрены действия, не влияющие на выполнение требований безопасности к ПО «KeyStack SE»:

– поиск оповещений

– фильтрация оповещений.

При вызове указанного интерфейса не предусмотрены ошибки безопасности.

Параметры, используемые интерфейсом просмотра оповещений:

– наименование триггера;

– количество активных (не подтвержденных) оповещений;

– количество подтвержденных оповещений;

– количество возникших ошибок при работе триггера;

– дата и время начала работы триггера;

– дата и время изменений состояния триггера;

– уровень строгости срабатывания триггера;

наименование монитора.

Способ использования интерфейса:

– использование ui элементов (кнопок и списков)

Адрес обработки запроса:

“GET /api/alerting/alerts?{параметры}”

8.8.7 Интерфейс просмотра списка мониторов

На Рисунке 1.65 приведён интерфейс ПО «OpenSearch Dashboards», назначением которого является реализация требований безопасности, связанных регистрацией событий безопасности. Интерфейс представлен в GUI и используется для просмотра списка мониторов в ПО «OpenSearch Dashboards».

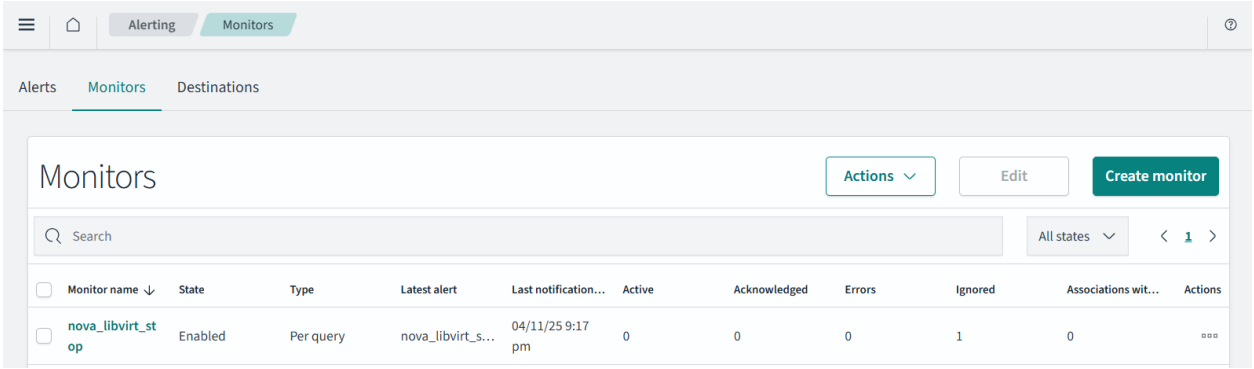

Рисунок 1.65

Интерфейс просмотра списка мониторов реализует следующие требования по безопасности информации:

– ПО «KeyStack SE» должно:

- обеспечивать регистрацию событий безопасности, связанных с функционированием ПО «KeyStack SE»;
- оповещать администратора безопасности ПО «KeyStack SE» о событиях безопасности;
- выполнять действия, являющиеся реакцией на события безопасности самостоятельно или с применением сертифицированных средств защиты информации;
- осуществлять сбор и хранение записей в журнале событий безопасности, которые позволяют определить, когда и какие действия происходили;
- обеспечивать чтение записей о событиях безопасности, формирование отчетов с учетом заданных критериев отбора, выгрузку (экспорт) данных из журнала событий безопасности ПО «KeyStack SE».

– Регистрация событий безопасности в ПО «KeyStack SE» должна осуществляться с учетом разделов 3 - 6 ГОСТ Р 59548-2022 «Защита информации. Регистрация событий безопасности. Требования к регистрируемой информации».

– Для каждой функции безопасности в ПО «KeyStack SE» должен быть определен перечень событий, необходимых для регистрации и учета.

– Для регистрируемых событий безопасности в каждой записи журнала событий безопасности должны регистрироваться:

- номер (уникальный идентификатор) события, дата, время, тип события безопасности;
- описание события безопасности, включающее сведения о его важности.

– Записи журнала событий безопасности должны представляться в структурированном виде и содержать время события безопасности, взятое из аппаратной платформы или хостовой операционной системы.

– Регистрации подлежат, как минимум, следующие события безопасности:

- успешные и неуспешные попытки аутентификации пользователей ПО «KeyStack SE»;
- доступ пользователей ПО «KeyStack SE» к виртуальным машинам;
- создание и удаление виртуальных машин;

- запуск и остановка ПО «KeyStack SE» с указанием причины остановки;
- запуск и остановка виртуальных машин с указанием причины остановки;
- изменение ролевой модели;
- изменение конфигурации ПО «KeyStack SE»;
- изменение конфигураций виртуальных машин;
- факты нарушения целостности объектов контроля.

Интерфейс позволяет выполнять следующие действия:

– просматривать список мониторов;

– переходить к интерфейсам создания, отключения, включения, удаления просмотра монитора и подтверждения оповещения.

В интерфейсе предусмотрены действия, не влияющие на выполнение требований безопасности к ПО «KeyStack SE»:

– просматривать параметры монитора;

– фильтрация списка;

– поиск по наименованию.

При вызове указанного интерфейса не предусмотрены ошибки безопасности.

Параметры, используемые интерфейсом просмотра списка мониторов:

– наименование монитора;

– состояние монитора;

– тип монитора;

– последнее оповещение;

– дата и время последнего оповещения;

– количество активных (не подтвержденных) оповещений;

– количество подтвержденных оповещений;

– количество возникших ошибок при работе триггера;

– количество проигнорированных оповещений.

Способ использования интерфейса:

– ввод данных в графический пользовательский интерфейс, использование ui элементов (кнопок и списков)

Адрес обработки запроса:

“GET /api/alerting/monitors?{параметры}”

8.8.8 Интерфейс просмотра монитора

На Рисунке 1.66 приведён интерфейс ПО «OpenSearch Dashboards», назначением которого является реализация требований безопасности, связанных регистрацией событий безопасности. Интерфейс представлен в GUI и используется для просмотра монитора в ПО «OpenSearch Dashboards».

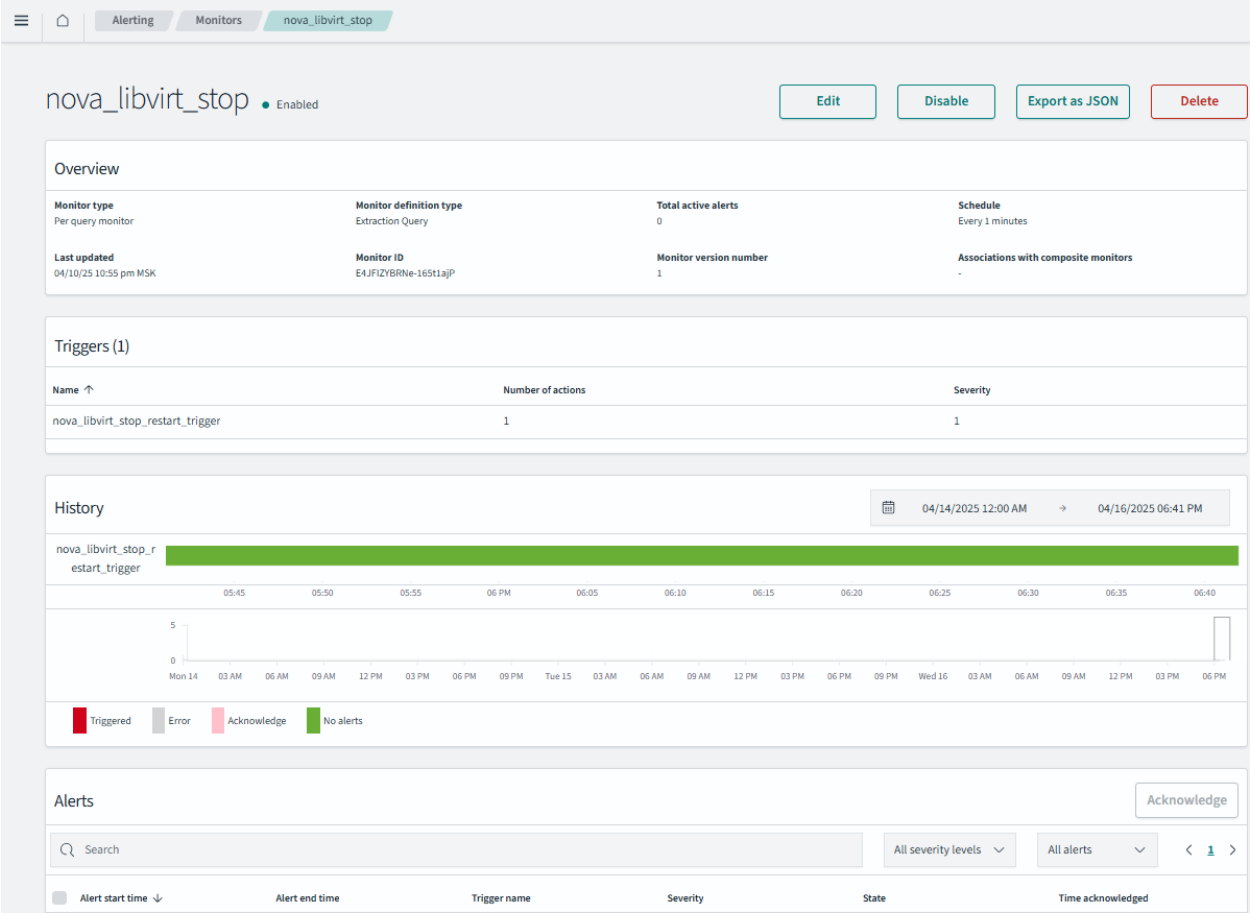

Рисунок 1.66

Интерфейс просмотра монитора реализует следующие требования по безопасности информации:

– ПО «KeyStack SE» должно:

- обеспечивать регистрацию событий безопасности, связанных с функционированием ПО «KeyStack SE»;
- оповещать администратора безопасности ПО «KeyStack SE» о событиях безопасности;
- выполнять действия, являющиеся реакцией на события безопасности самостоятельно или с применением сертифицированных средств защиты информации;

- осуществлять сбор и хранение записей в журнале событий безопасности, которые позволяют определить, когда и какие действия происходили;
- обеспечивать чтение записей о событиях безопасности, формирование отчетов с учетом заданных критериев отбора, выгрузку (экспорт) данных из журнала событий безопасности ПО «KeyStack SE».

– Регистрация событий безопасности в ПО «KeyStack SE» должна осуществляться с учетом разделов 3 - 6 ГОСТ Р 59548-2022 «Защита информации. Регистрация событий безопасности. Требования к регистрируемой информации».

– Для каждой функции безопасности в ПО «KeyStack SE» должен быть определен перечень событий, необходимых для регистрации и учета.

– Для регистрируемых событий безопасности в каждой записи журнала событий безопасности должны регистрироваться:

- номер (уникальный идентификатор) события, дата, время, тип события безопасности;
- описание события безопасности, включающее сведения о его важности.

– Записи журнала событий безопасности должны представляться в структурированном виде и содержать время события безопасности, взятое из аппаратной платформы или хостовой операционной системы.

– Регистрации подлежат, как минимум, следующие события безопасности:

- успешные и неуспешные попытки аутентификации пользователей ПО «KeyStack SE»;
- доступ пользователей ПО «KeyStack SE» к виртуальным машинам;
- создание и удаление виртуальных машин;
- запуск и остановка ПО «KeyStack SE» с указанием причины остановки;
- запуск и остановка виртуальных машин с указанием причины остановки;
- изменение ролевой модели;
- изменение конфигурации ПО «KeyStack SE»;
- изменение конфигураций виртуальных машин;
- факты нарушения целостности объектов контроля.

Интерфейс позволяет выполнять следующие действия:

– просматривать содержимое монитора;

– переходить к интерфейсам отключения, включения, удаления экспорта и редактирования монитора.

В интерфейсе не предусмотрены действия, не влияющие на выполнение требований безопасности к ПО «KeyStack SE».

При вызове указанного интерфейса не предусмотрены ошибки безопасности.

Параметры, используемые интерфейсом просмотра монитора:

– наименование монитора;
– состояние монитора;
– тип монитора;
– тип определения монитора;
– итоговое количество активных (не подтвержденных) оповещений;
– расписание выполнения;
– дата и время последнего обновления;
– идентификатор монитора;
– номер версии монитора;
– связь с составными мониторами;
– наименование триггера;
– количество действий;
– уровень строгости срабатывания триггера;
– история срабатывания триггеров монитора.

Способ использования интерфейса:

– использование ui элементов (кнопок и списков)

Адрес обработки запроса:

“GET /api/alerting/alerts?{параметры выбранного монитора}”

8.8.9 Интерфейс создания монитора

На Рисунке 1.67 приведён интерфейс ПО «OpenSearch Dashboards», назначением которого является реализация требований безопасности, связанных регистрацией событий безопасности. Интерфейс представлен в GUI и используется для создания монитора в ПО «OpenSearch Dashboards».

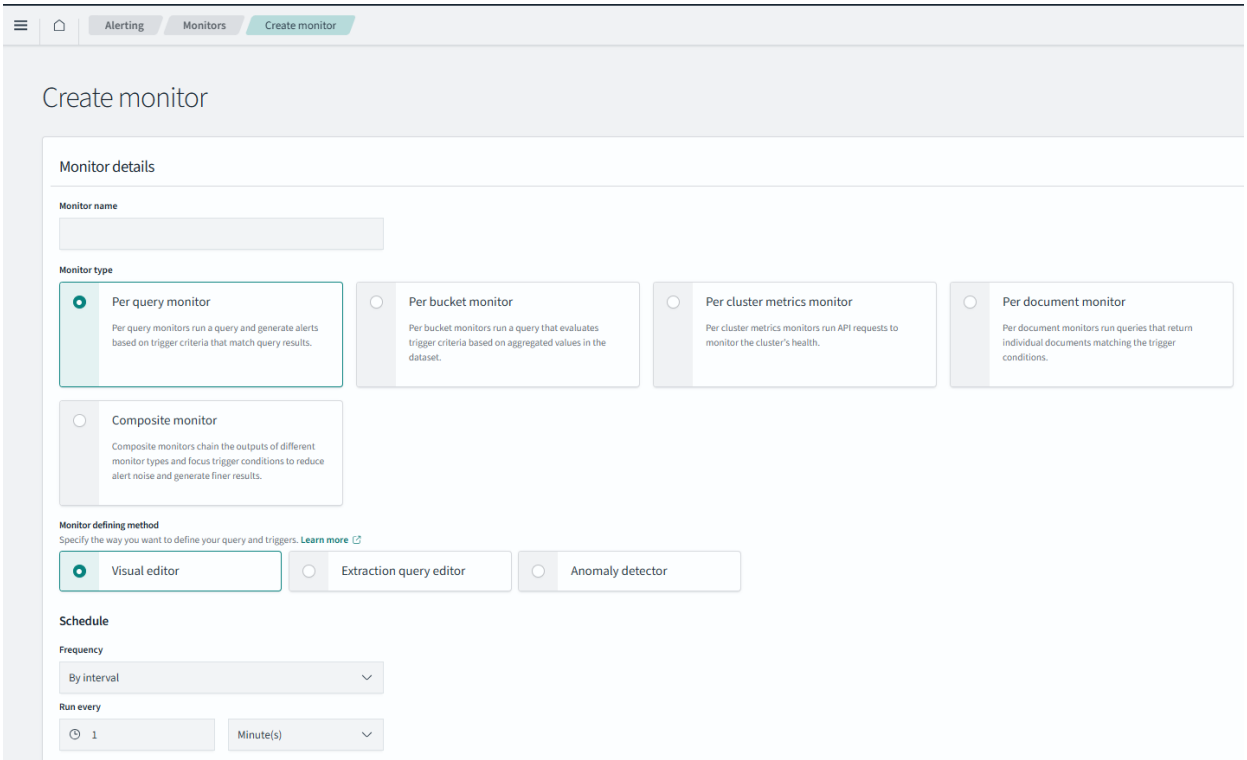

Рисунок 1.67

Интерфейс создания монитора реализует следующие требования по безопасности информации:

– ПО «KeyStack SE» должно:

- обеспечивать регистрацию событий безопасности, связанных с функционированием ПО «KeyStack SE»;
- оповещать администратора безопасности ПО «KeyStack SE» о событиях безопасности;
- выполнять действия, являющиеся реакцией на события безопасности самостоятельно или с применением сертифицированных средств защиты информации;
- осуществлять сбор и хранение записей в журнале событий безопасности, которые позволяют определить, когда и какие действия происходили;
- обеспечивать чтение записей о событиях безопасности, формирование отчетов с учетом заданных критериев отбора, выгрузку (экспорт) данных из журнала событий безопасности ПО «KeyStack SE».

– Регистрация событий безопасности в ПО «KeyStack SE» должна осуществляться с учетом разделов 3 - 6 ГОСТ Р 59548-2022 «Защита информации. Регистрация событий безопасности. Требования к регистрируемой информации».

– Для каждой функции безопасности в ПО «KeyStack SE» должен быть определен перечень событий, необходимых для регистрации и учета.

– Для регистрируемых событий безопасности в каждой записи журнала событий безопасности должны регистрироваться:

- номер (уникальный идентификатор) события, дата, время, тип события безопасности;
- описание события безопасности, включающее сведения о его важности.

– Записи журнала событий безопасности должны представляться в структурированном виде и содержать время события безопасности, взятое из аппаратной платформы или хостовой операционной системы.

– Регистрации подлежат, как минимум, следующие события безопасности:

- успешные и неуспешные попытки аутентификации пользователей ПО «KeyStack SE»;
- доступ пользователей ПО «KeyStack SE» к виртуальным машинам;
- создание и удаление виртуальных машин;
- запуск и остановка ПО «KeyStack SE» с указанием причины остановки;
- запуск и остановка виртуальных машин с указанием причины остановки;
- изменение ролевой модели;
- изменение конфигурации ПО «KeyStack SE»;
- изменение конфигураций виртуальных машин;
- факты нарушения целостности объектов контроля.

Интерфейс позволяет выполнять следующие действия:

– создавать монитор;

– переходить к интерфейсу создания триггера.

В интерфейсе не предусмотрены действия, не влияющие на выполнение требований безопасности к ПО «KeyStack SE».

При вызове указанного интерфейса не предусмотрены ошибки безопасности.

Параметры, используемые интерфейсом создания монитора:

– наименование монитора;

– тип монитора;

– метод определения монитора;

– расписание;

– источник данных;

– запрос;

– триггеры.

Способ использования интерфейса:

– ввод данных в графический пользовательский интерфейс, использование ui элементов (кнопок и списков)

Адрес обработки запроса:

“POST /api/alerting/monitors ”

8.8.10 Интерфейс редактирования монитора

На Рисунке 1.68 приведён интерфейс ПО «OpenSearch Dashboards», назначением которого является реализация требований безопасности, связанных регистрацией событий безопасности. Интерфейс представлен в GUI и используется для редактирования монитора в ПО «OpenSearch Dashboards».

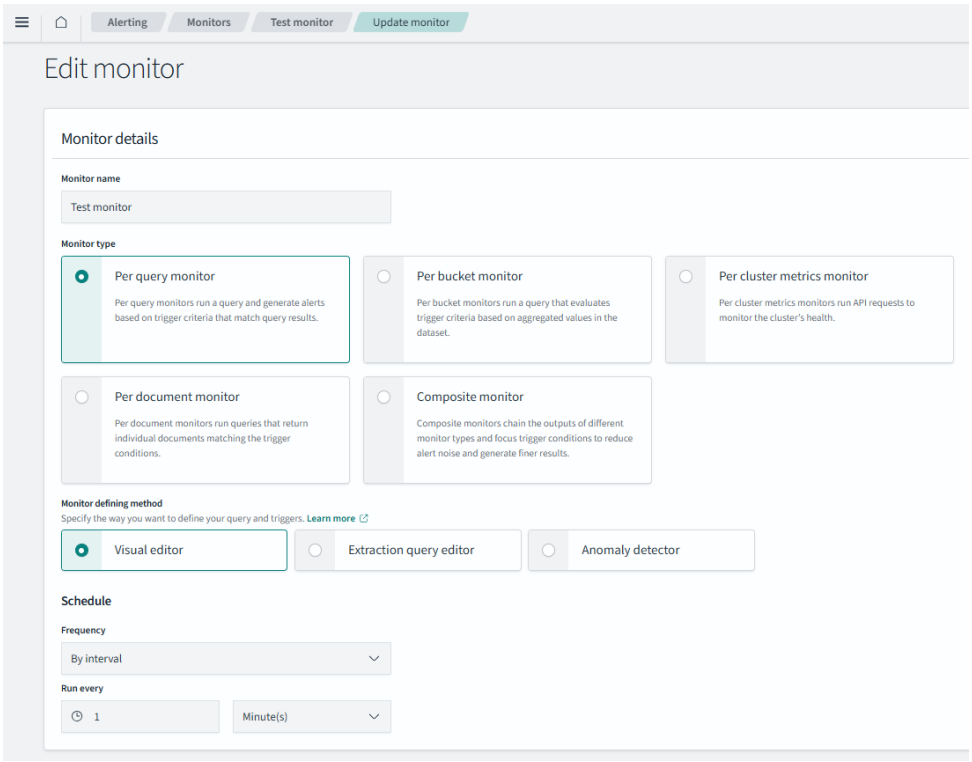

Рисунок 1.68

Интерфейс редактирования монитора реализует следующие требования по безопасности информации:

– ПО «KeyStack SE» должно:

- обеспечивать регистрацию событий безопасности, связанных с функционированием ПО «KeyStack SE»;

- оповещать администратора безопасности ПО «KeyStack SE» о событиях безопасности;
- выполнять действия, являющиеся реакцией на события безопасности самостоятельно или с применением сертифицированных средств защиты информации;
- осуществлять сбор и хранение записей в журнале событий безопасности, которые позволяют определить, когда и какие действия происходили;
- обеспечивать чтение записей о событиях безопасности, формирование отчетов с учетом заданных критериев отбора, выгрузку (экспорт) данных из журнала событий безопасности ПО «KeyStack SE».

– Регистрация событий безопасности в ПО «KeyStack SE» должна осуществляться с учетом разделов 3 - 6 ГОСТ Р 59548-2022 «Защита информации. Регистрация событий безопасности. Требования к регистрируемой информации».

– Для каждой функции безопасности в ПО «KeyStack SE» должен быть определен перечень событий, необходимых для регистрации и учета.

– Для регистрируемых событий безопасности в каждой записи журнала событий безопасности должны регистрироваться:

- номер (уникальный идентификатор) события, дата, время, тип события безопасности;
- описание события безопасности, включающее сведения о его важности.

– Записи журнала событий безопасности должны представляться в структурированном виде и содержать время события безопасности, взятое из аппаратной платформы или хостовой операционной системы.

– Регистрации подлежат, как минимум, следующие события безопасности:

- успешные и неуспешные попытки аутентификации пользователей ПО «KeyStack SE»;
- доступ пользователей ПО «KeyStack SE» к виртуальным машинам;
- создание и удаление виртуальных машин;
- запуск и остановка ПО «KeyStack SE» с указанием причины остановки;
- запуск и остановка виртуальных машин с указанием причины остановки;
- изменение ролевой модели;
- изменение конфигурации ПО «KeyStack SE»;

- изменение конфигураций виртуальных машин;
- факты нарушения целостности объектов контроля.

Интерфейс позволяет выполнять следующие действия:

– редактировать монитор;

– переходить к интерфейсу создания триггера.

В интерфейсе не предусмотрены действия, не влияющие на выполнение требований безопасности к ПО «KeyStack SE».

При вызове указанного интерфейса не предусмотрены ошибки безопасности.

Параметры, используемые интерфейсом редактирования монитора:

– наименование монитора;

– тип монитора;

– метод определения монитора;

– расписание;

– источник данных;

– запрос;

– триггеры.

Способ использования интерфейса:

– ввод данных в графический пользовательский интерфейс, использование ui элементов (кнопок и списков)

Адрес обработки запроса:

“PUT /api/alerting/monitors/{id монитора}?{параметры}”

8.8.11 Интерфейс отключения монитора

На Рисунке 1.69 приведён интерфейс ПО «OpenSearch Dashboards», назначением которого является реализация требований безопасности, связанных регистрацией событий безопасности. Интерфейс представлен в GUI и используется для отключения монитора в ПО «OpenSearch Dashboards».

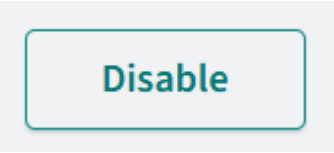

Рисунок 1.69

Интерфейс отключения монитора реализует следующие требования по безопасности информации:

– ПО «KeyStack SE» должно:

- обеспечивать регистрацию событий безопасности, связанных с функционированием ПО «KeyStack SE»;
- оповещать администратора безопасности ПО «KeyStack SE» о событиях безопасности;
- выполнять действия, являющиеся реакцией на события безопасности самостоятельно или с применением сертифицированных средств защиты информации;
- осуществлять сбор и хранение записей в журнале событий безопасности, которые позволяют определить, когда и какие действия происходили;
- обеспечивать чтение записей о событиях безопасности, формирование отчетов с учетом заданных критериев отбора, выгрузку (экспорт) данных из журнала событий безопасности ПО «KeyStack SE».

– Регистрация событий безопасности в ПО «KeyStack SE» должна осуществляться с учетом разделов 3 - 6 ГОСТ Р 59548-2022 «Защита информации. Регистрация событий безопасности. Требования к регистрируемой информации».

– Для каждой функции безопасности в ПО «KeyStack SE» должен быть определен перечень событий, необходимых для регистрации и учета.

– Для регистрируемых событий безопасности в каждой записи журнала событий безопасности должны регистрироваться:

- номер (уникальный идентификатор) события, дата, время, тип события безопасности;
- описание события безопасности, включающее сведения о его важности.

– Записи журнала событий безопасности должны представляться в структурированном виде и содержать время события безопасности, взятое из аппаратной платформы или хостовой операционной системы.

– Регистрации подлежат, как минимум, следующие события безопасности:

- успешные и неуспешные попытки аутентификации пользователей ПО «KeyStack SE»;
- доступ пользователей ПО «KeyStack SE» к виртуальным машинам;
- создание и удаление виртуальных машин;
- запуск и остановка ПО «KeyStack SE» с указанием причины остановки;
- запуск и остановка виртуальных машин с указанием причины остановки;

- изменение ролевой модели;
- изменение конфигурации ПО «KeyStack SE»;
- изменение конфигураций виртуальных машин;
- факты нарушения целостности объектов контроля.

Интерфейс позволяет выполнять следующие действия:

– отключать монитор.

В интерфейсе не предусмотрены действия, не влияющие на выполнение требований безопасности к ПО «KeyStack SE».

При вызове указанного интерфейса не предусмотрены ошибки безопасности.

Параметры интерфейсом отключения монитора не используются.

Способ использования интерфейса:

– использование ui элементов (кнопок)

Адрес обработки запроса:

“PUT /api/alerting/monitors/{id монитора}?{параметры}”

8.8.12 Интерфейс включения монитора

На Рисунке 1.70 приведён интерфейс ПО «OpenSearch Dashboards», назначением которого является реализация требований безопасности, связанных регистрацией событий безопасности. Интерфейс представлен в GUI и используется для включения монитора в ПО «OpenSearch Dashboards».

Рисунок 1.70

Интерфейс включения монитора реализует следующие требования по безопасности информации:

– ПО «KeyStack SE» должно:

- обеспечивать регистрацию событий безопасности, связанных с функционированием ПО «KeyStack SE»;
- оповещать администратора безопасности ПО «KeyStack SE» о событиях безопасности;
- выполнять действия, являющиеся реакцией на события безопасности самостоятельно или с применением сертифицированных средств защиты информации;

- осуществлять сбор и хранение записей в журнале событий безопасности, которые позволяют определить, когда и какие действия происходили;
- обеспечивать чтение записей о событиях безопасности, формирование отчетов с учетом заданных критериев отбора, выгрузку (экспорт) данных из журнала событий безопасности ПО «KeyStack SE».

– Регистрация событий безопасности в ПО «KeyStack SE» должна осуществляться с учетом разделов 3 - 6 ГОСТ Р 59548-2022 «Защита информации. Регистрация событий безопасности. Требования к регистрируемой информации».

– Для каждой функции безопасности в ПО «KeyStack SE» должен быть определен перечень событий, необходимых для регистрации и учета.

– Для регистрируемых событий безопасности в каждой записи журнала событий безопасности должны регистрироваться:

- номер (уникальный идентификатор) события, дата, время, тип события безопасности;
- описание события безопасности, включающее сведения о его важности.

– Записи журнала событий безопасности должны представляться в структурированном виде и содержать время события безопасности, взятое из аппаратной платформы или хостовой операционной системы.

– Регистрации подлежат, как минимум, следующие события безопасности:

- успешные и неуспешные попытки аутентификации пользователей ПО «KeyStack SE»;
- доступ пользователей ПО «KeyStack SE» к виртуальным машинам;
- создание и удаление виртуальных машин;
- запуск и остановка ПО «KeyStack SE» с указанием причины остановки;
- запуск и остановка виртуальных машин с указанием причины остановки;
- изменение ролевой модели;
- изменение конфигурации ПО «KeyStack SE»;
- изменение конфигураций виртуальных машин;
- факты нарушения целостности объектов контроля.

Интерфейс позволяет выполнять следующие действия:

– включать монитор.

В интерфейсе не предусмотрены действия, не влияющие на выполнение требований безопасности к ПО «KeyStack SE».

При вызове указанного интерфейса не предусмотрены ошибки безопасности.

Параметры интерфейсом включения монитора не используются.

Способ использования интерфейса:

– использование ui элементов (кнопок)

Адрес обработки запроса:

“PUT /api/alerting/monitors/{id монитора}?{параметры}”

8.8.13 Интерфейс экспорта монитора

На Рисунке 1.71 приведён интерфейс ПО «OpenSearch Dashboards», назначением которого является реализация требований безопасности, связанных регистрацией событий безопасности. Интерфейс представлен в GUI и используется для экспорта монитора в ПО «OpenSearch Dashboards».

Рисунок 1.71

Интерфейс экспорта монитора реализует следующие требования по безопасности информации:

– ПО «KeyStack SE» должно:

- обеспечивать регистрацию событий безопасности, связанных с функционированием ПО «KeyStack SE»;
- оповещать администратора безопасности ПО «KeyStack SE» о событиях безопасности;
- выполнять действия, являющиеся реакцией на события безопасности самостоятельно или с применением сертифицированных средств защиты информации;
- осуществлять сбор и хранение записей в журнале событий безопасности, которые позволяют определить, когда и какие действия происходили;
- обеспечивать чтение записей о событиях безопасности, формирование отчетов с учетом заданных критериев отбора, выгрузку (экспорт) данных из журнала событий безопасности ПО «KeyStack SE».

– Регистрация событий безопасности в ПО «KeyStack SE» должна осуществляться с учетом разделов 3 - 6 ГОСТ Р 59548-2022 «Защита информации. Регистрация событий безопасности. Требования к регистрируемой информации».

– Для каждой функции безопасности в ПО «KeyStack SE» должен быть определен перечень событий, необходимых для регистрации и учета.

– Для регистрируемых событий безопасности в каждой записи журнала событий безопасности должны регистрироваться:

- номер (уникальный идентификатор) события, дата, время, тип события безопасности;
- описание события безопасности, включающее сведения о его важности.

– Записи журнала событий безопасности должны представляться в структурированном виде и содержать время события безопасности, взятое из аппаратной платформы или хостовой операционной системы.

– Регистрации подлежат, как минимум, следующие события безопасности:

- успешные и неуспешные попытки аутентификации пользователей ПО «KeyStack SE»;
- доступ пользователей ПО «KeyStack SE» к виртуальным машинам;
- создание и удаление виртуальных машин;
- запуск и остановка ПО «KeyStack SE» с указанием причины остановки;
- запуск и остановка виртуальных машин с указанием причины остановки;
- изменение ролевой модели;
- изменение конфигурации ПО «KeyStack SE»;
- изменение конфигураций виртуальных машин;
- факты нарушения целостности объектов контроля.

Интерфейс позволяет выполнять следующие действия:

– экспортировать монитор в json формате.

В интерфейсе не предусмотрены действия, не влияющие на выполнение требований безопасности к ПО «KeyStack SE».

При вызове указанного интерфейса не предусмотрены ошибки безопасности.

Параметры интерфейсом экспорта монитора не используются.

Способ использования интерфейса:

– использование ui элементов (кнопок)

Адрес обработки запроса:

“POST /api/alerting/monitors/{id монитора}”

8.8.14 Интерфейс создания триггера

На Рисунке 1.72 приведён интерфейс ПО «OpenSearch Dashboards», назначением которого является реализация требований безопасности, связанных регистрацией событий безопасности. Интерфейс представлен в GUI и используется для создания триггера в ПО «OpenSearch Dashboards».

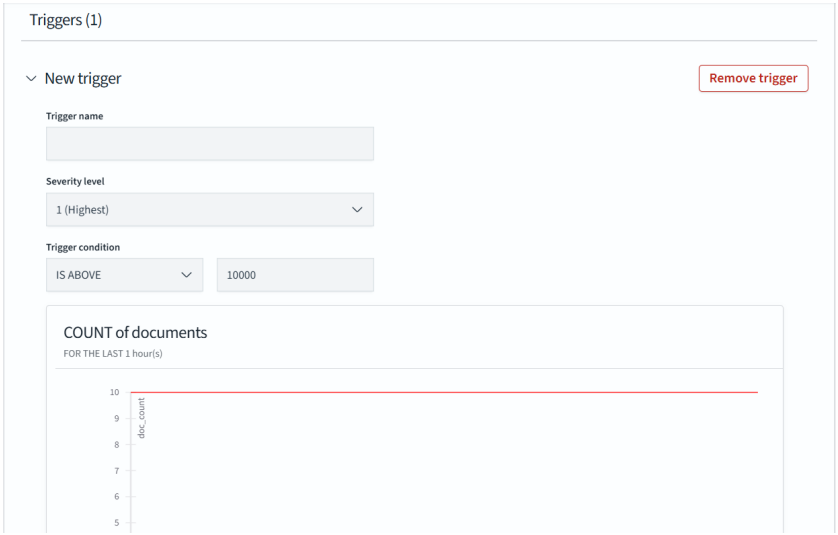

Рисунок 1.72

Интерфейс создания триггера реализует следующие требования по безопасности информации:

– ПО «KeyStack SE» должно:

- обеспечивать регистрацию событий безопасности, связанных с функционированием ПО «KeyStack SE»;
- оповещать администратора безопасности ПО «KeyStack SE» о событиях безопасности;
- выполнять действия, являющиеся реакцией на события безопасности самостоятельно или с применением сертифицированных средств защиты информации;
- осуществлять сбор и хранение записей в журнале событий безопасности, которые позволяют определить, когда и какие действия происходили;
- обеспечивать чтение записей о событиях безопасности, формирование отчетов с учетом заданных критериев отбора, выгрузку (экспорт) данных из журнала событий безопасности ПО «KeyStack SE».

– Регистрация событий безопасности в ПО «KeyStack SE» должна осуществляться с учетом разделов 3 - 6 ГОСТ Р 59548-2022 «Защита информации. Регистрация событий безопасности. Требования к регистрируемой информации».

– Для каждой функции безопасности в ПО «KeyStack SE» должен быть определен перечень событий, необходимых для регистрации и учета.

– Для регистрируемых событий безопасности в каждой записи журнала событий безопасности должны регистрироваться:

- номер (уникальный идентификатор) события, дата, время, тип события безопасности;
- описание события безопасности, включающее сведения о его важности.

– Записи журнала событий безопасности должны представляться в структурированном виде и содержать время события безопасности, взятое из аппаратной платформы или хостовой операционной системы.

– Регистрации подлежат, как минимум, следующие события безопасности:

- успешные и неуспешные попытки аутентификации пользователей ПО «KeyStack SE»;
- доступ пользователей ПО «KeyStack SE» к виртуальным машинам;
- создание и удаление виртуальных машин;
- запуск и остановка ПО «KeyStack SE» с указанием причины остановки;
- запуск и остановка виртуальных машин с указанием причины остановки;
- изменение ролевой модели;
- изменение конфигурации ПО «KeyStack SE»;
- изменение конфигураций виртуальных машин;
- факты нарушения целостности объектов контроля.

Интерфейс позволяет выполнять следующие действия:

- создавать триггер;
- удалять триггер.

В интерфейсе не предусмотрены действия, не влияющие на выполнение требований безопасности к ПО «KeyStack SE».

При вызове указанного интерфейса не предусмотрены ошибки безопасности.

Параметры, используемые интерфейсом создания триггера:

- наименование триггера;
- уровень строгости;

– условия вызова триггера;

– действия триггера.

Способ использования интерфейса:

– ввод данных в графический пользовательский интерфейс, использование ui элементов (кнопок)

Адрес обработки запроса:

“POST /api/alerting/monitors/_execute”

8.8.15 Интерфейс удаления монитора

На Рисунке 1.73 приведён интерфейс ПО «OpenSearch Dashboards», назначением которого является реализация требований безопасности, связанных регистрацией событий безопасности. Интерфейс представлен в GUI и используется для удаления монитора в ПО «OpenSearch Dashboards».

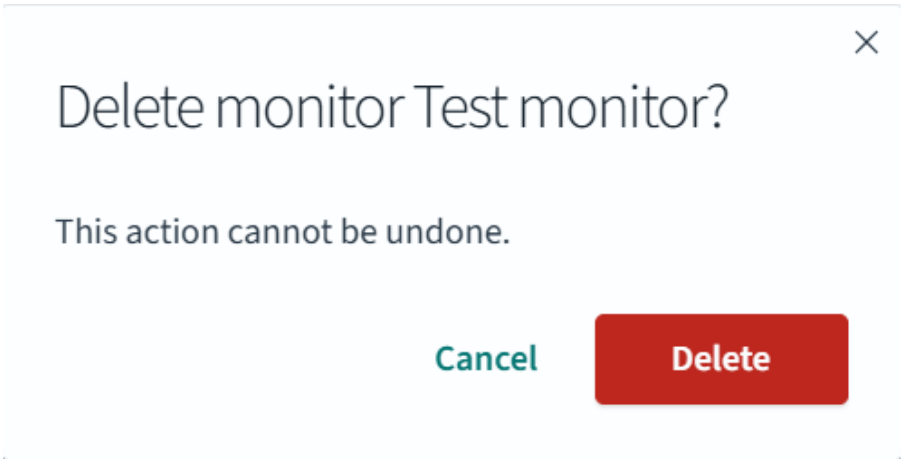

Рисунок 1.73

Интерфейс удаления монитора реализует следующие требования по безопасности информации:

– ПО «KeyStack SE» должно:

- обеспечивать регистрацию событий безопасности, связанных с функционированием ПО «KeyStack SE»;
- оповещать администратора безопасности ПО «KeyStack SE» о событиях безопасности;
- выполнять действия, являющиеся реакцией на события безопасности самостоятельно или с применением сертифицированных средств защиты информации;

- осуществлять сбор и хранение записей в журнале событий безопасности, которые позволяют определить, когда и какие действия происходили;
- обеспечивать чтение записей о событиях безопасности, формирование отчетов с учетом заданных критериев отбора, выгрузку (экспорт) данных из журнала событий безопасности ПО «KeyStack SE».

– Регистрация событий безопасности в ПО «KeyStack SE» должна осуществляться с учетом разделов 3 - 6 ГОСТ Р 59548-2022 «Защита информации. Регистрация событий безопасности. Требования к регистрируемой информации».

– Для каждой функции безопасности в ПО «KeyStack SE» должен быть определен перечень событий, необходимых для регистрации и учета.

– Для регистрируемых событий безопасности в каждой записи журнала событий безопасности должны регистрироваться:

- номер (уникальный идентификатор) события, дата, время, тип события безопасности;
- описание события безопасности, включающее сведения о его важности.

– Записи журнала событий безопасности должны представляться в структурированном виде и содержать время события безопасности, взятое из аппаратной платформы или хостовой операционной системы.

– Регистрации подлежат, как минимум, следующие события безопасности:

- успешные и неуспешные попытки аутентификации пользователей ПО «KeyStack SE»;
- доступ пользователей ПО «KeyStack SE» к виртуальным машинам;
- создание и удаление виртуальных машин;
- запуск и остановка ПО «KeyStack SE» с указанием причины остановки;
- запуск и остановка виртуальных машин с указанием причины остановки;
- изменение ролевой модели;
- изменение конфигурации ПО «KeyStack SE»;
- изменение конфигураций виртуальных машин;
- факты нарушения целостности объектов контроля.

Интерфейс позволяет выполнять следующие действия:

– удалять монитор.

В интерфейсе не предусмотрены действия, не влияющие на выполнение требований безопасности к ПО «KeyStack SE».

При вызове указанного интерфейса не предусмотрены ошибки безопасности.

Параметры, используемые интерфейсом удаления монитора:

– наименование монитора.

Способ использования интерфейса:

– использование ui элементов (кнопок).

Адрес обработки запроса:

“DELETE /api/alerting/monitors/{id монитора}?{параметры}”

8.8.16 Интерфейс подтверждения оповещения

На Рисунке 1.74 приведён интерфейс ПО «OpenSearch Dashboards», назначением которого является реализация требований безопасности, связанных регистрацией событий безопасности. Интерфейс представлен в GUI и используется для подтверждения оповещения в ПО «OpenSearch Dashboards».

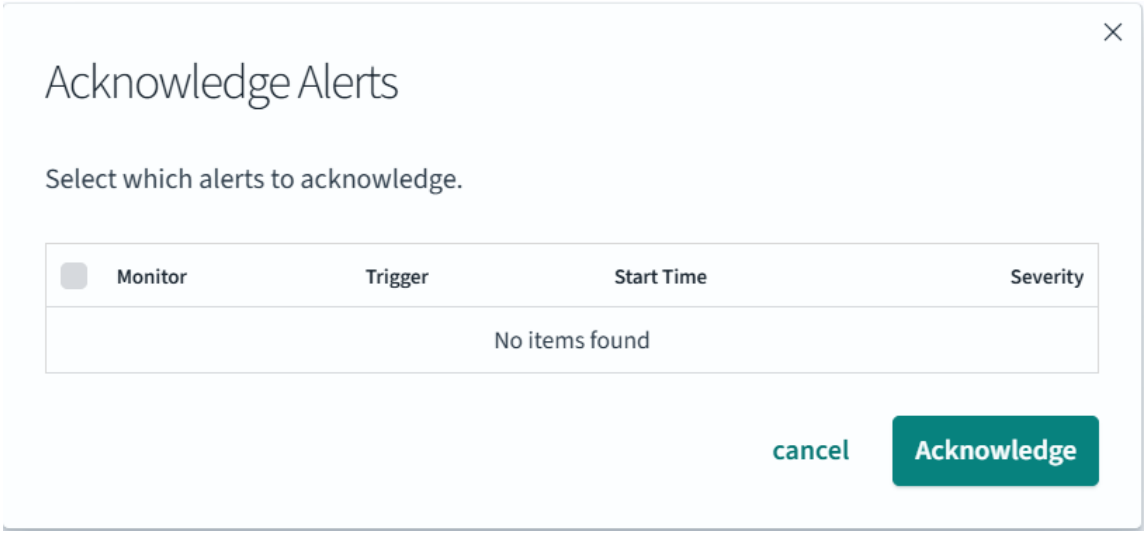

Рисунок 1.74

Интерфейс подтверждения оповещения реализует следующие требования по безопасности информации:

– ПО «KeyStack SE» должно:

- обеспечивать регистрацию событий безопасности, связанных с функционированием ПО «KeyStack SE»;
- оповещать администратора безопасности ПО «KeyStack SE» о событиях безопасности;

- выполнять действия, являющиеся реакцией на события безопасности самостоятельно или с применением сертифицированных средств защиты информации;
- осуществлять сбор и хранение записей в журнале событий безопасности, которые позволяют определить, когда и какие действия происходили;
- обеспечивать чтение записей о событиях безопасности, формирование отчетов с учетом заданных критериев отбора, выгрузку (экспорт) данных из журнала событий безопасности ПО «KeyStack SE».

– Регистрация событий безопасности в ПО «KeyStack SE» должна осуществляться с учетом разделов 3 - 6 ГОСТ Р 59548-2022 «Защита информации. Регистрация событий безопасности. Требования к регистрируемой информации».

– Для каждой функции безопасности в ПО «KeyStack SE» должен быть определен перечень событий, необходимых для регистрации и учета.

– Для регистрируемых событий безопасности в каждой записи журнала событий безопасности должны регистрироваться:

- номер (уникальный идентификатор) события, дата, время, тип события безопасности;
- описание события безопасности, включающее сведения о его важности.

– Записи журнала событий безопасности должны представляться в структурированном виде и содержать время события безопасности, взятое из аппаратной платформы или хостовой операционной системы.

– Регистрации подлежат, как минимум, следующие события безопасности:

- успешные и неуспешные попытки аутентификации пользователей ПО «KeyStack SE»;
- доступ пользователей ПО «KeyStack SE» к виртуальным машинам;
- создание и удаление виртуальных машин;
- запуск и остановка ПО «KeyStack SE» с указанием причины остановки;
- запуск и остановка виртуальных машин с указанием причины остановки;
- изменение ролевой модели;
- изменение конфигурации ПО «KeyStack SE»;
- изменение конфигураций виртуальных машин;
- факты нарушения целостности объектов контроля.

Интерфейс позволяет выполнять следующие действия:

– подтверждать оповещение.

В интерфейсе не предусмотрены действия, не влияющие на выполнение требований безопасности к ПО «KeyStack SE».

При вызове указанного интерфейса не предусмотрены ошибки безопасности.

Параметры, используемые интерфейсом подтверждения оповещения:

– наименование монитора;

– наименование триггера;

– время запуска;

– строгость срабатывания.

Способ использования интерфейса:

– использование ui элементов (кнопок и списков)

Адрес обработки запроса:

“POST /api/alerting/monitors/{id монитора}/_acknowledge/alerts”

8.8.17 Интерфейс просмотра списка каналов уведомлений

На Рисунке 1.75 приведён интерфейс ПО «OpenSearch Dashboards», назначением которого является реализация требований безопасности, связанных регистрацией событий безопасности. Интерфейс представлен в GUI и используется для просмотра списка каналов уведомлений в ПО «OpenSearch Dashboards».

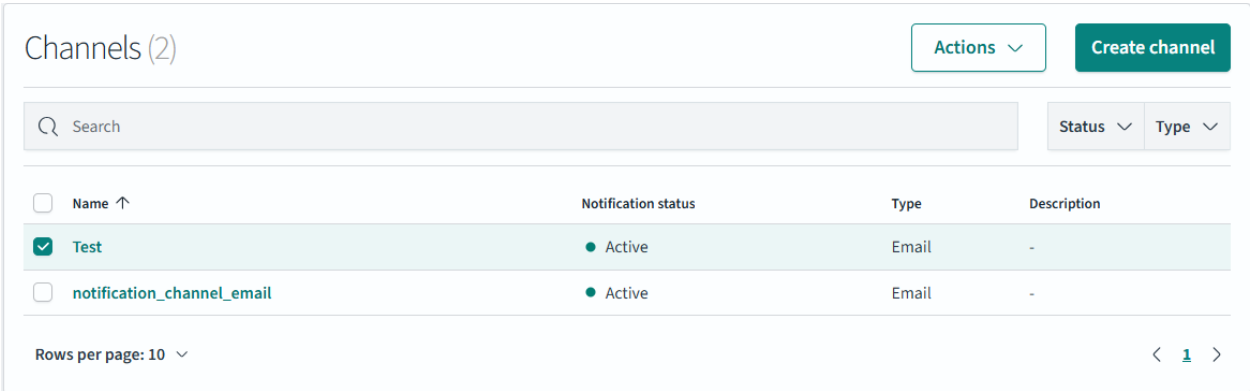

Рисунок 1.75

Интерфейс просмотра списка каналов уведомлений реализует следующие требования по безопасности информации:

– ПО «KeyStack SE» должно:

- обеспечивать регистрацию событий безопасности, связанных с функционированием ПО «KeyStack SE»;

- оповещать администратора безопасности ПО «KeyStack SE» о событиях безопасности;
- выполнять действия, являющиеся реакцией на события безопасности самостоятельно или с применением сертифицированных средств защиты информации;
- осуществлять сбор и хранение записей в журнале событий безопасности, которые позволяют определить, когда и какие действия происходили;
- обеспечивать чтение записей о событиях безопасности, формирование отчетов с учетом заданных критериев отбора, выгрузку (экспорт) данных из журнала событий безопасности ПО «KeyStack SE».

Интерфейс позволяет выполнять следующие действия:

– просматривать список каналов уведомлений;

– переходить к интерфейсам создания, редактирования, удаления, включения и отключения канала уведомлений.

В интерфейсе предусмотрены действия, не влияющие на выполнение требований безопасности к ПО «KeyStack SE»:

– фильтрация списка;

– поиск по наименованию.

При вызове указанного интерфейса не предусмотрены ошибки безопасности.

Параметры, используемые интерфейсом просмотра списка каналов уведомлений:

– наименование канала уведомлений;

– тип канала уведомлений;

– статус канала уведомлений;

– описание.

Способ использования интерфейса:

– ввод данных в графический пользовательский интерфейс, использование ui элементов (кнопок и списков)

Адрес обработки запроса:

“GET /api/notifications/get_configs?{параметры}”

8.8.18 Интерфейс создания канала уведомлений

На Рисунке 1.76 приведён интерфейс ПО «OpenSearch Dashboards», назначением которого является реализация требований безопасности, связанных регистрацией событий

безопасности. Интерфейс представлен в GUI и используется для создания канала уведомлений в ПО «OpenSearch Dashboards».

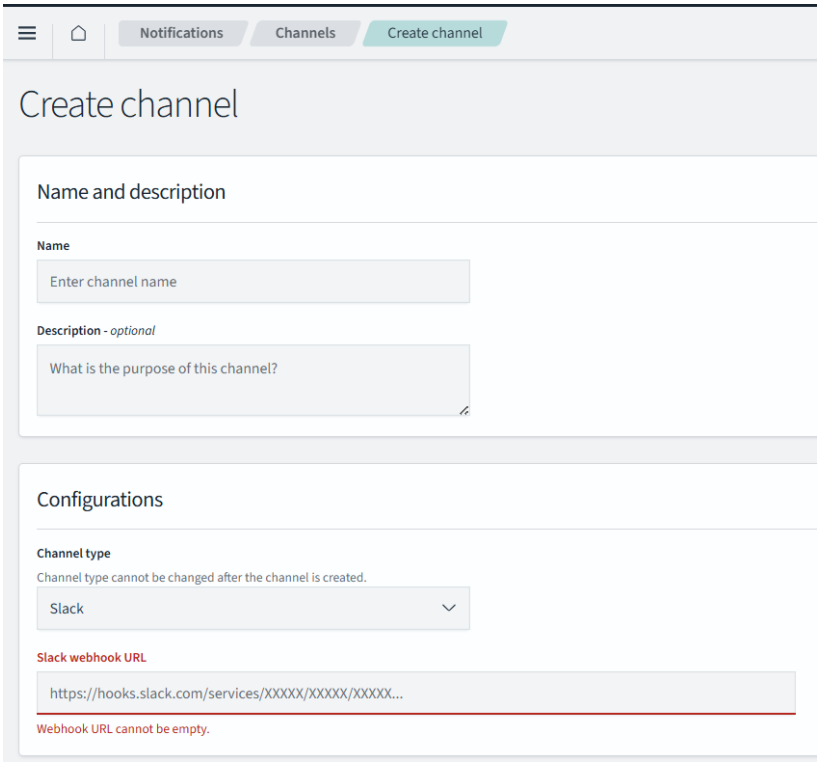

Рисунок 1.76

Интерфейс создания канала уведомлений реализует следующие требования по безопасности информации:

– ПО «KeyStack SE» должно:

- обеспечивать регистрацию событий безопасности, связанных с функционированием ПО «KeyStack SE»;
- оповещать администратора безопасности ПО «KeyStack SE» о событиях безопасности;
- выполнять действия, являющиеся реакцией на события безопасности самостоятельно или с применением сертифицированных средств защиты информации;
- осуществлять сбор и хранение записей в журнале событий безопасности, которые позволяют определить, когда и какие действия происходили;
- обеспечивать чтение записей о событиях безопасности, формирование отчетов с учетом заданных критериев отбора, выгрузку (экспорт) данных из журнала событий безопасности ПО «KeyStack SE».

Интерфейс позволяет выполнять следующие действия:

– создавать канал уведомлений.

В интерфейсе не предусмотрены действия, не влияющие на выполнение требований безопасности к ПО «KeyStack SE».

При вызове указанного интерфейса не предусмотрены ошибки безопасности.

Параметры, используемые интерфейсом создания канала уведомлений:

– наименование канала уведомлений;

– описание канала уведомлений;

– тип канала уведомлений;

– тип отправки уведомлений;

– smtp отправитель;

– получатели по-умолчанию.

Способ использования интерфейса:

– ввод данных в графический пользовательский интерфейс, использование ui элементов (кнопок и списков)

Адрес обработки запроса:

“POST /api/notifications/create_config”

8.8.19 Интерфейс редактирования канала уведомлений

На Рисунке 1.77 приведён интерфейс ПО «OpenSearch Dashboards», назначением которого является реализация требований безопасности, связанных регистрацией событий безопасности. Интерфейс представлен в GUI и используется для редактирования канала уведомлений в ПО «OpenSearch Dashboards».

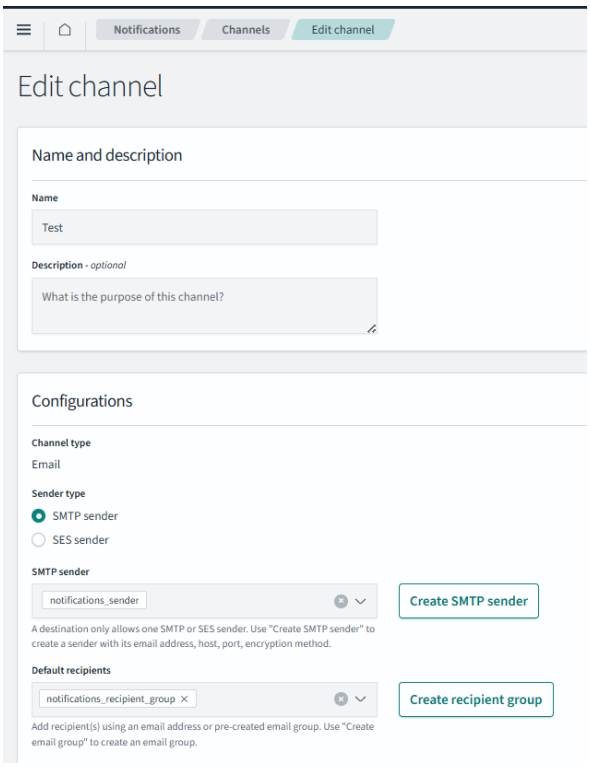

Рисунок 1.77

Интерфейс редактирования канала уведомлений реализует следующие требования по безопасности информации:

– ПО «KeyStack SE» должно:

- обеспечивать регистрацию событий безопасности, связанных с функционированием ПО «KeyStack SE»;
- оповещать администратора безопасности ПО «KeyStack SE» о событиях безопасности;
- выполнять действия, являющиеся реакцией на события безопасности самостоятельно или с применением сертифицированных средств защиты информации;
- осуществлять сбор и хранение записей в журнале событий безопасности, которые позволяют определить, когда и какие действия происходили;
- обеспечивать чтение записей о событиях безопасности, формирование отчетов с учетом заданных критериев отбора, выгрузку (экспорт) данных из журнала событий безопасности ПО «KeyStack SE».

Интерфейс позволяет выполнять следующие действия:

– редактировать канал уведомлений.

В интерфейсе не предусмотрены действия, не влияющие на выполнение требований безопасности к ПО «KeyStack SE».

При вызове указанного интерфейса не предусмотрены ошибки безопасности.

Параметры, используемые интерфейсом редактирования канала уведомлений:

– наименование канала уведомлений;

– описание канала уведомлений;

– тип канала уведомлений;

– тип отправки уведомлений;

– smtp отправитель;

– получатели по-умолчанию.

Способ использования интерфейса:

– ввод данных в графический пользовательский интерфейс, использование ui элементов (кнопок и списков)

Адрес обработки запроса:

“PUT /api/notifications/update_config/{id канала уведомлений}”

8.8.20 Интерфейс отключения канала уведомлений

На Рисунке 1.78 приведён интерфейс ПО «OpenSearch Dashboards», назначением которого является реализация требований безопасности, связанных регистрацией событий безопасности. Интерфейс представлен в GUI и используется для отключения канала уведомлений в ПО «OpenSearch Dashboards».

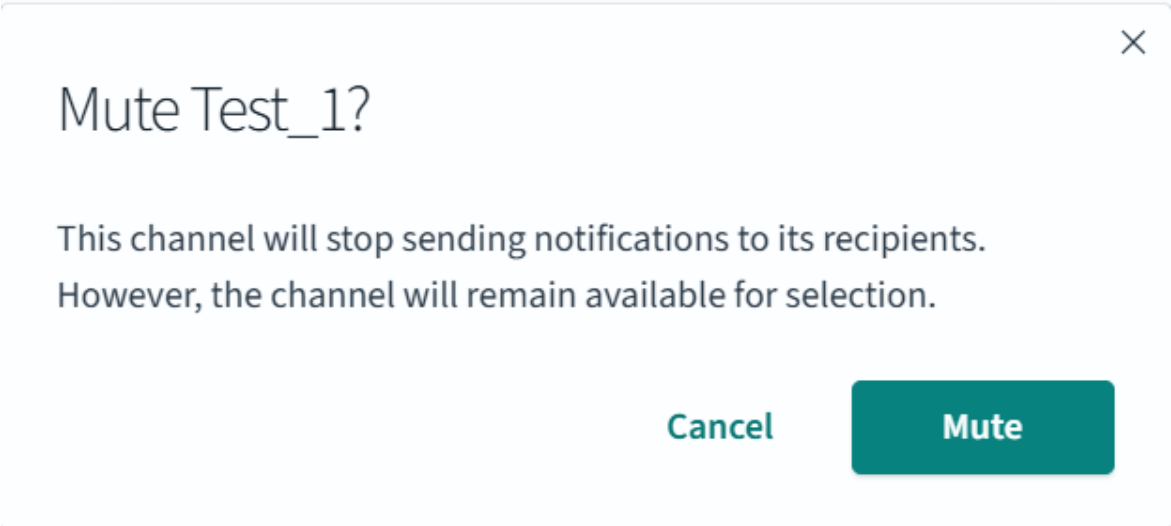

Рисунок 1.78

Интерфейс отключения канала уведомлений реализует следующие требования по безопасности информации:

– ПО «KeyStack SE» должно:

- обеспечивать регистрацию событий безопасности, связанных с функционированием ПО «KeyStack SE»;
- оповещать администратора безопасности ПО «KeyStack SE» о событиях безопасности;
- выполнять действия, являющиеся реакцией на события безопасности самостоятельно или с применением сертифицированных средств защиты информации;
- осуществлять сбор и хранение записей в журнале событий безопасности, которые позволяют определить, когда и какие действия происходили;
- обеспечивать чтение записей о событиях безопасности, формирование отчетов с учетом заданных критериев отбора, выгрузку (экспорт) данных из журнала событий безопасности ПО «KeyStack SE».

Интерфейс позволяет выполнять следующие действия:

– отключать канал уведомлений.

В интерфейсе не предусмотрены действия, не влияющие на выполнение требований безопасности к ПО «KeyStack SE».

При вызове указанного интерфейса не предусмотрены ошибки безопасности.

Параметры, используемые интерфейсом отключения канала уведомлений:

– наименование канала уведомлений.

Способ использования интерфейса:

– использование ui элементов (кнопок)

Адрес обработки запроса:

“PUT /api/notifications/update_config/{id канала уведомлений}”

8.8.21 Интерфейс включения канала уведомлений

На Рисунке 1.79 приведён интерфейс ПО «OpenSearch Dashboards», назначением которого является реализация требований безопасности, связанных регистрацией событий безопасности. Интерфейс представлен в GUI и используется для включения канала уведомлений в ПО «OpenSearch Dashboards».

Рисунок 1.79

Интерфейс включения канала уведомлений реализует следующие требования по безопасности информации:

– ПО «KeyStack SE» должно:

- обеспечивать регистрацию событий безопасности, связанных с функционированием ПО «KeyStack SE»;
- оповещать администратора безопасности ПО «KeyStack SE» о событиях безопасности;
- выполнять действия, являющиеся реакцией на события безопасности самостоятельно или с применением сертифицированных средств защиты информации;
- осуществлять сбор и хранение записей в журнале событий безопасности, которые позволяют определить, когда и какие действия происходили;
- обеспечивать чтение записей о событиях безопасности, формирование отчетов с учетом заданных критериев отбора, выгрузку (экспорт) данных из журнала событий безопасности ПО «KeyStack SE».

Интерфейс позволяет выполнять следующие действия:

– включать канал уведомлений.

В интерфейсе не предусмотрены действия, не влияющие на выполнение требований безопасности к ПО «KeyStack SE».

При вызове указанного интерфейса не предусмотрены ошибки безопасности.

Параметры интерфейсом включения канала уведомлений не используются.

Способ использования интерфейса:

– использование ui элементов (кнопок)

Адрес обработки запроса:

“PUT /api/notifications/update_config/{id канала уведомлений}”

8.8.22 Интерфейс удаления канала уведомлений

На Рисунке 1.80 приведён интерфейс ПО «OpenSearch Dashboards», назначением которого является реализация требований безопасности, связанных регистрацией событий безопасности. Интерфейс представлен в GUI и используется для удаления канала уведомлений в ПО «OpenSearch Dashboards».

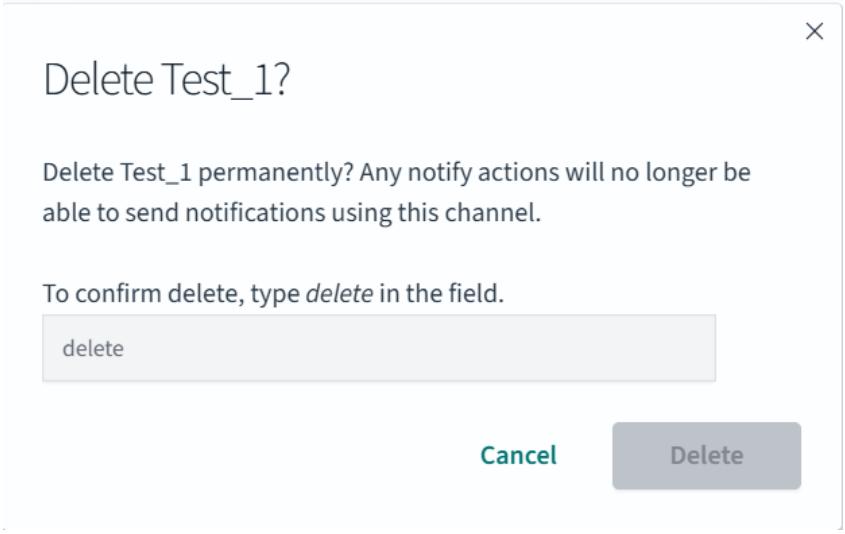

Рисунок 1.80

Интерфейс удаления канала уведомлений реализует следующие требования по безопасности информации:

– ПО «KeyStack SE» должно:

- обеспечивать регистрацию событий безопасности, связанных с функционированием ПО «KeyStack SE»;
- оповещать администратора безопасности ПО «KeyStack SE» о событиях безопасности;
- выполнять действия, являющиеся реакцией на события безопасности самостоятельно или с применением сертифицированных средств защиты информации;
- осуществлять сбор и хранение записей в журнале событий безопасности, которые позволяют определить, когда и какие действия происходили;
- обеспечивать чтение записей о событиях безопасности, формирование отчетов с учетом заданных критериев отбора, выгрузку (экспорт) данных из журнала событий безопасности ПО «KeyStack SE».

Интерфейс позволяет выполнять следующие действия:

– удалять канал уведомлений.

В интерфейсе не предусмотрены действия, не влияющие на выполнение требований безопасности к ПО «KeyStack SE».

При вызове указанного интерфейса не предусмотрены ошибки безопасности.

Параметры, используемые интерфейсом удаления канала уведомлений:

– наименование канала уведомлений;

– слово для подтверждения удаления.

Способ использования интерфейса:

– ввод данных в графический пользовательский интерфейс, использование ui элементов (кнопок)

Адрес обработки запроса:

“DELETE /api/notifications/delete_configs?{параметры}”

8.9 Интерфейсы модуля KeyStone

В Таблице 1 приведены интерфейсы модуля KeyStone, назначением которых является, в том числе, реализация требований безопасности, связанных с идентификацией и аутентификацией пользователей, регистрацией событий безопасности и управлением доступом в ПО «KeyStack SE». Интерфейсы представлены API и могут быть использованы посредством применения вызовов по протоколу REST API.

Таблица 1 – Интерфейсы модуля KeyStone и их назначение

Интерфейсы		Является ли ИФБО применительно к ОО	Назначение	Комментарий
Аутентификация и управление токенами	POST /v3/auth/tokens	ИФБО	Аутентификация по паролю с неограниченной (базовой) авторизацией	Интерфейс доступный внешним пользователям (Интерфейс идентификации и аутентификации пользователя Портала Администрирования)
			Аутентификация по паролю с ограниченной авторизацией (детальный доступ к данным)	
			Аутентификация по паролю с явным указанием области базовой авторизации	
			Аутентификация по токену с неограниченной (базовой) авторизацией	
			Аутентификация по токену с ограниченной авторизацией (детальный доступ к данным)	
			Аутентификация по токену с явным указанием области авторизации	
			Многоступенчатая аутентификация (двухфакторная: пароль и одноразовый код)	

	GET /v3/auth/tokens	ИФБО	Подтверждение и отображение информации для токена	Интерфейс межмодульного взаимодействия
	HEAD /v3/auth/tokens	ИФБО	Проверка токена	Интерфейс межмодульного взаимодействия
	DELETE /v3/auth/tokens	ИФБО	Отозвать токен	Интерфейс межмодульного взаимодействия
	GET /v3/auth/projects	ИФБО	Получить доступные проекты	Интерфейс межмодульного взаимодействия
	GET /v3/auth/domains	ИФБО	Получить доступные домены	Интерфейс межмодульного взаимодействия
	GET /v3/auth/system	ИФБО	Получить доступные системы	Интерфейс межмодульного взаимодействия
Учетные данные	POST /v3/credentials		Создание учетных данных	
	GET /v3/credentials		Список учетных данных	
	GET /v3/credentials/{credential_id}		Показать сведения об учетных данных	
	PATCH /v3/credentials/{credential_id}		Обновить учетные данные	
	DELETE /v3/credentials/{credential_id}		Удалить учетные данные	
Домены	GET /v3/domains		Список доменов	
	POST /v3/domains		Создать домен	
	GET /v3/domains/{domain_id}		Показать сведения о домене	

	PATCH /v3/domains/{domain_id}		Обновить домен	
	DELETE /v3/domains/{domain_id}		Удалить домен	
Конфигурация домена	GET /v3/domains/config/default		Показать параметры конфигурации по умолчанию	
	GET /v3/domains/config/{group}/default		Показать конфигурацию по умолчанию для группы	
	GET /v3/domains/config/{group}/{option}/default		Показать параметр по умолчанию для группы	
	GET /v3/domains/{domain_id}/config/{group}/{option}		Показать конфигурацию параметров для группы пользователей домена	
	PATCH /v3/domains/{domain_id}/config/{group}/{option}		Обновить конфигурацию параметров для группы пользователей домена	
	DELETE /v3/domains/{domain_id}/config/{group}/{option}		Удалить конфигурацию параметров для группы пользователей домена	
	GET /v3/domains/{domain_id}/config/{group}		Показать конфигурацию группы пользователей домена	
	PATCH /v3/domains/{domain_id}/config/{group}		Обновить конфигурацию группы пользователей домена	
	DELETE /v3/domains/{domain_id}/config/{group}		Удалить конфигурацию группы пользователей домена	
	PUT /v3/domains/{domain_id}/config		Создать конфигурацию домена	
	GET /v3/domains/{d		Показать конфигурацию домена	

	omain_id}/config			
	PATCH /v3/domains/{domain_id}/config		Обновить конфигурацию домена	
	DELETE /v3/domains/{domain_id}/config		Удалить конфигурацию домена	
Группы	GET /v3/groups		Список групп	
	POST /v3/groups		Создать группу	
	GET /v3/groups/{group_id}		Показать сведения о группе	
	PATCH /v3/groups/{group_id}		Обновить группу	
	DELETE /v3/groups/{group_id}		Удалить группу	
	GET /v3/groups/{group_id}/users		Список пользователей группы	
	PUT /v3/groups/{group_id}/users/{user_id}		Добавить пользователя в группу	
	HEAD /v3/groups/{group_id}/users/{user_id}		Проверить принадлежность пользователя к группе	
	DELETE /v3/groups/{group_id}/users/{user_id}		Исключить пользователя из группы	
Расширение OS-INHERIT (позволяет проектам наследовать назначения ролей либо от принадлежащего им домена, либо от проектов,	PUT /v3/OS-INHERIT/domains/{domain_id}/users/{user_id}/roles/{role_id}/inherited_to_projects		Назначить роль пользователю в проектах, принадлежащих домену	
	PUT /v3/OS-INHERIT/domains/{domain_i		Назначить роль группе в проектах, принадлежащих домену	

стоящих выше в иерархии)	d}/groups/{group_id}/roles/{role_id}/inherited_to_projects			
	GET /v3/OS-INHERIT/domains/{domain_id}/users/{user_id}/roles/inherited_to_projects		Список унаследованных проектных ролей пользователя в домене	
	GET /v3/OS-INHERIT/domains/{domain_id}/groups/{group_id}/roles/inherited_to_projects		Список унаследованных проектных ролей групп в домене	
	HEAD /v3/OS-INHERIT/domains/{domain_id}/users/{user_id}/roles/{role_id}/inherited_to_projects		Проверить, есть ли у пользователя унаследованная роль проекта в домене	
	HEAD /v3/OS-INHERIT/domains/{domain_id}/groups/{group_id}/roles/{role_id}/inherited_to_projects		Проверить, есть ли у группы унаследованная роль проекта в домене	
	DELETE /v3/OS-INHERIT/domains/{domain_id}/users/{user_id}/roles/{role_id}/inherited_to_projects		Отозвать унаследованную роль проекта у пользователя в домене	
	DELETE /v3/OS-INHERIT/domains/{domain_id}/groups/{group_id}/roles/{role_id}/inherited_to_projects		Отозвать унаследованную роль проекта у группы в домене	

	PUT /v3/OS-INHERIT/projects/{project_id}/users/{user_id}/roles/{role_id}/inherited_to_projects		Назначить роль пользователю в проектах в ветке	
	PUT /v3/OS-INHERIT/projects/{project_id}/groups/{group_id}/roles/{role_id}/inherited_to_projects		Назначить роль группе в проектах в ветке	
	HEAD /v3/OS-INHERIT/projects/{project_id}/users/{user_id}/roles/{role_id}/inherited_to_projects		Проверить, есть ли у пользователя унаследованная проектная роль в проекте	
	HEAD /v3/OS-INHERIT/projects/{project_id}/groups/{group_id}/roles/{role_id}/inherited_to_projects		Проверить, есть ли у группы унаследованная проектная роль в проекте	
	DELETE /v3/OS-INHERIT/projects/{project_id}/users/{user_id}/roles/{role_id}/inherited_to_projects		Отозвать унаследованную проектную роль у пользователя в проекте	
	DELETE /v3/OS-INHERIT/projects/{project_id}/groups/{group_id}/roles/{role_id}/inherited_to_projects		Отозвать унаследованную проектную роль у группы в проекте	
	GET /v3/role_assignments		Список назначений ролей	

OS-PKI (Public Key Infrastructure) Инфраструктура открытых ключей	GET /v3/auth/tokens/OS-PKI/revoked		Список отозванных токенов	
Политики	POST /v3/policies		Создать политику	
	GET /v3/policies		Список политик	
	GET /v3/policies/{policy_id}		Показать сведения о политике	
	PATCH /v3/policies/{policy_id}		Обновить политику	
	DELETE /v3/policies/{policy_id}		Удалить политику	
Проекты	GET /v3/projects		Список проектов	
	POST /v3/projects		Создать проект	
	GET /v3/projects/{project_id}		Показать сведения о проектах	
	PATCH /v3/projects/{project_id}		Обновить проект	
	DELETE /v3/projects/{project_id}		Удалить проект	
Теги для проекта	GET /v3/projects/{project_id}/tags		Список тегов для проекта	
	PUT /v3/projects/{project_id}/tags		Изменить список тегов для проекта	
	DELETE /v3/projects/{project_id}/tags		Удалить все теги для проекта	
	GET /v3/projects/{project_id}/tags/{value}		Проверить, содержит ли проект тег	
	PUT /v3/projects/{project_id}/tags/{value}		Добавить одиночный тег в проект	

	DELETE /v3/projects/{project_id}/tags/{value}		Удалить одиночный тег из проекта	
Регионы	GET /v3/regions/{region_id}		Показать сведения о регионе	
	PATCH /v3/regions/{region_id}		Обновить регион	
	DELETE /v3/regions/{region_id}		Удалить регион	
	GET /v3/regions		Список регионов	
	POST /v3/regions		Создать регион	
Роли	GET /v3/roles	ИФБО	Список ролей	Интерфейс межмодульного взаимодействия
	POST /v3/roles	ИФБО	Создать роль	Интерфейс межмодульного взаимодействия
	GET /v3/roles/{role_id}	ИФБО	Показать сведения о роли	Интерфейс межмодульного взаимодействия
	PATCH /v3/roles/{role_id}	ИФБО	Обновить роль	Интерфейс межмодульного взаимодействия
	DELETE /v3/roles/{role_id}	ИФБО	Удалить роль	Интерфейс межмодульного взаимодействия
	GET /v3/domains/{domain_id}/groups/{group_id}/roles		Список назначений ролей для группы в домене	
	PUT /v3/domains/{domain_id}/gro		Назначить роль для группы в домене	

	ups/{group_id}/roles/{role_id}			
	HEAD /v3/domains/{domain_id}/groups/{group_id}/roles/{role_id}		Проверить, назначена ли группе роль в домене	
	DELETE /v3/domains/{domain_id}/groups/{group_id}/roles/{role_id}		Отменить назначение роли для группы в домене	
	GET /v3/domains/{domain_id}/users/{user_id}/roles	ИФБО	Список назначенных для пользователя ролей в домене	Интерфейс межмодульного взаимодействия
	PUT /v3/domains/{domain_id}/users/{user_id}/roles/{role_id}	ИФБО	Назначить роль пользователю в домене	Интерфейс межмодульного взаимодействия
	HEAD /v3/domains/{domain_id}/users/{user_id}/roles/{role_id}	ИФБО	Проверить, назначена ли пользователю роль в домене	Интерфейс межмодульного взаимодействия
	DELETE /v3/domains/{domain_id}/users/{user_id}/roles/{role_id}	ИФБО	Отменить назначение роли для пользователя в домене	Интерфейс межмодульного взаимодействия
	GET /v3/projects/{project_id}/groups/{group_id}/roles		Список назначенных для группы ролей в проекте	
	PUT /v3/projects/{project_id}/groups/{group_id}/roles/{role_id}		Назначить роль для группы в проекте	
	HEAD /v3/projects/{project_id}/groups/{group_id}/roles/{role_id}		Проверить, назначена ли для группы роль в проекте	

	DELETE /v3/projects/{project_id}/groups/{group_id}/roles/{role_id}		Отменить назначение роли для группы в проекте	
	GET /v3/projects/{project_id}/users/{user_id}/roles		Список назначенных для пользователя ролей в проекте	
	PUT /v3/projects/{project_id}/users/{user_id}/roles/{role_id}		Назначить роль для пользователя в проекте	Интерфейс доступный внешним пользователям(Интерфейс изменения роли Портала Администрирования)
	HEAD /v3/projects/{project_id}/users/{user_id}/roles/{role_id}		Проверить, назначена ли для пользователя роль в проекте	
	DELETE /v3/projects/{project_id}/users/{user_id}/roles/{role_id}		Отменить назначение роли для пользователя в проекте	
	GET /v3/roles/{prior_role_id}/implies		Список подразумеваемых (логический вывод) правил для роли	
	PUT /v3/roles/{prior_role_id}/implies/{implied_role_id}		Создать правило вывода роли	
	GET /v3/roles/{prior_role_id}/implies/{implied_role_id}		Получить правило вывода роли	
	HEAD /v3/roles/{prior_role_id}/implies/{implied_role_id}		Подтвердить правило вывода роли	
	DELETE /v3/roles/{prior_role_id}/impli		Удалить правило вывода роли	

	es/{implied_role_id}			
	GET /v3/role_assignments		Список назначений роли	
	GET /v3/role_inferences		Список всех правил вывода роли	
Назначение системных ролей	GET /v3/system/users/{user_id}/roles		Список системных ролей, назначенных пользователю	
	PUT /v3/system/users/{user_id}/roles/{role_id}		Назначение системной роли пользователю	
	HEAD /v3/system/users/{user_id}/roles/{role_id}		Проверить пользователя на предмет назначения системной роли	
	GET /v3/system/users/{user_id}/roles/{role_id}		Получить назначение системной роли для пользователя	
	DELETE /v3/system/users/{user_id}/roles/{role_id}		Удалить назначение системной роли для пользователя	
	GET /v3/system/groups/{group_id}/roles		Список назначений системных ролей для группы	
	PUT /v3/system/groups/{group_id}/roles/{role_id}		Назначить системную роль группе	
	HEAD /v3/system/groups/{group_id}/roles/{role_id}		Проверить группу на предмет назначения системной роли	
	GET /v3/system/groups/{group_id}/roles/{role_id}		Получить назначение системной роли для группы	
	DELETE /v3/system/groups/{group_id}/roles/{role_id}		Удалить назначение системной роли для группы	
	GET /v3/services		Список сервисов	

Каталог сервисов и конечные точки	POST /v3/services		Создать сервис	
	GET /v3/services/{service_id}		Показать сведения о сервисе	
	PATCH /v3/services/{service_id}		Обновить сервис	
	DELETE /v3/services/{service_id}		Удалить сервис	
	GET /v3/endpoints		Список конечных точек	
	POST /v3/endpoints		Создать конечную точку	
	GET /v3/endpoints/{endpoint_id}		Показать сведения о конечной точке	
	PATCH /v3/endpoints/{endpoint_id}		Обновить конечную точку	
	DELETE /v3/endpoints/{endpoint_id}		Удалить конечную точку	
Унифицированные ограничения	GET /v3/registered_limits		Список зарегистрированных ограничений	
	POST /v3/registered_limits		Создать зарегистрированные ограничения	
	PATCH /v3/registered_limits/{registered_limit_id}		Обновить зарегистрированные ограничения	
	GET /v3/registered_limits/{registered_limit_id}		Показать сведения о зарегистрированных ограничениях	
	DELETE /v3/registered_limits/{registered_limit_id}		Удалить зарегистрированное ограничение	
	GET /v3/limits/model		Получить модель исполнения (правоприменения)	
	GET /v3/limits		Список ограничений	
	POST /v3/limits		Создать ограничения	

	PATCH /v3/limits/{limit_id}		Обновить ограничение	
	GET /v3/limits/{limit_id}		Показать сведения об ограничениях	
	DELETE /v3/limits/{limit_id}		Удалить ограничение	
Пользователи	GET /v3/users	ИФБО	Список пользователей	Интерфейс межмодульного взаимодействия
	POST /v3/users	ИФБО	Создать пользователя	Интерфейс доступный внешним пользователям (Интерфейс создания пользователя Портала Администрирования)
	GET /v3/users/{user_id}		Показать сведения о пользователе	
	PATCH /v3/users/{user_id}	ИФБО	Обновить пользователя	Интерфейс доступный внешним пользователям (Интерфейс редактирования пользователя Портала Администрирования)
	DELETE /v3/users/{user_id}	ИФБО	Удалить пользователя	Интерфейс доступный внешним пользователям (Интерфейс удаления пользователя Портала Администрирования)
	GET /v3/users/{user_id}/groups		Список групп, к которым принадлежит пользователь	

	GET /v3/users/{user_id}/projects		Список проектов для пользователя	
	POST /v3/users/{user_id}/password	ИФБО	Сменить пароль пользователю	Интерфейс доступный внешним пользователям (Интерфейс изменения пароля пользователя)

Для данных интерфейсов параметры указаны в электронном приложении к документу «Программное обеспечение «Облачная платформа KeyStack SE v.1». Руководство пользователя» (Каталог – «Электронное приложение» – «Интерфейсы» – «интерфейсы_keystone_v3.14.yaml»). Для поиска параметров в электронном приложении необходимо выполнить команду Ctrl + F и ввести в строку поиска API, после чего в файле будет найдено указанное API и приведены его параметры.

8.10 Интерфейсы модуля Nova

В Таблице 2 приведены интерфейсы модуля Nova, назначением которых является, в том числе, реализация требований безопасности, связанных с централизованным управлением образами виртуальных машин и виртуальными машинами в ПО «KeyStack SE». Интерфейсы представлены API и могут быть использованы посредством применения вызовов по протоколу REST API.

Таблица 2 – Интерфейсы модуля Nova и их назначение

Интерфейсы		Является ли ИФБО применительно к ОО	Назначение	Комментарий
Версии API	GET /{v2.1}/		Показать сведения о конкретной версии API	
Серверы	GET /servers	ИФБО	Список серверов	Интерфейс межмодульного взаимодействия
	POST /servers	ИФБО	Создать сервер	Интерфейс доступный внешним пользователям (Интерфейс создания виртуальной машины Портала Администрирования)
	POST /servers	ИФБО	Создать множество серверов	Интерфейс межмодульного взаимодействия
	GET /servers/detail	ИФБО	Подробный список серверов	Интерфейс межмодульного взаимодействия

	GET /servers/{id}	ИФБО	Показать сведения о сервере	Интерфейс межмодульного взаимодействия
	PUT /servers/{id}	ИФБО	Обновить сервер	Интерфейс доступный внешним пользователям (Интерфейс изменения виртуальной машины Портала Администрирования)
	DELETE /servers/{id}	ИФБО	Удалить сервер	Интерфейс доступный внешним пользователям (Интерфейс удаления виртуальной машины Портала Администрирования)
Серверы - выполнить действие	POST /servers/{id}/ action	ИФБО	Добавить (связать) Плавающий Ip-адрес (действие addFloatingIp)	Интерфейс межмодульного взаимодействия
		ИФБО	Добавить группу безопасности на сервер (Действие addSecurityGroup)	Интерфейс межмодульного взаимодействия
			Изменить пароль администратора (Действие ChangePassword)	
			Подтвердить изменение размера сервера (действие confirmResize)	
			Создать резервную копию сервера (действие createBackup)	
			Создать образ (действие createImage)	
			Блокировка сервера (действие lock)	
			Приостановить сервер (действие pause)	
		ИФБО	Перезагрузка сервера (Действие reboot)	Интерфейс доступный внешним пользователям (Интерфейс просмотра списка виртуальных машин Портала Администрирования)

			Пересобрать сервер (Действие rebuild)	
		ИФБО	Удалить (отсоединить) плавающий IP-адрес (действие removeFloatingIp)	Интерфейс межмодульного взаимодействия
		ИФБО	Удалить группу безопасности с сервера (действие removeSecurityGroup)	Интерфейс межмодульного взаимодействия
		ИФБО	Перевести сервер в режим восстановления (действие rescue)	Интерфейс межмодульного взаимодействия
			Изменение размера сервера (действие resize)	
			Возобновить работу приостановленного сервера (действие resume)	
			Отменить изменение размера сервера (действие revertResize)	
			Запуск сервера (действие os-start)	
			Остановка сервера (действие os-stop)	
			Приостановить сервер (suspend действие)	
			Разблокировать сервер (действие unlock)	
			Снять паузу с приостановленного сервера (действие unpause)	
			Восстановить сервер (действие unrescue)	
		ИФБО	Добавить (связать) фиксированный IP-адрес (действие addFixedIp)	Интерфейс межмодульного взаимодействия
		ИФБО	Удалить (отсоединить) фиксированный IP-адрес (действие removeFixedIp)	Интерфейс межмодульного взаимодействия
			Сервер принудительного удаления (действие forceDelete)	

			Восстановить обратимо удаленный экземпляр (действие restore)	
			Показать вывод консоли (действие os-getConsoleOutput)	
			Отложить сервер (действие shelve)	
			Отложить в архив сервер (действие shelveOffload)	
			Восстановить отложенный сервер (действие unshelve)	
			Запуск аварийного дампа на сервере	
			Получить последовательную консоль (действие os-getSerialConsole)	
			Получить SPICE консоль (протокол удалённого доступа) (действие os-getSPICEConsole)	
		ИФБО	Получить VNC консоль (инструмент диагностики и управления виртуальными машинами) (действие os-getVNCConsole)	Интерфейс межмодульного взаимодействия
Серверы - выполнить административное действие	POST /servers/{id}/action	ИФБО	Внедрение информации о сети (действие injectNetworkInfo)	Интерфейс межмодульного взаимодействия
		ИФБО	Переместить сервер (действие migrate)	Интерфейс доступный внешним пользователям (Интерфейс оперативной миграции виртуальной машины)

			Оперативное перемещение сервера (действие os-migrateLive)	
			Сбросить сетевое взаимодействие на сервере (действие resetNetwork)	
		ИФБО	Сброс состояния сервера (действие os-resetState)	Интерфейс межмодульного взаимодействия
		ИФБО	Эвакуировать сервер (Действие evacuate)	Интерфейс доступный внешним пользователям (Интерфейс просмотра списка виртуальных машин)
Серверные консоли	POST /servers/{server_id}/remote-consoles	ИФБО	Создать консоль	Интерфейс межмодульного взаимодействия
	GET /os-console-auth-tokens/{id}		Показать информацию о подключении к консоли	
Группы безопасности серверов	GET /servers/{server_id}/os-security-groups	ИФБО	Список групп безопасности по серверам	Интерфейс межмодульного взаимодействия
Диагностика сервера	GET /servers/{server_id}/diagnostics	ИФБО	Показать диагностику сервера	Интерфейс межмодульного взаимодействия
IP-адреса серверов	GET /servers/{server_id}/ips	ИФБО	Список Ip-адресов	Интерфейс межмодульного взаимодействия
	GET /servers/{server_id}/ips/{id}		Показать сведения об Ip-адресе	
Метаданные сервера	GET /servers/{server_id}/metadata	ИФБО	Список всех Метаданных сервера	Интерфейс межмодульного взаимодействия
	POST /servers/{server_id}/metadata	ИФБО	Создание или обновление элементов Метаданных	Интерфейс межмодульного взаимодействия

	PUT /servers/{server_id}/metadata	ИФБО	Заменить элементы Метаданных сервера	Интерфейс межмодульного взаимодействия
	GET /servers/{server_id}/metadata/{id}	ИФБО	Показать сведения об элементе Метаданных сервера	Интерфейс межмодульного взаимодействия
	PUT /servers/{server_id}/metadata/{id}	ИФБО	Создание или обновление элемента Метаданных сервера	Интерфейс межмодульного взаимодействия
	DELETE /servers/{server_id}/metadata/{id}	ИФБО	Удалить элемент Метаданных сервера	Интерфейс межмодульного взаимодействия
Действия над серверами	GET /servers/{server_id}/os-instance-actions		Список действий над сервером	
	GET /servers/{server_id}/os-instance-actions/{id}		Показать сведения о действии над сервером	
Порты сервера	GET /servers/{server_id}/os-interface		Список портов сервера	
	POST /servers/{server_id}/os-interface		Создать порт	
	GET /servers/{server_id}/os-interface/{id}		Показать сведения об портах сервера	
	DELETE /servers/{server_id}/os-interface/{id}		Отсоединить порт	
Пароли серверов	GET /servers/{server_id}/os-server-password		Показать пароль сервера	
	DELETE /servers/{server_id}/os-		Очистить пароль администратора	

	server-password			
Серверы с подключенными томами	GET /servers/{server_id}/os-volume_attachments		Список прикреплений тома для экземпляра	
	POST /servers/{server_id}/os-volume_attachments		Прикрепить том к экземпляру	
	GET /servers/{server_id}/os-volume_attachments/{id}		Показать сведения о прикреплении тома	
	PUT /servers/{server_id}/os-volume_attachments/{id}		Обновить прикрепление тома	
	DELETE /servers/{server_id}/os-volume_attachments/{id}		Отсоединить том от экземпляра	
Конфигурации	GET /flavors		Список конфигураций	
	POST /flavors		Создать конфигурацию	
	GET /flavors/detail		Детальный список конфигураций	
	GET /flavors/{id}		Показать сведения конфигурации	
	PUT /flavors/{id}		Обновить описание конфигурации	
	DELETE /flavors/{id}		Удалить конфигурацию	
Доступ к конфигурации	GET /flavors/{flavor_id}/os-flavor-access		Список правил доступа к конфигурации для данной конфигурации	
	POST /flavors/{id}/action		Добавить доступ к конфигурации клиенту (Действие addTenantAccess)	

	POST /flavors/{id}/action		Убрать доступ к конфигурации клиенту (Действие removeTenantAccess)	
Дополнительные характеристики для конфигураций	GET /flavors/{flavor_id}/os-extra_specs		Список дополнительных характеристик для конфигурации	
	POST /flavors/{flavor_id}/os-extra_specs		Создать дополнительную характеристику для конфигурации	
	GET /flavors/{flavor_id}/os-extra_specs/{id}		Показать дополнительную характеристику для конфигурации	
	PUT /flavors/{flavor_id}/os-extra_specs/{id}		Обновить дополнительную характеристику для конфигурации	
	DELETE /flavors/{flavor_id}/os-extra_specs/{id}		Удалить дополнительную характеристику для конфигурации	
Пары ключей	GET /os-keypairs		Список пар ключей (имя и открытый ключ)	
	POST /os-keypairs		Импорт (или создание) пары ключей	
	GET /os-keypairs/{id}		Показать сведения о парах ключей	
	DELETE /os-keypairs/{id}		Удалить пару ключей	
Ограничения	GET /limits		Показать ограничения скорости и абсолютные ограничения	
Группировки узлов (Аггрегаты)	GET /os-aggregates		Список аггрегатов (объединений узлов в группы)	
	POST /os-aggregates		Создать аггрегат (группировку узлов)	
	GET /os-aggregates/{id}		Показать сведения об аггрегате (группировке узлов)	

	PUT /os-aggregates/{id}		Обновить аггрегат (группировку узлов)	
	DELETE /os-aggregates/{id}		Удалить аггрегат (группировку узлов)	
	POST /os-aggregates/{id}/action		Добавить узел	
	POST /os-aggregates/{id}/action		Убрать узел	
	POST /os-aggregates/{id}/action		Создать или обновить метаданные аггрегата (группировки узлов)	
	POST /os-aggregates/{id}/images		Запросить предварительное кэширование образов для аггрегата (группировки узлов)	
Вспомогательные образы (снимки) тома	POST /os-assisted-volume-snapshots		Создать вспомогательные образы (снимки) тома (объёма диска)	
	DELETE /os-assisted-volume-snapshots/{id}		Удалить вспомогательный образ тома	
Зоны доступности	GET /os-availability-zone		Получить информацию о зоне доступности	
	GET /os-availability-zone/detail		Получить подробную информацию о зоне доступности	
Гипервизоры	GET /os-hypervisors		Список гипервизиров (технология виртуализации)	
	GET /os-hypervisors/detail		Список сведений о гипервизорах	

	GET /os-hypervisors/statistics		Показать статистику гипервизора	
	GET /os-hypervisors/{id}		Показать сведения о гипервизоре	
	GET /os-hypervisors/{id}/uptime		Показать время безотказной работы гипервизора	
	GET /os-hypervisors/{id}/search		Найти гипервизор	
	GET /os-hypervisors/{id}/servers		Список серверов гипервизора	
Лог (журнал) аудита использования сервера	GET /os-instance_usage_audit_log	ИФБО	Список аудита использования сервера	Интерфейс межмодульного взаимодействия
	GET /os-instance_usage_audit_log/{id}	ИФБО	Список аудита использования до указанного времени	Интерфейс межмодульного взаимодействия
Миграции	GET /os-migrations		Список миграций	
Миграция серверов	GET /servers/{server_id}/migrations	ИФБО	Список миграций заданного сервера	Интерфейс межмодульного взаимодействия
	GET /servers/{server_id}/migrations/{id}	ИФБО	Показать сведения о миграции	Интерфейс межмодульного взаимодействия
	POST /servers/{server_id}/migrations/{id}/action	ИФБО	Принудительное дозавершение миграции (Завершает действие)	Интерфейс межмодульного взаимодействия
	DELETE /servers/{server_id}/migrations/{id}	ИФБО	Удалить (прервать) миграцию	Интерфейс межмодульного взаимодействия

Настройка квот	GET /os-quota-sets/{id}		Показать квоту	
	PUT /os-quota-sets/{id}		Обновить квоты	
	DELETE /os-quota-sets/{id}		Вернуть квоты к значениям по умолчанию	
	GET /os-quota-sets/{id}/defaults		Список квот по умолчанию для клиента	
	GET /os-quota-sets/{id}/detail		Показать сведения о квоте	
Настройка классов квот	GET /os-quota-class-sets/{id}		Показать квоту для класса квот	
	PUT /os-quota-class-sets/{id}		Создать или обновить квоту для класса квот	
Группы сервера	GET /os-server-groups		Список групп серверов	
	POST /os-server-groups		Создать группу сервера	
	GET /os-server-groups/{id}		Показать сведения о группе сервера	
	DELETE /os-server-groups/{id}		Удалить группу сервера	
Теги сервера	GET /servers/{server_id}/tags		Список тегов	
	PUT /servers/{server_id}/tags		Заменить теги	
	DELETE /servers/{server_id}/tags		Удалить все теги	
	GET /servers/{server_id}/tags/{id}		Проверить наличие тега	

	PUT /servers/{server_id}/tags/{id}		Добавить одиночный тег	
	DELETE /servers/{server_id}/tags/{id}		Удалить одиночный тег	
Вычислительные сервисы	GET /os-services		Список вычислительных сервисов	
	PUT /os-services/disable		Отключить планирование для сервиса вычислений	
	PUT /os-services/{id}		Обновить вычислительный сервис	
	DELETE /os-services/{id}		Удалить вычислительный сервис	
Отчеты об использовании	GET /os-simple-tenant-usage		Вывести статистику использования клиента для всех клиентов	
	GET /os-simple-tenant-usage/{id}		Вывести статистику использования для клиента	
Создание внешних событий	POST /os-server-external-events		Запустить события	
Топология серверов	GET /servers/{server_id}/topology		Показать топологию сервера	
Расширения	GET /extensions		Список расширений	
	GET /extensions/{id}		Показать сведения о расширении	
Сети	GET /os-networks		Список сетей	
	POST /os-networks		Создать сеть	
	POST /os-networks/add		Добавить сеть	
	GET /os-		Показать сведения о сети	

	networks/{id}			
	DELETE /os-networks/{id}		Удалить сеть	
	POST /os-networks/{id}/action		Объединить узел	
	POST /os-networks/{id}/action		Разъединить сеть	
	POST /os-networks/{id}/action		Разъединить узел	
	POST /os-networks/{id}/action		Разъединить проект	
Расширения томов	GET /os-volumes		Список томов	
	POST /os-volumes		Создать том	
	GET /os-volumes/detail		Список томов со сведениями	
	GET /os-volumes/{id}		Показать сведения о томе	
	DELETE /os-volumes/{id}		Удалить том	
	GET /os-snapshots		Список образов (шаблонов, "мгновенный снимок")	
	POST /os-snapshots		Создать образ	
	GET /os-snapshots/detail		Список образов со сведениями	
	GET /os-snapshots/{id}		Показать сведения об образе	

	DELETE /os-snapshots/{id}		Удалить образ	
Образы	GET /images	ИФБО	Список образов	Интерфейс межмодульного взаимодействия
	GET /images/detail	ИФБО	Список образов со сведениями	Интерфейс межмодульного взаимодействия
	GET /images/{id}	ИФБО	Показать сведения об образе	Интерфейс межмодульного взаимодействия
	DELETE /images/{id}	ИФБО	Удалить образ	Интерфейс межмодульного взаимодействия
	GET /images/{image_id}/metadata	ИФБО	Список метаданных образа	Интерфейс межмодульного взаимодействия
	POST /images/{image_id}/metadata		Создать метаданные образа	
	PUT /images/{image_id}/metadata		Обновить метаданные образа	
	GET /images/{image_id}/metadata/{id}		Показать элемент метаданных образа	
	PUT /images/{image_id}/metadata/{id}		Создать или обновить элемент метаданных образа	
	DELETE /images/{image_id}/metadata/{id}		Удалить элемент Метаданных образа	
Bare-metal-узлы (узел, созданный непосредственно на физической машине)	GET /os-baremetal-nodes		Список Bare-metal-узлов (узел, созданный непосредственно на физической машине)	
	GET /os-baremetal-nodes/{id}		Показать сведения о Bare-metal-узлах	

Проектные сети	GET /os-tenant-networks		Список проектных сетей	
	POST /os-tenant-networks		Создать проектную сеть	
	GET /os-tenant-networks/{id}		Показать сведения о проектной сети	
	DELETE /os-tenant-networks/{id}		Удалить проектную сеть	
Пулы плавающих IP-адресов	GET /os-floating-ip-pools		Список пулов плавающих Ip-адресов	
Плавающие IP-адреса	GET /os-floating-ips		Список плавающих Ip-адресов	
	POST /os-floating-ips		Создать (выделить) плавающий Ip-адрес	
	GET /os-floating-ips/{id}		Показать сведения о плавающем Ip-адресе	
	DELETE /os-floating-ips/{id}		Удалить (убрать выделение) плавающего Ip-адреса	
Группы безопасности	GET /os-security-groups	ИФБО	Список групп безопасности	Интерфейс межмодульного взаимодействия
	POST /os-security-groups	ИФБО	Создать группу безопасности	Интерфейс доступный внешним пользователям (Интерфейс создания группы безопасности)
	GET /os-security-groups/{id}	ИФБО	Показать сведения о группе безопасности	Интерфейс межмодульного взаимодействия
	PUT /os-security-groups/{id}	ИФБО	Обновить группу безопасности	Интерфейс межмодульного взаимодействия
	DELETE /os-security-groups/{id}	ИФБО	Удалить группу безопасности	Интерфейс доступный внешним пользователям (Интерфейс удаления группы безопасности)

Правила для группы безопасности	POST /os-security-group-rules	ИФБО	Создать правило группы безопасности	Интерфейс доступный внешним пользователям (Интерфейс создания правил безопасности)
	DELETE /os-security-group-rules/{id}	ИФБО	Удалить правило группы безопасности	Интерфейс доступный внешним пользователям (Интерфейс удаления правил безопасности)
Узлы	GET /os-hosts		Список узлов	
	GET /os-hosts/{id}		Показать сведения об узле	
	PUT /os-hosts/{id}		Обновить статус узлов	
	GET /os-hosts/{id}/reboot		Перезагрузить узел	
	GET /os-hosts/{id}/shutdown		Выключить узел	
	GET /os-hosts/{id}/startup		Запустить узел	
Корневой сертификат	POST /os-certificates		Создать корневой сертификат	
Облачные каналы	GET /os-cloudpipe		Список облачных каналов	
	POST /os-cloudpipe		Создать облачный канал	
Пинг (проверка) экземпляров	GET /os-fping		Проверить качество соединения до серверов (пропинговать)	
	GET /os-fping/{id}		Проверить качество соединения до одного из серверов (пропинговать)	
Виртуальные интерфейсы серверов	GET /servers/{server_id}/os-virtual-interfaces		Список виртуальных интерфейсов	
Фиксированный IP-адрес	GET /os-fixed-ips/{id}		Показать сведения о фиксированном Ip-адресе	

	POST /os-fixed-ips/{id}/action		Резервировать или выпустить фиксированный Ip-адрес	
Плавающие IP-адреса	GET /os-floating-ips-bulk		Список плавающих Ip-адресов	
	POST /os-floating-ips-bulk		Создать плавающие Ip-адреса	
	GET /os-floating-ips-bulk/{id}		Получить список плавающих Ip-адресов хоста	
Плавающие записи IP DNS	GET /os-floating-ip-dns		Список DNS (система доменных имён) доменов	
	PUT /os-floating-ip-dns/{id}		Создать или обновить DNS домен	
	DELETE /os-floating-ip-dns/{id}		Удалить DNS домен	
	GET /os-floating-ip-dns/{domain}/entries/{id}		Список DNS входов	
	GET /os-floating-ip-dns/{domain}/entries/{id}		Найти уникальный DNS вход	
	PUT /os-floating-ip-dns/{domain}/entries/{id}		Создать или обновить уникальный DNS вход	
	DELETE /os-floating-ip-dns/{domain}/entries/{id}		Удалить DNS вход	
Ячейки	GET /os-cells		Список ячеек (групп хостов)	
	POST /os-cells		Создать ячейку	
	GET /os-cells/capacities		Список возможностей (ёмкостей)	

	GET /os-cells/detail		Список сведений о ячейке	
	GET /os-cells/info		Информация для данной ячейки	
	GET /os-cells/{id}		Показать данные ячейки	
	PUT /os-cells/{id}		Обновить ячейку	
	DELETE /os-cells/{id}		Удалить ячейку	
	GET /os-cells/{id}/capacities		Показать возможности ячейки	
XenServer VNC Proxy (XVP) (прокси-сервер, который обеспечивает защищённый паролем доступ на основе VNC к консолям виртуальных машин)	GET /servers/{server_id}/consoles		Список консолей	
	POST /servers/{server_id}/consoles		Создать консоль	
	GET /servers/{server_id}/consoles/{id}		Показать сведения о консоли	
	DELETE /servers/{server_id}/consoles/{id}		Удалить консоль	
Правила для групп безопасности по умолчанию	GET /os-security-group-default-rules		Список правил групп безопасности по умолчанию	
	GET /os-security-group-default-rules/{id}		Показать сведения о правилах групп безопасности по умолчанию	
	POST /os-security-group-default-rules		Создать правило группы безопасности по умолчанию	
	DELETE /os-security-group-default-rules/{id}		Удалить правило группы безопасности по умолчанию	

Гостевые агенты	GET /os-agents		Список сборок агента	
	POST /os-agents		Создать сборку агента	
	PUT /os-agents/{id}		Обновить сборку агента	
	DELETE /os-agents/{id}		Удалить сборку агента	
	POST /servers/{id}/action		Получить консоль RDP (графическая консоль) (Действие os-getRDPConsole)	

Для данных интерфейсов параметры указаны в электронном приложении к документу «Программное обеспечение «Облачная платформа KeyStack SE v.1». Руководство пользователя (Каталог – «Электронное приложение» – «Интерфейсы» – «интерфейсы_nova_v2.96.yaml»). Для поиска параметров в электронном приложении необходимо выполнить команду Ctrl + F и ввести в строку поиска API, после чего в файле будет найдено указанное API и приведены его параметры.

8.11 Интерфейсы модуля Neutron

В Таблице 3 приведены интерфейсы модуля Neutron, назначением которых является, в том числе, реализация требований безопасности, связанных с управлением потоками информации в ПО «KeyStack SE». Интерфейсы представлены API и могут быть использованы посредством применения вызовов по протоколу REST API.

Таблица 3 – Интерфейсы модуля Neutron и их назначение

Интерфейсы		Является ли ИФБО применительно к ОО	Назначение	Комментарий
Расширения API	GET /v2.0/extensions		Список расширений API	
	GET /v2.0/extensions/{id}		Показать сведения о расширении API	
Сети	GET /v2.0/networks/{network_id}		Показать сведения о сети	
	PUT /v2.0/networks/{network_id}		Обновить сеть	
	DELETE /v2.0/networks/{network_id}		Удалить сеть	
	GET /v2.0/networks	ИФБО	Список сетей	Интерфейс межмоду

				льного взаимодействия
	POST /v2.0/networks		Создать сеть	
	POST /v2.0/networks		Массовое создание сетей	
Диапазоны сегментов сети	GET /v2.0/network_segment_ranges/{network_segment_range_id}		Показать информацию о диапазоне сегментов сети	
	PUT /v2.0/network_segment_ranges/{network_segment_range_id}		Обновить диапазон сетевых сегментов	
	DELETE /v2.0/network_segment_ranges/{network_segment_range_id}		Удалить диапазон сетевых сегментов	
	GET /v2.0/network_segment_ranges		Список диапазонов сетевых сегментов	
	POST /v2.0/network_segment_ranges		Создать диапазон сетевых сегментов	
Порты	GET /v2.0/ports/{port_id}		Показать детали портов	
	PUT /v2.0/ports/{port_id}	ИФБО	Обновить порт	Интерфейс межмодульного взаимодействия
	DELETE /v2.0/ports/{port_id}		Удалить порт	
	GET /v2.0/ports	ИФБО	Список портов	Интерфейс межмодульного взаимодействия
	POST /v2.0/ports	ИФБО	Создать порт	Интерфейс межмодульного взаимодействия
	POST /v2.0/ports		Массовое создание портов	

	PUT /v2.0/ports/{port_id}/ add_allowed_address_ pairs		Добавление пар разрешённых адресов (allowed address pairs) к порту	
Привязка портов	GET /v2.0/ports/{port_id}/ bindings		Показать привязки портов	
	POST /v2.0/ports/{port_id}/ bindings/		Создать привязки портов	
	PUT /v2.0/ports/{port_id}/ bindings/{id}/activate		Активация привязки портов	
	DELETE /v2.0/ports/{port_id}/ bindings/{id}		Удалить привязки портов	
Сегменты	GET /v2.0/segments/{id}		Показать информацию о сегменте	
	PUT /v2.0/segments/{id}		Обновить сегмент	
	DELETE /v2.0/segments/{id}		Удалить сегмент	
	GET /v2.0/segments		Список сегментов	
	POST /v2.0/segments		Создать сегмент	
Магистральный порт	GET /v2.0/trunks		Список магистральных портов	
	POST /v2.0/trunks		Создать магистральный порт	
	PUT /v2.0/trunks/{trunk_id}		Обновить магистральный порт	
	GET /v2.0/trunks/{trunk_id}		Показать магистральный порт	
	DELETE /v2.0/trunks/{trunk_id}		Удалить магистральный порт	
Расширенные атрибуты порта, входящего в магистральный порт	GET /v2.0/ports/{port_id}		Показать информацию о магистральном порте	
Области действия адресов	GET /v2.0/address-scopes/{id}		Показать область действия адреса	

	PUT /v2.0/address-scopes/{id}		Обновить область действия адреса	
	DELETE /v2.0/address-scopes/{id}		Удалить области действия адреса	
	GET /v2.0/address-scopes		Список областей действия адресов	
	POST /v2.0/address-scopes		Создать область действия адреса	
Правила назначения Conntrack Helper (CT) для маршрутизаторов	GET /v2.0/routers/{router_id}/conntrack_helpers/{id}		Показать conntrack helper	
	PUT /v2.0/routers/{router_id}/conntrack_helpers/{id}		Обновить conntrack helper	
	DELETE /v2.0/routers/{router_id}/conntrack_helpers/{id}		Удалить conntrack helper	
	GET /v2.0/routers/{router_id}/conntrack_helpers		Перечислить вспомогательные модули (conntrack helpers) для маршрутизатора	
	POST /v2.0/routers/{router_id}/conntrack_helpers		Создать conntrack helper	
Плавающие IP-адреса	GET /v2.0/floatingips		Список плавающих IP-адресов	
	POST /v2.0/floatingips		Создать плавающий IP-адрес	
	GET /v2.0/floatingips/{id}		Показать плавающий IP-адрес	
	PUT /v2.0/floatingips/{id}		Обновить плавающий IP-адрес	
	DELETE /v2.0/floatingips/{id}		Удалить плавающий IP-адрес	
Переадресация плавающего IP-порта	GET /v2.0/floatingips/{floatingip_id}/port_forwardings/{id}		Показать переадресацию портов	
	PUT /v2.0/floatingips/{floatingip_id}/port_forwardings/{id}		Обновить переадресацию портов	
	DELETE /v2.0/floatingips/{floa		Удаление переадресации плавающего IP-порта	

	tingip_id}/port_forwardings/{id}			
	GET /v2.0/floatingips/{floatingip_id}/port_forwardings		Список переадресаций плавающего IP-порта	
	POST /v2.0/floatingips/{floatingip_id}/port_forwardings		Создать переадресацию портов	
Маршрутизаторы	GET /v2.0/routers		Список маршрутизаторов	
	POST /v2.0/routers		Создать маршрутизатор	
	GET /v2.0/routers/{id}		Показать информацию о маршрутизаторах	
	PUT /v2.0/routers/{id}		Обновить маршрутизатор	
	DELETE /v2.0/routers/{id}		Удалить маршрутизатор	
	PUT /v2.0/routers/{id}/add_router_interface		Добавить интерфейс к маршрутизатору	
	PUT /v2.0/routers/{id}/remove_router_interface		Удалить интерфейс с маршрутизатора	
	PUT /v2.0/routers/{id}/add_extraroutes		Добавить дополнительные маршруты к маршрутизатору	
	PUT /v2.0/routers/{id}/remove_extraroutes		Удалить дополнительные маршруты из маршрутизатора	
	PUT /v2.0/routers/{id}/add_external_gateways		Добавление внешних шлюзов к маршрутизатору	
	PUT /v2.0/routers/{id}/update_external_gateways		Обновить внешние шлюзы маршрутизатора	
	PUT /v2.0/routers/{id}/remove_external_gateways		Удалить внешние шлюзы с маршрутизатора	
Расширение пулов подсетей	GET /v2.0/subnetpools/{id}		Показать пул подсетей	
	PUT /v2.0/subnetpools/{id}		Обновить пул подсетей	
	DELETE /v2.0/subnetpools/{id}		Удалить пул подсетей	

	GET /v2.0/subnetpools		Список пулов подсетей	
	POST /v2.0/subnetpools		Создать пул подсетей	
Операции с префиксом пула подсетей	PUT /v2.0/subnetpools/{id} /add_prefixes		Добавить префиксы	
	PUT /v2.0/subnetpools/{id} /remove_prefixes		Удалить префиксы	
Подсети	GET /v2.0/subnets	ИФБО	Список подсетей	Интерфей с межмоду льного взаимоде йствия
	POST /v2.0/subnets		Создать подсеть	
	POST /v2.0/subnets		Массовое создание подсети	
	GET /v2.0/subnets/{subnet _id}		Показать информацию о подсети	
	PUT /v2.0/subnets/{subnet _id}		Обновить подсеть	
	DELETE /v2.0/subnets/{subnet _id}		Удалить подсеть	
Операция добавления подсетей конкретной сети в пул подсетей	PUT /v2.0/subnetpools/{id} /onboard_network_su bnets		Добавить подсети	
Локальные IP-адреса	GET /v2.0/local_ips		Список Локальных IP-адресов	
	POST /v2.0/local_ips		Создать Локальный IP-адрес	
	GET /v2.0/local_ips/{local_ ip_id}		Показать сведения о Локальном IP-адресе	
	PUT /v2.0/local_ips/{local_ ip_id}		Обновить Локальный IP-адрес	
	DELETE /v2.0/local_ips/{local_ ip_id}		Удалить Локальный IP-адрес	
	GET /v2.0/local_ips/{local_		Список Ассоциаций локальных IP-адресов	

Ассоциации локальных IP-адресов	ip_id}/port_associations			
	POST /v2.0/local_ips/{local_ip_id}/port_associations		Создать Ассоциацию локальных IP-адресов	
	DELETE /v2.0/local_ips/{local_ip_id}/port_associations/{id}		Удалить Ассоциации локальных IP-адресов	
Адресные группы	GET /v2.0/address-groups/{id}		Показать группу адресов	
	PUT /v2.0/address-groups/{id}		Обновить группу адресов	
	DELETE /v2.0/address-groups/{id}		Удалить группу адресов	
	GET /v2.0/address-groups		Список групп адресов	
	POST /v2.0/address-groups		Создать группу адресов	
	PUT /v2.0/address-group/{id}/add_addresses		Добавить IP-адреса в группу адресов	
	PUT /v2.0/address-group/{id}/remove_addresses		Удалить IP-адреса из группы адресов	
Политики RBAC (система управления доступом на основе ролей)	GET /v2.0/rbac-policies/{id}		Вывести детали политики управления доступом на основе ролей (RBAC)	
	PUT /v2.0/rbac-policies/{id}		Обновить политику RBAC	
	DELETE /v2.0/rbac-policies/{id}		Удалить политику RBAC	
	GET /v2.0/rbac-policies		Список политик RBAC	
	POST /v2.0/rbac-policies		Создать политику RBAC	
Правила группы безопасности	GET /v2.0/security-group-rules	ИФБО	Список правил группы безопасности	Интерфейс межмодульного взаимодействия

	POST /v2.0/security-group-rules	ИФБО	Создать правило группы безопасности	Интерфейс межмодульного взаимодействия
	POST /v2.0/security-group-rules		Массовое создание правил групп безопасности	
	GET /v2.0/security-group-rules/{id}	ИФБО	Показать правило группы безопасности	Интерфейс межмодульного взаимодействия
	DELETE /v2.0/security-group-rules/{id}	ИФБО	Удалить правило группы безопасности	Интерфейс межмодульного взаимодействия
Группы безопасности	GET /v2.0/security-groups	ИФБО	Список групп безопасности	Интерфейс межмодульного взаимодействия
	POST /v2.0/security-groups	ИФБО	Создать группу безопасности	Интерфейс межмодульного взаимодействия
	GET /v2.0/security-groups/{id}	ИФБО	Показать группу безопасности	Интерфейс межмодульного взаимодействия
	PUT /v2.0/security-groups/{id}	ИФБО	Обновить группу безопасности	Интерфейс межмодульного взаимодействия
	DELETE /v2.0/security-groups/{id}	ИФБО	Удалить группу безопасности	Интерфейс межмодульного взаимодействия

Правила группы безопасности по умолчанию	GET /v2.0/default-security-group-rules		Список правил группы безопасности по умолчанию	
	POST /v2.0/default-security-group-rules		Создание правила группы безопасности по умолчанию	
	GET /v2.0/default-security-group-rules/{id}		Показать правило группы безопасности по умолчанию	
	DELETE /v2.0/default-security-group-rules/{id}		Удалить правило группы безопасности по умолчанию	
Конфигурации VPN	GET /v2.0/vpn/ikepolicies		Список политик IKE	
	POST /v2.0/vpn/ikepolicies		Создание политики IKE	
	GET /v2.0/vpn/ikepolicies/{ikepolicy_id}		Показать информацию о политике IKE	
	PUT /v2.0/vpn/ikepolicies/{ikepolicy_id}		Обновить политику IKE	
	DELETE /v2.0/vpn/ikepolicies/{ikepolicy_id}		Удалить политику IKE	
	GET /v2.0/vpn/ipsecpolicies		Список политик IPSec	
	POST /v2.0/vpn/ipsecpolicies		Создание политики IPSec	
	GET /v2.0/vpn/ipsecpolicies/{ipsecpolicy_id}		Показать политику IPSec	
	PUT /v2.0/vpn/ipsecpolicies/{ipsecpolicy_id}		Обновить политику IPSec	
	DELETE /v2.0/vpn/ipsecpolicies/{ipsecpolicy_id}		Удалить политику IPSec	
	GET /v2.0/vpn/ipsec-site-connections		Список подключений IPSec	
	POST /v2.0/vpn/ipsec-site-connections		Создание IPSec-соединения	
	GET /v2.0/vpn/ipsec-site-connections/{connection_id}		Показывать подключение по IPSec	

	PUT /v2.0/vpn/ipsec-site-connections/{connection_id}		Обновить IPSec-соединение	
	DELETE /v2.0/vpn/ipsec-site-connections/{connection_id}		Удалить IPSec-соединение	
	GET /v2.0/vpn/endpoint-groups		Список групп конечных точек VPN	
	POST /v2.0/vpn/endpoint-groups		Создание группы конечных точек VPN	
	GET /v2.0/vpn/endpoint-groups/{endpoint_group_id}		Показать группу конечных точек VPN	
	PUT /v2.0/vpn/endpoint-groups/{endpoint_group_id}		Обновить группу конечных точек VPN	
	DELETE /v2.0/vpn/endpoint-groups/{endpoint_group_id}		Удалить группу конечных точек VPN	
	GET /v2.0/vpn/vpnservices		Список VPN-сервисов	
	POST /v2.0/vpn/vpnservices		Создание VPN-сервиса	
	GET /v2.0/vpn/vpnservices/{service_id}		Показать информацию о VPN-сервисе	
	PUT /v2.0/vpn/vpnservices/{service_id}		Обновить VPN-сервис	
	DELETE /v2.0/vpn/vpnservices/{service_id}		Удалить VPN-сервис	
Networking Flavors Framework 2.0 (Фреймфорк для сетевых конфигураций)	GET /v2.0/flavors		Список конфигураций	
	POST /v2.0/flavors		Создать конфигурацию	
	GET /v2.0/flavors/{id}		Показать информацию о конфигурации	
	PUT /v2.0/flavors/{id}		Обновить конфигурацию	
	DELETE /v2.0/flavors/{id}		Удалить конфигурацию	

	POST /v2.0/flavors/{flavor_id}/service_profiles		Связать конфигурацию с профилем сервиса	
	DELETE /v2.0/flavors/{flavor_id}/service_profiles/{id}		Отвязать конфигурацию	
	GET /v2.0/service_profiles		Список сервисных профилей	
	POST /v2.0/service_profiles		Создать профиль сервиса	
	GET /v2.0/service_profiles/{id}		Показать сведения о профиле сервиса	
	PUT /v2.0/service_profiles/{id}		Обновить профиль сервиса	
	DELETE /v2.0/service_profiles/{id}		Удалить профиль сервиса	
Метки и правила измерения	GET /v2.0/metering/metering-labels		Список меток измерения	
	POST /v2.0/metering/metering-labels		Создать метки измерения	
	GET /v2.0/metering/metering-labels/{id}		Показать сведения о метках измерения	
	DELETE /v2.0/metering/metering-labels/{id}		Удалить метки измерения	
	GET /v2.0/metering/metering-label-rules		Список правил меток измерения	
	POST /v2.0/metering/metering-label-rules		Создать правило меток измерения	
	GET /v2.0/metering/metering-label-rules/{id}		Показать сведения о правилах меток измерения	
	DELETE /v2.0/metering/metering-label-rules/{id}		Удалить правило меток измерения	
Статистика доступности и использования IP-адреса сети	GET /v2.0/network-ip-availabilities/{id}		Показать Доступность IP-адреса Сети	
	GET /v2.0/network-ip-availabilities		Список Доступных сетевых IP-адресов	

Расширение квот	GET /v2.0/quotas			Список квот для всех проектов с нештатными значениями	
	GET /v2.0/quotas/{id}			Перечислить квоты для проекта	
	PUT /v2.0/quotas/{id}			Обновить квоты для проекта	
	DELETE /v2.0/quotas/{id}			Сброс квот для проектов	
	GET /v2.0/quotas/{id}/default			Список квот по умолчанию для проекта	
Расширение сведений о квотах	GET /v2.0/quotas/{project_id}/details			Показать сведения о квоте для тенант	
Поставщики услуг	GET /v2.0/service-providers			Список поставщиков услуг	
Расширения тегов (общее описание API)	POST /v2.0/{resource_type}/{resource_id}/tags	/v2.0/networks/{network_id}/tags /v2.0/networks/{network_id}/tags/{id} /v2.0/network_segment_ranges/{network_segment_range_id}/tags/{id} /v2.0/network_segment_ranges/{networ		Создать теги	
	PUT /v2.0/{resource_type}/{resource_id}/tags			Заменить все теги	
	DELETE /v2.0/{resource_type}/{resource_id}/tags			Удалить все теги	
	GET /v2.0/{resource_type}/{resource_id}/tags/{tag}			Подтвердить тег	
	PUT /v2.0/{resource_type}/{resource_id}/tags/{tag}			Добавить тег	

	GET /v2.0/{resource_type}/{resource_id}/tags	k_segment_range_id}/tags /v2.0/ports/{port_id}/tags /v2.0/ports/{port_id}/tags/{id} /v2.0/trunks/{trunk_id}/tags /v2.0/trunks/{trunk_id}/tags/{id} /v2.0/floatingips/{floatingip_id}/tags /v2.0/floatingips/{floatingip_id}/tags/{id} /v2.0/routers/{router_id}/tags /v2.0/routers/{router_id}/tags/{id} /v2.0/subnetpools/{subnetpool_id}/tags/{id}		Получить список тегов	
	DELETE /v2.0/{resource_type}/{resource_id}/tags/{tag}			Удалить тег	

		/v2.0/subnetpools/{subnetpool_id}/tags /v2.0/subnets/{subnet_id}/tags /v2.0/subnets/{subnet_id}/tags/{id} /v2.0/security-groups/{security_group_id}/tags /v2.0/security-groups/{security_group_id}/tags/{id}			
Типы правил QoS (Качество сервиса)	GET /v2.0/qos/rule-types			Перечислить типы правил QoS	
	GET /v2.0/qos/rule-types/{id}			Показать сведения о типе правила QoS	
Политики QoS	GET /v2.0/qos/policies			Список политик QoS	
	POST /v2.0/qos/policies			Создать политики QoS	
	GET /v2.0/qos/policies/{id}			Показать сведения о политиках QoS	
	PUT /v2.0/qos/policies/{id}			Обновить политику QoS	
	DELETE /v2.0/qos/policies/{id}			Удалить политику QoS	

Правила ограничения пропускной способности QoS	GET /v2.0/qos/policies/{policy_id}/bandwidth_limit_rules		Перечислить правила ограничения пропускной способности для политики QoS	
	POST /v2.0/qos/policies/{policy_id}/bandwidth_limit_rules		Создать правила ограничения пропускной способности	
	GET /v2.0/qos/policies/{policy_id}/bandwidth_limit_rules/{id}		Показать сведения о правиле ограничения пропускной способности	
	PUT /v2.0/qos/policies/{policy_id}/bandwidth_limit_rules/{id}		Обновить правило ограничения пропускной способности	
	DELETE /v2.0/qos/policies/{policy_id}/bandwidth_limit_rules/{id}		Удалить правило ограничения пропускной способности	
Правила маркировки трафика с помощью DSCP (Точка кода дифференцированных услуг) в рамках QoS	GET /v2.0/qos/policies/{policy_id}/dscp_marking_rules		Перечислить правила маркировки DSCP для политики QoS	
	POST /v2.0/qos/policies/{policy_id}/dscp_marking_rules		Создать правила маркировки DSCP	
	GET /v2.0/qos/policies/{policy_id}/dscp_marking_rules/{id}		Показать информацию о правилах маркировки DSCP	
	PUT /v2.0/qos/policies/{policy_id}/dscp_marking_rules/{id}		Обновить правило маркировки DSCP	
	DELETE /v2.0/qos/policies/{policy_id}/dscp_marking_rules/{id}		Удалить правило маркировки DSCP	
Правила минимальной пропускной способности в QoS	GET /v2.0/qos/policies/{policy_id}/minimum_bandwidth_rules		Перечислить правила минимальной пропускной способности для политики QoS	
	POST /v2.0/qos/policies/{policy_id}/minimum_bandwidth_rules		Создать правило минимальной пропускной способности	
	GET /v2.0/qos/policies/{pol		Показать сведения о правиле минимальной пропускной способности	

	icy_id}/minimum_bandwidth_rules/{id}			
	PUT /v2.0/qos/policies/{policy_id}/minimum_bandwidth_rules/{id}		Обновить правило минимальной пропускной способности	
	DELETE /v2.0/qos/policies/{policy_id}/minimum_bandwidth_rules/{id}		Удалить правило минимальной пропускной способности	
Правила минимальной скорости передачи пакетов QoS	GET /v2.0/qos/policies/{policy_id}/minimum_packet_rate_rules		Перечислить правила минимальной скорости передачи пакетов для политики QoS	
	POST /v2.0/qos/policies/{policy_id}/minimum_packet_rate_rules		Создать правила минимальной скорости передачи пакетов	
	GET /v2.0/qos/policies/{policy_id}/minimum_packet_rate_rules/{id}		Показать сведения о правиле минимальной скорости передачи пакетов	
	PUT /v2.0/qos/policies/{policy_id}/minimum_packet_rate_rules/{id}		Обновить правило минимальной скорости передачи пакетов	
	DELETE /v2.0/qos/policies/{policy_id}/minimum_packet_rate_rules/{id}		Удалить правило минимальной скорости передачи пакетов	
Ресурс логов	GET /v2.0/log/logs	ИФБО	Список логов	Интерфейс межмодульного взаимодействия
	POST /v2.0/log/logs	ИФБО	Создать лог	Интерфейс межмодульного взаимодействия
	GET /v2.0/log/logs/{id}	ИФБО	Показать лог	Интерфейс межмодульного взаимодействия
	PUT /v2.0/log/logs/{id}	ИФБО	Обновить лог	Интерфейс межмоду

				льного взаимодействия
	DELETE /v2.0/log/logs/{id}	ИФБО	Удалить лог	Интерфейс межмодульного взаимодействия
Логируемый ресурс	GET /v2.0/log/loggable-resources	ИФБО	Список логируемых ресурсов	Интерфейс межмодульного взаимодействия
Сетевые агенты	GET /v2.0/agents		Список всех агентов	
	GET /v2.0/agents/{id}		Показать информацию об агенте	
	PUT /v2.0/agents/{id}		Обновить агента	
	DELETE /v2.0/agents/{id}		Удалить агента	
Зоны доступности	GET /v2.0/availability_zones		Перечислить все зоны доступности	
Планировщик агентов L3	GET /v2.0/agents/{agent_id}/l3-routers		Список маршрутизаторов, размещенных агентом L3	
	POST /v2.0/agents/{agent_id}/l3-routers		Запланировать подключение маршрутизатора к агенту l3	
	DELETE /v2.0/agents/{agent_id}/l3-routers/{id}		Удалить маршрутизатор l3 из агента l3	
	GET /v2.0/routers/{router_id}/l3-agents		Список агентов L3, размещающих маршрутизатор	
Планировщик агентов DHCP	GET /v2.0/agents/{agent_id}/dhcp-networks		Список сетей, размещенных агентом DHCP	
	POST /v2.0/agents/{agent_id}/dhcp-networks		Запланировать подключение к сети с помощью агента DHCP	
	DELETE /v2.0/agents/{agent_id}/dhcp-networks/{id}		Удалить сеть из агента DHCP	

	GET /v2.0/networks/{network_id}/dhcp-agents		Список агентов DHCP, размещающих сеть	
Автоматически выделяемая топология (сети)	GET /v2.0/auto-allocated-topology/{id}		Отображение сведений об автоматически выделенной топологии	
	DELETE /v2.0/auto-allocated-topology/{id}		Удалить автоматически выделенную топологию	

Для данных интерфейсов параметры указаны в электронном приложении к документу «Программное обеспечение «Облачная платформа KeyStack SE v.1». Руководство пользователя» (Каталог – «Электронное приложение» – «Интерфейсы» – «интерфейсы_neutron_v2.26.yaml»). Для поиска параметров в электронном приложении необходимо выполнить команду Ctrl + F и ввести в строку поиска API, после чего в файле будет найдено указанное API и приведены его параметры.

8.12 Интерфейсы модуля Cinder

В Таблице 4 приведены интерфейсы модуля Cinder, назначением которых является, в том числе, реализация требований безопасности, связанных с резервным копированием в ПО «KeyStack SE». Интерфейсы представлены API и могут быть использованы посредством применения вызовов по протоколу REST API.

Таблица 4 – Интерфейсы модуля Cinder и их назначение

Интерфейсы		Является ли ИФБО применительно к ОО	Назначение	Комментарий
Сведения о версии API	GET /v3/		Показать детали API v3	
Расширения API	GET /v3/{project_id}/extensions		Список известных расширений API	
Типы томов	PUT /v3/{project_id}/types/{id}		Обновить тип тома	
	POST /v3/{project_id}/types/{type_id}/extra_specs		Создание или обновление дополнительных спецификаций для типа тома	
	GET /v3/{project_id}/types/{type_id}/extra_specs		Показать все дополнительные характеристики для типа тома	
	GET /v3/{project_id}/types/{type_id}/extra_specs/{id}		Показать дополнительную спецификацию для типа тома	

	PUT /v3/{project_id}/types/{type_id}/extra_specs/{id}		Обновите дополнительную спецификацию для типа тома	
	DELETE /v3/{project_id}/types/{type_id}/extra_specs/{id}		Удалить дополнительную спецификацию для типа тома	
	GET /v3/{project_id}/types/{id}		Показать подробную информацию о типе тома	
	DELETE /v3/{project_id}/types/{id}		Удаление типа тома	
	GET /v3/{project_id}/types		Перечислите все типы томов	
	POST /v3/{project_id}/types		Создание типа тома	
	GET /v3/{project_id}/types/{type_id}/encryption		Показать тип шифрования	
	GET /v3/{project_id}/types/{type_id}/encryption/{id}		Показать элемент спецификации шифрования	
	DELETE /v3/{project_id}/types/{type_id}/encryption/{id}		Удаление типа шифрования	
	POST /v3/{project_id}/types/{type_id}/encryption		Создание типа шифрования	
	PUT /v3/{project_id}/types/{type_id}/encryption/{id}		Обновить тип шифрования	
Доступ к типу тома	POST /v3/{project_id}/types/{id}/action		Добавление доступа к типу частного тома в проект	
	POST /v3/{project_id}/types/{id}/action		Удалить доступ к типу частного тома из проекта	
	GET /v3/{project_id}/types/{type_id}/os-volume-type-access		Список сведений о доступе к типу частного тома	
Типы томов по умолчанию	PUT /v3/default-types/{id}		Создайте или обновите тип тома по умолчанию	
	GET /v3/default-types/{id}		Показать тип тома по умолчанию	

	DELETE /v3/default-types/{id}		Удаление типа тома по умолчанию	
Тома	GET /v3/{project_id}/volumes/detail		Перечислите доступные тома с подробной информацией	
	POST /v3/{project_id}/volumes	ИФБО	Создание тома	Интерфейс межмодульного взаимодействия
	GET /v3/{project_id}/volumes		Список доступных томов	
	GET /v3/{project_id}/volumes/{id}	ИФБО	Показать сведения о томе	Интерфейс межмодульного взаимодействия
	PUT /v3/{project_id}/volumes/{id}		Обновить том	
	DELETE /v3/{project_id}/volumes/{id}		Удаление тома	
	POST /v3/{project_id}/volumes/{volume_id}/metadata		Создание метаданных для тома	
	GET /v3/{project_id}/volumes/{volume_id}/metadata		Отображение метаданных тома	
	PUT /v3/{project_id}/volumes/{volume_id}/metadata		Обновление метаданных тома	
	GET /v3/{project_id}/volumes/{volume_id}/metadata/{id}		Показать метаданные тома для определенного ключа	
	DELETE /v3/{project_id}/volumes/{volume_id}/metadata/{id}		Удаление метаданных тома	
	PUT /v3/{project_id}/volumes/{volume_id}/metadata/{id}		Обновить метаданные тома для определенного ключа	

	GET /v3/{project_id}/volumes/summary		Получить сводку томов	
Действия с томами	POST /v3/{project_id}/volumes/{id}/action		Увеличить размер тома	
			Завершите расширение тома	
			Сброс статусов тома	
			Возврат тома к образу (моментальному снимку)	
			Настройка метаданных образадля тома	
			Удаление метаданных образа из тома	
			Отображение метаданных образа для тома	
			Присоединить том к серверу	
			Отсоединить том от сервера	
			Отключение управления томом	
			Принудительное отсоединение тома	
			Смена типа тома	
			Перенос тома	
			Завершение перемещения тома	
			Принудительное удаление тома	
			Обновите загрузочный статус тома	
			Загрузить том в образ	
			Резервировать том	
			Снять пометку с тома как зарезервированного	
			Обновить состояние тома до отсоединения	
			Откатить состояние тома до "используется"	
			Завершить прикрепление тома	
			Инициализировать прикрепление тома	
			Обновляет флаг режима доступа только для чтения тома	

			Перезалить из образа том	
Расширение для управления томом	POST /v3/{project_id}/manageable_volumes		Управление существующим томом	
	GET /v3/{project_id}/manageable_volumes		Краткий список томов, доступных для управления	
	GET /v3/{project_id}/manageable_volumes/detail		Подробный список томов, доступных для управления	
Моментальные снимки томов	GET /v3/{project_id}/snapshots/detail		Перечислите моментальные снимки (образы, шаблоны) и подробную информацию	
	POST /v3/{project_id}/snapshots		Создание моментального снимка	
	GET /v3/{project_id}/snapshots		Список доступных моментальных снимков	
	GET /v3/{project_id}/snapshots/{snapshot_id}/metadata		Показать метаданные моментального снимка	
	POST /v3/{project_id}/snapshots/{snapshot_id}/metadata		Создание метаданных моментального снимка	
	PUT /v3/{project_id}/snapshots/{snapshot_id}/metadata		Обновить метаданные моментального снимка	
	GET /v3/{project_id}/snapshots/{id}		Показать детали моментального снимка	
	PUT /v3/{project_id}/snapshots/{id}		Обновить моментальный снимок	
	DELETE /v3/{project_id}/snapshots/{id}		Удаление моментального снимка	
	GET /v3/{project_id}/snapshot/{snapshot_id}/metadata/{id}		Отображение метаданных моментального снимка для определенного ключа	

	DELETE /v3/{project_id}/snapshots/{snapshot_id}/metadata/{id}		Удаление метаданных моментального снимка	
	PUT /v3/{project_id}/snapshots/{snapshot_id}/metadata/{id}		Обновите метаданные моментального снимка для определенного ключа	
Действия с моментальным снимком	POST /v3/{project_id}/snapshots/{id}/action		Сброс состояния моментального снимка	
			Состояние обновления моментального снимка	
			Принудительное удаление моментального снимка	
Расширение для управления моментальными снимками	POST /v3/{project_id}/manageable_snapshots		Управление существующим моментальным снимком	
	GET /v3/{project_id}/manageable_snapshots		Краткий список моментальных снимков, доступных для управления	
	GET /v3/{project_id}/manageable_snapshots/detail		Подробный список моментальных снимков, доступных для управления	
Передача томов	POST /v3/{project_id}/volume-transfer/{id}/accept		Принять передачу тома	
	POST /v3/{project_id}/volume-transfer		Создание передачи тома	
	GET /v3/{project_id}/volume-transfer		Перечислите передачи тома для проекта	
	GET /v3/{project_id}/volume-transfer/{id}		Показать подробную информацию о передаче тома	
	DELETE /v3/{project_id}/volume-transfer/{id}		Удаление передачи тома	
	GET /v3/{project_id}/volume-transfer/detail		Список и подробная информация о передаче томов	
Прикрепления	DELETE /v3/{project_id}/attachments/{id}	ИФБО	Удалить прикрепление	Интерфей с межмодульного

				взаимодействия
	GET /v3/{project_id}/attachments/{id}		Показать сведения о прикреплении	
	GET /v3/{project_id}/attachments/detail		Список прикреплений с подробной информацией	
	GET /v3/{project_id}/attachments		Список прикреплений	
	POST /v3/{project_id}/attachments	ИФБО	Создать прикрепление	Интерфейс межмодульного взаимодействия
	PUT /v3/{project_id}/attachments/{id}		Обновить прикрепление	
	POST /v3/{project_id}/attachments/{id}/action	ИФБО	Завершить прикрепление	Интерфейс межмодульного взаимодействия
Зоны доступности	GET /v3/{project_id}/os-availability-zone		Перечислить информацию о зоне доступности	
Внутренние пулы хранения	GET /v3/{project_id}/scheduler-stats/get_pools		Перечислите все внутренние пулы хранения	
Резервные копии	GET /v3/{project_id}/backups/detail		Список резервных копий с подробной информацией	
	GET /v3/{project_id}/backups/{id}		Показать подробную информацию о резервной копии	
	DELETE /v3/{project_id}/backups/{id}		Удаление резервной копии	
	POST /v3/{project_id}/backups/{id}/restore		Восстановить резервную копию	
	POST /v3/{project_id}/backups		Создайте резервную копию	
	PUT /v3/{project_id}/backups/{id}		Обновите резервную копию	

	GET /v3/{project_id}/backups		Список резервных копий для проекта	
	GET /v3/{project_id}/backups/{id}/export_record		Экспортируйте резервную копию	
	POST /v3/{project_id}/backups/import_record		Импортируйте резервную копию	
Действия с резервными копиями	POST /v3/{project_id}/backups/{id}/action		Принудительное удаление резервной копии	
	POST /v3/{project_id}/backups/{id}/action		Сброс состояния резервной копии	
Возможности для серверных частей хранилища	GET /v3/{project_id}/capabilities/{id}		Показать все внутренние возможности (серверная часть)	
Кластеры	GET /v3/{project_id}/clusters/{id}		Показать сведения о кластере	
	GET /v3/{project_id}/clusters		Список кластеров	
	GET /v3/{project_id}/clusters/detail		Список кластеров с подробной информацией	
Консистентные группы (согласованности)	GET /v3/{project_id}/consistencygroups		Перечислите группы согласованности проекта	
	POST /v3/{project_id}/consistencygroups		Создайте консистентную группу	
	GET /v3/{project_id}/consistencygroups/{id}		Показать сведения о консистентной группе	
	POST /v3/{project_id}/consistencygroups/create_from_src		Создайте консистентную группу из источника (исходного кода)	
	POST /v3/{project_id}/consistencygroups/{id}/delete		Удаление консистентной группы	
	GET /v3/{project_id}/consistencygroups/detail		Перечислите консистентные группы и подробные сведения	

	PUT /v3/{project_id}/consistencygroups/{id}/update		Обновить консистентную группу	
Моментальные снимки консистентной группы	DELETE /v3/{project_id}/cgsnapshots/{id}		Удаление моментального снимка консистентной группы	
	GET /v3/{project_id}/cgsnapshots/{id}		Показать подробные сведения о моментальном снимке консистентной группы	
	GET /v3/{project_id}/cgsnapshots/detail		Список всех моментальных снимков консистентной группы с подробной информацией	
	GET /v3/{project_id}/cgsnapshots		Список всех моментальных снимков консистентной группы	
	POST /v3/{project_id}/cgsnapshots		Создание моментального снимка консистентной группы	
Сервисы	GET /v3/{project_id}/os-services		Перечислите все сервисы работы с блочными устройствами хранения данных	
Общие группы томов	GET /v3/{project_id}/groups		Список групп	
	POST /v3/{project_id}/groups		Создать группу	
	GET /v3/{project_id}/groups/{id}		Показать сведения о группе	
	POST /v3/{project_id}/groups/action		Создать группу из источника (исходного кода)	
	POST /v3/{project_id}/groups/{id}/action		Удалить группу	
	GET /v3/{project_id}/groups/detail		Список групп с подробной информацией	
	PUT /v3/{project_id}/groups/{id}		Обновить группу	
	POST /v3/{project_id}/groups/{id}/action		Сброс статуса группы	
Групповая репликация			Список целевых объектов репликации	

	POST /v3/{project_id}/groups/{id}/action		Включить групповую репликацию	
			Отключить групповую репликацию	
			Отказоустойчивая репликация	
Моментальные снимки группы	DELETE /v3/{project_id}/group_snapshots/{id}		Удалить снимок группы	
	GET /v3/{project_id}/group_snapshots/{id}		Показать сведения о моментальном снимке группы	
	GET /v3/{project_id}/group_snapshots/detail		Список снимков группы с подробной информацией	
	GET /v3/{project_id}/group_snapshots		Список моментальных снимков группы	
	POST /v3/{project_id}/group_snapshots		Создание моментального снимка группы	
	POST /v3/{project_id}/group_snapshots/{id}/action		Сброс состояния моментального снимка группы	
Типы групп	PUT /v3/{project_id}/group_types/{id}		Обновить тип группы	
	GET /v3/{project_id}/group_types/{id}		Показать сведения о типе группы	
	GET /v3/{project_id}/group_types/default		Показать сведения о типе группы по умолчанию	
	DELETE /v3/{project_id}/group_types/{id}		Удалить тип группы	
	GET /v3/{project_id}/group_types		Список типов групп	
	POST /v3/{project_id}/group_types		Создать тип группы	
Спецификации группового типа	POST /v3/{project_id}/group_types/{group_type_id}/group_specs		Создание или обновление групповых спецификаций для типа группы	
	GET /v3/{project_id}/group_types/{group_type_id}/group_specs		Перечислите спецификации группы для типа группы	

	GET /v3/{project_id}/group_types/{group_type_id}/group_specs/{id}		Показать одну конкретную спецификацию группы для типа группы	
	PUT /v3/{project_id}/group_types/{group_type_id}/group_specs/{id}		Обновить спецификацию одной конкретной группы для типа группы	
	DELETE /v3/{project_id}/group_types/{group_type_id}/group_specs/{id}		Удалить одну конкретную спецификацию группы для типа группы	
Расширение хостов	GET /v3/{project_id}/os-hosts		Список всех хостов для проекта	
	GET /v3/{project_id}/os-hosts/{id}		Показать сведения о хосте для проекта	
Ограничения	GET /v3/{project_id}/limits		Показать абсолютные ограничения для проекта	
Сообщения	DELETE /v3/{project_id}/messages/{id}		Удалить сообщение	
	GET /v3/{project_id}/messages/{id}		Показать сведения сообщения	
	GET /v3/{project_id}/messages		Список сообщений	
Фильтры ресурсов	GET /v3/{project_id}/resource_filters		Список фильтров ресурсов	
Технические спецификации (характеристики), определяющие качество функций системы	GET /v3/{project_id}/qos-specs/{id}/disassociate_all		Отделите спецификацию QoS (набор инструментов для управления пропускной способностью, задержками и приоритетами трафика) от всех ассоциаций	
	PUT /v3/{project_id}/qos-specs/{id}/delete_keys		Отмените установку ключей в спецификации QoS	
	GET /v3/{project_id}/qos-specs/{id}/associations		Получите все ассоциации для спецификации QoS	

	GET /v3/{project_id}/qos-specs/{id}/associate		Свяжите спецификацию QoS с типом тома	
	GET /v3/{project_id}/qos-specs/{id}/disassociate		Отделите спецификацию QoS от типа тома	
	GET /v3/{project_id}/qos-specs/{id}		Показать подробную информацию о спецификации QoS	
	PUT /v3/{project_id}/qos-specs/{id}		Установите ключи в спецификации QoS	
	DELETE /v3/{project_id}/qos-specs/{id}		Удаление спецификации QoS	
	POST /v3/{project_id}/qos-specs		Создайте спецификацию QoS	
	GET /v3/{project_id}/qos-specs		Перечислите Спецификации QoS	
Расширение для управления классами квот	GET /v3/{project_id}/os-quota-class-sets/{id}		Показывать классы квот для проекта	
	PUT /v3/{project_id}/os-quota-class-sets/{id}		Обновление классов квот для проекта	
Расширение для управления квотами	GET /v3/{project_id}/os-quota-sets/{id}		Показать квоты для проекта	
	PUT /v3/{project_id}/os-quota-sets/{id}		Обновление квот для проекта	
	DELETE /v3/{project_id}/os-quota-sets/{id}		Удаление квот для проекта	
	GET /v3/{project_id}/os-quota-sets/{id}/defaults		Получение квот по умолчанию для проекта	
Скрипты (workers)	POST v3/{project_id}/workers /cleanup		Очистка сервисов	

Для данных интерфейсов параметры указаны в электронном приложении к документу «Программное обеспечение «Облачная платформа KeyStack SE v.1». Руководство пользователя» (Каталог – «Электронное приложение» – «Интерфейсы» – «интерфейсы_cinder_v3.71.yaml»). Для поиска параметров в электронном приложении необходимо выполнить команду Ctrl + F и ввести в строку поиска API, после чего в файле будет найдено указанное API и приведены его параметры.

8.13 Интерфейсы модуля Glance

В Таблице 5 приведены интерфейсы модуля Glance, назначением которых является реализация, в том числе, требований безопасности, связанных с централизованным управлением образами виртуальных машин и виртуальными машинами в ПО «KeyStack SE». Интерфейсы представлены API и могут быть использованы посредством применения вызовов по протоколу REST API.

Таблица 5 – Интерфейсы модуля Glance и их назначение

Интерфейсы		Является ли ИФБО применительно к ОО	Назначение	Комментарий
Образы	POST /v2/images	ИФБО	Создать образ	Интерфейс доступный внешним пользователям (интерфейс создания образа виртуальной машины Портала Администрирования)
	GET /v2/images/{image_id}	ИФБО	Показать образ	Интерфейс межмодульного взаимодействия
	GET /v2/images/{image_id}/tasks		Показать задачи, связанные с образом	
	GET /v2/images	ИФБО	Список образов	Интерфейс межмодульного взаимодействия
	PATCH /v2/images/{image_id}		Обновить образ	Интерфейс доступный внешним пользователям
	DELETE /v2/images/{image_id}	ИФБО	Удалить образ	Интерфейс доступный внешним пользователям (интерфейс удаления образа виртуальной

				машины Портала Администрирования)
	POST /v2/images/{image_id}/actions/deactivate		Деактивировать образ	
	POST /v2/images/{image_id}/actions/reactivate		Повторно активировать образ	
Общий доступ	POST /v2/images/{image_id}/members		Создать пользователя образа	
	GET /v2/images/{image_id}/members/{member_id}		Показать сведения о пользователе образа	
	GET /v2/images/{image_id}/members		Список пользователей образа	
	PUT /v2/images/{image_id}/members/{member_id}		Обновить пользователя образа	
	DELETE /v2/images/{image_id}/members/{member_id}		Удалить пользователя образа	
Тег образа	PUT /v2/images/{image_id}/tags/{tag_value}		Добавить тег образа	
	DELETE /v2/images/{image_id}/tags/{tag_value}		Удалить тег образа	
Схема образа	GET /v2/schemas/images		Показать схему образов	
	GET /v2/schemas/image		Показать схему образов	
	GET /v2/schemas/members		Показать схему пользователей образов	
	GET /v2/schemas/member		Показать схему пользователя образов	
Данные образа	PUT /v2/images/{image_id}/file		Загрузка двоичных данных образа	
	GET /v2/images/{image_id}/file	ИФБО	Скачивание двоичных данных образа	Интерфейс межмодульного взаимодействия

Совместимый импорт образа	PUT /v2/images/{image_id}/stage		Поместить двоичные данные образа в область подготовки	
	POST /v2/images/{image_id}/import		Импорт образа	
Хранилища	DELETE /v2/stores/{store_id}/{image_id}		Удалить образ из хранилища	
Информация о сервисе образов (обнаружение)	GET /v2/info/import		Получить информацию о методах импорта и значениях (размер, формат и т.д.)	
	GET /v2/info/stores		Список хранилищ	
	GET /v2/info/usage		Использование квоты	
	GET /info/stores/detail		Список сведений о хранилищах	
Задачи	POST /v2/tasks		Создать задачу	
	GET /v2/tasks		Список задач	
	GET /v2/tasks/{task_id}		Показать детали задачи	
Схемы задач	GET /v2/schemas/tasks		Показать схему задач	
	GET /v2/schemas/task		Показать схему задачи	
Управление кэшем	GET /v2/cache		Состояние кэша запросов	
	PUT /v2/cache/{image_id}		Постановка образа в очередь	
	DELETE /v2/cache/{image_id}		Удалить образ из кэша	
	DELETE /v2/cache		Очистка образов из кэша	

Для данных интерфейсов параметры указаны в электронном приложении к документу «Программное обеспечение «Облачная платформа KeyStack SE v.1». Руководство пользователя» (Каталог – «Электронное приложение» – «Интерфейсы» – «интерфейсы_glance_v2.16.yaml»). Для поиска параметров в электронном приложении необходимо выполнить команду Ctrl + F и ввести в строку поиска API, после чего в файле будет найдено указанное API и приведены его параметры.

8.14 Интерфейсы модуля OVS

Интерфейсы модуля OVS, их назначение и параметры приведены в электронном приложении к документу «Программное обеспечение «Облачная платформа KeyStack SE

v.1». Руководство пользователя» (Каталог – «Электронное приложение» – «Интерфейсы» – «Описание_интерфейсов_ovs-vsctl.docx»). Интерфейс представлен командной строкой, принимающей на вход команды и их параметры.

Назначением интерфейсов является реализация, в том числе, требований безопасности, связанных с управлением потоками информации в ПО «KeyStack SE».

8.15 Интерфейсы модуля Fluentd

Интерфейсы модуля Fluentd и их параметры представлены в электронном приложении к документу «Программное обеспечение «Облачная платформа KeyStack SE v.1». Руководство пользователя» (Каталог – «Электронное приложение» – «Интерфейсы» – «интерфейсы_fluentd.conf»). Интерфейс представлен конфигурационным файлом.

Назначением интерфейсов является реализация требований безопасности, связанных с регистрацией событий безопасности в ПО «KeyStack SE».

8.16 Интерфейсы модуля Gitlab

Интерфейсы модуля Gitlab и их параметры представлены в электронном приложении к документу «Программное обеспечение «Облачная платформа KeyStack SE v.1». Руководство пользователя» (Каталог – «Электронное приложение» – «Интерфейсы» – «Интерфейсы» – «интерфейсы_gitlab_v3.0.1.yaml»). Интерфейсы представлены API и могут быть использованы посредством применения вызовов по протоколу REST API.

8.17 Интерфейсы модуля Hashicorp Vault

Интерфейсы модуля Hashicorp Vault и их параметры представлены в электронном приложении к документу «Программное обеспечение «Облачная платформа KeyStack SE v.1». Руководство пользователя» (Каталог – «Электронное приложение» – «Интерфейсы» – «Интерфейсы» – «интерфейсы_hashicorp vault_v3.0.2.yaml»). Интерфейсы представлены API и могут быть использованы посредством применения вызовов по протоколу REST API.

8.18 Интерфейсы модуля RPM-repo

Модуль RPM-repo не имеет интерфейсов взаимодействия с пользователем. Интерфейсы, обеспечивающие создание и обновление RPM-репозитория, приведены в электронном приложении к документу «Программное обеспечение «Облачная платформа KeyStack SE v.1». Функциональная спецификация» (Каталог – «Электронное приложение» – «Интерфейсы» – «Описание_интерфейсов_rpm-repo.docx»). Интерфейсы представлены CLI. Доступ к файлам репозитория обеспечивает веб-сервер (Nginx) посредством применения вызовов по протоколу HTTPS

8.19 Интерфейсы модуля NetBox

Интерфейсы модуля NetBox и их параметры представлены в электронном приложении к документу «Программное обеспечение «Облачная платформа KeyStack SE v.1». Руководство пользователя» (Каталог – «Электронное приложение» – «Интерфейсы» – «Интерфейсы» – «интерфейсы_netbox_v3.0.3.yaml»). Интерфейсы представлены API и могут быть использованы посредством применения вызовов по протоколу REST API.

8.20 Интерфейсы модуля Grafana

Интерфейсы модуля Grafana и их параметры представлены в электронном приложении к документу «Программное обеспечение «Облачная платформа KeyStack SE v.1». Руководство пользователя» (Каталог – «Электронное приложение» – «Интерфейсы» – «Интерфейсы» – «интерфейсы_grafana_v.3.0.3.yaml»). Интерфейсы представлены API и могут быть использованы посредством применения вызовов по протоколу REST API.

8.21 Интерфейсы модуля Placement

В Таблице 6 приведены интерфейсы модуля Placement, позволяющие осуществлять создание, удаление и управление классами ресурсов, а также поставщиками этих ресурсов в ПО «KeyStack SE». Интерфейсы представлены API и могут быть использованы посредством применения вызовов по протоколу REST API.

Интерфейсы модуля Placement не реализуют функции безопасности и не влияют на них.

Таблица 6 – Интерфейсы модуля Placement и их назначение

Интерфейсы		Назначение
Поставщики ресурсов	GET /resource_providers	Список поставщиков ресурсов
	POST /resource_providers	Создать поставщика ресурсов
Поставщик ресурсов	GET /resource_providers/{uuid}	Показать поставщика ресурсов
	PUT /resource_providers/{uuid}	Обновить поставщика ресурсов
	DELETE /resource_providers/{uuid}	Удалить поставщика ресурсов
Классы ресурсов	GET /resource_classes	Список классов ресурсов
	POST /resource_classes	Создать класс ресурсов
Класс ресурсов	GET /resource_classes/{name}	Показать класс ресурсов
	PUT /resource_classes/{name}	Обновить класс ресурсов
	DELETE /resource_classes/{name}	Удалить класс ресурсов
Инвентарные записи поставщика ресурсов	GET /resource_providers/{uuid}/inventories	Перечислить записи поставщика ресурсов
	PUT /resource_providers/{uuid}/inventories	Обновить записи поставщика ресурсов
	DELETE /resource_providers/{uuid}/inventories	Удалить записи поставщика ресурсов
Инвентаризация поставщика ресурсов	GET /resource_providers/{uuid}/inventories/{resource_class}	Показать инвентаризацию поставщиков ресурсов

	PUT /resource_providers/{uuid}/inventories/{resource_class}	Обновление инвентаря поставщиков ресурсов
	DELETE /resource_providers/{uuid}/inventories/{resource_class}	Удалить инвентаризацию поставщиков ресурсов
Аггрегаты (группы) поставщиков ресурсов	GET /resource_providers/{uuid}/aggregates	Список аггрегатов поставщиков ресурсов
	PUT /resource_providers/{uuid}/aggregates	Обновление аггрегатов поставщиков ресурсов
Характеристики	GET /traits	Список характеристик
	GET /traits/{name}	Показать характеристики
	PUT /traits/{name}	Обновить характеристики
	DELETE /traits/{name}	Удалить характеристики
Характеристики поставщика ресурсов	GET /resource_providers/{uuid}/traits	Перечислить характеристики поставщика ресурсов
	PUT /resource_providers/{uuid}/traits	Обновление характеристик поставщика ресурсов
	DELETE /resource_providers/{uuid}/traits	Удаление характеристик поставщика ресурсов
Распределения	POST /allocations	Управление распределениями
	GET /allocations/{consumer_uuid}	Список распределений потребителя
	PUT /allocations/{consumer_uuid}	Обновить распределения потребителя
	DELETE /allocations/{consumer_uuid}	Удалить распределения потребителя
Распределение ресурсов между поставщиками	GET /resource_providers/{uuid}/allocations	Перечислить распределения ресурсов между поставщиками

Использование ресурсов	GET /usages	Список использования ресурсов
Использование поставщика ресурсов	GET /resource_providers/{uuid}/usages	Список использований поставщика ресурсов
Кандидаты на распределение	GET /allocation_candidates	Список кандидатов на распределение
Операция по преобразованию поставщиков ресурсов (Reshaper)	POST /reshaper	Операция по преобразованию поставщиков ресурсов (Reshaper)

8.22 Интерфейсы модуля Octavia

В Таблице 7 приведены интерфейсы модуля Octavia, позволяющие осуществлять создание, удаление и управление балансировщиком сетевой нагрузки, пулами, компонентами, политиками и правилами L7, квотами, конфигурациями, зонами доступности, а также проверками работоспособности в ПО «KeyStack SE». Интерфейсы представлены API и могут быть использованы посредством применения вызовов по протоколу REST API.

Интерфейсы модуля Octavia не реализуют функции безопасности и не влияют на них.

Таблица 7 – Интерфейсы модуля Octavia и их назначение

Интерфейсы		Назначение
Балансировщики нагрузки	GET /v2/lbaas/loadbalancers	Список балансировщиков нагрузки
	POST /v2/lbaas/loadbalancers	Создать балансировщик нагрузки
	GET /v2/lbaas/loadbalancers/{loadbalancer_id}	Показать сведения о балансировщике нагрузки
	PUT /v2/lbaas/loadbalancers/{loadbalancer_id}	Обновить балансировщик нагрузки
	DELETE /v2/lbaas/loadbalancers/{loadbalancer_id}	Удалить балансировщик нагрузки
	GET /v2/lbaas/loadbalancers/{loadbalancer_id}/stats	Получить статистику балансировщика нагрузки
	GET /v2/lbaas/loadbalancers/{loadbalancer_id}/status	Получить дерево состояния балансировщика нагрузки
	PUT /v2/lbaas/loadbalancers/{loadbalancer_id}/failover	Переключение после сбоев балансировщика нагрузки

Слушатели	GET /v2/lbaas/listeners	Список слушателей
	POST /v2/lbaas/listeners	Создать слушателя
	GET /v2/lbaas/listeners/{listener_id}	Показать сведения о слушателе
	PUT /v2/lbaas/listeners/{listener_id}	Обновить слушателя
	DELETE /v2/lbaas/listeners/{listener_id}	Удалить слушателя
	GET /v2/lbaas/listeners/{listener_id}/stats	Получение статистики слушателей
Пулы	GET /v2/lbaas/pools	Список пулов
	POST /v2/lbaas/pools	Создать пул
	GET /v2/lbaas/pools/{pool_id}	Показать сведения о пуле
	PUT /v2/lbaas/pools/{pool_id}	Обновить пул
	DELETE /v2/lbaas/pools/{pool_id}	Удалить пул
Компоненты	GET /v2/lbaas/pools/{pool_id}/members	Список компонентов
	POST /v2/lbaas/pools/{pool_id}/members	Создать компонент
	GET /v2/lbaas/pools/{pool_id}/members/{member-id}	Показать сведения о компоненте
	PUT /v2/lbaas/pools/{pool_id}/members/{member_id}	Обновить компонент
	PUT /v2/lbaas/pools/{pool_id}/members	Пакетное обновление компонентов
	DELETE /v2/lbaas/pools/{pool_id}/members/{member_id}	Удалить компонент
Проверка работоспособности	GET /v2/lbaas/healthmonitors	Список проверок работоспособности
	POST /v2/lbaas/healthmonitors	Создать проверку работоспособности
	GET /v2/lbaas/healthmonitors/{healthmonitor_id}	Показать сведения о проверке работоспособности
	PUT /v2/lbaas/healthmonitors/{healthmonitor_id}	Обновить проверку работоспособности

	DELETE /v2/lbaas/healthmonitors/{healthmonitor_id}	Удалить проверку работоспособности
Политики L7	GET /v2/lbaas/l7policies	Список политик L7
	POST /v2/lbaas/l7policies	Создать политику L7
	GET /v2/lbaas/l7policies/{l7policy_id}	Показать информацию о политике L7
	PUT /v2/lbaas/l7policies/{l7policy_id}	Обновить политику L7
	DELETE /v2/lbaas/l7policies/{l7policy_id}	Удалить политику L7
Правила L7	GET /v2/lbaas/l7policies/{l7policy_id}/rules	Список правил L7
	POST /v2/lbaas/l7policies/{l7policy_id}/rules	Создать правило L7
	GET /v2/lbaas/l7policies/{l7policy_id}/rules/{l7rule_id}	Показать информацию о правилах L7
	PUT /v2/lbaas/l7policies/{l7policy_id}/rules/{l7rule_id}	Обновить правило L7
	DELETE /v2/lbaas/l7policies/{l7policy_id}/rules/{l7rule_id}	Удалить правило L7
Квоты	GET /v2/lbaas/quotas	Список Квот
	GET /v2/lbaas/quotas/defaults	Показывать значения по умолчанию для квот
	GET /v2/lbaas/quotas/{project_id}	Показать Квоту проекта
	PUT /v2/lbaas/quotas/{project_id}	Обновить квоту
	DELETE /v2/lbaas/quotas/{project_id}	Сброс квоты
Поставщики	GET /v2/lbaas/providers	Список Поставщиков
	GET /v2/lbaas/providers/{provider}/flavor_capabilities	Описание возможностей конфигурации поставщика
	GET /v2/lbaas/providers/{provider}/availability_zone_capabilities	Показать возможности зоны доступности поставщика
Конфигурации	GET /v2/lbaas/flavors	Список конфигураций
	POST /v2/lbaas/flavors	Создать конфигурацию

	GET /v2/lbaas/flavors/{flavor_id}	Показать сведения о конфигурации
	PUT /v2/lbaas/flavors/{flavor_id}	Обновить конфигурацию
	DELETE /v2/lbaas/flavors/{flavor_id}	Удалить конфигурацию
Профили конфигурации	GET /v2/lbaas/flavorprofiles	Список профилей конфигурации
	POST /v2/lbaas/flavorprofiles	Создать профиль конфигурации
	GET /v2/lbaas/flavorprofiles/{flavorprofile_id}	Показать сведения о профиле конфигурации
	PUT /v2/lbaas/flavorprofiles/{flavorprofile_id}	Обновить профиль конфигурации
	DELETE /v2/lbaas/flavorprofiles/{flavorprofile_id}	Удалить профиль конфигурации
Зоны доступности	GET /v2/lbaas/availabilityzones	Список зон доступности
	POST /v2/lbaas/availabilityzones	Создание зоны доступности
	GET /v2/lbaas/availabilityzones/{availabilityzone_id}	Показать информацию о зоне доступности
	PUT /v2/lbaas/availabilityzones/{availabilityzone_id}	Обновить зону доступности
	DELETE /v2/lbaas/availabilityzones/{availabilityzone_id}	Удаление зоны доступности
Профили зон доступности	GET /v2/lbaas/availabilityzoneprofiles	Список профилей зоны доступности
	POST /v2/lbaas/availabilityzoneprofiles	Создание профиля зоны доступности
	GET /v2/lbaas/availabilityzoneprofiles/{availabilityzoneprofile_id}	Показать сведения о профиле зоны доступности
	PUT /v2/lbaas/availabilityzoneprofiles/{availabilityzoneprofile_id}	Обновить профиль зоны доступности
	DELETE /v2/lbaas/availabilityzoneprofiles/{availabilityzoneprofile_id}	Удаление профиля зоны доступности
Амфора (компонент балансировки нагрузки)	GET /v2/octavia/amphorae	Список амфор (компонентов балансировки нагрузки)
	GET /v2/octavia/amphorae/{amphora_id}	Показать сведения об амфорах (компонентах балансировки нагрузки)

	GET /v2/octavia/amphorae/{amphora_id}/stats	Показать статистику амфор (компонента балансировки нагрузки)
	PUT /v2/octavia/amphorae/{amphora_id}/config	Настройка амфор (компонента балансировки нагрузки)
	PUT /v2/octavia/amphorae/{amphora_id}/failover	Переключение амфоры (компонента балансировки нагрузки) после сбоев
	DELETE /v2/octavia/amphorae/{amphora_id}	Удалить амфору (компонент балансировки нагрузки)

8.23 Интерфейсы модуля Barbican

В Таблице 8 приведены интерфейсы модуля Barbican, позволяющие осуществлять создание, удаление и управление секретами, метаданными и хранилищами секретов, потребителями секретов, квотами, заказами, а также контейнерами и их потребителями в ПО «KeyStack SE». Интерфейсы представлены API и могут быть использованы посредством применения вызовов по протоколу REST API.

Интерфейсы модуля Barbican не реализуют функции безопасности и не влияют на них.

Таблица 8 – Интерфейсы модуля Barbican и их назначение

Интерфейсы			Назначение
API секретов	GET /v1/secrets		Перечисляет секреты проекта
	POST /v1/secrets		Создает секретную сущность
	GET /v1/secrets/{secret_id}		Извлекает метаданные секрета
	PUT /v1/secrets/{secret_id}		Добавляет полезную нагрузку к существующему секрету, состоящему только из метаданных
	DELETE /v1/secrets/{secret_id}		Удаляет секрет
	GET /v1/secrets/{secret_id}/payload		Извлекает полезную нагрузку секрета
API потребителей секрета	GET {secret_ref}/consumers	/v1/secrets/{secret_id}/consumers	Перечисляет потребителей секрета
	POST {secret_ref}/consumers		Создает потребителя
	DELETE {secret_ref}/consumers		Удаляет потребителя
API метаданных секрета	GET /v1/secrets/{secret_id}/metadata		Перечисляет пользовательские метаданные секрета
	PUT /v1/secrets/{secret_id}/metadata		Устанавливает метаданные для секрета
	GET /v1/secrets/{secret_id}/metadata/{key}		Извлекает метаданные секрета, добавленные пользователем

	POST /v1/secrets/{secret_id}/metadata/		Добавляет новую пару ключ / значение к пользовательским метаданным секрета
	PUT /v1/secrets/{secret_id}/metadata/{key}		Обновляет существующую пару ключ / значение в метаданных пользователя секрета
	DELETE /v1/secrets/{secret_id}/metadata/{key}		Удаляет метаданные секрета по ключу
API хранилищ секретов	GET /v1/secret-stores		Администратор проекта может запросить список доступных бэкендов (серверных частей) для хранилища секретов
	GET /v1/secret-stores/{secret_store_id}		Администратор проекта (пользователь с ролью администратора) может запросить сведения о хранилище секретов по его идентификатору
	GET /v1/secret-stores/preferred		Администратор проекта (пользователь с ролью администратора) может запросить ссылку на предпочтительное хранилище секретов, если оно было назначено ранее
	POST /v1/secret-stores/{secret_store_id}/preferred		Администратор проекта может установить предпочтительный бэкенд (серверную часть) хранилища секретов для своего проекта
	DELETE /v1/secret-stores/{secret_store_id}/preferred		Администратор проекта может удалить предпочтительную настройку бэкенда (серверной части) хранилища секретов
	GET /v1/secret-stores/global-default		Администратор проекта или сервиса может запросить ссылку на хранилище секретов, которое используется в качестве бэкэнда по умолчанию для развертывания
API контейнеров	GET /v1/containers		Содержит список контейнеров проекта
	GET /v1/containers/{container_id}		Извлекает отдельный контейнер
	POST /v1/containers		Создает контейнер
	DELETE /v1/containers/{container_id}		Удаляет контейнер
	POST /v1/containers/{container_id}/secrets		Добавляет секрет в существующий контейнер
	DELETE /v1/containers/{container_id}/secrets		Извлекает секрет из контейнера
API для потребителей	GET {container_ref}/consumers	/v1/containers/{container_id}/consumers	Перечисляет потребителей контейнера

контейнеров	POST {container_ref}/consumers		Создает потребителя
	DELETE {container_ref}/consumers		Удаляет потребителя
ACL API (список контроля доступа)	GET /v1/secrets/{secret_id}/acl		Получает настройки списка управления доступом (ACL) для заданного секрета
	PUT /v1/secrets/{secret_id}/acl		Создает новый или заменяет существующий список контроля доступа (ACL) для заданного секрета
	PATCH /v1/secrets/{secret_id}/acl		Обновляет существующий список контроля доступа (ACL) для заданного секрета
	DELETE /v1/secrets/{secret_id}/acl		Удаляет ACL для заданного секрета
API квот	GET /v1/quotas		Получить действующие квоты для проекта заявителя
	GET /v1/project-quotas		Получает список настроенных записей квот проекта
	GET /v1/project-quotas/{project-quota_id}		Извлекает информацию о настроенной квоте проекта
	PUT /v1/project-quotas/{project-quota_id}		Создает или обновляет настроенные квоты проекта для проекта с указанным UUID
	DELETE /v1/project-quotas/{project-quota_id}		Удаляет конфигурацию квот проекта для проекта с указанным UUID
API заказов	GET /v1/orders		Перечисляет заказы проекта
	POST /v1/orders		Создает заказ
	GET /v1/orders/{order_id}		Извлекает метаданные заказа
	DELETE /v1/orders/{order_id}		Удаляет заказ

8.24 Описание иных интерфейсов модулей ПО «KeyStack SE», не влияющих на функции безопасности

8.24.1 Интерфейсы модулей, представленных в электронных приложениях

Интерфейсы модуля Heat, не влияющие на функции безопасности, представлены в электронном приложении к документу «Программное обеспечение «Облачная платформа KeyStack SE v.1». Руководство пользователя» (Каталог – «Электронное приложение» – «Интерфейсы» – «Описание_интерфейсов_heat.docx»). Интерфейсы представлены API и могут быть использованы посредством применения вызовов с использованием API.

Интерфейсы модуля Hashicorp consul, не влияющие на функции безопасности, представлены в электронном приложении к документу «Программное обеспечение «Облачная платформа KeyStack SE v.1». Руководство пользователя» (Каталог – «Электронное приложение» – «Интерфейсы» – «Описание_интерфейсов_hashicorp_consul.docx»). Интерфейсы представлены API и могут быть использованы посредством применения вызовов с использованием API.

Интерфейсы модуля DRS, не влияющие на функции безопасности, представлены в электронном приложении к документу «Программное обеспечение «Облачная платформа KeyStack SE v.1». Руководство пользователя» (Каталог – «Электронное приложение» –

«Интерфейсы» – «интерфейсы_drs.yaml»). Интерфейсы представлены API и могут быть использованы посредством применения вызовов по с использованием REST API.

Интерфейсы модуля FRR, не влияющие на функции безопасности, представлены в электронном приложении к документу «Программное обеспечение «Облачная платформа KeyStack SE v.1». Руководство пользователя» (Каталог – «Электронное приложение» – «Интерфейсы» – «Описание_интерфейсов_frr.docx»). Интерфейс представлен конфигурационным файлом и использует команды для настройки конфигурации.

Интерфейсы модуля OVN, не влияющие на функции безопасности, представлены в электронном приложении к документу «Программное обеспечение «Облачная платформа KeyStack SE v.1». Руководство пользователя» (Каталог – «Электронное приложение» – «Интерфейсы» – «Описание_интерфейсов_ovn–sbctl.docx»). Интерфейс представлен командной строкой, принимающей на вход команды и их параметры.

Интерфейсы модуля Prometheus, не влияющие на функции безопасности, представлены в электронном приложении к документу «Программное обеспечение «Облачная платформа KeyStack SE v.1». Руководство пользователя» (Каталог – «Электронное приложение» – «Интерфейсы» – «интерфейсы_prometheus_v.3.0.1.yaml»). Интерфейсы представлены API и могут быть использованы посредством применения вызовов с использованием API.

Интерфейсы модуля Prometheus Alertmanager, не влияющие на функции безопасности, представлены в электронном приложении к документу «Программное обеспечение «Облачная платформа KeyStack SE v.1». Руководство пользователя» (Каталог – «Электронное приложение» – «Интерфейсы» – «интерфейсы_alertmanager_v.0.0.1.yaml»). Интерфейсы представлены API и могут быть использованы посредством применения вызовов с использованием API.

Интерфейсы модуля Bifrost, не влияющие на функции безопасности, представлены в электронном приложении к документу «Программное обеспечение «Облачная платформа KeyStack SE v.1». Руководство пользователя» (Каталог – «Электронное приложение» – «Интерфейсы» – «Описание_интерфейсов_bare_metal.docx»). Интерфейсы представлены API и могут быть использованы посредством применения вызовов по протоколу REST API.

Интерфейсы модуля Multipathd, не влияющие на функции безопасности, представлены в электронном приложении к документу «Программное обеспечение «Облачная платформа KeyStack SE v.1». Руководство пользователя» (Каталог – «Электронное приложение» – «Интерфейсы» – «Описание_интерфейсов_multipathd.docx»). Интерфейс представлен конфигурационным файлом и использует команды для настройки конфигурации.

Интерфейсы модуля Iscsid, не влияющие на функции безопасности, представлены в электронном приложении к документу «Программное обеспечение «Облачная платформа KeyStack SE v.1». Руководство пользователя» (Каталог – «Электронное приложение» – «Интерфейсы» – «Описание_интерфейсов_iscsid.docx»). Интерфейс представлен конфигурационным файлом и реализует канал управления протоколом iSCSI.

Интерфейсы модуля Redis Sentinel, не влияющие на функции безопасности, представлены в электронном приложении к документу «Программное обеспечение «Облачная платформа KeyStack SE v.1». Руководство пользователя» (Каталог – «Электронное приложение» – «Интерфейсы» – «Описание_интерфейса_sentinel_redis.docx»). Интерфейс представлен конфигурационным файлом.

Интерфейсы модуля ProxySQL, не влияющие на функции безопасности, представлены в электронном приложении к документу «Программное обеспечение «Облачная платформа KeyStack SE v.1». Руководство пользователя» (Каталог – «Электронное приложение» – «Интерфейсы» – «Описание_интерфейсов_proxySQL.docx»). Интерфейс представлен конфигурационным файлом.

Интерфейсы модуля HAProxy, не влияющие на функции безопасности, представлены в электронном приложении к документу «Программное обеспечение «Облачная платформа KeyStack SE v.1». Руководство пользователя» (Каталог – «Электронное приложение» – «Интерфейсы» – «интерфейсы_HAproxy.rar»). Интерфейс представлен конфигурационным файлом.

Интерфейсы модуля Bird, не влияющие на функции безопасности, представлены в электронном приложении к документу «Программное обеспечение «Облачная платформа KeyStack SE v.1». Руководство пользователя» (Каталог – «Электронное приложение» – «Интерфейсы» – «Описание_интерфейсов_bird.docx»). Интерфейс представлен конфигурационным файлом и использует команды для настройки конфигурации.

Интерфейсы модуля ExaBGP, не влияющие на функции безопасности, представлены в электронном приложении к документу «Программное обеспечение «Облачная платформа KeyStack SE v.1». Руководство пользователя» (Каталог – «Электронное приложение» – «Интерфейсы» – «Описание_интерфейсов_exabgp.docx»). Интерфейс представлен командами для взаимодействия с ExaBGP из API.

8.24.2 Интерфейсы, представленные строкой подключения

В Таблице 9 приведены интерфейсы модулей, представленные строкой подключения.

Таблица 9 – Интерфейсы модулей, представленные строкой подключения

Компонент (модуль)	Протокол	Порт	Строка подключения
RabbitMQ	AMPQ	5672/tcp	rabbit://user:password@IP_adress:port
MariaDB	mysql	3306/tcp	mysql+pymysql://user:password@IP_adress:port
Memcached	memcache	11211/tcp	memcached_servers =IP_adress:port
Redis	RESP	6379/tcp	redis://user:password@IP_adress:port?sentinel=kolla&db=0&socket_timeout=60&retry_on_timeout=yes
Victoria Metrics	HTTPS	8428	Запросы к API
Kolla-ansible	SSH	22	ssh user@ip –p22

8.25 Интерфейсы среды функционирования, используемые для реализации контроля и доверенной загрузки ПО «KeyStack SE»

8.25.1 Проверка реализации функции контроля целостности конфигурационных параметров виртуальных машин

Для проверки реализации функции контроля целостности конфигурационных параметров виртуальных машин в средстве виртуализации используется команда virsh edit <имя_ВМ>, позволяющая вручную изменить XML-описание виртуального оборудования. После внесения изменений средство виртуализации фиксирует нарушение целостности и инициирует соответствующее защитное действие.

Порядок выполнения контроля целостности:

1. Создать экземпляр виртуальной машины (далее — ВМ), имя которого (например, instance_name) будет использоваться на протяжении проверки.

2. На вычислительном узле (compute node), где размещена данная ВМ, выполнить:

   o Подключение в интерактивном режиме к контейнеру nova_libvirt под пользователем root:

   podman exec -itu0 nova_libvirt bash

   o Выполнить команду:

   virsh edit <имя_ВМ>

Изменить значение MAC-адреса сетевого интерфейса ВМ и сохранить изменения.

3. Перейти на контроллер (control node) и ожидать автоматического перевода состояния ВМ в SHUTOFF. Это происходит при обнаружении расхождения контрольных сумм, проверка выполняется каждые 30 секунд.

   o Контролировать статус ВМ можно командой:

   openstack server show <instance_id>

4. После перевода ВМ в состояние SHUTOFF, вернуться на compute-узел и выполнить:

   less /var/log/kolla/nova/nova-compute.log

В конце журнала должно присутствовать сообщение:

WARNING nova.compute.manager [...] Checksum mismatch detected – powering off instance <instance_id> ...

Конфигурация контроля целостности указывается в файле /etc/kolla/nova-compute/nova.conf:

```
[libvirt]
monitor_domain_checksums = true       # включение контроля изменений
enforce_domain_checksums = true       # принудительное отключение ВМ при обнаружении изменений
```

Дополнительная проверка: изменение ОЗУ виртуальной машины

Также была проведена проверка при помощи команды:

virsh setmem <имя_ВМ> 256M --live

Команда изменяет значение currentMemory в режиме реального времени(с 512 до 256 МБ), при этом:

- XML-конфигурация (virsh edit) не фиксирует эти изменения;
- Контроль целостности при таком изменении срабатывает;
- Изменение подтверждается командой:

  virsh dumpxml <имя_ВМ>

  В результате фиксируется обновленное значение параметра currentMemory.

8.25.2 Проверка конфигурационных файлов

Цель проверки: демонстрация срабатывания механизма контроля целостности при внесении изменений в конфигурационные и бинарные файлы, от которых зависит корректное функционирование компонентов средства виртуализации. Проверка проводится на примере:

- модификации бинарного BIOS-файла, используемого контейнером nova_libvirt;

- внесения изменений в конфигурационный файл nova.conf.

Как включается контроль целостности:

- Задаётся переменной enable_integrity_check: "yes" в файле globals.d/REGION.yml.
- Kolla-ansible разворачивает вспомогательные скрипты, использующие podman diff, чтобы при каждом запуске контейнера nova-libvirt сравнивать текущее состояние файловой системы с эталонным слой-имаджем.
- Отслеживаются любые отклонения, в том числе BIOS-файлы виртуальной машины и все конфигурационные файлы, смонтированные в контейнер.

1. **Проверка изменения BIOS-файла контейнера nova_libvirt**
   Шаги выполнения:
   1) На вычислительном узле (compute node) выполнить подключение к контейнеру nova_libvirt от имени пользователя root:
      podman exec -itu0 nova_libvirt bash
   2) Внести изменение в бинарный файл BIOS:
      echo 0 >> /usr/share/bios/bios-256k.bin
   Изменение одного байта нарушает структуру BIOS-файла, что приводит к отказу контейнера при его последующем использовании.
   3) Проверить состояние контейнера:
      podman ps -a
   Ожидаемый результат: контейнер nova_libvirt находится в состоянии exited.
   4) Проверить наличие сообщения о нарушении целостности в лог-файле проверки BIOS:
      less /var/log/kolla/nova-libvirt-check.log
   В журнале должно содержаться сообщение вида:
      Integrity check failed, Inconsistent files: {... /usr/share/bios/bios-256k.bin ...}

2. **Проверка изменения конфигурационного файла nova.conf**
   Шаги выполнения:
   1) На том же compute-узле отредактировать конфигурационный файл nova.conf:
      vim /etc/kolla/nova-compute/nova.conf
   Добавить или изменить параметр:
      debug = True
   2) Перезапустить контейнер nova_compute:
      podman restart nova_compute
   3) Проверить состояние контейнера:
      podman ps -a
   Ожидаемый результат: контейнер nova_compute завершил работу с ошибкой (статус failed).
   4) Проанализировать журнал запуска контейнера:
      podman logs nova_compute
   В журнале должно содержаться сообщение о несоответствии контрольных сумм, например:
      Integrity check failed, Inconsistent files: {... /etc/kolla/nova-compute/nova.conf ...}

   Комментарии по механизму:
- Контроль целостности активируется одной переменной в globals.d/REGION.yml и не требует донастроек на узлах.

- В ПО «KeyStack SE» реализован механизм контроля целостности конфигурационных файлов с использованием предрасчитанных хэш-сумм.
- Проверка осуществляется при старте контейнера: текущие контрольные суммы сравниваются с эталонными.
- В случае расхождения срабатывает защитное действие — контейнер аварийно завершается.
- В настоящий момент отсутствует возможность перечитать конфигурационный файл без перезапуска контейнера, то есть для применения изменений требуется restart.

8.25.3 Проверка невозможности запуска бинарных файлов вне доверенного списка при помощи fapolicyd в SberLinux

Цель проверки: подтвердить, что в SberLinux с активным сервисом fapolicyd выполнение бинарных файлов, не находящихся в базе разрешённых (whitelist), блокируется согласно установленной политике контроля исполнения.

Предварительные условия:

- Операционная система: SberLinux (вариант исполнения: контейнеризация с использованием podman).
- Сервис контроля выполнения: fapolicyd активен.
- Конфигурация fapolicyd по умолчанию: запрещён запуск любых бинарных файлов, отсутствующих в базе доверенных (RPM DB + SHA256 checksum).

Порядок проведения проверки:

1. **Запуск службы контроля исполнения:**
   systemctl start fapolicyd.service

Убедиться, что служба успешно запущена:

   systemctl status fapolicyd

2. **Выполнение разрешённой команды ls:**
   ls /home

Ожидаемый результат: команда выполняется корректно, так как бинарник /usr/bin/ls входит в RPM-базу системы и зарегистрирован в fapolicyd.

3. **Копирование бинарника ls в нестандартное место:**
   cp /usr/bin/ls /tmp/ls
4. **Попытка запуска скопированного бинарного файла:**
   /tmp/ls

Ожидаемый результат: выполнение заблокировано:

   -bash: /tmp/ls: Operation not permitted

Причина: файл /tmp/ls отсутствует в базе fapolicyd (отсутствует запись о происхождении, подписи и контрольной сумме).

Применённые настройки fapolicyd:

- Используется политика по умолчанию, согласно которой разрешено выполнение только тех бинарных файлов, которые:
  - зарегистрированы в RPM-базе;
  - либо явно добавлены в список доверенных (fapolicyd-cli --add-trust ...).
- Подключение бинарников без записи в базу приводит к отказу в выполнении.

Особенности поведения в SberLinux:

- SberLinux поддерживает три типа исполнения (варианта установки), в т.ч. контейнеризованное, используемое в данной проверке.
- При исполнении в контейнерной среде (podman) fapolicyd не применяется внутри контейнеров.

- Это объясняется архитектурой контейнеризации: контроль целостности внутри контейнера осуществляется средствами podman, а не fapolicyd.

- В текущем тестовом окружении:
  - Контейнер nova_libvirt добавлен в исключения fapolicyd вручную (на уровне хоста);
  - podman не добавлен в исключения, что сохраняет возможность проверок вне контейнерной среды;
  - Контроль исполнения работает только на хостовой ОС, в контейнере — не функционирует.

Выводы:

- Сервис fapolicyd в SberLinux корректно блокирует выполнение бинарных файлов, отсутствующих в доверенной базе.
- Механизм эффективен для защиты хостовой системы от запуска непроверенных или модифицированных исполняемых файлов.
- В контейнерной среде механизм контроля исполнения fapolicyd не действует — целостность контролируется на уровне инфраструктуры podman.
- Для контейнерной изоляции и контроля используется собственная логика podman, включая overlayfs и контроль запуска.

В составе SberLinux реализована система hardening, активируемая автоматически при установке в соответствии с выбранным профилем исполнения. Скрипты hardening выполняют настройку механизмов защиты, включая активацию fapolicyd, auditd, ограничение сервисов и сетевой фильтрации. Для контейнерной среды предусмотрены отдельные меры изоляции, так как fapolicyd внутри контейнера не применяется. Контроль исполнения осуществляется на хостовом уровне, а контроль целостности — через механизмы контейнеризации (podman, overlayfs).

8.25.4 Информирование администратора безопасности средства виртуализации о нарушении целостности объектов контроля

Нарушения целостности (сообщения вида Integrity check failed …) автоматически индексируются в OpenSearch (например, в индекс integrity-alerts-*). Чтобы администратор мгновенно получал уведомления, настройте канал оповещений и монитор, как описано ниже.

1. **Создайте канал уведомлений**
   a. Войдите в **OpenSearch Dashboards** под учётной записью с правами alerting_full_access.
   b. Откройте меню OpenSearch Plugins → Index Management → Notification Settings.
   c. Нажмите Create channel

Поле	**Что указать**
Name	Security-Integrity-Alerts
Description	Уведомления о сбоях контроля целостности
Channel type	Выберите подходящее: Email (SMTP), Slack, Microsoft Teams, Custom Webhook и т. д. (OpenSearch)
Connection details	Заполните адрес сервера, токен, учётные данные или URL веб-хука.
Destination	Добавьте e-mail получателей, Slack-канал, URL вашей системы тикетов и т. д.

Поле	Что указать
Send test message	Убедитесь, что сообщение доставлено.
Save	Сохраните канал.

Совет. Для почты используйте отдельный почтовый ящик «noreply@…» и включите TLS/STARTTLS.

2. **Создайте монитор, отслеживающий ошибки контроля целостности**
   a. Перейдите OpenSearch Plugins → Alerting → Monitors → Create monitor.
   b. В разделе Define monitor выберите:
      - **Monitor type** — Query level.
      - **Index** — integrity-alerts-* (или шаблон индекса, куда отправляются логи контейнеров).
      - **Schedule** — Every 1 minute.
   c. В разделе Define queries нажмите Add query и укажите:

```
{
 "size": 0,
 "query": {
  "match_phrase": {
   "message": "Integrity check failed"
  }
 }
}
```

   d. В разделе Create trigger:
      - Trigger name — Integrity-Failure-Trigger.
      - Severity — High.
      - Trigger condition —

```
ctx.results[0].hits.total.value > 0
```

   e. В разделе Actions нажмите Add action и выберите созданный ранее канал Security-Integrity-Alerts. Укажите тему письма (или заголовок сообщения) вида

```
Нарушение целостности: {{ctx.monitor.name}}
```

   а в теле используйте переменные:

```
Детали: {{ctx.results[0].hits.hits.0._source.message}}
Время: {{ctx.trigger.scheduled_time}}
```

   f. Сохраните монитор.

8.25.5 Обеспечение резервного копирования параметров настройки средства виртуализации

Резервное копирование параметров настройки средств виртуализации обеспечивается с помощью скрипта mariadb_backup.sh.

В случае, если данный скрипт отсутсвует, то необходимо его создать, используя следующий код:

```
#!/bin/bash
set -e
set +x

echo "Парсинг входных параметров..."
while getopts ":h:k:u:" opt; do
  case $opt in
```

```
        h) HOST="$OPTARG" ;;
        k) KEY="$OPTARG" ;;
        u) SSH_USR="$OPTARG" ;;
        \?) echo "Error: Invalid option -$OPTARG" >&2; exit 1 ;;
        :) echo "Error: Option -$OPTARG requires an argument" >&2; exit 1 ;;
    esac
done

echo "Проверка наличия обязательных параметров..."
if [[ -z "$HOST" || -z "$KEY" || -z "$SSH_USR" ]]; then
    echo "Error: Missing required parameters:" >&2
    echo "  ssh-host (-h): $HOST" >&2
    echo "  ssh-key (-k): $KEY" >&2
    echo "  ssh-user (-u): $SSH_USR" >&2
    exit 1
fi

SSH_CMD="ssh -i $KEY $SSH_USR@$HOST"
echo "Создана команда SSH для подключения к $HOST"

echo "Проверка наличия контейнера mariadb на $HOST..."
CONTAINER=$($SSH_CMD "sudo podman ps -a --format '{{.Names}}' | grep -w mariadb")
[[ -z "$CONTAINER" ]] && {
    echo "Error: Container named 'mariadb' not found on $HOST" >&2
    $SSH_CMD "sudo podman ps -a" >&2
    exit 1
}
echo "Контейнер mariadb найден"

echo "Получение пароля MariaDB..."
PASS=$($SSH_CMD "sudo grep '^wsrep_sst_auth = root:' /etc/kolla/mariadb/galera.cnf | cut -
d':' -f2")
[[ -z "$PASS" ]] && { echo "Error: Failed to retrieve MariaDB password" >&2; exit 1; }
echo "Пароль MariaDB успешно получен"

echo "Запуск резервного копирования базы данных MariaDB..."
$SSH_CMD "sudo podman exec -u0 mariadb bash -c 'mariadb-backup --backup --
password=$PASS --target-dir=/var/lib/mysql/backup'"
echo "Резервное копирование завершено"

echo "Получение пути к тому MariaDB..."
BACKUP_LOCATION=$($SSH_CMD "sudo podman volume inspect mariadb --format
'{{.Mountpoint}}'/backup")
[[ -z "$BACKUP_LOCATION" ]] && { echo "Error: Cannot find mariadb volume" >&2; exit 1;
}
echo "Путь к тому MariaDB: $BACKUP_LOCATION"

TIMESTAMP=$(date +%Y-%m-%d_%H-%M-%S)
ARCHIVE_NAME="mariadb_backup_${TIMESTAMP}.tar.gz"
echo "Создание имени архива: $ARCHIVE_NAME"
```

```
echo "Создание архива на удалённом сервере..."
$SSH_CMD "sudo tar -czf /tmp/$ARCHIVE_NAME -C $BACKUP_LOCATION . && sudo
chmod 644 /tmp/$ARCHIVE_NAME"
echo "Архив создан, копирование на локальную машину..."
scp -i "$KEY" "$SSH_USR@$HOST:/tmp/$ARCHIVE_NAME" .
echo "Архив скопирован, удаление временных файлов на сервере..."
$SSH_CMD "sudo rm -f /tmp/$ARCHIVE_NAME && sudo rm -rf $BACKUP_LOCATION"
echo "Временные файлы удалены. Процесс завершён."
```

Файл сохранить под названием mariadb_backup.sh.
После сохранения файла выложить его в ту же папку на узле LCM, в которой находится инсталлер.
Запуск скрипта производится с помощью следующей команды (пример):
./backup_mariadb.sh -h [имя хоста] -k ~/.ssh/id_rsa -u [имя пользователя]

Описание параметров команды:

Фрагмент	**Расшифровка**	**Что задаёт**
./backup_mariadb.sh	Запуск скрипта **backup_mariadb.sh** из текущего каталога (точка ./ указывает именно на «здесь»).	Саму процедуру резервного копирования MariaDB.
-h [имя хоста]	**h = host**	Имя или IP-адрес хоста, на котором запущена MariaDB.
-k ~/.ssh/id_rsa	**k = key**	Путь к приватному SSH-ключу, которым скрипт будет аутентифицироваться при подключении к хосту. По умолчанию это файл ~/.ssh/id_rsa.
-u [имя пользователя]	**u = user**	Учётная запись, под которой скрипт подключается по SSH к удалённому серверу. Чаще всего это системный (Linux) пользователь, а не пользователь БД.

8.25.6 Обеспечение резервного копирования сведений о событиях безопасности

Резервное копирование сведений о событиях безопасности обеспечивается с помощью скрипта opensearch_backup.sh.

В случае, если данный скрипт отсутсвует, то необходимо его создать, используя следующий код:

```
#!/bin/bash
set -e
set +x

echo "Парсинг входных параметров..."
while getopts ":h:k:u:o:" opt; do
  case $opt in
    h) HOST="$OPTARG" ;;
```

```
        k) KEY="$OPTARG" ;;
        u) SSH_USR="$OPTARG" ;;
        o) OPENSEARCH_ADDR="$OPTARG" ;;
        \?) echo "Error: Invalid option -$OPTARG" >&2; exit 1 ;;
        :) echo "Error: Option -$OPTARG requires an argument" >&2; exit 1 ;;
      esac
    done

    echo "Проверка наличия обязательных параметров..."
    if [[ -z "$HOST" || -z "$KEY" || -z "$SSH_USR" ]]; then
      echo "Error: Missing required parameters:" >&2
      echo "  ssh-host (-h): $HOST" >&2
      echo "  ssh-key (-k): $KEY" >&2
      echo "  ssh-user (-u): $SSH_USR" >&2
      echo "  opensearch-address (-o): $OPENSEARCH_ADDR" >&2
      exit 1
    fi

    SNAPSHOT_NAME="1"
    CONFIG_FILE="/etc/kolla/opensearch/opensearch.yml"
    REPO_PATH="path.repo: /var/lib/opensearch/data/backup"
    CURL_CMD="curl -k -s"
    SSH_CMD="ssh -i $KEY $SSH_USR@$HOST"

    echo "Очистка репозитория резервных копий..."
    $CURL_CMD -XDELETE "$OPENSEARCH_ADDR"/_snapshot/backup/$SNAPSHOT_NAME -H "Content-Type: application/json" > /dev/null
    if [ $? -ne 0 ]; then
      echo "Ошибка при удалении снимка $SNAPSHOT_NAME" >&2
    fi
    $CURL_CMD -XDELETE "$OPENSEARCH_ADDR"/_snapshot/backup/ -H "Content-Type: application/json" > /dev/null
    if [ $? -ne 0 ]; then
      echo "Ошибка при удалении репозитория" >&2
    fi

    echo "Проверка наличия контейнера opensearch на $HOST..."
    CONTAINER=$($SSH_CMD "sudo podman ps -a --format '{{.Names}}' | grep -w opensearch")
    [[ -z "$CONTAINER" ]] && {
      echo "Error: Container named 'opensearch' not found on $HOST" >&2
      $SSH_CMD "sudo podman ps -a" >&2
      exit 1
    }
    echo "Контейнер opensearch найден"

    if ! $SSH_CMD "sudo grep -Fx \"$REPO_PATH\" \"$CONFIG_FILE\" > /dev/null"; then
      echo "Добавляем строку $REPO_PATH в $CONFIG_FILE"
      $SSH_CMD "echo \"$REPO_PATH\" | sudo tee -a \"$CONFIG_FILE\" > /dev/null"
```

```
        echo "Перезапускаем контейнер opensearch..."
        $SSH_CMD "sudo podman restart opensearch"
        echo "Ожидаем запуска opensearch..."
        until $SSH_CMD "sudo podman inspect opensearch | grep '\"Status\": \"running\"'" > /dev/null; do
            sleep 5
        done

    until $CURL_CMD $OPENSEARCH_ADDR/_cat/health | grep -E 'green|yellow' > /dev/null && [ $? -eq 0 ]; do
        echo "..."
        sleep 5
    done

        echo "OpenSearch успешно перезапущен и готов к работе"
    else
        echo "$REPO_PATH уже присутствует в $CONFIG_FILE"
    fi

    echo "Получение пути к тому opensearch..."
    BACKUP_LOCATION=$($SSH_CMD "sudo podman volume inspect opensearch --format '{{.Mountpoint}}'/backup")
    [[ -z "$BACKUP_LOCATION" ]] && { echo "Error: Cannot find opensearch volume" >&2; exit 1; }
    echo "Путь к тому opensearch: $BACKUP_LOCATION"

    echo "Создание репозитория для резервных копий..."
    DATA=`jq -n '{"type": "fs", "settings": {"location": "/var/lib/opensearch/data/backup"}}'`
    BACKUP_DIR=`$CURL_CMD -XPUT $OPENSEARCH_ADDR/_snapshot/backup -H "Content-Type: application/json" --data "$DATA" | jq .acknowledged`

    if [ "$BACKUP_DIR" == true ]; then
        echo "Репозиторий успешно создан"
    else
        echo "Ошибка при создании репозитория"
        exit 1
    fi

    BACKUP=`$CURL_CMD -XPUT "$OPENSEARCH_ADDR"/_snapshot/backup/$SNAPSHOT_NAME | jq .accepted`

    TIMESTAMP=$(date +%Y-%m-%d_%H-%M-%S)
    ARCHIVE_NAME="opensearch_backup_${TIMESTAMP}.tar.gz"
    echo "Создание имени архива: $ARCHIVE_NAME"

    if [ "$BACKUP" == true ]; then
        echo "Начат процесс резервного копирования..."
    else
        echo "Ошибка создания резервной копии"
        exit 1
    fi
```

```
    while true
    do
                                                                ANS=`$CURL_CMD
"$OPENSEARCH_ADDR"/_snapshot/backup/$SNAPSHOT_NAME/_status | jq
.snapshots[0].state`
        STATUS=`echo $ANS`
        if [ "$STATUS" == '"FAILED"' ]; then
                    echo "Backup error. See 'podman exec -u0 opensearch ls
/var/lib/opensearch/data/backup'"
           exit
        elif [ "$STATUS" == '"IN_PROGRESS"' ]; then
           sleep 10
           continue
           echo "..."
        elif [ "$STATUS" == '"STARTED"' ]; then
           sleep 10
           echo "..."
           continue
        elif [ "$STATUS" == '"PARTIAL"' ]; then
            echo "The global cluster state was stored, but data from at least one shard was not
stored. The failures property of the Create snapshot response contains additional details.
(https://docs.opensearch.org/docs/latest/api-reference/snapshots/create-snapshot)"
           exit
        elif [ "$STATUS" == '"SUCCESS"' ]; then
           echo "Создание резеврной копии завершено"
           echo "Создание архива на удаленном севере..."
              $SSH_CMD "sudo tar --checkpoint=10000 -czf /tmp/$ARCHIVE_NAME -C
$BACKUP_LOCATION ."
           $SSH_CMD sudo chmod 644 /tmp/$ARCHIVE_NAME
           echo "Архив создан, копирование на локальную машину..."
           break
        else
           echo "Неизвестная ошибка"
           exit
        fi
    done

    scp -i $KEY $SSH_USR@$HOST:/tmp/$ARCHIVE_NAME .
    echo "Архив скопирован, удаление временных файлов на сервере..."
    $CURL_CMD                                                -XDELETE
"$OPENSEARCH_ADDR"/_snapshot/backup/$SNAPSHOT_NAME -H "Content-Type:
application/json" > /dev/null
    if [ $? -ne 0 ]; then
       echo "Ошибка при удалении снимка $SNAPSHOT_NAME" >&2
    fi
    $CURL_CMD -XDELETE "$OPENSEARCH_ADDR"/_snapshot/backup/ -H "Content-
Type: application/json" > /dev/null
    if [ $? -ne 0 ]; then
       echo "Ошибка при удалении репозитория" >&2
    fi
```

```
$SSH_CMD "sudo rm -f /tmp/$ARCHIVE_NAME"
echo "Временные файлы удалены. Процесс завершён."
```

Файл сохранить под названием opensearch_backup.sh.

После сохранения файла выложить его в ту же папку на узле LCM, в которой находится инсталлер.

Запуск скрипта производится с помощью следующей команды (пример):
./opensearch_backup.sh -o [URL:9200] -h [имя хоста] -u [имя пользователя] -k ~/.ssh/id_rsa

Описание параметров команды:

Фрагмент	Расшифровка	Что задаёт / зачем нужен
./opensearch_backup.sh	Имя исполняемого скрипта. ./ указывает, что он находится в текущем каталоге.	Запускает процедуру резервного копирования OpenSearch.
-o [URL:9200]	**o = opensearch-endpoint**	Полный URL (протокол + FQDN + порт) координатора/ноды кластера OpenSearch, над которым выполняется Snapshot API. Скрипт будет посылать запросы /_snapshot/... именно на этот энд-поинт.
-h [имя хоста]	**h = host**	IP-адрес или имя Linux-узла, на котором физически запущены сервисы OpenSearch и где нужно собрать снапшот. Туда будет установлено SSH-подключение.
-u kpudov	**u = user**	Системная учётная запись Linux, под которой скрипт подключается по SSH к узлу 10.224.138.241. Обычно это sudo-пользователь с правами на выполнение opensearch-dashboards-backup или аналогичных команд.
-k ~/.ssh/id_rsa	**k = key**	Путь к приватному SSH-ключу, который используется для аутентификации при подключении к удалённому узлу. Позволяет выполнять резервное копирование без ввода пароля.

8.25.7 Обеспечение архивирования журнала с последующей очисткой высвобождаемой области памяти

Данное требование обеспечивается с помощью двух методов:

1) Реализация скрипта, описанного в разделе 8.25.6
2) Создания ISM политики в OpenSearch для удаления индексов журналов старше заданного периода (согласно регламенту Клиента), которая решает задачу очистки высвобождаемой области памяти

Так как п.1 был описан ранее, то далее предлагается описание реализации п.2 «Создание ISM политики».

8.25.7.1 Создание ISM-политики через OpenSearch Dashboards

OpenSearch Dashboards предоставляет интерфейс для создания и управления ISM-политиками. Вот пошаговая инструкция:

1. **Вход в OpenSearch Dashboards**:
    - Откройте OpenSearch Dashboards (обычно доступен по адресу http://<your-opensearch-host>:5601) и войдите с учетной записью, имеющей права на управление индексами.
2. **Переход в раздел Index Management**:
    - В главном меню выберите **Index Management** (Управление индексами), который находится в разделе плагинов OpenSearch.
3. **Создание новой политики**[3]:
    - Перейдите на вкладку **State Management Policies** (Политики) и нажмите **Create policy** (Создать политику).
4. **Выбор редактора**:
    - Выберите **Visual editor** (Визуальный редактор) для упрощения настройки или **JSON editor** (JSON-редактор) для большей гибкости. Для данного случая визуальный редактор подходит, так как требование простое.
5. **Настройка политики в визуальном редакторе**:
    - **Policy Info**:
        - Введите уникальный идентификатор политики, например, security-logs-policy.
        - Добавьте описание, например: "Удаление логов безопасности через 60 дней".
    - **Error Notification** (Уведомления об ошибках):
        - (Опционально) Настройте канал уведомлений (например, email или webhook) для получения сообщений о сбоях в выполнении политики. Это можно сделать через плагин Notifications, как описано ранее.
    - **ISM Templates**:
        - Укажите шаблон индексов, к которым будет применяться политика, например, security-auditlog-* (возможно наименование шаблона

[3] Имейте в виду, что создаваемая политика автоматически применяется только к новым индексам, соответствующим указанному шаблону (например, security-auditlog-*). Для существующих индексов, созданных до создания политики, требуется ручное действие для привязки политики

может отличаться, тогда следует указать тот шаблон логов, в котором содержатся данные журналов безопасности)

- Это гарантирует, что новые индексы, соответствующие шаблону, автоматически попадут под управление политики.
- Установите приоритет (например, 100), чтобы определить порядок применения, если есть несколько шаблонов.

- **States (Состояния)**:
  - Добавьте состояние hot:
    - **Actions**: Оставьте пустым, так как в активной фазе действия не требуются.
    - **Transitions**: Добавьте переход в состояние delete с условием min_index_age: 60d (пример – 60 дней, но можно указать другое значение).
  - Добавьте состояние delete:
    - **Actions**: Выберите действие Delete (Удаление).
    - **Transitions**: Оставьте пустым, так как это конечное состояние.
- Нажмите **Create** для сохранения политики.

6. **Проверка применения**:
   - Перейдите в раздел **Policy Managed Indexes** (Управляемые индексы) и убедитесь, что индексы security-auditlog-* связаны с новой политикой.
   - Проверьте статус выполнения политики через API:

```
GET _plugins/_ism/explain/security-auditlog-*
```

8.25.7.2 Создание ISM-политики через OpenSearch API

Для автоматизации или интеграции с другими скриптами можно использовать API OpenSearch. Ниже предоставлен пример команды для создания политики, которая удаляет индексы через 60 дней:

```
{
 "policy": {
  "description": "Политика для удаления логов безопасности через 60 дней",
  "default_state": "hot",
  "schema_version": 1,
  "states": [
   {
    "name": "hot",
    "actions": [],
    "transitions": [
     {
```

```
          "state_name": "delete",
          "conditions": {
            "min_index_age": "60d"
          }
        }
      ]
    },
    {
      "name": "delete",
      "actions": [
        {
          "delete": {}
        }
      ],
      "transitions": []
    }
  ],
  "ism_template": [
    {
      "index_patterns": ["security-auditlog-*"],
      "priority": 100
    }
  ]
 }
}
```

Команда для применения:

curl -XPUT "https://<your-opensearch-host>:9200/_plugins/_ism/policies/security-logs-policy" -H 'Content-Type: application/json' -d @ISM_policy_for_log_deletion.json

8.25.8 Интерфейсы, используемые для ограничения программной среды

При освобождении или перераспределении памяти виртуальных машин гипервизор использует механизмы сертифицированной операционной системы (SberLinux) для очистки памяти. Это достигается с помощью функции (пример: madvise (MADV_DONTNEED) или аналогичных средств, которые обнуляют страницы памяти перед их повторным выделением. Дополнительно, доступ к остаточной информации блокируется через изоляцию адресного пространства, обеспечиваемую гипвивизором и настройками ядра (например, SELinux или AppArmor).

Для удаления объектов файловой системы, используемых средством виртуализации (например, томов виртуальных машин), применяется безопасное удаление с перезаписью случайной битовой последовательностью. В случае использования драйвера Cinder (iSCSI LVM) в OpenStack, операция "secure delete" выполняется автоматически при удалении тома. Лог cinder-volume подтверждает выполнение операции: Performing secure delete on volume: /dev/mapper/cinder--volumes-volume-.

Код гипервизора размещается в области памяти, защищенной от одновременной записи и выполнения, с использованием технологий NX-bit (No-eXecute) или DEP (Data Execution Prevention), поддерживаемых современными процессорами (Intel VT-x, AMD-V). SberLinux OS Server включает ядро с активированными настройками защиты памяти,

такими как CONFIG_PAX_MEMORY_UDEREF, предотвращающими выполнение кода из модифицируемых страниц.

Изоляция памяти виртуальных машин обеспечивается гипервизором KVM, интегрированным с SberLinux OS Server, с использованием аппаратной виртуализации (Intel VT-x или AMD-V). Каждая виртуальная машина работает в изолированном адресном пространстве, управляемом гипервизором, а доступ к памяти других виртуальных машин блокируется через механизмы MMU (Memory Management Unit) и настройки ядра. SberLinux отключает Kernel Same-page Merging (KSM) для предотвращения утечек данных между виртуальными машинами.

8.25.9 Интерфейсы, используемые для защиты памяти

Осуществляется с помощью сервиса fapolicyd на сертифицированной ОС Sberlinux.

- Используется политика по умолчанию, согласно которой разрешено выполнение только тех бинарных файлов, которые:
  - зарегистрированы в RPM-базе;
  - либо явно добавлены в список доверенных (fapolicyd-cli --add-trust ...).
- Конфигурация fapolicyd по умолчанию: запрещён запуск любых бинарных файлов, отсутствующих в базе доверенных (RPM DB + SHA256 checksum).
- Запуск сервиса: systemctl start fapolicyd.service.

9. ТИПЫ СОБЫТИЙ БЕЗОПАСНОСТИ, ДОСТУПНЫХ ПОЛЬЗОВАТЕЛЮ

ПО «KeyStack SE» обеспечивает доступ пользователя с ролью администратора безопасности к следующим событиям безопасности:

- успешные и неуспешные попытки аутентификации пользователей ПО «KeyStack SE»;
- доступ пользователей ПО «KeyStack SE» к виртуальным машинам;
- создание и удаление виртуальных машин;
- запуск и остановка ПО «KeyStack SE» с указанием причины остановки;
- запуск и остановка виртуальных машин с указанием причины остановки;
- изменение ролевой модели;
- изменение конфигурации ПО «KeyStack SE»;
- изменение конфигураций виртуальных машин;
- факты нарушения целостности объектов контроля.

Указанные события доступны в Opensearch.

10. АВАРИЙНЫЕ СИТУАЦИИ

10.1 Сбои и ошибки эксплуатации

В ходе эксплуатации изделия могут возникнуть сбои и допускаться ошибки эксплуатации.

Сбои в работе ПО «KeyStack SE» могут возникнуть вследствие:

- отказа оборудования;
- сбоев в работе программного обеспечения;
- внесения некорректных изменений в настройки конфигурации программного продукта и реализуемых им функций безопасности;
- нарушений порядка работы с ПО «KeyStack SE» и режима эксплуатации, определенных эксплуатационной документацией на изделие.

10.2 Признаки наличия сбоев

Наличие сбоев и неполадок в работе изделия может быть идентифицировано по следующим признакам:

- сообщения об ошибках (текстовые сообщения), отображаемые в веб-интерфейсе пользователя;
- сообщения средств мониторинга защищаемой сети об отсутствии отклика от ПО «KeyStack SE»;
- программные сообщения об отсутствии отклика от компонентов ПО «KeyStack SE».

10.3 Действия пользователя при наличии сбоев

В случае возникновения проблем с работой ПО «KeyStack SE» следует направить сообщение для диагностики и устранения неисправностей в службу технической поддержки ПО «KeyStack SE».

11. РЕКОМЕНДАЦИИ ПО ОСВОЕНИЮ

Для освоения ПО «KeyStack SE» рекомендуем ознакомиться с настоящим документом «Программное обеспечение «Облачная платформа KeyStack SE v.1». Руководство администратора», 1087746411378.62.01.29.000.001 91.

Описание Openstack CLI доступно по ссылке: https://docs.openstack.org/python-openstackclient/latest/index.html

Описание Интеграции с LDAP доступно по ссылке: https://docs.openstack.org/keystone/pike/admin/identity-integrate-with-ldap.html