Kaspersky Container Security

Краткое руководство

Версия: beta

Содержание

О Kaspersky Container Security

Kaspersky Container Security (далее также KCS, решение) обеспечивает комплексную защиту контейнерных сред, а также приложений и сервисов, реализованных в контейнерах. KCS обеспечивает защиту контейнерных приложений от разработки и контроля развертывания до работы в среде выполнения (runtime) и позволяет выявлять проблемы безопасности на всех этапах жизненного цикла контейнерных приложений.

Функциональные возможности решения:

- Интеграция с публичными реестрами образов (Docker Hub, JFrog Artifactory, Sonatype Nexus Repository OSS) для проверки образов в реестре на наличие известных уязвимостей по базам уязвимостей NVD и БДУ (ФСТЭК), секретов (паролей, ключей доступа, токенов) и вредоносного ПО.
- Встраивание в процесс непрерывной интеграции / непрерывной доставки (CI/CD) в виде этапа пайплайн (pipeline) и проверка IaC и образов контейнеров на уязвимости, вредоносное ПО, ошибки конфигурации и наличие конфиденциальных данных (секретов).
- Проверка узлов (nodes) кластеров на соответствие общим отраслевым стандартам информационной безопасности (Benchmarks).
- Контроль соблюдения настроенных политик безопасности на этапах сборки и эксплуатации приложений, в том числе проверка запущенных контейнеров в среде выполнения (runtime).
- Мониторинг ресурсов контролируемых кластеров Kubernetes.
- Анализ и контроль конфигураций кластера Kubernetes.
- Контроль сетевых соединений и системных вызовов внутри контейнеров в кластере.

> В бета-версии функциональность решения ограничена.

Настройку KCS и использование функциональных возможностей решения обеспечивает Консоль управления (см. «Интерфейс»). Консоль реализована в виде веб-интерфейса, доступного через браузер на движке Chromium (Google Chrome, Microsoft Edge, Apple Safari) или Mozilla Firefox.

Программные и аппаратные требования

Для установки и функционирования решения KCS может инфраструктура должна удовлетворять следующим требованиям:

- Одна из следующих платформ оркестрации:
  - Kubernetes версии 1.22 или выше.
  - OpenShift версии 4.11 или выше.

- CI система – GitLab CI.
- Установленный менеджер пакетов Helm.

Решение KCS поддерживает возможность интеграции со следующими реестрами образов:

- Docker Hub.
- JFrog Artifactory.
- Sonatype Nexus Repository OSS.

Требования к кластеру Kubernetes:

- Количество процессоров узла – 4.
- Оперативной памяти на узле – 8 ГБ.
- Объем свободного места на жестком диске узла – 40 ГБ.
- Пропускная способность каналов связи между компонентами кластера – не менее 1 Гбит/с.

Рабочее место пользователя решения KCS должно соответствовать следующим требованиям:

- При использовании схемы развертывания в открытом контуре корпоративной сети (см. «Типовые схемы развертывания») – постоянное подключение к сети интернет.
- Наличие доступа к странице консоли управления KCS (адрес внутри корпоративного контура клиента, указанный при установке Сервера KCS).
- Минимальная пропускная способность каналов связи – не менее 10 Мбит/с;
- Один из следующих браузеров:
    - Google Chrome версии 73.
    - Microsoft Edge версии 79.
    - Mozilla Firefox версии 63.
    - Apple Safari версии 12.1.
    - Opera версии 60.

Архитектура решения

Платформа KCS состоит из следующих компонентов:

- Сервер. Компонент выполняет следующие функции:
    - предоставляет интерфейс для интерактивного управления решением (консоль управления);
    - обеспечивает интеграцию со сторонними программными компонентами (SIEM, CI, реестры образов);
    - координирует работу других компонентов KCS;
    - обеспечивает управление политиками.
- Агент. Компонент контролирует безопасность на узлах (nodes) в соответствии с настроенным политиками безопасности, в частности:

- контролирует безопасность среды выполнения контейнеров, запущенных на узлах;
- контролирует сетевое взаимодействие подов (pods);
- контролирует запуск образов с целью не допускать запуска непроверенных образов.

Агенты устанавливаются на все узлы (nodes) всех кластеров, которые требуется защищать.

- Сканер. Компонент обеспечивает сканирование образов в подключенных реестрах и выполнение проверок при встраивании решения в CI/CD.
- Сервер обновлений – разворачивается как отдельный компонент решения в случае развертывания в закрытом контуре корпоративной сети (см. «Типовые схемы развертывания»). Компонент обеспечивает обновление баз данных уязвимостей и угроз, используемых решением в работе. В случае развертывания в открытом контуре корпоративной сети базы обновляются через интернет.

В бета-версии функциональность и состав компонентов решения ограничены.

Типовые схемы развертывания

Для решения KCS предусмотрены следующие схемы развертывания:

Развертывание в открытом контуре корпоративной сети (разрешен доступ в интернет из кластера Kubernetes)

- Образы, из которых разворачиваются компоненты решения KCS, расположены в публичном репозитории.
- После установки компоненты решения обращаются к базам уязвимостей и стандартам безопасности, расположенным в интернете.
- Обновление баз выполняется с помощью Сервера обновлений, доступного через интернет.

Развертывание в закрытом контуре корпоративной сети (запрещен доступ в интернет из кластера Kubernetes)

- Для размещения образов, из которых разворачиваются компоненты решения KCS, используется внутренний репозиторий.
- Установка компонентов выполняется из специального образа, который содержит базы уязвимостей и стандарты безопасности, необходимые для работы решения.
- После установки компоненты решения обращаются к базам уязвимостей и стандартам безопасности, расположенным внутри корпоративной сети.
- Сервер обновлений, обеспечивающий обновление баз данных угроз, разворачивается в качестве отдельного компонента внутри корпоративной сети.

В закрытом контуре корпоративной сети также возможен сценарий развертывания с использованием прокси-сервера. За подробной информацией обращайтесь в службу технической поддержки производителя KCS.

Установка решения

Компоненты KCS поставляются в виде образов в реестре производителя KCS и развертываются в виде контейнеров.

Установка Платформы контейнерной безопасности KCS состоит из следующих этапов:

1. Установка компонента Сервер.

В зависимости от выбранной схемы развертывания (см. «Типовые схемы развертывания») предусмотрена процедура установки Сервера в закрытом контуре корпоративной сети, без доступа в интернет из кластера (см. «Установка Сервера в закрытом контуре»), и процедура установки Сервера в открытом контуре корпоративной сети, с доступом в интернет из кластера (см. «Установка Сервера в открытом контуре»).

2. Первый запуск консоли управления.
3. Настройка групп Агентов и развертывание Агентов на контролируемых узлах кластеров.

После завершения установки нужно подготовить решение к работе:

- Настроить интеграцию с реестрами образов (см. «Настройка интеграции с внешними реестрами образов»).
- Настроить интеграцию со средствами уведомлений (см. «Настройка интеграции со средствами уведомления»).
- Настроить политики безопасности (см. «Настройка политик безопасности»).

> В бета-версии в комплект поставки входит политика сканирования по умолчанию. Создание пользовательских политик сканирования недоступно.

- Настроить интеграцию с CI/CD (см. «Настройка интеграции с CI/CD»).

Установка Сервера в закрытом контуре

Для установки сервера KCS в закрытом контуре корпоративной сети (без доступа в интернет из кластера) требуется подготовить:

- Внутренний репозиторий. Необходимо настроить проксирующий репозиторий для образов контейнеров, обращающийся к репозиторию производителя KCS с учетными данными, предоставленными производителем KCS.
- Рабочую станцию с доступом в интернет (далее – рабочая станция 1).

На рабочей станции 1 необходимо установить менеджер пакетов Helm.

- Рабочую станцию оператора кластера без доступа в интернет (далее – рабочая станция 2).

Рабочая станция 2 должна удовлетворять следующим требованиям:

- установленный менеджер пакетов Helm;
- доступ к внутреннему репозиторию;
- доступ к кластеру Kubernetes;
- файл kubeconfig для подключения к кластеру, на который выполняется установка (далее – целевой кластер), с правами администратора.

► *Чтобы выполнить установку сервера KCS в закрытом контуре корпоративной сети:*

1. На рабочей станции 1 создайте файл .env с переменными окружения (env vars), который будет использоваться для скачивания скриптов и Helm-чартов (Helm Charts) и последующей установки решения. В файле вам нужно указать данные, предоставленные вам производителем решения KCS.

Файл .env должен иметь следующее содержание:

```
# Устанавливаемая версия Tron
export TRON_VERSION=<номер версии>

# Целевое пространство имен (namespace) для установки Tron
export PROJECT_NAMESPACE=<пространство имен>

# Доменное имя консоли управления Tron внутри контура корпоративной сети
  заказчика
export DOMAIN=<доменное имя>

# Включение или выключение создания Ingress (самостоятельное добавление после
  установки)
export INGRESS_CREATE=<true | false>
# Используемый IngressClass (при INGRESS_CREATE=true)
export INGRESS_CLASS=nginx

# Имя учетной записи администратора и временный пароль для первого запуска
  консоли управления KCS
export ADMIN_LOGIN=<имя учетной записи>
export ADMIN_PASSWORD=<временный пароль>

# Параметры для подключения к внутреннему проксирующему репозиторию
export REGISTRY_URL=<доменное имя репозитория>
export REGISTRY_URL_FULLPATH=<путь к репозиторию, включающий доменное имя>
export REGISTRY_USERNAME=<имя учетной записи>
export REGISTRY_PASSWORD=<пароль>
export REGISTRY_EMAIL=<адрес электронной почты пользователя>

# Параметры для подключения к Helm-репозиторию производителя KCS
export CHART_URL=charts.cloud.tronsec.ru
```

```
export CHART_USERNAME=<имя учетной записи>
export CHART_PASSWORD=<пароль>

# Адрес локального сервера обновлений
export UPDATE_SERVER_URL=http://tron-updates.<пространство
 имен>.svc.cluster.local

# Секреты для инфраструктурных микросервисов решения
# APP_SECRET - строка произвольного содержания длиной 32 символа, разрешается
 использование строчных латинских букв и цифр
export APP_SECRET=<секрет>
export RABBIT_USER=rabbituser
export RABBIT_PASSWORD=<пароль>
export POSTGRES_USER=pguser
export POSTGRES_PASSWORD=<пароль>
export MINIO_ACCESS_KEY=minioaccess
export MINIO_SECRET_KEY=<пароль>

# Параметры хранилища Persistent Volume для микросервисов решения
export REDIS_DISK_SIZE=1Gi
export S3_DISK_SIZE=1Gi
export RABBIT_DISK_SIZE=1Gi
export TRON_PANEL_DISK_SIZE=1Gi
export POSTGRES_DISK_SIZE=1Gi
```

2. На рабочей станции 1 выполните экспорт переменных окружения для скачивания артефактов:

```
source .env
```

3. На рабочую станцию 1 скачайте артефакты, необходимые для установки Сервера KCS:

   - Helm-чарт:

```
helm repo add tron https://$CHART_URL/repository/public-charts/ \
--username $CHART_USERNAME --password $CHART_PASSWORD
helm repo update
helm pull tron/tron --version $TRON_VERSION
```

   - Bash-скрипт:

```
curl -u $CHART_USERNAME:$CHART_PASSWORD \
https://$CHART_URL/repository/public-scripts/install/$TRON_VERSION/helm.sh -O
```

4. Перенесите все полученные артефакты на рабочую станцию 2:

```
% ls -a
.  ..  .env   helm.sh   tron-<номер версии>.tgz
```

5. На рабочей станции 2 выполните подготовительные действия для установки:

   a. Экспортируйте файл kubeconfig для целевого кластера.

Пример экспорта:

```
export KUBECONFIG=~/.kube/config
kubectl config get-contexts
kubectl config use-context <необходимый контекст>
```

b. Экспортируйте переменные окружения для скрипта установки:

```
source .env
```

c. Распакуйте Helm-чарт и перенесите скрипт установки helm.sh в папку чарта:

```
tar zxvf tron-${TRON_VERSION}.tgz
chmod +x helm.sh
mv helm.sh tron/
cd tron
```

6. На рабочей станции 2 запустите установку Сервера:

```
./helm.sh
```

Дождитесь завершения установки.

7. После завершения установки на рабочей станции 2 создайте учетную запись для первого запуска консоли управления:

```
kubectl exec \
-i -t \
-n $PROJECT_NAMESPACE \
$(kubectl get pod -l "app=tron-core" -o name -n $PROJECT_NAMESPACE) \
-- ./bin/console api:user:make --username "$ADMIN_LOGIN" --password
  "$ADMIN_PASSWORD"
```

В результате установки на целевом кластере будут развернуты компоненты Сервер и Сканер.

Панель управления будет доступна по адресу, указанному в файле .env

```
http://${DOMAIN}
```

Установка Сервера в открытом контуре

Для установки сервера KCS в открытом контуре корпоративной сети (с доступом в интернет из кластера) требуется подготовить рабочую станцию оператора кластера с доступом в интернет (далее – рабочая станция).

Рабочая станция должна удовлетворять следующим требованиям:

- установленный менеджер пакетов Helm;
- доступ к кластеру Kubernetes;
- файл kubeconfig для подключения к кластеру, на который выполняется установка (далее – целевой кластер), с правами администратора.

► *Чтобы выполнить установку сервера KCS в открытом контуре корпоративной сети:*

1. На рабочей станции создайте файл .env с переменными окружения (env vars), который будет использоваться для скачивания скриптов и Helm-чартов (Helm Charts) и последующей установки решения. В файле вам нужно указать данные, предоставленные вам производителем решения KCS.

Файл .env должен иметь следующее содержание:

```
# Устанавливаемая версия Tron
export TRON_VERSION=<номер версии>

# Целевое пространство имен (namespace) для установки Tron
export PROJECT_NAMESPACE=<пространство имен>

# Доменное имя консоли управления Tron внутри контура корпоративной сети
  заказчика
export DOMAIN=<доменное имя>

# Включение или выключение создания Ingress (самостоятельное добавление после
  установки)
export INGRESS_CREATE=<true | false>
# Используемый IngressClass (при INGRESS_CREATE=true)
export INGRESS_CLASS=nginx

# Имя учетной записи администратора и временный пароль для первого запуска
  консоли управления KCS
export ADMIN_LOGIN=<имя учетной записи>
export ADMIN_PASSWORD=<временный пароль>

# Параметры для подключения к реестру образов производителя KCS
export REGISTRY_URL=repo.cloud.tronsec.ru
export REGISTRY_URL_FULLPATH=repo.cloud.tronsec.ru/repository/tron-customer/
export REGISTRY_USERNAME=<имя учетной записи>
export REGISTRY_PASSWORD=<пароль>
export REGISTRY_EMAIL=<адрес электронной почты пользователя>

# Параметры для подключения к Helm-репозиторию производителя KCS
export CHART_URL=charts.cloud.tronsec.ru

# Адрес сервера обновлений
export UPDATE_SERVER_URL=https://tron-update-bucket.website.yandexcloud.net/

# Секреты для инфраструктурных микросервисов решения
# APP_SECRET - строка произвольного содержания длиной 32 символа, разрешается
```

```
 использование строчных латинских букв и цифр
export APP_SECRET=<секрет>
export RABBIT_USER=rabbituser
export RABBIT_PASSWORD=<пароль>
export POSTGRES_USER=pguser
export POSTGRES_PASSWORD=<пароль>
export MINIO_ACCESS_KEY=minioaccess
export MINIO_SECRET_KEY=<пароль>

# Параметры хранилища Persistent Volume для микросервисов решения
export REDIS_DISK_SIZE=1Gi
export S3_DISK_SIZE=1Gi
export RABBIT_DISK_SIZE=1Gi
export TRON_PANEL_DISK_SIZE=1Gi
export POSTGRES_DISK_SIZE=1Gi
```

8. На рабочей станции выполните экспорт переменных окружения для скачивания артефактов:

```
source .env
```

9. Добавьте репозиторий с Helm-чартом, необходимым для установки Сервера KCS:

```
helm repo add tron https://$CHART_URL/repository/public-charts/\
 --username $REGISTRY_USERNAME --password $REGISTRY_PASSWORD
helm repo update
```

10. Экспортируйте файл kubeconfig для целевого кластера.

Пример экспорта:

```
export KUBECONFIG=~/.kube/config
kubectl config get-contexts
kubectl config use-context <необходимый контекст>
```

11. На рабочей станции запустите установку Сервера:

```
curl -u $REGISTRY_USERNAME:$REGISTRY_PASSWORD \
https://$CHART_URL/repository/public-scripts/install/$TRON_VERSION/helm.sh |
 bash
```

Дождитесь завершения установки.

12. После завершения установки на рабочей станции создайте учетную запись для первого запуска консоли управления:

```
kubectl exec \
-i -t \
-n $PROJECT_NAMESPACE \
$(kubectl get pod -l "app=tron-core" -o name -n $PROJECT_NAMESPACE) \
-- ./bin/console api:user:make --username "$ADMIN_LOGIN" --password
 "$ADMIN_PASSWORD"
```

В результате установки на целевом кластере будут развернуты компоненты Сервер и Сканер.

Панель управления будет доступна по адресу, указанному в файле .env

`http://${DOMAIN}`

Первый запуск консоли управления

► *Чтобы запустить консоль управления KCS:*

1. В браузере перейдите по адресу, заданному для консоли управления при установке Сервера.

Откроется страница авторизации.

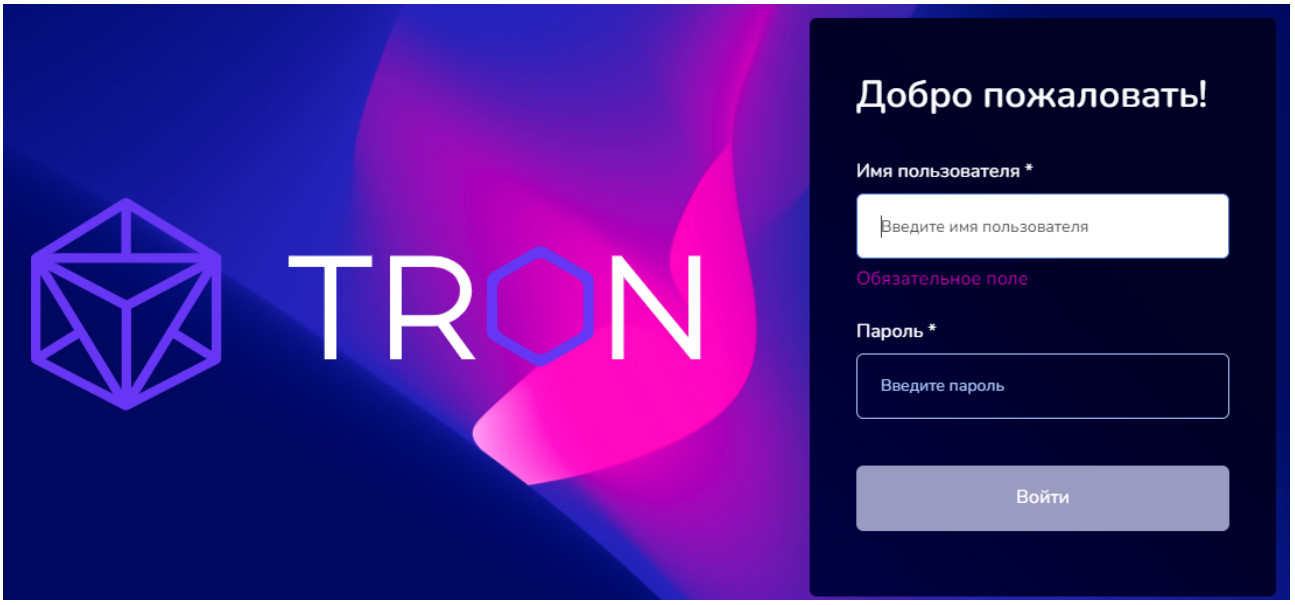

Рис. 1. Страница авторизации консоли управления KCS

2. Введите имя и пароль учетной записи нажмите на кнопку **Войти**.
3. По запросу измените текущий пароль учетной записи: укажите новый пароль и подтверждение пароля и нажмите на кнопку **Изменить**.

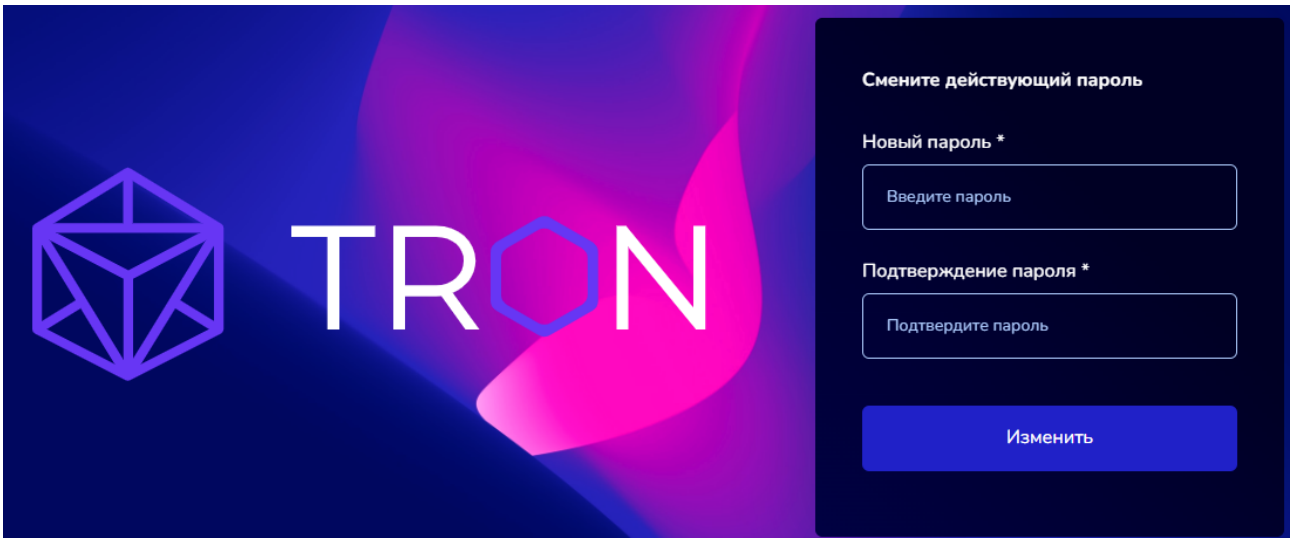

Рис. 2. Запрос на изменение пароля

Откроется главная страница консоли управления.

Развертывание Агентов

Агенты должны быть установлены на всех узлах (nodes) кластера, который вы хотите защищать.

► *Чтобы развернуть Агентов в кластере:*

1. В Консоли управления создайте группу Агентов:
   a. В главном меню перейдите в подраздел **Агенты** раздела **Компоненты KCS**.
   b. В рабочей области нажмите на кнопку **Добавить группу Агентов**.
   c. Заполните поля формы.
      - Введите название группы и ее описание. В качестве названия группы рекомендуется указывать имя кластера, на узах которого будут развернуты Агенты, для удобства управления Агентами.
      - Выберите тип Агента.
      - Выберите тип операционной системы целевого узла.
      - Выберите используемый оркестратор.
      - Если требуется, введите токен для развертывания – это идентификатор, который будет использовать Агент при подключении к Серверу. Вы можете ввести токен или оставить поле пустым, тогда токен сгенерируется автоматически.
   d. Нажмите на кнопку **Добавить**.

В правой части рабочей области отобразятся данные, необходимые для продолжения развертывания Агентов на кластере.

2. Используйте инструкцию из поля **Конфигурация** (в формате yaml) для развертывания Агентов на кластере.

После применения инструкции на кластере Агент будет развернут на всех рабочих узлах (worker nodes) кластера.

В таблице в разделе **Агенты** отображаются созданная группа и развернутые Агенты. Вы можете посмотреть статус подключения Агентов к Серверу.

Удаление решения

► *Чтобы удалить Сервер KCS, выполните одно из следующих действий:*

- На рабочей станции с установленным менеджером пакетов Helm, доступом к целевому кластеру и пространству имен (namespace), в которое установлено решение KCS, выполните команду:

```
helm uninstall tron-release
```

Менеджер пакетов Helm не удаляет объекты PVC, PV и секреты. Вам нужно удалить их вручную с помощью команд:

```
kubectl delete pvc <имя PVC>
kubectl delete secret <имя секрета>
kubectl delete pv <имя PV>
```

- Если решение KCS установлено в отдельное пространство имен (namespace), выполните команду:

```
kubectl delete ns <пространство имен>
```

► *Чтобы удалить Агент KCS,*

на узле кластера, где установлен Агент, выполните команду:

```
kubectl delete -f <файл>
```

где <файл> – имя yaml-файла с конфигурацией, который использовался для развертывания Агента.

Если вы удалили всех Агентов на узлах какого-либо кластера, рекомендуется удалить группу, в которую входили эти Агенты.

► *Чтобы удалить группу Агентов:*

1. В главном меню перейдите в подраздел **Агенты** раздела **Компоненты KCS**.
2. В списке выберите нужную группу. В столбце **Статус** для удаленных Агентов отображается **Отключено**.
3. Откройте меню действий, расположенное в строке группы в последнем столбце, и выберите команду **Удалить группу**.
4. Подтвердите удаление в открывшемся окне.

Интерфейс

Консоль управления реализована в виде веб-интерфейса и состоит из следующих элементов:

- Главное меню. Разделы и подразделы главного меню обеспечивают доступ к основным функциям решения.
- Рабочая область. Информация и элементы управления в рабочей области зависят от раздела или подраздела, выбранного в главном меню.

Главное меню

Раздел Ресурсы

Раздел содержит результаты контроля всех доступных решению KCS ресурсов: кластеров Kubernetes (см. «Просмотр ресурсов кластера»), реестров, интегрированных с решением (см. «Проверка образов из реестров»), и процессов CI/CD (см. «Проверка образов из CI/CD»).

В бета-версии решения возможности просмотра информация о результатах проверки контролируемых кластеров Kubernetes ограничены.

Раздел Компоненты KCS

Раздел содержит информацию о состоянии компонентов решения. Подраздел **Агенты** также позволяет создавать и удалять группы Агентов и содержит информацию, необходимую для развертывания Агентов (см. «Развертывание Агентов»).

В бета-версии решения информация о состоянии компонентов Сервер и Сканер недоступна.

Раздел Среда выполнения

Раздел содержит результаты проверки работающих контейнеров в среде выполнения (runtime).

В бета-версии решения проверка контейнеров в среде выполнения не выполняется.

Раздел Соответствие стандартам

Раздел содержит результаты проверки узлов (nodes) кластера на соответствие стандартам CIS Kubernetes, PCI DSS, ФСТЭК а также стандартам, которые добавлены в подразделе **Пользовательские стандарты** (см. «Проверка на соответствие стандартам»). Вы можете добавлять стандарты, по которым вам нужно выполнять проверку, например, отраслевые стандарты.

В бета-версии решения проверка на соответствие стандартам PCI DSS, ФСТЭК и пользовательским стандартам недоступна.

Раздел Политики

Раздел позволяет настраивать политики безопасности, применяемые в работе решения (см. «Настройка политик безопасности»).

Подраздел **Принятые риски** содержит список всех обнаруженных угроз и уязвимостей, риск наличия которых принят пользователем. В подразделе вы можете отменять принятие рисков или устанавливать срок, в течение которого риск считается принятым (см. «Работа с рисками»).

В бета-версии решения политики проверок среды выполнения и профили образов недоступны.

Раздел Отчеты

Раздел позволяет сформировать в формате, доступном для выгрузки, отчеты о выявленных уязвимостях, об обнаруженных несоответствиях требованиям политик и стандартов информационной безопасности.

В бета-версии решения отчеты недоступны.

Раздел Администрирование

Раздел позволяет выполнять следующие задачи:

- управлять правами доступа пользователей и групп пользователей (см. «Управление доступом пользователей»);
- настраивать интеграцию с публичными реестрами образов (см. «Настройка интеграции с внешними реестрами образов»);
- настраивать интеграцию со средствами уведомлений (см. «Настройка интеграции со средствами уведомления»);
- управлять параметрами запуска задач проверки.

В бета-версии решения возможности управления пользователями ограничены, параметры запуска задач проверки недоступны.

Раздел Параметры

Раздел позволяет настраивать параметры запуска консоли управления KCS и управлять параметрами лицензирования.

В бета-версии решения параметры лицензирования недоступны.

Раздел О платформе

Раздел содержит информацию о версии решения и веб-адрес службы технической поддержки.

Блок с именем текущего пользователя

В блоке отображается информация о пользователе, под учетной записью которого запущена консоль управления KCS. С помощью команд всплывающего меню в блоке вы можете изменить пароль текущего пользователя и выйти из консоли.

Некоторые способы настройки отображения данных

Для табличных представлений в интерфейсе KCS предусмотрены следующие способы настройки отображения данных:

- Фильтрация. Поля фильтра расположены над таблицами данных. Состав полей фильтра и способы управления фильтром зависят от специфики данных, отображаемых в разделе.

В некоторых разделах для открытия полей фильтра требуется нажать на значок фильтра.

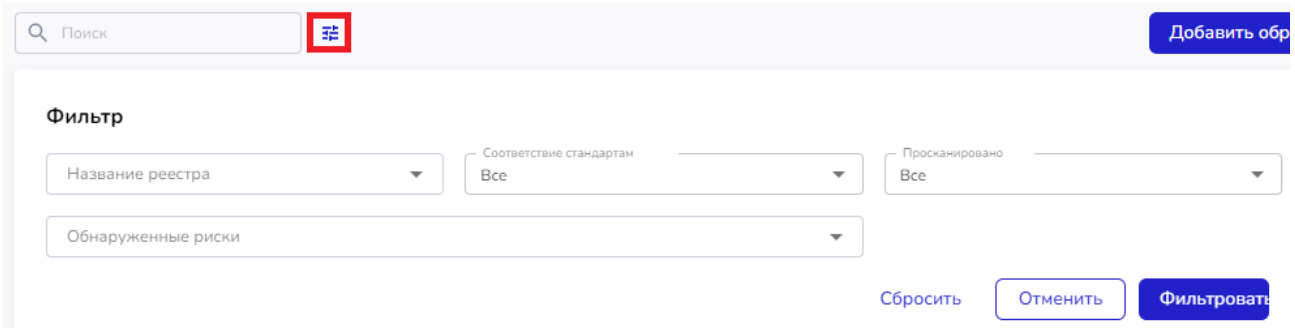

*Рис. 3. Фильтр в разделе **Реестры образов***

- Сортировка по возрастания или убыванию. В некоторых разделах вы можете сортировать список данных по выбранному столбцу с помощью значков в заголовке столбца.

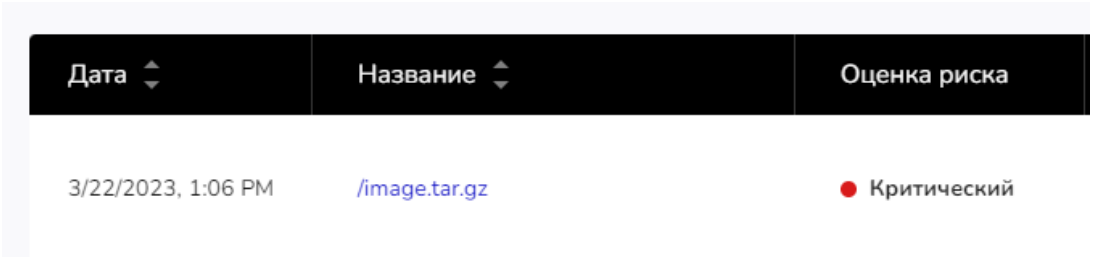

*Рис. 4. Возможность сортировки по столбцам **Дата** и **Название***

- Поиск. Вы можете выполнять поиск по отображаемым данных с помощью поля **Поиск**, расположенного над таблицей.

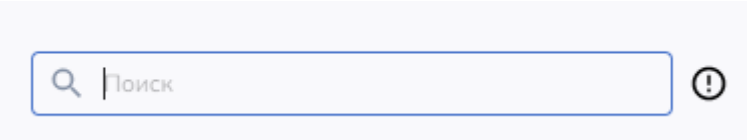

*Рис. 5. Поле **Поиск***

Просмотр ресурсов кластера

Подраздел **Активы** → **Кластеры** раздела **Ресурсы** содержит визуальное представление связей различных ресурсов внутри пространств имен (namespaces) в кластерах Kubernetes.

В подразделе отображается в виде таблицы список кластеров Kubernetes, на узлах которых установлены Агенты KCS.

► *Чтобы открыть схему взаимодействия ресурсов пространства имен:*

1. Перейдите по ссылке на имени кластера в таблице.
2. В открывшемся перечне пространств имен кластера выберите нужное пространство имен.
3. Перейдите по ссылке на названии пространства имен.

Откроется схема взаимодействия ресурсов кластера в рамках выбранного пространства имен. По нажатию на значок ресурса вы можете открыть окно с информацией о ресурсе.

В бета-версии решения возможности просмотра взаимодействия ресурсов кластера ограничены.

Проверка образов из реестров

Подраздел **Активы** → **Реестры** раздела **Ресурсы** содержит список образов, которые сканирует решение KCS, и результаты сканирования образов. В список попадают образы из реестров, интегрированных с решением KCS (см. «Настройка интеграции с внешними реестрами образов»). Образы могут добавляются в список автоматически или вручную.

Список образов пуст, пока вы не настроили интеграцию с реестрами и параметры выгрузки и сканирования образов для реестра в разделе Администрирование (см. «Настройка интеграции с внешними реестрами образов»).

Список образов отображается в виде таблицы, образы сгруппированы по репозиториям.

Вы можете выполнять следующие действия в подразделе **Активы** → **Реестры**:

- Искать образы по имени или контрольной сумме образа.
- Фильтровать список. Фильтр позволяет отображать в списке образы, соответствующие указанным критериям:
  - только образы из определенных реестров;
  - образы, соответствующие или не соответствующие стандартам;
  - образы, просканированные в определенный промежуток времени;
  - образы, в которых обнаружены указанные риски.
- Запускать повторное сканирование выбранных образов (кнопка **Сканировать повторно** отображается над таблицей после выбора одного или нескольких образов).
- Добавлять образы в список и удалять образы из списка (см. «Добавление и удаление образов»).
- Просматривать подробную информацию о результатах сканирования образа (см. «Просмотр результатов сканирования образов из реестров»).

Добавление и удаление образов

Образы из реестров, интегрированных с решением KCS, могут добавляться в список образов автоматически, в соответствии с настроенными параметрами выгрузки и сканирования образов для каждого реестра (см. «Настройка интеграции с внешними реестрами образов»). Также вы можете добавлять образы в список образов из реестров вручную. Новые образы ставятся в очередь на сканирование.

► *Чтобы вручную добавить образы в список:*

1. В подразделе **Активы** → **Реестры** раздела **Ресурсы** выполните одно из следующих действий:

- Выберите в списке репозиторий, откройте меню действий справа названия репозитория и выберите команду **Добавить образы**.
- Нажмите на кнопку **Добавить образы** над таблицей.

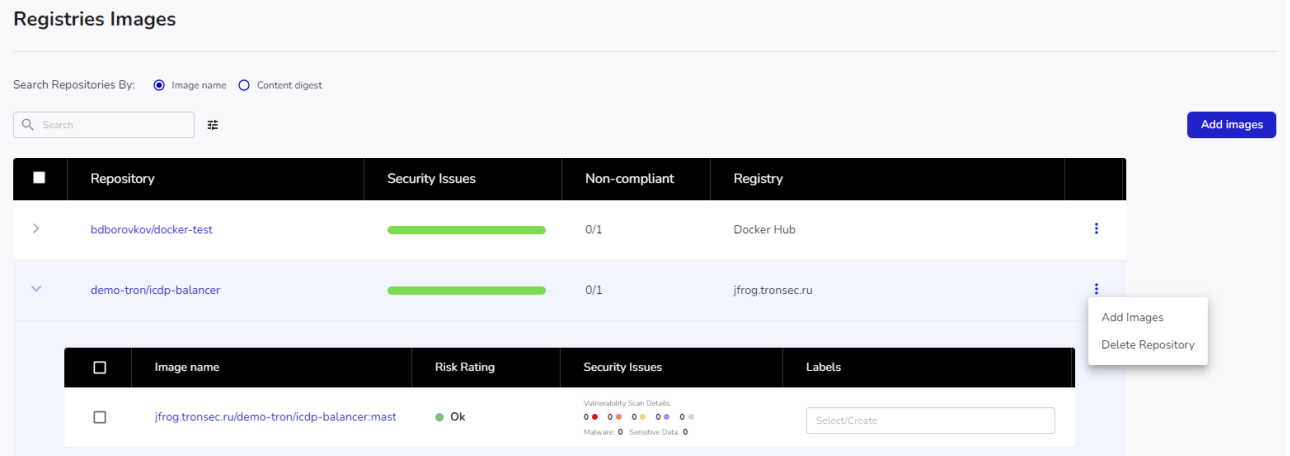

Рис. 6. Список образов из репозиториев

2. Если вы добавляете образы из выбранного репозитория, в открывшемся окне выберите нужные теги образов и нажмите на кнопку **Добавить образы**.
3. Если вы добавляете образы с помощью кнопки **Добавить образы** над таблицей, в открывшемся окне выберите реестр (1), репозиторий (2), один или несколько образов (3) и нажмите на кнопку **Добавить образы** (4).

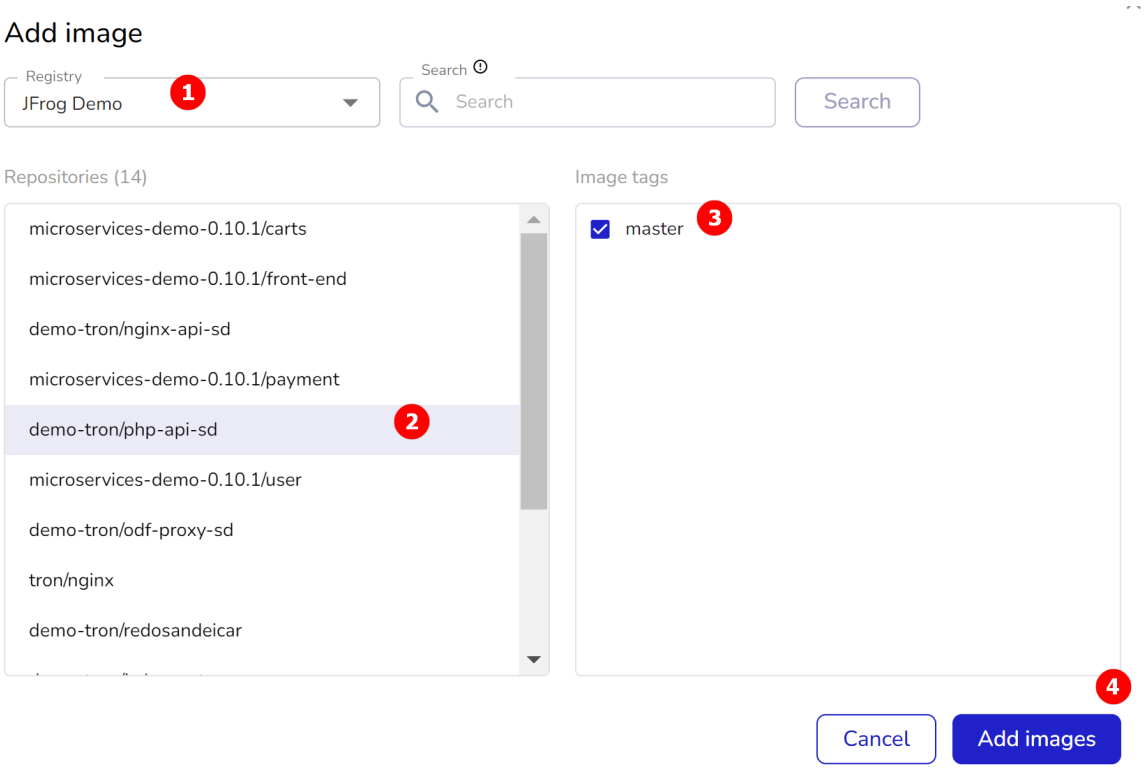

Рис. 7. Добавление образа

► *Чтобы удалить образы из списка:*

1. В подразделе **Активы** → **Реестры** раздела **Ресурсы** выполните одно из следующих действий:

- Выберите в списке один или несколько образов, которые вы хотите удалить, и запустите удаление по ссылке **Удалить**, расположенной над таблицей.
- Выберите в списке репозиторий, все образы которого вы хотите удалить, откройте меню действий в строке с названием репозитория и выберите команду **Удалить репозиторий**.

2. Подтвердите удаление в открывшемся окне.

Просмотр результатов сканирования образов из реестров

Краткая информация о результатах сканирования всех образов репозитория и каждого отдельного образа отображается в списке образов в подразделе **Активы** → **Реестры** раздела **Ресурсы**.

По ссылке на названии образа вы можете открыть страницу, содержащую подробную информацию о результатах сканирования образа.

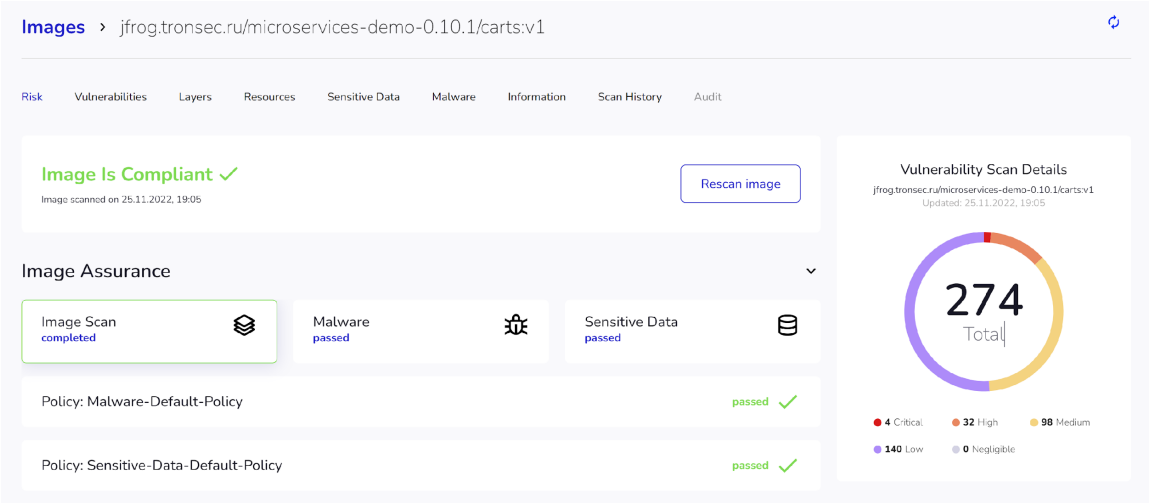

Рис. 8. Результаты сканирования образа

Вкладки, расположенные в верхней части окна, содержат следующую информацию:

- **Риск** – сводная информация о результатах сканирования. В нижней части страницы отображаются рекомендуемые действия для обеспечения безопасности образа, если в процессе сканирования выявлены угрозы. По кнопке **Сканировать повторно** можно запустить повторную проверку образа.
- **Уязвимости** – уязвимости, обнаруженные в образе, по базам NVD, БДУ. По ссылке в названии уязвимости вы можете открыть подробное описание уязвимости.
- **Слои** – слои, которые используются в образе, с указанием найденных уязвимостей. По ссылке в названии слоя вы можете открыть подробное описание найденных в нем уязвимостей.
- **Ресурсы** – ресурсы (компоненты) с указанием найденных уязвимостей. По ссылке в названии ресурса вы можете открыть подробное описание обнаруженных уязвимостей.
- **Вредоносное ПО** – обнаруженное в образе вредоносное ПО. По ссылке в названии вредоносного ПО вы можете открыть его подробное описание.

- **Конфиденциальные данные** – обнаруженные в образе конфиденциальные данные (секреты): пароли, ключи доступа, токены и другие.
- **Ошибки конфигурации** – обнаруженные ошибки конфигурации образа, представляющие угрозу. По ссылке в названии ошибки вы можете открыть ее подробное описание.
- **Информация** – основная информация об образе и история образа.
- **История сканирований** – история сканирований образа. По ссылке в ID образа вы можете открыть информация о результатах прошлого сканирования.

Каждый выявленный риск можно принять (см. «Работа с рисками»).

Проверка образов из CI/CD

С помощью решения KCS вы можете сканировать образы, которые используются в процессах CI/CD. Решение встраивается в CI/CD в виде этапа пайплайн (pipeline), на котором запускается сканер KCS.

Для проверки образов из CI/CD вам нужно настроить интеграцию решения KCS с процессами CI/CD (см. «Настройка интеграции с CI/CD»).

Результаты сканирования передаются на сервер KCS и отображаются в консоли управления в подразделе **CI/CD** раздела **Ресурсы**.

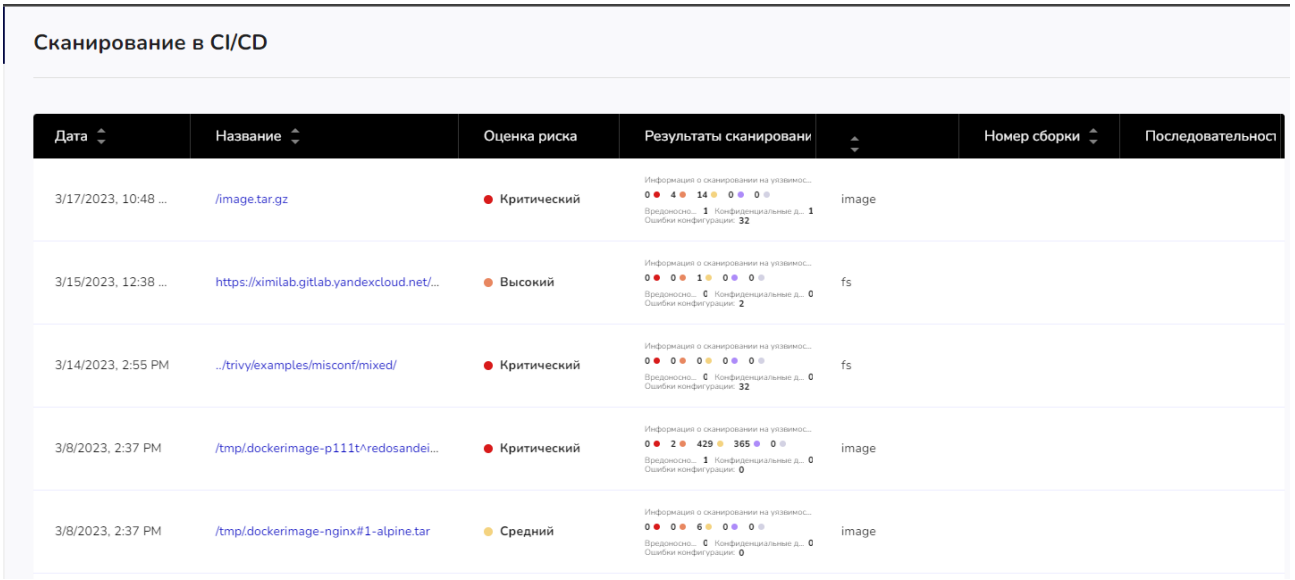

Рис. 9. Результаты сканирования образов из CI/CD

По ссылке в названии образа вы можете открыть страницу, содержащую подробную информацию о результатах сканирования образа. Страница аналогична странице с результатами сканирования образов из реестров (см. «Просмотр результатов сканирования образов из реестров»).

Для образов из CI/CD недоступно повторное сканирование.

Работа с рисками

Для угроз, выявленных решением KCS (уязвимостей, вредоносного ПО, конфиденциальных данных и ошибок конфигурации), предусмотрена процедура «принятия риска» (см. «Принятие риска»). Если риск наличия угрозы принят, в течение указанного промежутка времени (по умолчанию – 30 дней) эта угроза не учитывается политиками безопасности образов при определении статуса безопасности образа (соответствует / не соответствует политикам безопасности). Угроза по-прежнему обнаруживается при сканировании образа, но образ не отмечается как не соответствующий политикам безопасности в результате обнаружения этой угрозы.

Вы можете продлевать срок, в течение которого риск считается принятым. Вы также можете в любой момент отменить принятие риска (см. «Отмена принятия риска»). В случае отмены принятия риска угроза, связанная с риском, снова влияет на статус безопасности образа.

Вы можете просматривать список всех принятых рисков в подразделе **Принятые риски** раздела **Политики** (см. «Просмотр информации о принятых риск»).

Принятие риска

► *Чтобы принять риск:*

1. В окне результатов сканирования образа (см. «Просмотр результатов сканирования образов из реестров») откройте вкладку с информацией о выявленных угрозах нужного типа.
2. В таблице выберите угрозу и запустите принятие риска по ссылке **Принять** или по команде меню действий **Принять риск** (в зависимости от выбранной вкладки).
3. В открывшемся окне укажите параметры принятия риска:
   - Выберите, в каком объеме принимается риск:
     - для выбранного образа, в котором риск обнаружен;
     - для всех образов репозитория, в котором находится образ с обнаруженной угрозой;
     - для всех образов, в которых обнаружена или будет обнаружена эта угроза.
   - Если требуется, установите срок, по истечении которого эта угроза снова будет учитываться при определении статуса безопасности образа.
   - Укажите причину принятия риска.
4. Нажмите на кнопку **Принять**.

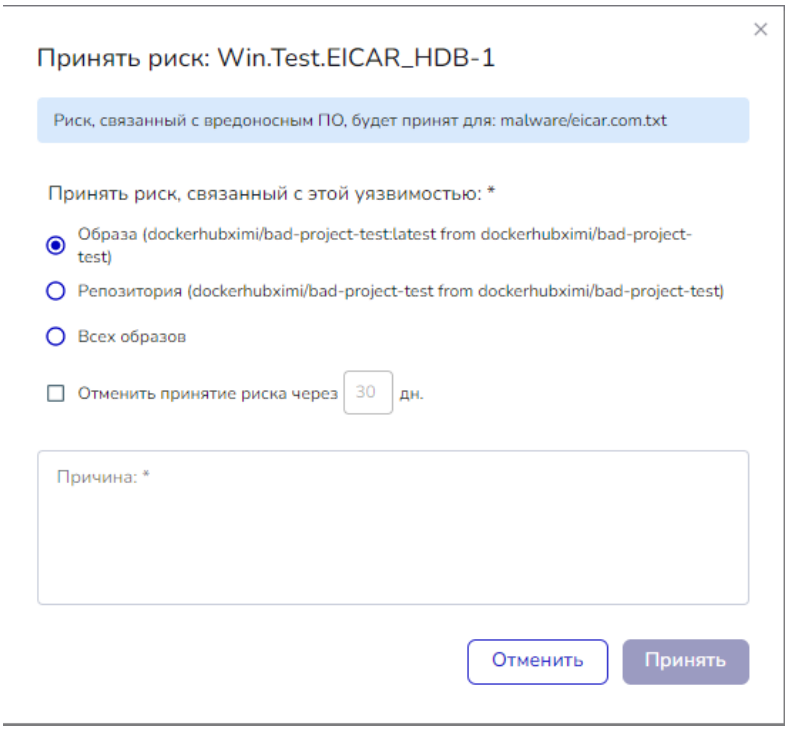

Рис. 10. Окно приятия риска

Выбранная угроза не влияет на статус безопасности образа, образов репозитория или всех образов в течение указанного количества дней или бессрочно.

Принятый риск отображается в подразделе **Принятые риски** раздела **Политики** (см. «Просмотр информации о принятых риск»).

Просмотр информации о принятых рисках

Список всех принятых рисков отображается в подразделе **Принятые риски** раздела **Политики**.

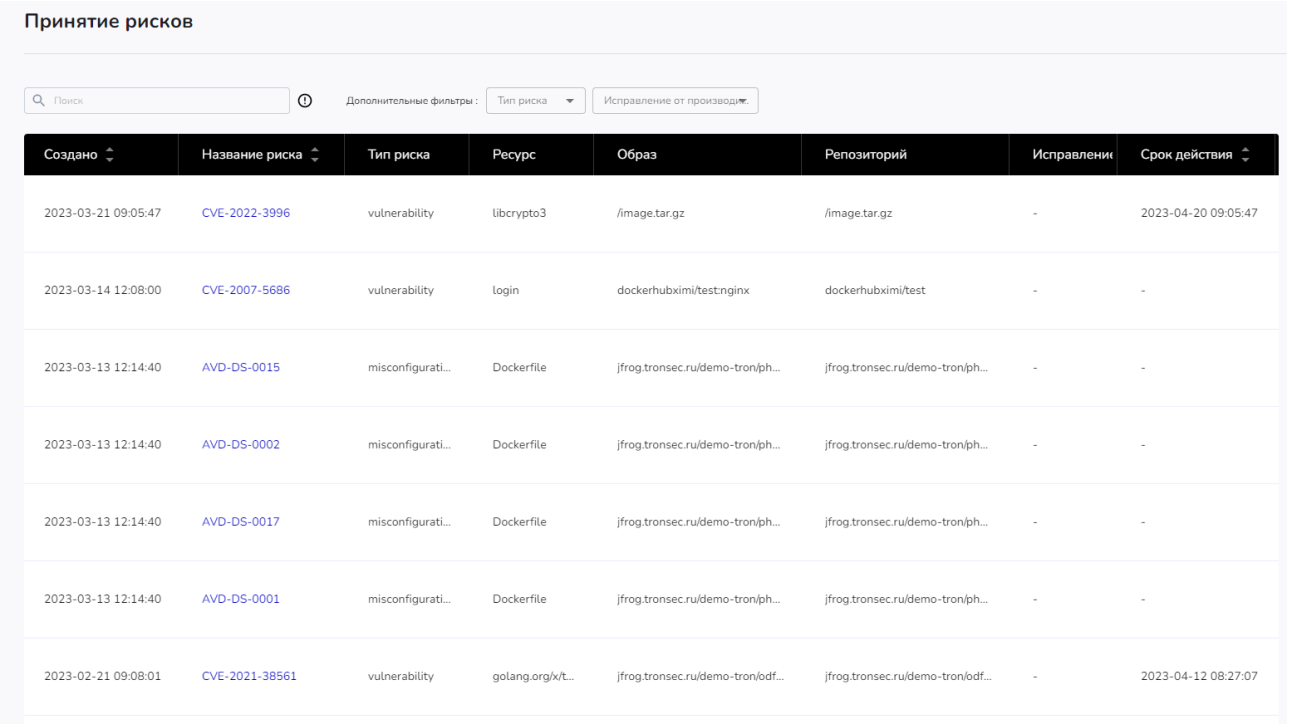

Рис. 11. Список всех принятых рисков

В списке вы можете выполнять следующие действия:

- Выполнять поиск по названию риска, имени репозитория, образа или ресурса, в котором риск обнаружен.
- Фильтровать список по типу риска и наличию исправления от производителя.
- Сортировать список по дате принятия, названию риска и сроку действия.
- Просматривать подробную информацию о принятии риска и связанной угрозе. Окно с подробной информацией открывается по ссылке на названии риска.

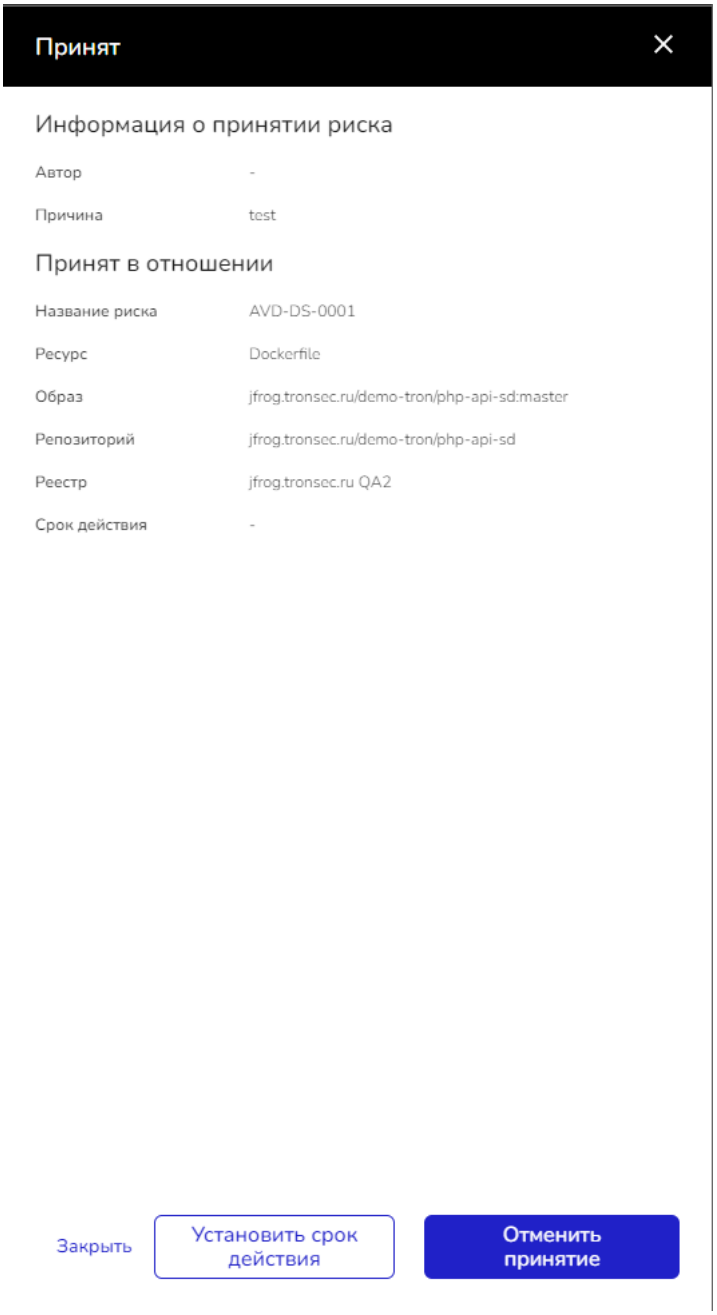

Рис. 12. Подробная информация о принятом риске

С помощью кнопок в окне с подробной информацией вы можете выполнить следующие действия:

- Установить или продлить срок, по истечении которого эта угроза снова будет учитываться при определении статуса безопасности образов.
- Отменить принятие риска (см. «Отмена принятия риска»).

Информацию о принятом риске вы также можете посмотреть в списке обнаруженных угроз в результатах сканирования образов. В строке с угрозой, риск наличия которой был принят, отображается время принятия риска, по ссылке доступно окно с подробной информацией о принятии риска и связанной угрозе.

Отмена принятия риска

► *Чтобы отменить принятие риска:*

1. Откройте окно с подробной информацией о принятии риска и связанной угрозе (см. «Просмотр информации о принятых рисках»). Окно доступно по ссылке на названии риска в списке принятых рисков или по ссылке в строке с угрозой, риск наличия которой был принят, в списке обнаруженных угроз в результатах сканирования образов.
2. Нажмите на кнопку **Отменить принятие риска** и подтвердите отмену в открывшемся окне.

В результате отмены принятия риска угроза, связанная с риском, снова влияет на статус безопасности образа или образов, для которых риск был принят.

Проверка на соответствие стандартам

Агенты KCS могут проверять узлы (nodes) кластеров Kubernetes на соответствие требованиям стандартов информационной безопасности. Поддерживаются следующие стандарты:

- CIS Kubernetes – набор рекомендаций от организации CIS (Center for Internet Security) по созданию надежной системы безопасности для ПО на базе Kubernetes.
- PCI DSS (Payment Card Industry Data Security Standard) – международный стандарт безопасности, созданный для защиты данных платежных карт.
- Стандарты от организации ФСТЭК.
- Пользовательские стандарты – вы можете добавлять стандарты, по которым вам нужно выполнять проверку, например, отраслевые стандарты.

В бета-версии решения проверка на соответствие стандартам PCI DSS, ФСТЭК и пользовательским стандартам недоступна.

Агент проверяет состояние узла, на котором он установлен, и отправляет данные о результатах проверки на сервер. Информация о результатах проверки отображается в разделе **Соответствие стандартам**.

В подразделе **Стандарты CIS** раздела **Соответствие стандартам** вы можете посмотреть результаты проверки узлов кластеров на соответствие стандартам CIS Kubernetes.

Результаты проверки узлов отображаются в виде таблицы, узлы сгруппированы по кластерам.

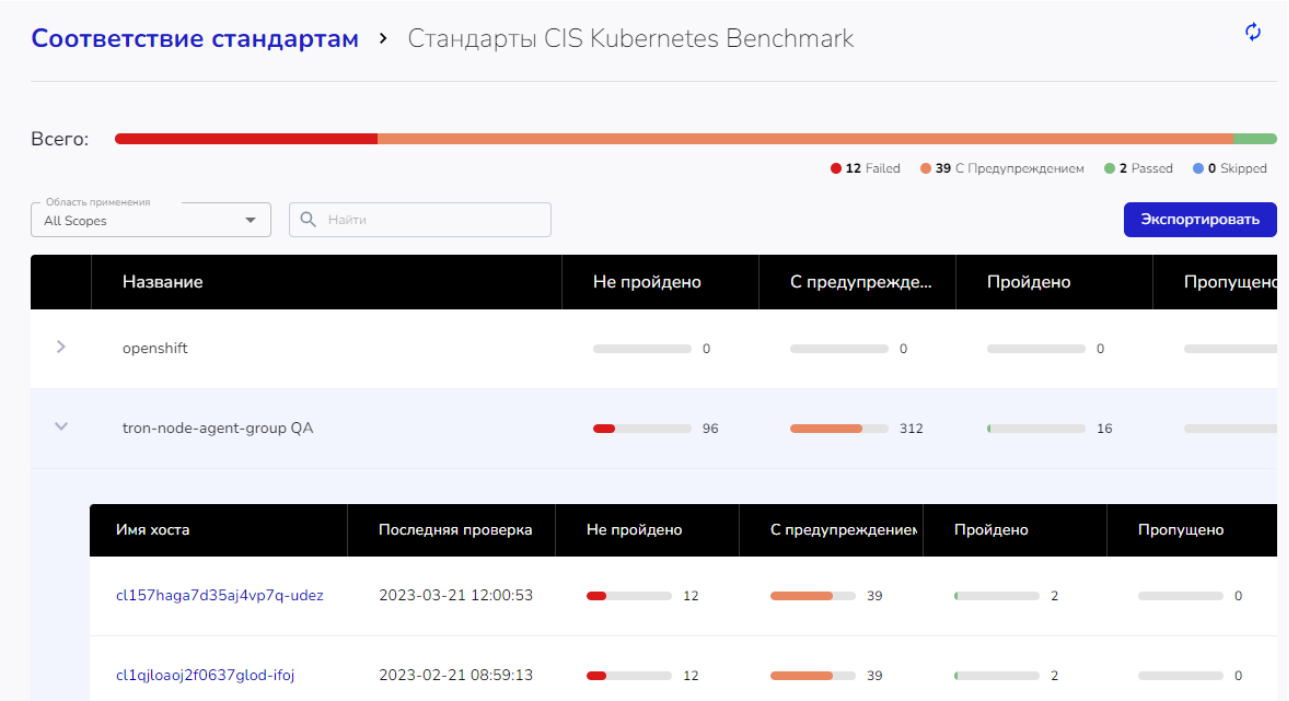

Рис. 13. Результаты проверки на соответствие стандартам

По ссылке на названии узла вы можете открыть страницу, содержащую подробную информацию о результатах проверки узла.

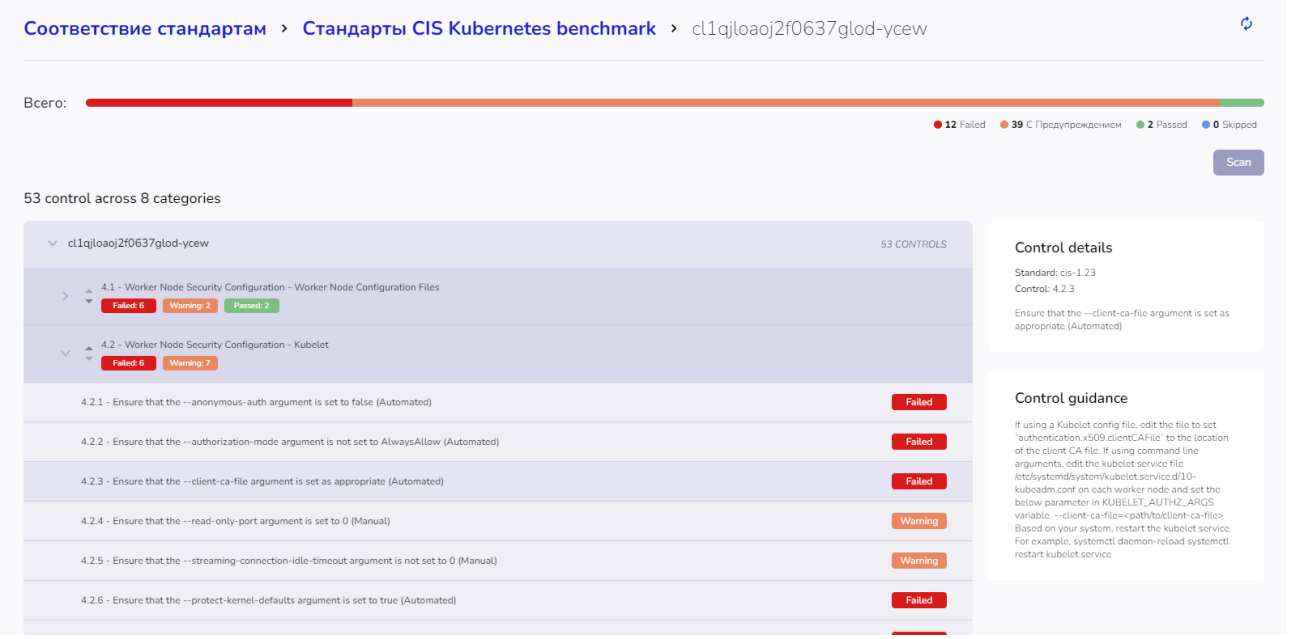

Рис. 14. Подробная информация о результатах проверки узла

В верхней части окна отображается сводная информация. В таблице для каждого контрольного показателя стандарта отображается статус соответствия узла этому показателю.

При нажатии на строке контрольного показателя справа от таблицы открывается и закрывается блок с подробной информацией о показателе.

С помощью кнопки **Сканировать** вы можете запускать проверку узла на соответствие контрольным показателям стандарта.

Настройка политик безопасности

Компоненты решения KCS используют в своей работе следующие политики безопасности:

- Политики сканирования определяют параметры, с которыми выполняется сканирование разных видов ресурсов (см. «Политики сканирования»). В политиках сканирования используются правила обнаружения конфиденциальных данных (см. «Настройка правил обнаружения конфиденциальных данных»).
- Политики безопасности образов определяют действия, которые решение выполняет для обеспечения безопасности, если угрозы, обнаруженные при сканировании образа, соответствуют указанным в политике критериям (см. «Политики безопасности образов»).
- Политики реагирования определяют действия, которые решение выполняет при наступлении определенных событий, заданных в политике (см. «Политики реагирования»). Например, KCS может уведомлять пользователя или удалять образ, в котором обнаружены угрозы.
- Политики проверки среды выполнения позволяют контролировать и при необходимости ограничивать развертывание и работу контейнеров на кластере в соответствии с требованиями безопасности вашей организации.
- Профили образов задают параметры безопасного развертывания образов и безопасного поведения приложения, развернутого из образа.

В бета-версии решения возможности использования политик ограничены. Политики проверки среды выполнения и профили образов недоступны.

Политики сканирования

Политика сканирования определяет параметры, с которыми выполняется сканирование разных видов ресурсов.

В подразделе **Сканирование** раздела **Политики** в виде таблицы отображается список настроенных политик сканирования.

☐	Policy name	Status	Vulnerabilities	Malware	Misconfigurations	Sensitive data
☐	Default Scanner Poli...	Enabled	✓	✓	✓	0/10

Рис. 15. Список политик сканирования

В списке вы можете выполнять следующие действия:

- Изменять параметры политики. Окно редактирования открывается по ссылке на названии политики.

В окне редактирования вы также можете включать и выключать политики. Выключенные политики не применяются в работе решения KCS.

- Удалять политики (см. «Удаление политик безопасности»).

В бета-версии в комплект поставки входит политика сканирования по умолчанию. Вы можете изменять параметры этой политики. Создание пользовательских политик сканирования недоступно.

► *Чтобы изменить параметры политики сканирования:*

1. В подразделе **Сканирование** раздела **Политики** перейдите по ссылке в названии политики.

Откроется окно редактирования параметров политики.

2. Если требуется, с помощью переключателя **Выключить / Включить** измените статус политики (включена / выключена). Выключенные политики не применяются в работе решения KCS.
3. Внесите нужные изменения в параметры политики. Для изменения доступны следующие параметры:
   - Название политики и ее описание.
   - Параметры проверки на уязвимости. С помощью флажков укажите базу или базы уязвимостей, по которым требуется проверять образы.
   - Параметры проверки на вредоносное ПО. Установите флажок, если требуется проверять образы на наличие вредоносного ПО. Проверка выполняется по антивирусной базе ClamAV.
   - Параметры проверки на ошибки конфигурации. Установите флажок, если требуется проверять образы на наличие ошибок конфигурации. Проверка выполняется с параметрами по умолчанию, заданными производителем решения KCS.
   - Параметры проверки на конфиденциальные данные. Вы можете выбрать правила, которые будут использоваться при проверке образов на наличие конфиденциальных данных. Список правил формируется в подразделе **Сканирование** → **Конфиденциальные данные** (см. «Настройка правил обнаружения конфиденциальных данных»).
4. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

Настройка правил обнаружения конфиденциальных данных

В подразделе **Сканирование** → **Конфиденциальные данные** раздела **Администрирование** отображается список настроенных правил обнаружения конфиденциальных данных (далее также – секретов) во время сканирования образов.

Правила сгруппированы по категориям в зависимости от назначения и области применения секретов, для обнаружения которых правила предназначены. Список категорий определен производителем решения KCS. Категории содержат предустановленные правила.

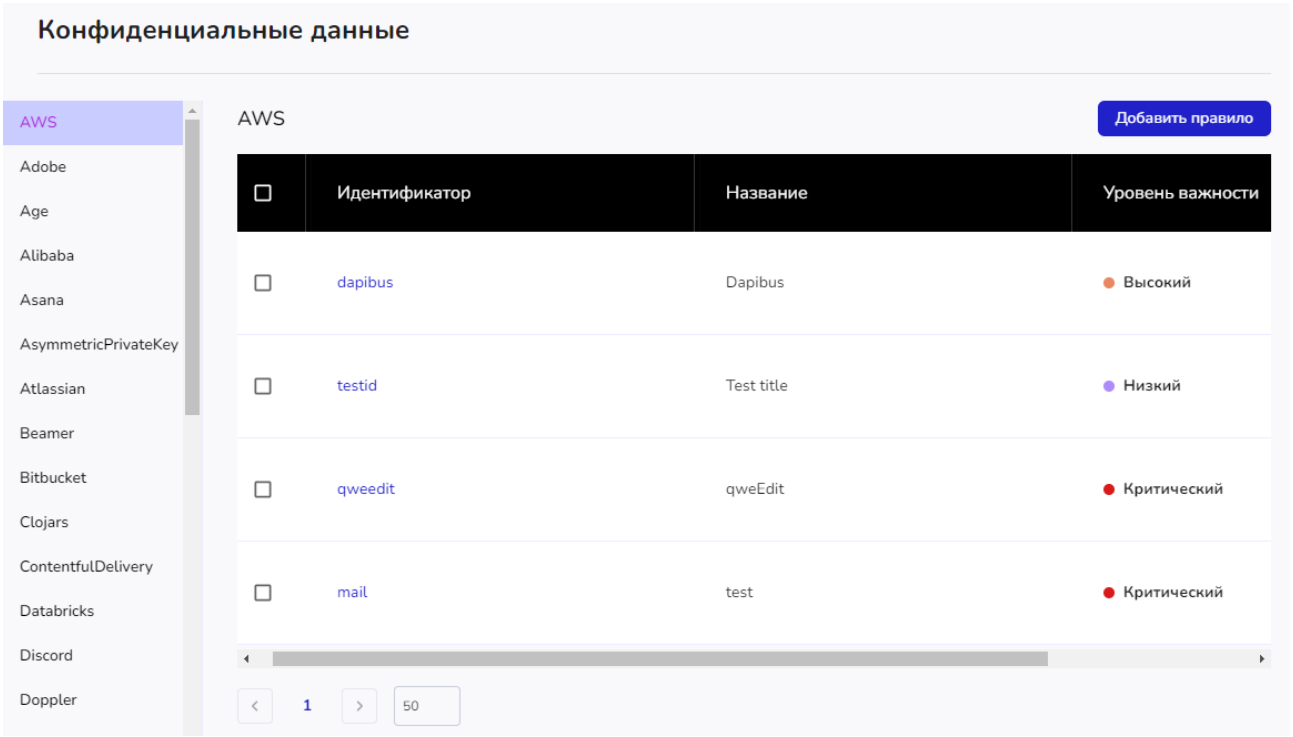

Рис. 16. Правила обнаружения конфиденциальных данных

В списке вы можете выполнять следующие действия:

- Просматривать и изменять параметры правил обнаружения секретов. Окно редактирования открывается по ссылке на идентификаторе правила.
- Добавлять новые правила в выбранную категорию. Окно ввода параметров интеграции открывается с помощью кнопки **Добавить правило**, расположенной над таблицей. Для добавления правил не относящимся ни к одной из предустановленных категорий, используйте категорию Другие.
- Удалять правила. Чтобы выбрать правило для удаления, установите флажок в строке с правилом. Значок удаления появляется при выборе одного или нескольких правил в списке.

Политики безопасности образов

Политика безопасности образов определяет действия, которые решение KCS выполняет для обеспечения безопасности, если угрозы, обнаруженные при сканировании образа, соответствуют указанным в политике критериям.

В подразделе **Безопасность образов** раздела **Политики** в виде таблицы отображается список настроенных политик безопасности образов.

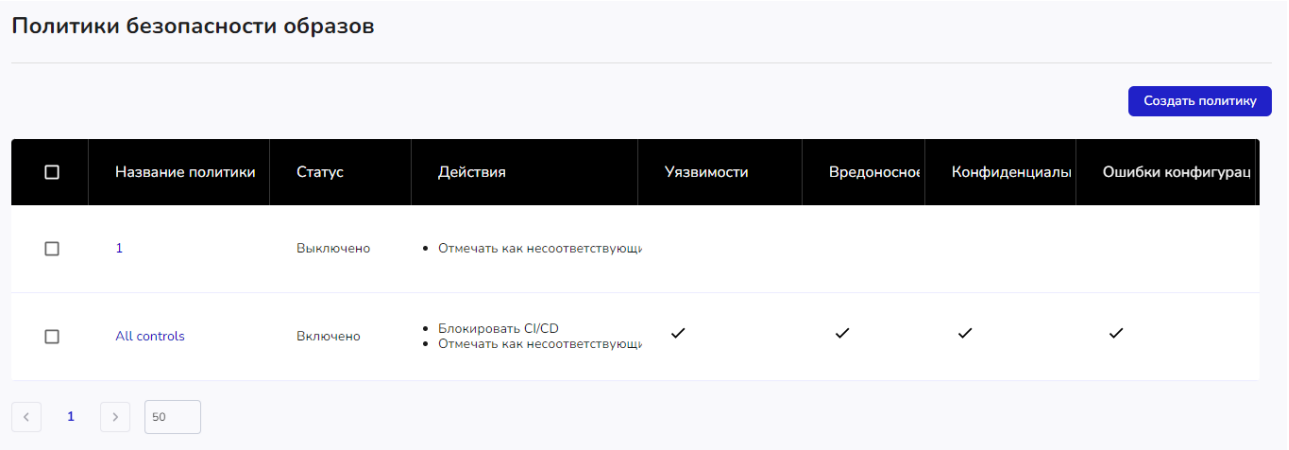

Рис. 17. Список политик безопасности образов

В списке вы можете выполнять следующие действия:

- Создавать новые политики. Окно ввода параметров политики открывается с помощью кнопки **Добавить политику** над списком.
- Изменять параметры политики. Окно редактирования открывается по ссылке на названии политики.

В окне редактирования вы также можете включать и выключать политики. Выключенные политики не применяются в работе решения KCS.

- Удалять политики (см. «Удаление политик безопасности»).

► *Чтобы создать политику безопасности образов:*

1. В подразделе **Безопасность образов** раздела **Политики** нажмите на кнопку **Добавить политику**.

Откроется окно ввода параметров политики.

2. Введите название политики и, если требуется, ее описание.
3. Укажите действия, которые решение KCS будет выполнять в соответствии с этой политикой:
   - **Блокировать этап CI/CD** – если на этапе проверки образа в пайплайне CI/CD сканер KCS обнаруживает в образе угрозы, соответствующие указанному в политике уровню критичности, этап проверки завершается с ошибкой (failed). Этот результат передается в CI-систему.
   - **Отмечать образы как несоответствующие требованиям безопасности** – KCS отмечает образы, в которых обнаружены угрозы, соответствующие указанным в политике критериям.
4. Настройте параметры обнаружения угроз: выберите проверки, которые требуется выполнять, и укажите для каждой проверки уровень критичности обнаруженных уязвимостей. Если в образе обнаружена уязвимость указанного уровня, KCS выполняет действия, заданные в политике.
5. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

По умолчанию политика создается в статусе **Включено**.

Политики реагирования

Политика реагирования определяет действия, которые решение выполняет при наступлении определенных событий, заданных в политике. Например, KCS может уведомлять пользователя или удалять образ, в котором обнаружены угрозы.

В бета-версии решения политики реагирования определяют только действия, которые решение KCS выполняет для уведомления пользователя в случае наступления определенного события, заданного в политике. Например, в случае обнаружения какого-либо актива с критической уязвимостью решение может отправлять уведомление пользователю на электронную почту.

Если вы хотите настроить политики реагирования для уведомления пользователя, вам нужно предварительно настроить интеграцию со средствами уведомления (см. «Настройка интеграции со средствами уведомления»).

В подразделе **Реагирование** раздела **Политики** в виде таблицы отображается список настроенных политик реагирования.

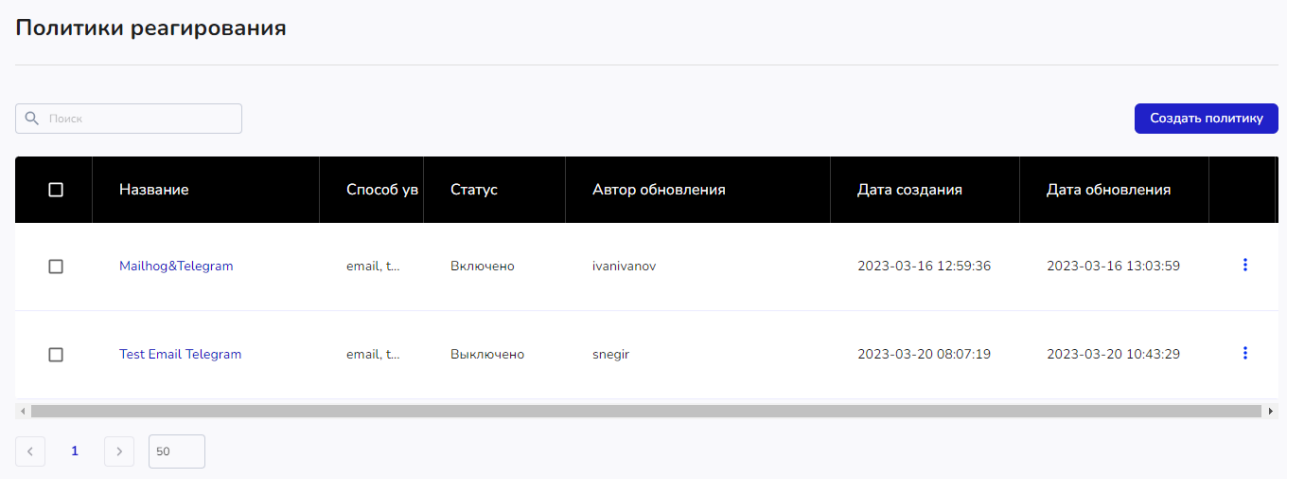

Рис. 18. Список политик реагирования

В списке вы можете выполнять следующие действия:

- Создавать новые политики. Окно ввода параметров политики открывается с помощью кнопки **Добавить политику** над списком.

Вы также можете добавить новую интеграцию путем копирования. Команда **Копировать** доступна в меню действий, которое расположено в последнем столбце таблицы.

- Изменять параметры политики. Окно редактирования открывается по ссылке на названии политики или по команде **Изменить** в меню действий, которое расположено в последнем столбце таблицы.
- Удалять политики (см. «Удаление политик безопасности»).

► *Чтобы создать политику реагирования:*

1. В подразделе **Реагирование** раздела **Политики** нажмите на кнопку **Добавить политику**.

Откроется окно ввода параметров политики.

2. Введите название политики и, если требуется, ее описание.
3. В поле **Триггер** выберите из раскрывающегося списка событие, при наступлении которого решение KCS должно уведомлять пользователя.
4. Настройте нужное количество способов уведомления:
   a. Выберите **Средство уведомления**: электронная почта или Telegram.
   b. В поле **Название интеграции** выберите из раскрывающегося списка название предварительно настроенной интеграции с выбранным средством уведомления (см. «Настройка интеграции со средствами уведомления»).
   c. Чтобы добавить еще один способ уведомления, нажмите на кнопку **Добавить** и заполните открывшиеся поля, как описано в пунктах a и b.

Если требуется вы можете удалять добавленные способы уведомления с помощью значка, расположенного справа от поля **Название интеграции**.

5. Нажмите на кнопку **Сохранить**, чтобы сохранить изменения.

По умолчанию политика создается в статусе **Включено**.

Удаление политик безопасности

► *Чтобы удалить политику безопасности:*

1. Откройте список настроенных политик сканирования (см. «Политики сканирования»), политик безопасности образов (см. «Политики безопасности образов») или политик реагирования (см. «Политики реагирования»).
1. Выберите в списке политику для удаления, установив флажок в строке с названием политики. Вы можете выбрать одну или несколько политик.
2. Нажмите на значок удаления, расположенный над таблицей. Значок появляется при выборе одной или нескольких политик в списке.
3. Подтвердите удаление в открывшемся окне.

Настройка интеграции с внешними реестрами образов

Решение KCS может сканировать образы из следующих внешних реестров образов:

- Docker Hub.
- JFrog Artifactory.
- Sonatype Nexus Repository OSS.

Чтобы KCS мог сканировать образы из внешних реестров, вам нужно настроить интеграцию KCS с этими реестрами. Образы из реестров, интегрированных с решением KCS, могут сканироваться автоматически или вручную, в зависимости от настроенных параметров выгрузки и сканирования образов для каждого реестра.

Просмотр информации об интеграциях с реестрами

В подразделе **Интеграции** → **Реестры образов** раздела **Администрирование** отображается список всех реестров, интегрированных с решением KCS.

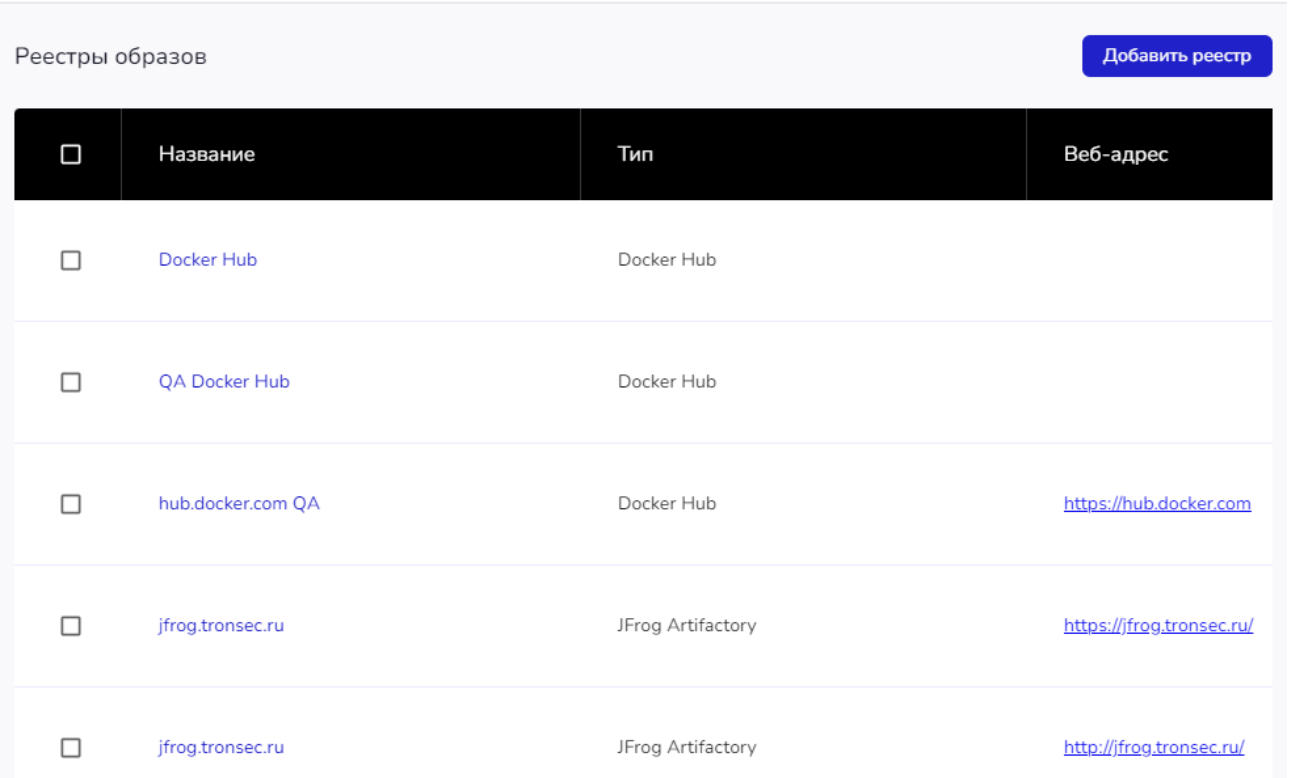

Рис. 19. Список реестров, интегрированных с решением KCS

В списке вы можете выполнять следующие действия:

- Добавлять новые интеграции с реестрами (см. «Создание интеграции с внешним реестром образов»). Окно ввода параметров интеграции открывается с помощью кнопки **Добавить реестр** над списком.
- Просматривать и изменять параметры интеграции с реестром, в том числе параметры выгрузки и сканирования образов. Окно редактирования открывается по ссылке на названии реестра.
- Удалять интеграции с реестром (см. «Удаление интеграции с внешним реестром»).

Создание интеграции с внешним реестром образов

► *Чтобы создать интеграцию с внешним реестром:*

1. В подразделе **Интеграции** → **Реестры образов** раздела **Администрирование** нажмите на кнопку **Добавить реестр**.

Откроется окно ввода параметров интеграции.

2. На вкладке **Параметры реестра** укажите параметры подключения к реестру:
   a. Введите название реестра.
   b. Если требуется, введите описание реестра.
   c. Выберите тип реестра из раскрывающегося списка поддерживаемых типов.

d. Если вы настраиваете интеграцию с реестром типа JFrog Artifactory, и в параметрах HTTP для JFrog Artifactory в качестве метода доступа к Docker выбрано **Repository Path**, установите флажок **Использовать метод Repository path**.

e. Если вы настраиваете интеграцию с реестром типа JFrog Artifactory или Sonatype Nexus Repository OSS, введите полный веб-адрес реестра. Рекомендуется использовать подключение по протоколу HTTPS (также поддерживается подключение по HTTP).

При использовании HTTP или HTTPS с самостоятельно подписанным или недействительным сертификатом нужно установить метку --insecure-registry для движка Docker (Docker engine) на узлах, где установлен сервер и сканер.

f. Если вы настраиваете интеграцию с реестром типа Docker Hub или JFrog Artifactory, выберите метод аутентификации: с помощью учетной записи или с помощью ключа API. Для реестров типа Sonatype Nexus Repository OSS может использоваться только аутентификация с помощью учетной записи.

g. Укажите необходимые данные для аутентификации.

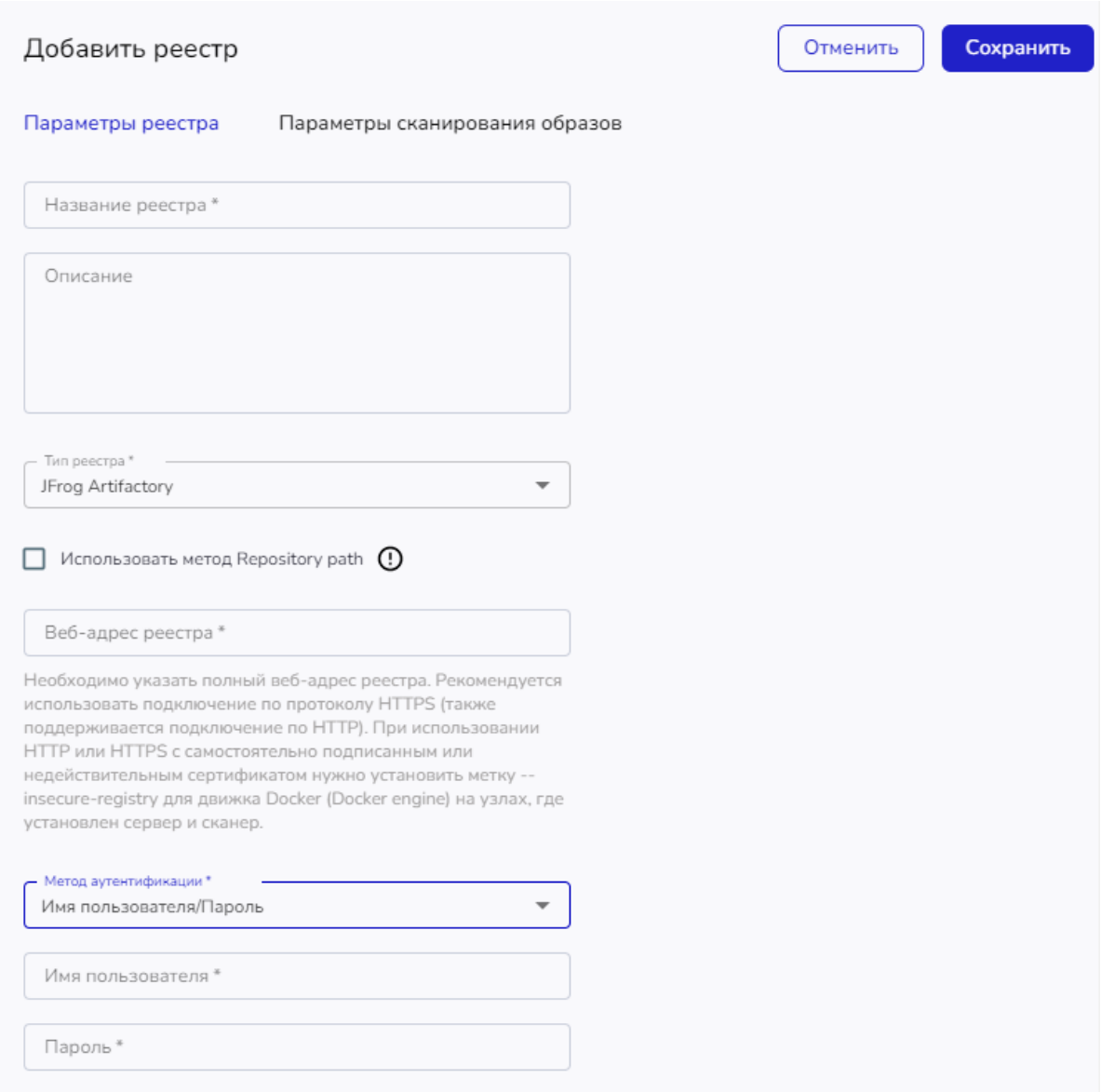

*Рис. 20. Окно добавления интеграции с реестром, вкладка **Параметры реестра***

3. Перейдите на вкладку **Параметры сканирования образов** и укажите максимальное время сканирования образов из этого реестра в минутах. Если сканирование образа продолжается дольше установленного времени, сканирование прекращается, и образ повторно помещается в очередь на сканирование.
4. Настройте параметры выгрузки и сканирования образов для реестра. По умолчанию в блоке **Выгрузка и сканирование образов** выбран вариант **Вручную**: образы автоматически не выгружаются из реестра, но пользователь может вручную добавлять образы в список образов, подлежащих сканированию (см. «Добавление и удаление образов»). Новые образы автоматически ставятся в очередь на сканирование.

Если вы хотите, чтобы образы выгружались из реестра и ставились в очередь на сканирование автоматически, в блоке **Выгрузка и сканирование образов** выберите вариант **Автоматически** и настройте параметры выгрузки и сканирования образов. Для настройки доступны следующие параметры:

- **Сканировать раз в** – блок параметров, определяющих периодичность выгрузки образов из реестра для сканирования. Время указывается в соответствии со временем узла, на котором развернут сервер KCS.
- **Сканировать образы повторно** – если флажок установлен, ранее выгруженные из реестра образы сканируются повторно при каждом сканировании новых образов.
- **Шаблоны имени/тега** – вы можете указать с помощью шаблонов имен и/или тегов образов, какие образы нужно выгружать и сканировать. Если флажок установлен, KCS будет выгружать для сканирования только те образы, которые соответствуют заданным шаблонам.

Вы можете использовать шаблоны следующих форматов:

- шаблон по имени и тегу образа – <имя><:тег>;
- шаблон только по имени образа – <имя>
- шаблон только по тегу образа – <:тег>.

Например:

- по шаблону `alpine` будут выгружаться все образы с именем alpine, независимо от тега;
- по шаблону `:4` будут выгружаться все образы с тегом 4, независимо от имени образа;
- по шаблону `alpine:4` будут выгружаться все образы, с именем alpine и с тегом 4.

При формировании шаблонов вы можете использовать символ *, который заменяет любое количество символов.

Чтобы добавить шаблон, введите его в поле и нажмите на кнопку **Добавить**. Вы можете добавить один или несколько шаблонов.

- Дополнительные условия для выгрузки образов.
  - Если дополнительные условия не требуются, выберите вариант **Без дополнительных условий**.
  - **Образы, созданные за период** – выберите этот вариант, если требуется выгружать только образы, созданные за определенный период (за указанное количество последних дней, месяцев или лет). Укажите в полях справа длительность периода и единицу измерения. По умолчанию установлено 60 дней.
  - **Последние** – выберите этот вариант, если требуется выгружать только образы с последними тегами, считая от даты создания образа. Укажите в поле справа, сколько последних тегов нужно учитывать.
- **Никогда не выгружать образы с шаблоном имени/тега** – вы можете указать с помощью шаблонов имен и/или тегов образов, какие образы исключаются из выгрузки и сканирования.
- **Всегда выгружать образы с шаблоном имени/тега** – вы можете указать с помощью шаблонов имен и/или тегов образов, какие образы всегда выгружаются и сканируются, независимо от других условий, заданных выше.

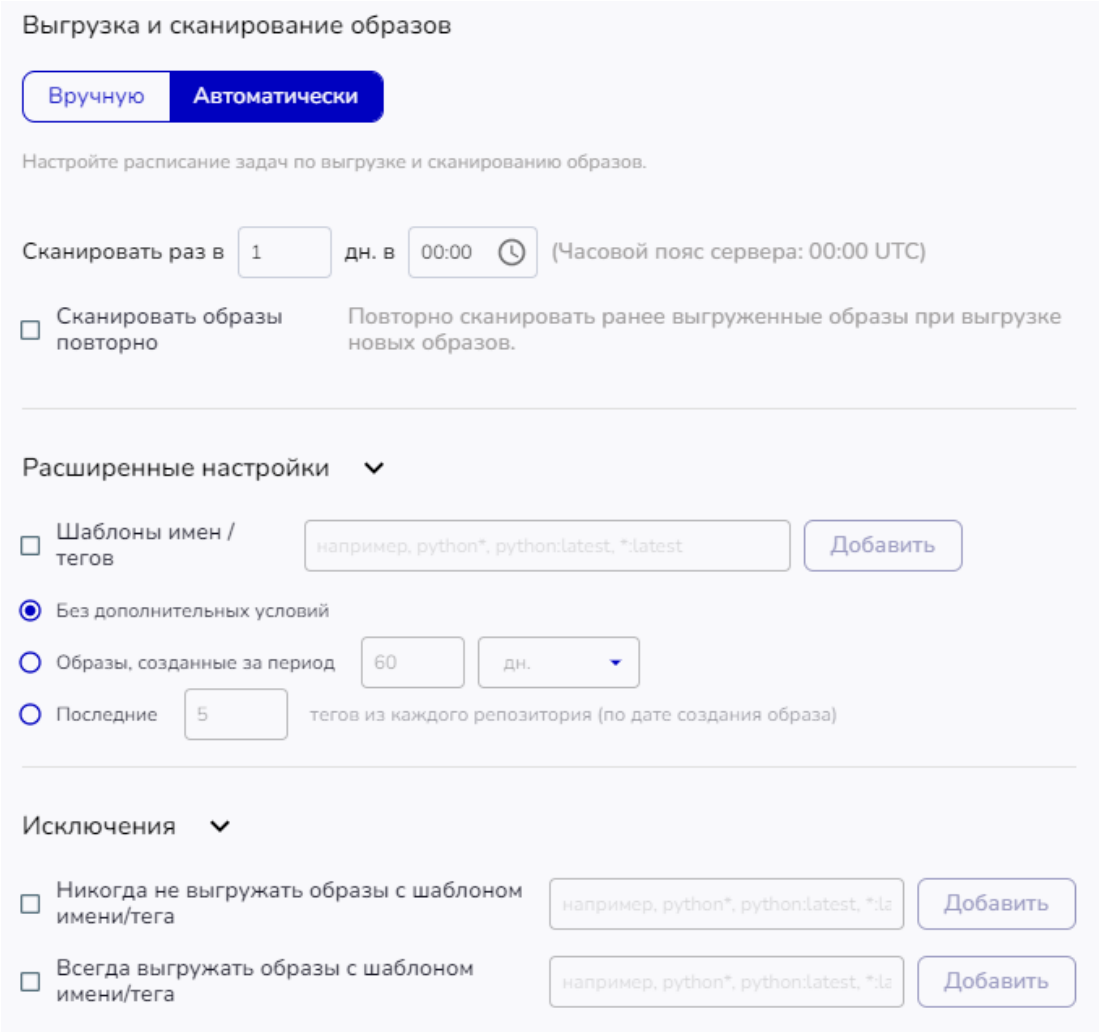

*Рис. 21. Окно добавления интеграции с реестром, вкладка **Выгрузка и сканирование образов***

5. Нажмите на кнопку **Сохранить** в верхней части окна, чтобы сохранить параметры интеграции с реестром.

Удаление интеграции с внешним реестром

► *Чтобы удалить интеграцию с внешним реестром:*

1. Выберите интеграцию для удаления, установив флажок в строке с названием реестра. Вы можете выбрать одну или несколько интеграций.
2. Нажмите на значок удаления, расположенный над таблицей. Значок появляется при выборе одного или нескольких реестров в списке.
3. Подтвердите удаление в открывшемся окне.

Решение KCS не сканирует образы из реестра, интеграция с которым удалена.

Настройка интеграции со средствами уведомления

Решение KCS может уведомлять пользователей о событиях в работе решения в соответствии с параметрами политики реагирования (см. «Политики реагирования»). Чтобы использовать функцию уведомления, вам нужно настроить интеграцию решения KCS с одним или несколькими средствами уведомления.

KCS может использовать следующие средства уведомления:

- электронная почта;
- система мгновенного обмена сообщениями Telegram.

Просмотр информации об интеграции с электронной почтой

Чтобы открыть список настроенных интеграций с электронной почтой, перейдите в подраздел **Интеграции** → **Уведомления** раздела **Администрирование** и выберите блок **Интеграции с электронной почтой**.

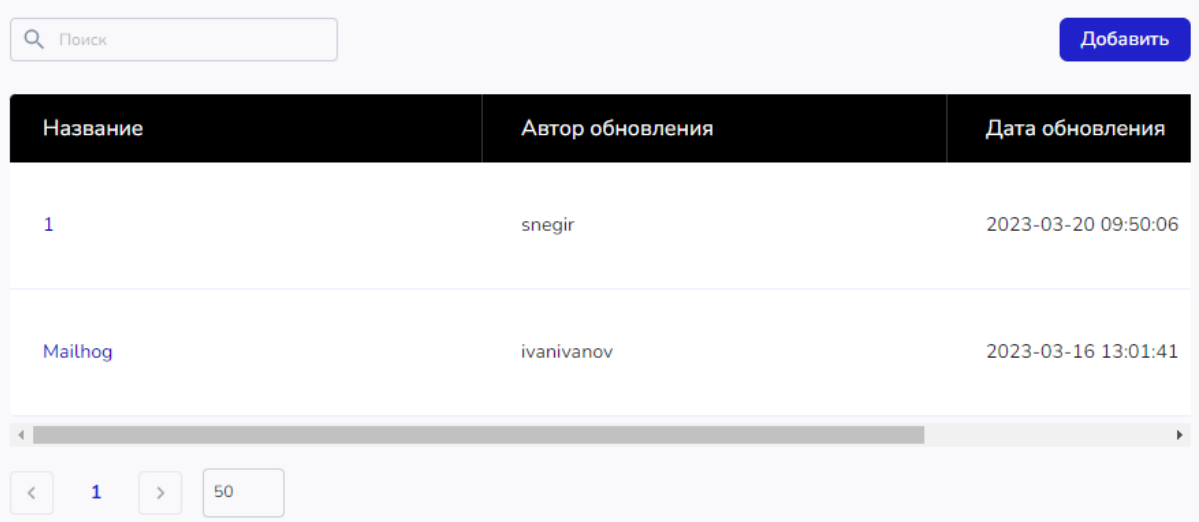

Рис. 22. Список интеграций с электронной почтой

В списке вы можете выполнять следующие действия:

- Добавлять новые интеграции с электронной почтой (см. «Создание интеграции с электронной почтой»). Окно ввода параметров интеграции открывается с помощью кнопки **Добавить** над списком.

Вы также можете добавить новую интеграцию путем копирования. Команда **Копировать** доступна в меню действий, которое расположено в последнем столбце таблицы.

- Просматривать и изменять параметры интеграции с электронной почтой. Окно редактирования открывается по ссылке на названии интеграции или по команде **Изменить** в меню действий, которое расположено в последнем столбце таблицы.
- Удалять интеграцию с электронной почтой (см. «Удаление интеграции со средством уведомления»).

Создание интеграции с электронной почтой

► *Чтобы создать интеграцию с электронной почтой:*

1. Выполните одно из следующих действий:
   - В подразделе **Интеграции** → **Уведомления** раздела **Администрирование** в блоке **Интеграции с электронной почтой** нажмите на кнопку **Добавить**.
   - В подразделе **Интеграции** → **Уведомления** раздела **Администрирование** выберите блок **Интеграции с электронной почтой**. В открывшемся окне нажмите на кнопку **Добавить**, расположенную над таблицей.

Откроется окно ввода параметров интеграции.

5. Укажите следующие параметры в полях формы:
   - Название интеграции. Это название будет отображаться в параметрах политики реагирования.
   - Имя и пароль учетной записи, которая используется для отправки сообщений.
   - Имя сервера SMTP.
   - Способ шифрования электронной почты.
   - Порт, который использует сервер SMTP.
   - Адрес электронной почты отправителя сообщений.
   - Адреса электронной почты получателей сообщений. Вы можете указать в поле один или несколько адресов.
6. Нажмите на кнопку **Сохранить** в верхней части окна, чтобы сохранить параметры интеграции с электронной почтой.

Настроенную интеграцию вы можете использовать в политиках реагирования (см. «Политики реагирования»).

Просмотр информации об интеграции с Telegram

Интеграция с Telegram позволяет настроить публикацию сообщений в чате с ботом Telegram.

Установка решения45

Чтобы открыть список настроенных интеграций с Telegram, перейдите в подраздел **Интеграции** → **Уведомления** раздела **Администрирование** и выберите блок **Интеграции с Telegram**.

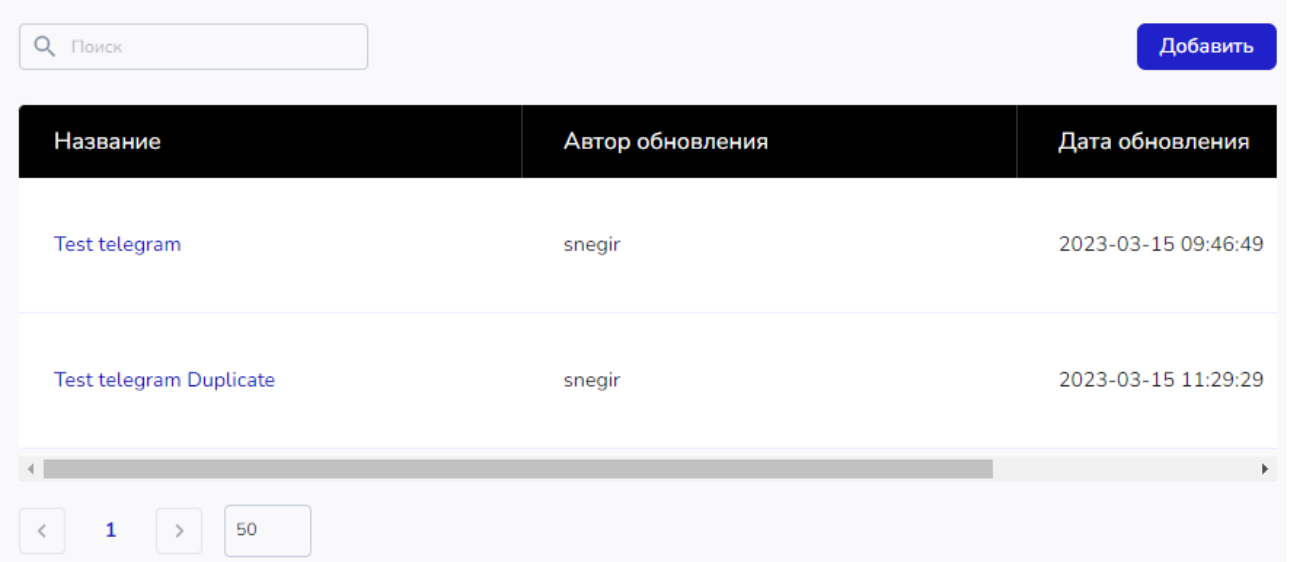

Рис. 23. Список интеграций с Telegram

В списке вы можете выполнять следующие действия:

- Добавлять новые интеграции с Telegram (см. «Создание интеграции с Telegram»). Окно ввода параметров интеграции открывается с помощью кнопки **Добавить** над списком.

Вы также можете добавить новую интеграцию путем копирования. Команда **Копировать** доступна в меню действий, которое расположено в последнем столбце таблицы.

- Просматривать и изменять параметры интеграции с Telegram. Окно редактирования открывается по ссылке на названии интеграции или по команде **Изменить** в меню действий, которое расположено в последнем столбце таблицы.
- Удалять интеграцию с Telegram (см. «Удаление интеграции со средством уведомления»).

Создание интеграции с Telegram

► *Чтобы создать интеграцию с Telegram:*

1. Выполните одно из следующих действий:
   - В подразделе **Интеграции** → **Уведомления** раздела **Администрирование** в блоке **Интеграции с Telegram** нажмите на кнопку **Добавить**.
   - В подразделе **Интеграции** → **Уведомления** раздела **Администрирование** выберите блок **Интеграции с Telegram**. В открывшемся окне нажмите на кнопку **Добавить**, расположенную над таблицей.

Откроется окно ввода параметров интеграции.

7. Укажите следующие параметры в полях формы:
   - Название интеграции. Это название будет отображаться в параметрах политики реагирования.

- Идентификатор чата, в котором будут публиковаться сообщения. Вы можете получить идентификатор следующим образом:

  a. Напишите первое сообщение боту, который будет публиковать сообщения. Идентификатор чата генерируется при первой отправке сообщения.

  b. Введите в адресной строке браузера:

`https://api.telegram.org/bot<токен>/getUpdates`

где <токен> – токен бота, который будет публиковать сообщения.

  c. В полученном json-ответе найдите значение «id» из объекта «chat» – это идентификатор чата.

- Токен бота, который будет публиковать сообщения. Токен вы получаете в результате создания бота по команде /newbot в боте BotFather. Вы также можете получить токен ранее созданного бота по команде /token.

8. Нажмите на кнопку **Сохранить** в верхней части окна, чтобы сохранить параметры интеграции с Telegram.

Настроенную интеграцию вы можете использовать в политиках реагирования (см. «Политики реагирования»).

Удаление интеграции со средством уведомления

► *Чтобы удалить интеграцию с электронной почтой или с Telegram:*

1. Откройте список настроенных интеграций с электронной почтой (см. «Просмотр информации об интеграции с электронной почтой») или с Telegram (см. «Просмотр информации об интеграции с Telegram»).
2. В строке с названием интеграции, которую вы хотите удалить, откройте меню действий, расположенное в последнем столбце, и выберите команду **Удалить**.
3. Подтвердите удаление в открывшемся окне.

Невозможно удалить интеграцию, которая используется в одной или нескольких политиках реагирования.

Настройка интеграции с CI/CD

Чтобы выполнять проверку образов, используемых в процессе CI/CD, вам нужно добавить в пайплайн CI/CD отдельный этап, на котором запускается сканер KCS. Результаты сканирования передаются на сервер KCS и отображаются в консоли управления в подразделе **CI/CD** раздела **Ресурсы** (см. «Проверка образов из CI/CD»).

Пример настройки интеграции с GitLab CI/CD

В этом примере используется специальный образ сканера со встроенными базами данных уязвимостей, размещенный в реестре образов производителя KCS.

Для использования возможности сканирования образов в процессе GitLab CI/CD вам нужно включить использование GitLab Container Registry (https://docs.gitlab.com/ee/administration/packages/container_registry.html).

Настройка интеграции состоит из следующих этапов:

1. Авторизация GitLab CI/CD в реестре образов производителя KCS.
    a. На рабочей станции оператора кластера подготовьте хеш по алгоритму Base64 от авторизационных данных, выполнив команду:

```
printf "login:password" | openssl base64 -A
```

где login и password – имя и пароль учетной записи в реестре образов производителя KCS.

    b. В переменных окружения GitLab CI/CD создайте переменную DOCKER_AUTH_CONFIG (в GitLab репозитории выберите **Settings -> CI/CD**, нажмите на кнопку **Expand**, чтобы развернуть блок **Variables**, затем нажмите на кнопку **Add variable**).
    c. Укажите содержимое переменной в следующем виде:

```
{
    "auths": {
        "repo.cloud.tronsec.ru": {
            "auth": "base64hash"
        }
    }
}
```

где base64hash – строка, полученная на шаге 1a.

2. Добавление этапа сканирования образов в процесс CI/CD.

Чтобы добавить этап сканирования в пайплайн CI/CD, необходимо добавить в файл .gitlab-ci.yml следующие строки:

```
# добавляем шаг после шага сборки кода
scan_image:
 stage: scanner
```

```
image:
  name: repo.cloud.tronsec.ru/repository/tron-customer/scanner:v0.7.1.3-with-db
  entrypoint: [""]
variables:
 # ссылка на образ, собранный на предыдущем шаге сборки кода. Обратите внимание, что в примере указан тэг master, в вашем случае это может быть другой тэг
  SCAN_TARGET: ${CI_REGISTRY_IMAGE}:master
 # если ваш репозиторий приватный, то для доступа сканера к образу необходимо указать авторизационные данные. Их можно задать в виде переменных (https://docs.gitlab.com/ee/ci/variables/#define-a-cicd-variable-in-the-ui)
  TRON_EXT_REGISTRY_USERNAME: ${TRON_EXT_REGISTRY_USERNAME}
  TRON_EXT_REGISTRY_PASSWORD: ${TRON_EXT_REGISTRY_PASSWORD}
 # доменное имя консоли управления Tron внутри контура корпоративной сети заказчика
  API_BASE_URL: <доменное имя>
script:
  - /bin/sh /entrypoint.sh $SCAN_TARGET
```

Управление доступом пользователей

В подразделе **Пользователи** раздела **Администрирование** отображается список пользователей решения KCS.

> В бета-версии решения возможности управления пользователями ограничены.

В списке вы можете выполнять следующие действия:

- Добавлять новых пользователей. Окно ввода параметров учетной записи открывается с помощью кнопки **Добавить пользователя**, расположенной над таблицей.
- Просматривать и изменять параметры учетных записей пользователей. Окно редактирования открывается по ссылке на отображаемом имени пользователя.
- Сбрасывать пароль для выбранных учетных записей. Чтобы выбрать пользователя, установите флажок в строке учетной записи. При выборе одного или нескольких пользователей над таблицей отображается ссылка **Сбросить пароль**.
- Удалять пользователей. Чтобы выбрать пользователя для удаления, установите флажок в строке учетной записи. Значок удаления появляется при выборе одного или нескольких правил в списке.

Глоссарий

CI/CD

Continuous Integration/Continuous Delivery – комбинация непрерывной интеграции и непрерывного развертывания программного обеспечения в процессе разработки.

CIS

Center for Internet Security – некоммерческая организация, которая занимается вопросами кибербезопасности, основываясь на обратной связи от сообщества. Контрольные показатели CIS представляют собой базовые показатели конфигурации и рекомендации для безопасной настройки системы.

CVE

Common Vulnerabilities and Exposures – база данных общеизвестных уязвимостей информационной безопасности. Каждой уязвимости присваивается идентификационный номер вида CVE-год-номер, описание и ряд общедоступных ссылок с описанием.

IaC

Infrastructure as a Code – подход для управления и описания инфраструктуры через конфигурационные файлы, а не через ручное редактирование конфигураций на серверах.

NVD

National Vulnerability Database – национальная база данных уязвимостей. Американский правительственный репозиторий данных управления уязвимостями на основе стандартов, представленных с использованием протокола автоматизации содержимого безопасности.

PCI SSC

PCI Security Standards Council – открытое глобальное сообщество, задачи которого включают непрерывное развитие, совершенствование, хранение, распространение и внедрение стандартов безопасности для защиты данных платежных карт.

SIEM

Security information and event management (управление событиями и информацией о безопасности) – класс программных продуктов, предназначенных для сбора и анализа информации о событиях безопасности.

БДУ

Банк данных угроз безопасности информации – база данных угроз информационной безопасности, разработанная ФСТЭК.

Пайплайн (pipeline)

Последовательность этапов непрерывной разработки и непрерывной доставки ПО (CI/CD), выполняемых в последовательности один за другим.

ПО

Программное обеспечение.

Под (Pod)

Абстрактный объект Kubernetes, группа из одного или нескольких контейнеров приложений, включающая общие используемые хранилища (тома), сетевые параметры и информацию по запуску приложений. Под является единицей управления для Kubernetes.

Пространство имен (namespace)

Виртуальный кластер внутри кластера Kubernetes, позволяет разграничить ресурсы кластера. В каждом пространстве имен есть свои ресурсы: сервисы, поды, развертывания. В одном пространстве имен они должны иметь уникальные названия, но эти же названия допустимо использовать в других пространствах.

Узел (node)

Физическая или виртуальная машины, на которой развертываются и запускаются контейнеры с приложениями. Совокупность узлов образует кластер Kubernetes. На кластере выделяются главный узел (master node), который управляет кластером, и рабочие узлы (worker nodes), на которых работают контейнеры.

ФСТЭК

Федеральная служба по техническому и экспортному контролю.

Уведомления о товарных знаках

Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

Adobe является либо зарегистрированным товарным знаком, либо товарным знаком компании Adobe в США и/или других странах.

AWS является товарным знаком Amazon.com, Inc. или аффилированных лиц компании.

Apple, Safari – товарные знаки Apple Inc.

CLAMAV является зарегистрированным товарным знаком или товарным знаком Cisco Systems, Inc. и/или ее аффилированных компаний в США и в определенных других странах.

Словесный знак Grafana и логотип Grafana являются зарегистрированными товарными знаками/знаками обслуживания или товарными знаками/знаками обслуживания Coding Instinct AB в США и других странах и используются с разрешения Coding Instinct. Мы не являемся аффилированной, поддерживаемой или спонсируемой со стороны Coding Instinct или сообщества Grafana компанией.

Docker и логотип Docker являются товарными знаками или зарегистрированными товарными знаками компании Docker, Inc. в США и/или других странах. Docker, Inc. и другие стороны могут также иметь права на товарные знаки, описанные другими терминами, используемыми в настоящем документе.

Dropbox – товарный знак Dropbox, Inc.

GITHUB – товарный знак GitHub, Inc., зарегистрированный в США и других странах.

GITLAB – товарный знак GitLab Inc. в США и других странах и регионах.

Google, Google Chrome, Chromium – товарные знаки Google LLC.

LinkedIn – товарный знак или зарегистрированный в США и/или других странах товарный знак LinkedIn Corporation и ее аффилированных компаний.