ОГРН 1247700390288 ИНН 9728133771 КПП 772801001
117246, г. Москва, Научный проезд, д.12
почта: info@atomic-ds.ru
веб-сайт: https://atomic-sec.ru/

Программное обеспечение для мониторинга и проверки контейнерных сред

АТОМИК

Руководство пользователя

На 26 листах

Москва
2023

ОГРН 1247700390288 ИНН 9728133771 КПП 772801001
117246, г. Москва, Научный проезд, д.12
почта: info@atomic-ds.ru
веб-сайт: https://atomic-sec.ru/

Содержание

ОГРН 1247700390288 ИНН 9728133771 КПП 772801001
117246, г. Москва, Научный проезд, д.12
почта: info@atomic-ds.ru
веб-сайт: https://atomic-sec.ru/

Список таблиц

ОГРН 1247700390288 ИНН 9728133771 КПП 772801001
117246, г. Москва, Научный проезд, д.12
почта: info@atomic-ds.ru
веб-сайт: https://atomic-sec.ru/

Список рисунков

ОГРН 1247700390288 ИНН 9728133771 КПП 772801001
117246, г. Москва, Научный проезд, д.12
почта: info@atomic-ds.ru
веб-сайт: https://atomic-sec.ru/

1 Введение

Настоящее руководство содержит информацию об основных операциях в рамках взаимодействия пользователей (операторов) с введенным в эксплуатацию продуктом АТОМИК (далее по тексту - Продукт) в составе Информационной системы Заказчика (далее по тексту - ИС).

ОГРН 1247700390288 ИНН 9728133771 КПП 772801001
117246, г. Москва, Научный проезд, д.12
почта: info@atomic-ds.ru
веб-сайт: https://atomic-sec.ru/

2 Общие сведения

Информационное взаимодействие пользователей с функциями АТОМИК осуществляется с использованием средств Веб-портала Управления АТОМИК (далее по тексту - Портал Управления).

Перечень реализованных разделов и соответствующих форм Портала Управления приведен в Табл.1

Табл. 1 – Перечень разделов и форм Портала управления

Наименование раздела/формы		**Описание**
Публичная часть / Аутентификация	Форма «Аутентификация пользователя»	Форма предназначена для ввода пользователями системы аутентификационных данных с последующим входом.
Главная	Форма «Главная»	Форма предназначена для просмотра статистических данных о количестве обнаруженных уязвимостей в виде графиков с распределением по образам и уровням опасности.
Анализ уязвимостей	[корневая форма]	Форма предназначена для просмотра и анализа информации по результатам проведенных сканирований приложений на наличие уязвимостей на этапе подготовки и сборки приложения (Pipeline) и на этапе функционирования приложений (Runtime).
	Сканирования Pipeline	Форма предназначена для просмотра и анализа информации по результатам проведенных сканирований приложений на наличие уязвимостей на этапе подготовки и сборки приложения (Pipeline).
	Сканирования Runtime	Форма предназначена для просмотра и анализа информации по результатам проведенных сканирований приложений на наличие уязвимостей

		на этапе функционирования приложений (Runtime).
Политики	[корневая форма]	Форма предназначена для просмотра, редактирования и создания политик сканирования приложений на наличие уязвимостей.
	Наборы правил	Форма предназначена для просмотра, редактирования и создания Наборов правил сканирования приложений на наличие уязвимостей с возможностью последующей привязки Наборов правил к Политикам.
	Агенты	Форма предназначена для просмотра, редактирования и создания Агентов сканирования.
Отчетность	Анализ уязвимостей	Форма предназначена для параметризованной выгрузки отчетной информации.
Администрирование	Пользователи	Форма предназначена для просмотра, редактирования и создания пользователей (операторов, администраторов) и назначения им соответствующих ролей в рамках Портала управления.
	Роли	Форма предназначена для просмотра, редактирования и создания ролей пользователей и назначения им соответствующих прав доступа в рамках Портала управления.
	Лицензии	Форма предназначена для управления доступными лицензиями.

ОГРН 1247700390288 ИНН 9728133771 КПП 772801001
117246, г. Москва, Научный проезд, д.12
почта: info@atomic-ds.ru
веб-сайт: https://atomic-sec.ru/

3 Аутентификация пользователя

3.1 Форма аутентификации пользователя

Вход в интерфейс Портала управления осуществляется путем предварительного ввода пользователем (оператором, администратором) аутентификационных данных (логина и пароля) с последующей его аутентификацией и авторизацией на Портале.

Описание действий:

- перейти по адресу Портала управления в соответствии с настройками Продукта;
- ввести логин и пароль в соответствующие поля «Имя», «Пароль» формы;
- нажать кнопку ВОЙТИ.

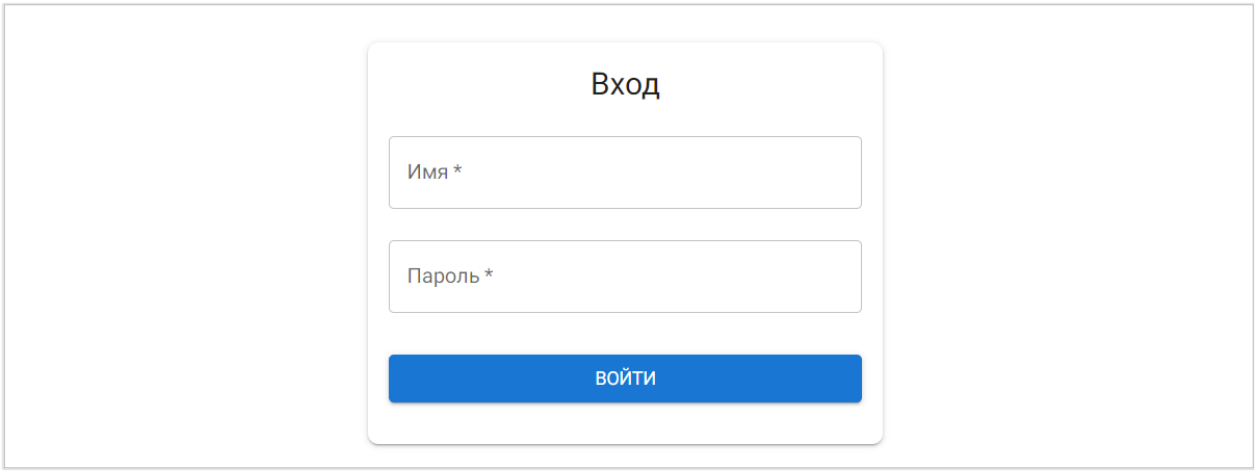

Рисунок 1 – Форма аутентификации пользователя

В зависимости от настроек прав и доступа пользователю может быть недоступна часть функционала.

Для осуществления входа администратора после первичной установки Продукта используются логин и пароль по-умолчанию: admin / admin.

ОГРН 1247700390288 ИНН 9728133771 КПП 772801001
117246, г. Москва, Научный проезд, д.12
почта: info@atomic-ds.ru
веб-сайт: https://atomic-sec.ru/

4 Главная страница

4.1 Форма «Главная»

После входа открывается главное окно панели администрирования. На нем можно просматривать данные о количестве обнаруженных уязвимостей в виде графиков с распределением по образам и уровням опасности.

Графики формируются из полученных результатов сканирований за указанный период

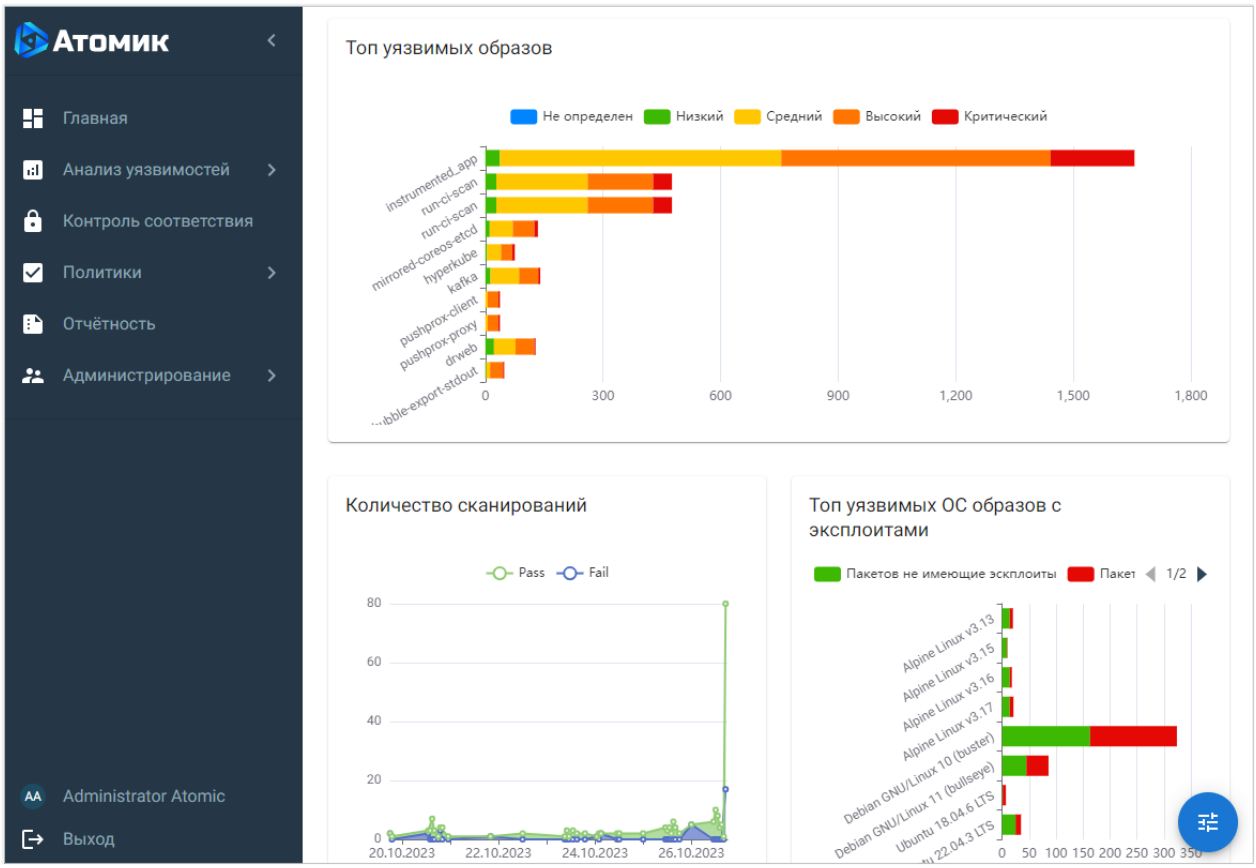

Рисунок 2 – Форма «Главная»

Для удобства отображения имеется ограничитель количества графиков.

4.2 Навигационная панель

Позволяет просматривать и переходить в доступные разделы системы.

Для удобства панель можно скрыть нажатием на функциональную стрелку.

В нижней части панели отображается имя пользователя и кнопка выхода из системы.

Панель отображает разделы:

- Главная;
- Анализ уязвимостей;
- Политики;
- Отчетность;
- Администрирование.

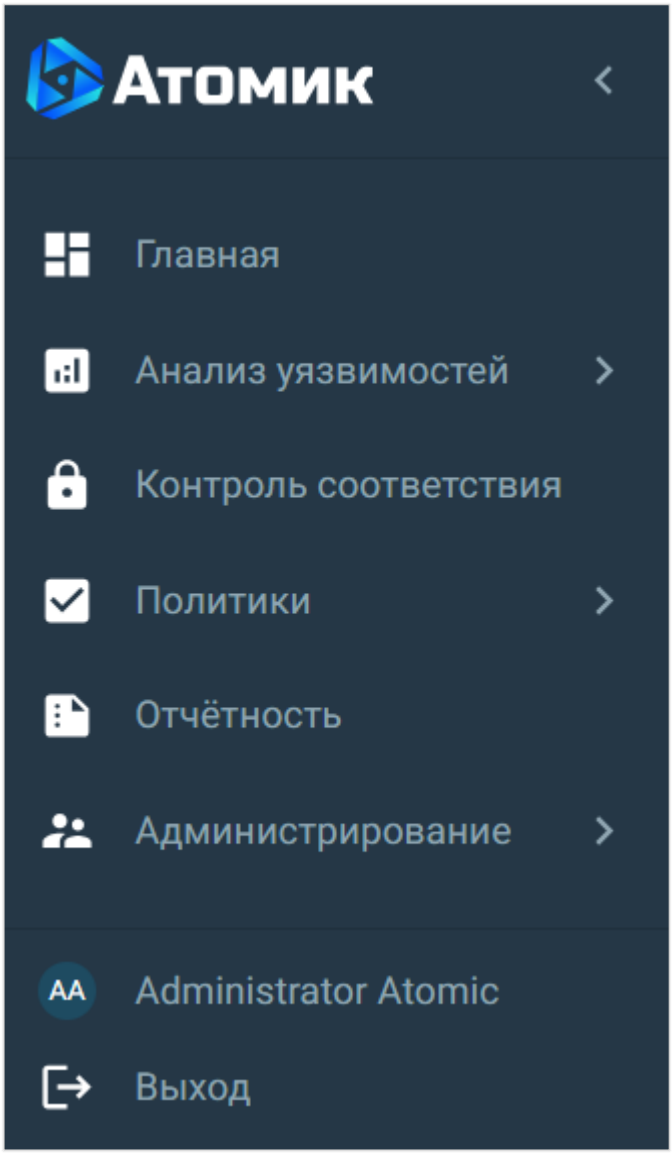

Рисунок 3 – Навигационная панель

ОГРН 1247700390288 ИНН 9728133771 КПП 772801001
117246, г. Москва, Научный проезд, д.12
почта: info@atomic-ds.ru
веб-сайт: https://atomic-sec.ru/

Перемещение по разделам происходит при нажатии указателем.

Разделы, оснащенные символом стрелки, имеют вложенные подразделы.

Перемещение в подраздел происходит при наведении указателя на раздел и нажатием указателя на подраздел.

5 Анализ уязвимостей

Позволяет просматривать список результатов сканирований Pipeline и Runtime приложений.

В данном разделе и его подразделах можно узнать:

- общее количество сканирований всех образов;
- общее количество запущенных образов в Runtime;
- имя и версии просканированных образов;
- ID образов;
- количество найденных уязвимостей в образах по уровню опасности;
- дату последнего сканирования образов.

Для удобства навигации имеется встроенный фильтр по названию, статусу и вердикту сканирования.

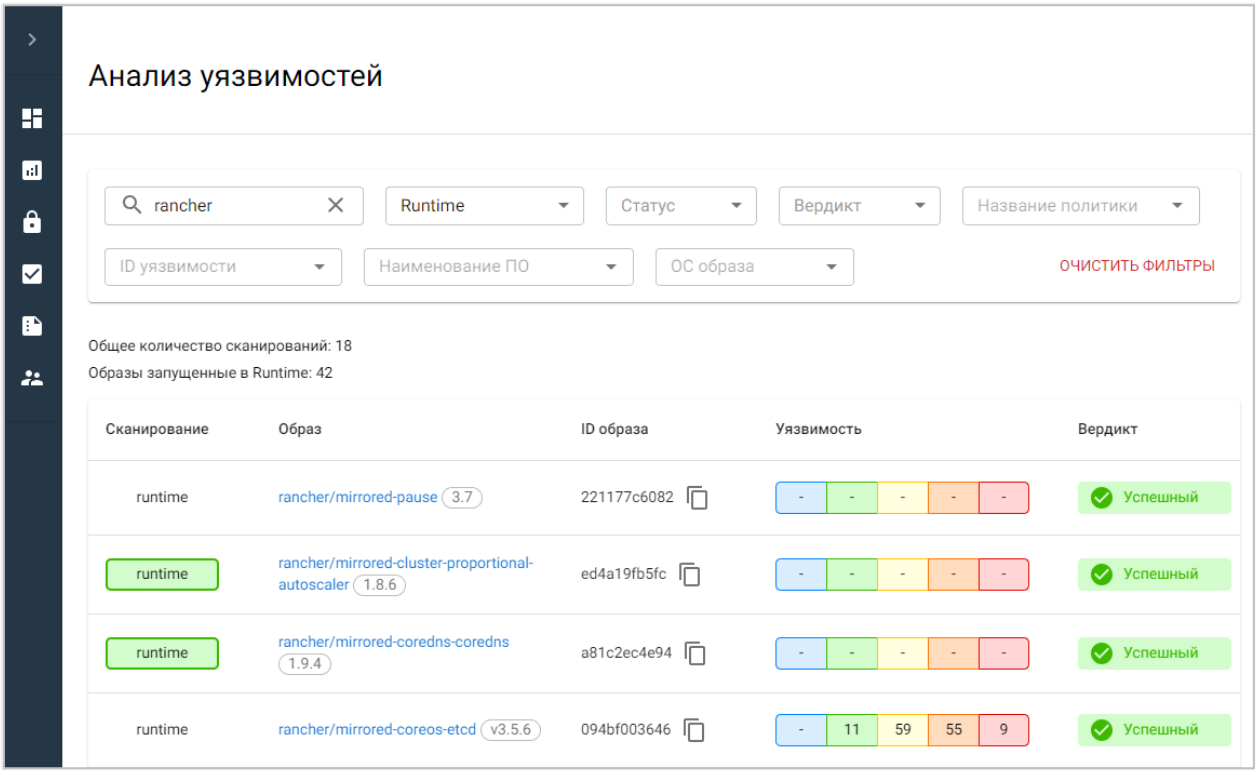

Рисунок 4 – Форма «Анализ уязвимостей»

Для перехода в просмотр собранных данных образа нажать указателем на название образа.

Для перехода в просмотр найденных уязвимостей образа нажать указателем на значение в столбце Уязвимость.

5.1 Сканирования Pipeline

Позволяет просматривать список результатов всех сканирований Pipeline образов.

Отображает общее количество выполненных Pipeline сканирований.

Управление просмотром аналогично разделу Анализ уязвимостей.

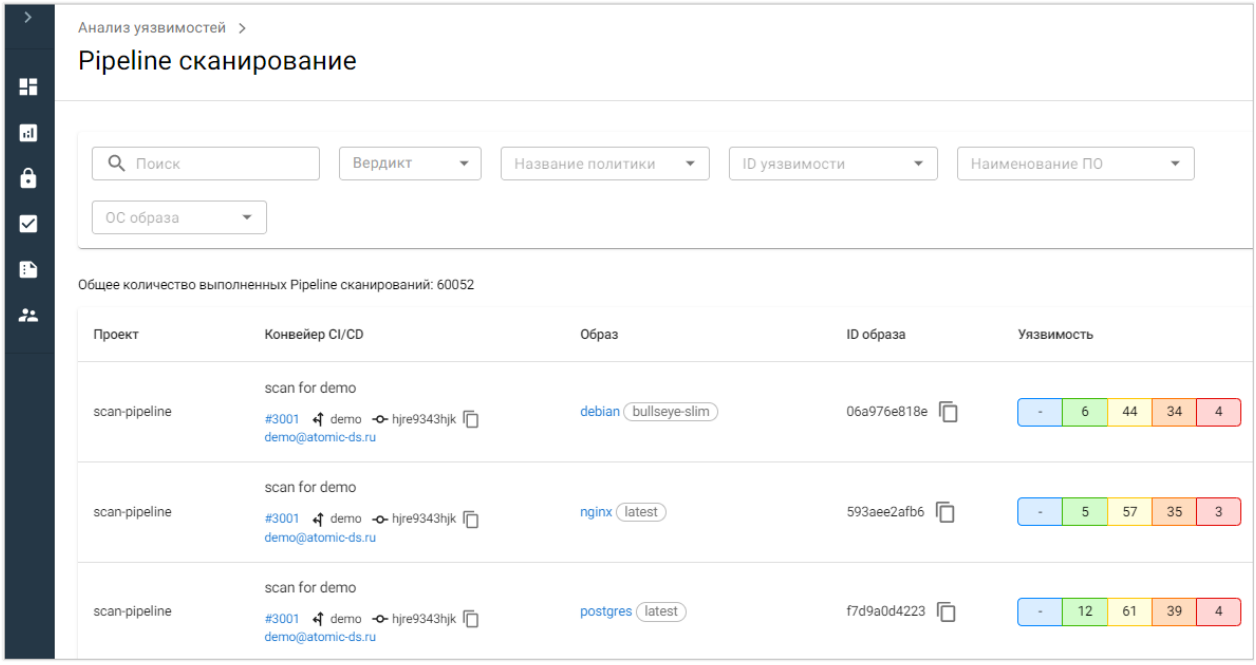

Рисунок 5 – Форма «Сканирования Pipeline»

Для удобства навигации имеется встроенный фильтр по названию и вердикту сканирования.

5.2 Сканирования Runtime

Позволяет просматривать список результатов последних сканирований образов в Runtime.

Отображает:

- общее количество запущенных образов в Runtime;
- принадлежность образов в Runtime к кластеру и Namespace;
- тип Runtime: Deployment; DaemonSet; Pod; CronJob; StatefulSet;

ОГРН 1247700390288 ИНН 9728133771 КПП 772801001
117246, г. Москва, Научный проезд, д.12
почта: info@atomic-ds.ru
веб-сайт: https://atomic-sec.ru/

– количество образов в каждом Runtime и вердикты их последних сканирований;
– количество найденных уязвимостей по уровню опасности.

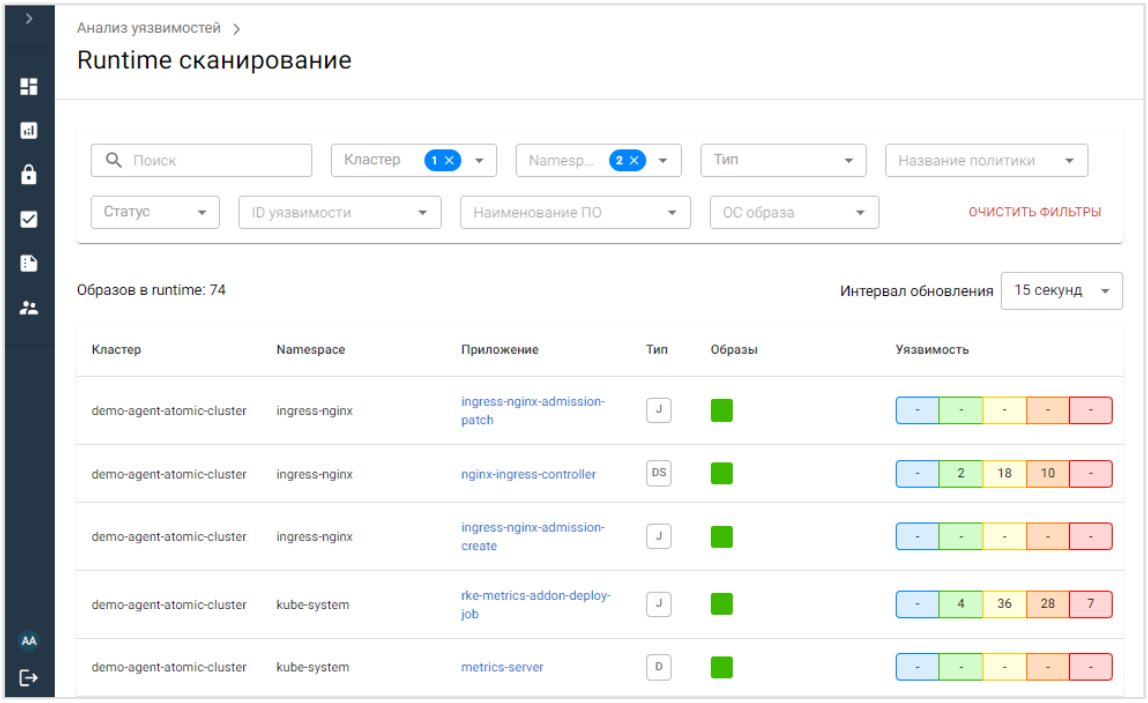

Рисунок 6 – Форма «Сканирования Runtime»

Для удобства навигации имеется встроенный фильтр по названию, кластеру, Namespace, Типу Runtime и текущему статусу .

Для просмотра просканированных образов в Runtime нажать указателем на название приложения.

Далее управление просмотром аналогично разделу Анализ уязвимостей.

5.3 Образ

Позволяет просматривать детальную информацию о сканируемом образе.

После перехода в просмотр образа открывается интерфейс со сгруппированной информацией, интерфейс содержит:

– указатель с типом сканирования, названием образа и его версией, ОС образа;
– дату последнего сканирования;

- панель вкладок: Обзор, Уязвимости, Список ПО, Политика сканирования, метаданные, История сканирований;
- область просмотра вкладки.

5.4 Обзор

Отображает вердикт последних сканирований с указанием назначенной политики сканирования и наглядный результат обнаружения уязвимостей.

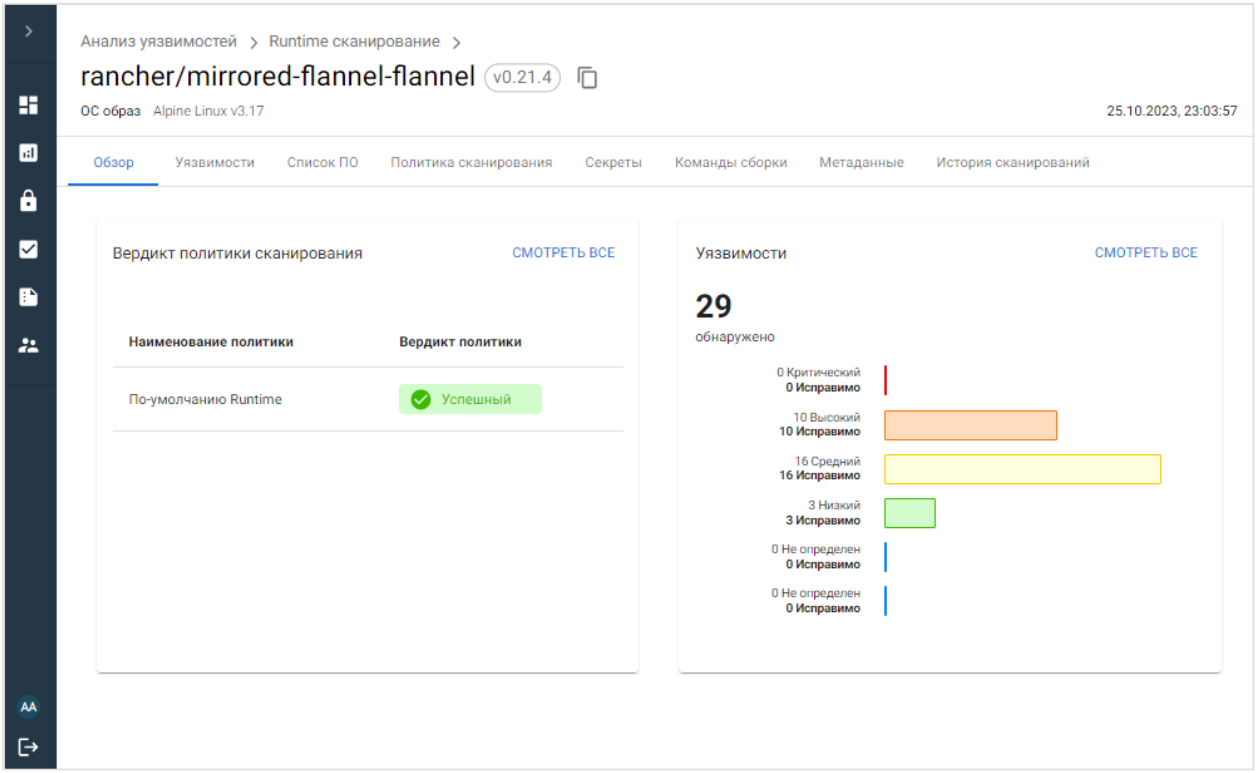

Рисунок 7 – Сканирование. Обзор

5.5 Уязвимости

Позволяет просматривать все найденные уязвимости в образе согласно политикам сканирования.

Область просмотра уязвимостей содержит:

- ID уязвимости;
- наличие эксплойта;
- уровень опасности;
- оценка CVSS;

– пакет и версия;
– наличие исправление;
– тип источника;
– дата выявления.

Для удобства навигации по списку встроен фильтр по названию пакета, уровню опасности, оценке CVSS V3, типу источника, наличию исправления и эксплойта.

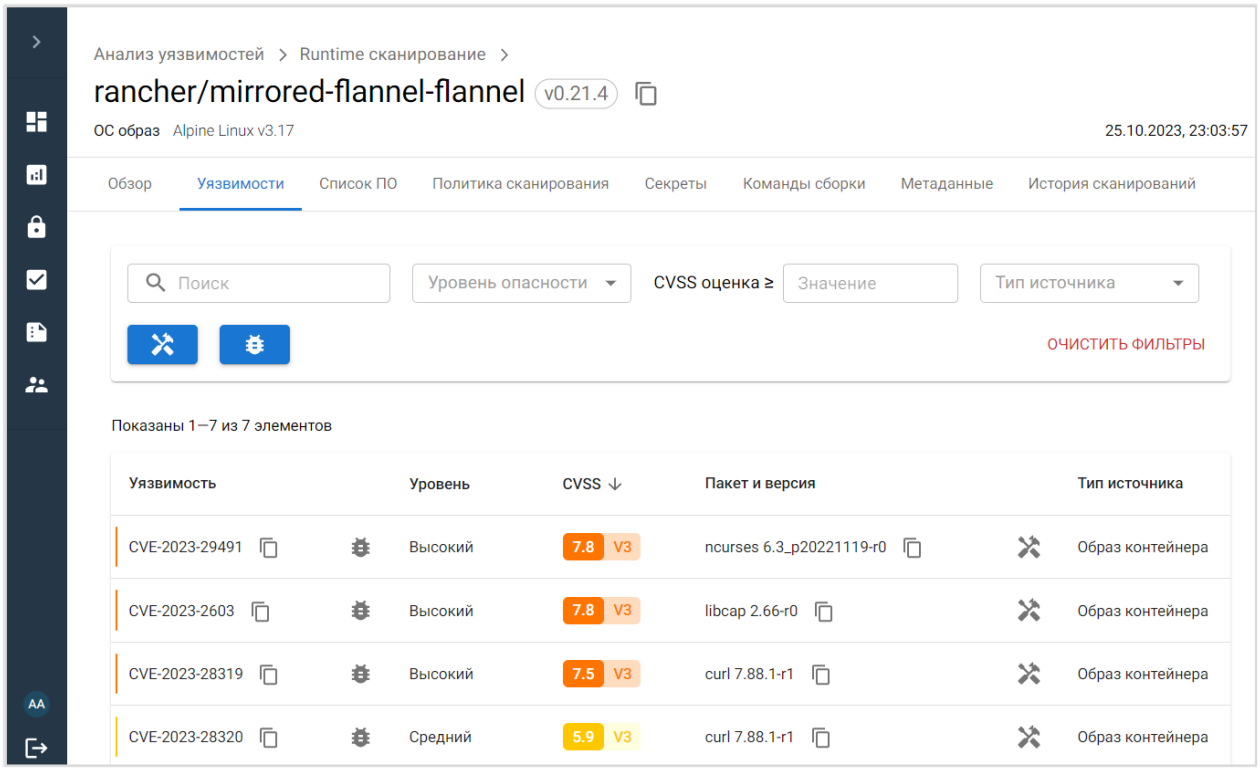

Рисунок 8 – Сканирование. Уязвимости

Для просмотра информации по конкретной уязвимости из списка надо нажать на нее указателем.

Просмотр уязвимости позволяет узнать:

– номера исправленных версий пакета, при наличии исправления;
– оценки уязвимости текущего пакета по дополнительным базам данных;
– детальное описание метрик эксплуатируемости и влияния уязвимости на систему;
– краткое описание уязвимости;

ОГРН 1247700390288 ИНН 9728133771 КПП 772801001
117246, г. Москва, Научный проезд, д.12
почта: info@atomic-ds.ru
веб-сайт: https://atomic-sec.ru/

Для просмотра детального описания метрик уязвимости навести и задержать указатель на иконке оценки уязвимости.

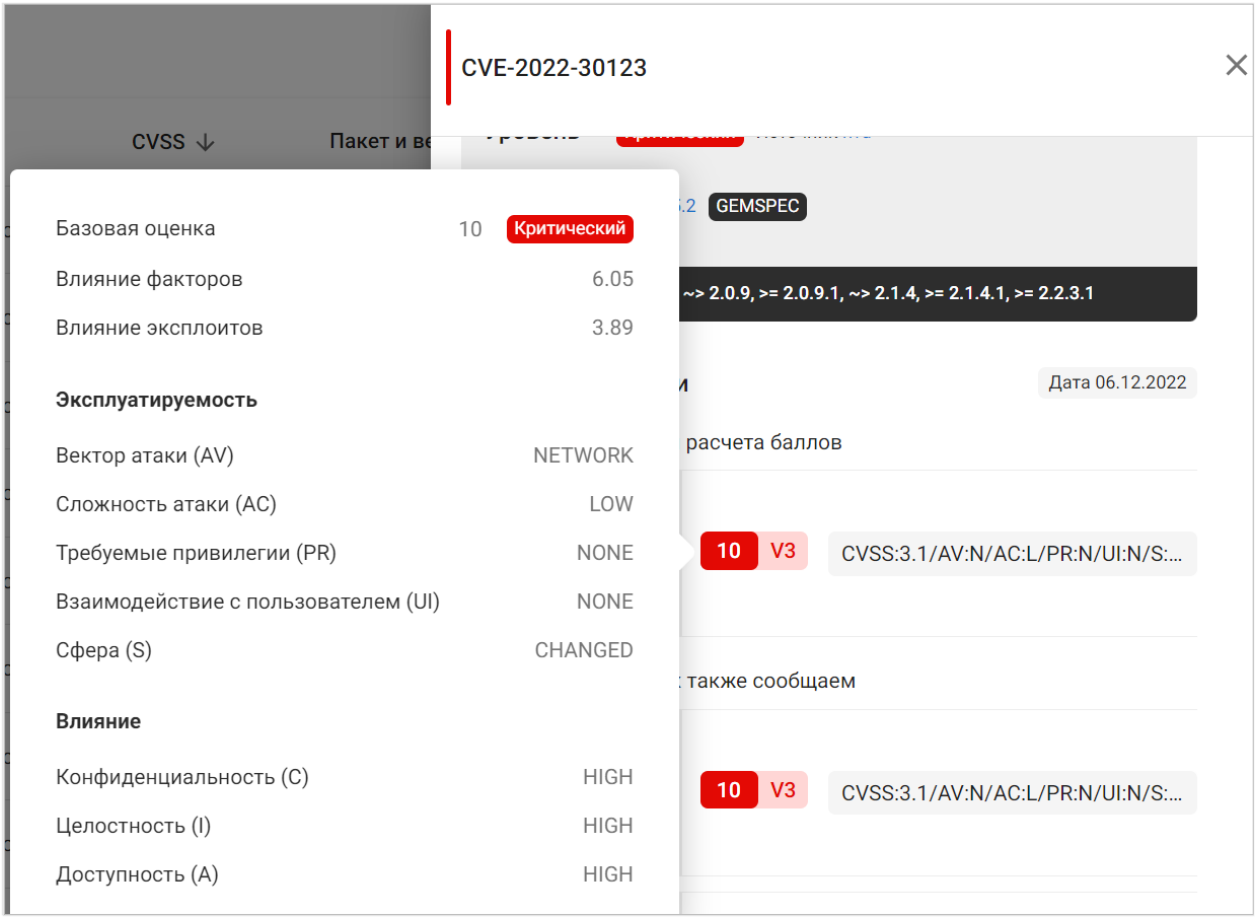

Рисунок 9 – Сканирование. Сведения об уязвимости

5.6 Список ПО

Позволяет просматривать список всех программных пакетов содержащихся в текущем образе.

Отображает:

- имя и версию пакета;
- тип пакета;
- количество уязвимостей в пакете по уровням опасности;
- наличие исправлений;
- наличие эксплойтов;
- тип источника.

Для удобства навигации по списку встроен фильтр по названию пакета, уровню опасности, типу источника, наличию исправления и эксплойта.

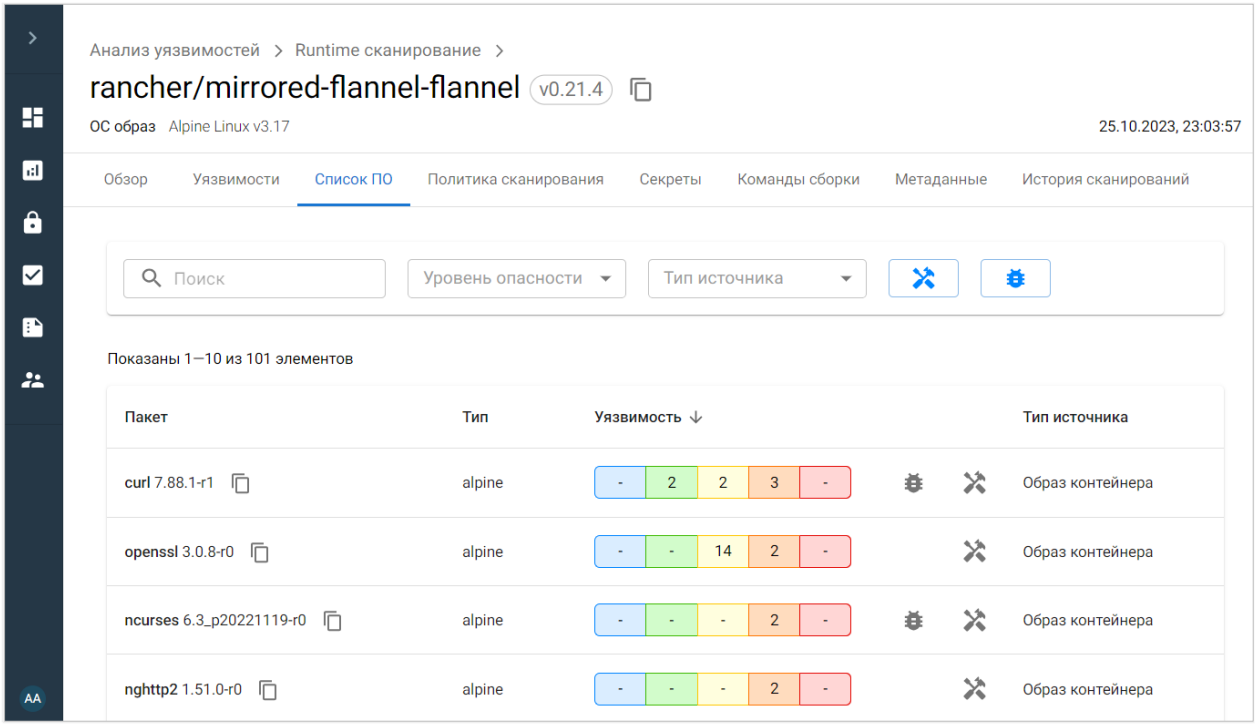

Рисунок 10 – Сканирование. Список ПО

Для просмотра списка всех уязвимостей в конкретном пакете нажать на него указателем.

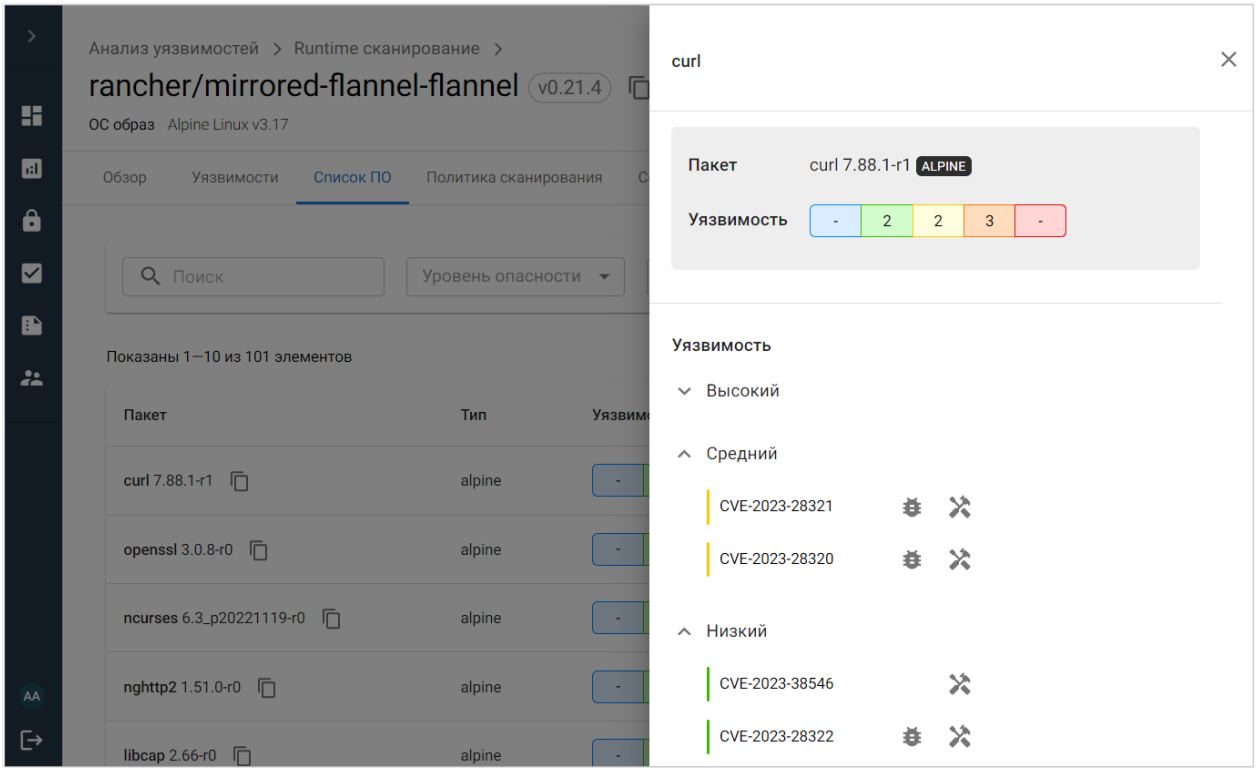

Рисунок 11 – Сканирование. Сведения о пакете ПО

5.7 Политика сканирования

Отображает общий и детальный вердикт последнего сканирования текущего образа с примененными политиками сканирования.

ОГРН 1247700390288 ИНН 9728133771 КПП 772801001
117246, г. Москва, Научный проезд, д.12
почта: info@atomic-ds.ru
веб-сайт: https://atomic-sec.ru/

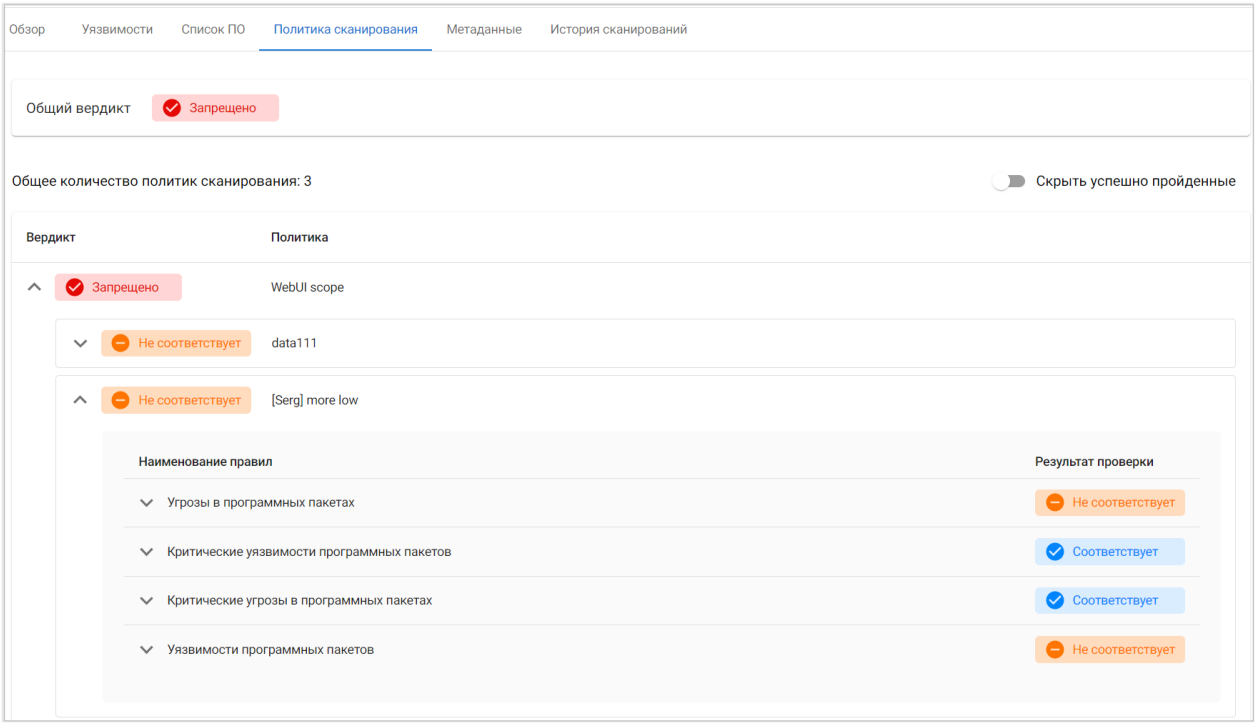

Рисунок 12 – Сканирование. Политика сканирования

5.8 Метаданные

Отображает дополнительную информацию текущего образа.

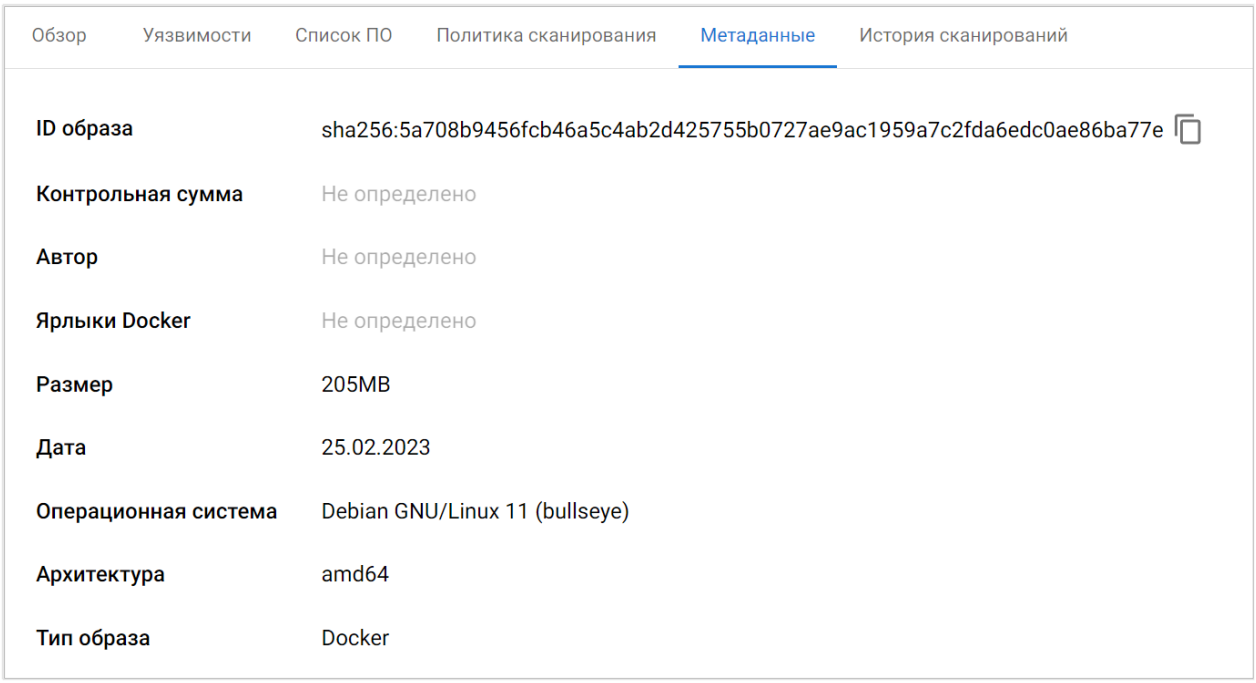

Рисунок 13 – Сканирование. Метаданные

ОГРН 1247700390288 ИНН 9728133771 КПП 772801001
117246, г. Москва, Научный проезд, д.12
почта: info@atomic-ds.ru
веб-сайт: https://atomic-sec.ru/

5.9 История сканирований

Отображает список всех сканирований текущего образа в Runtime и Pipeline.

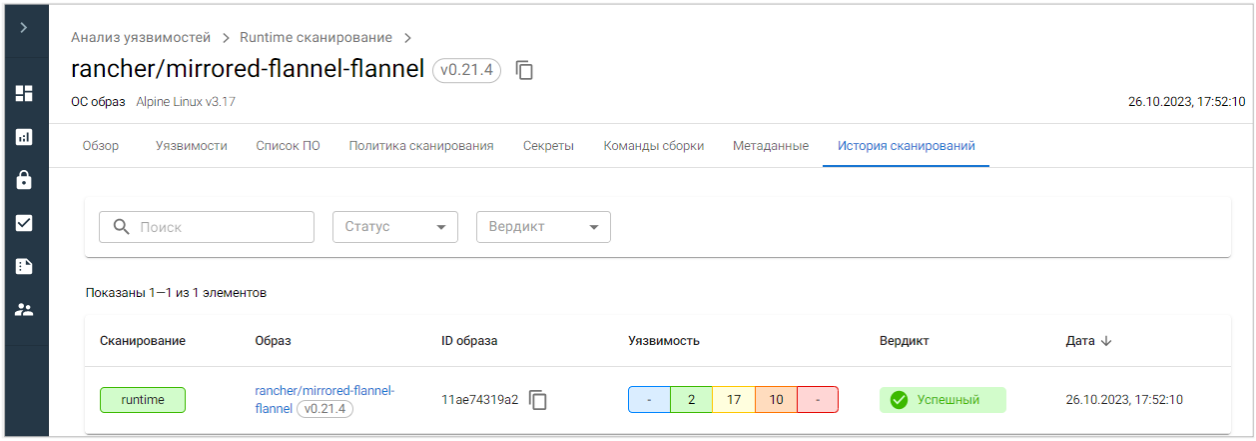

Рисунок 14 – Сканирование. История сканирований

Управление просмотром аналогично разделу Анализ уязвимостей.

6 Политики

Политики обнаружения уязвимостей предназначены для применения наборов правил и настроек, в соответствии с которыми производится сканирование контейнерной среды.

При создании политики учитываются параметры:

- сканирование образов в Pipeline или в Runtime (только одного типа);
- применять всегда (ко всем агентам указанного типа);
- запретить/разрешить действие политики;
- ограничение области действия Host или Workload (позволяет ограничить хосты к которым применяется политика);
- список наборов правил сканирования;
- список агентов к которым будет применяться политика.

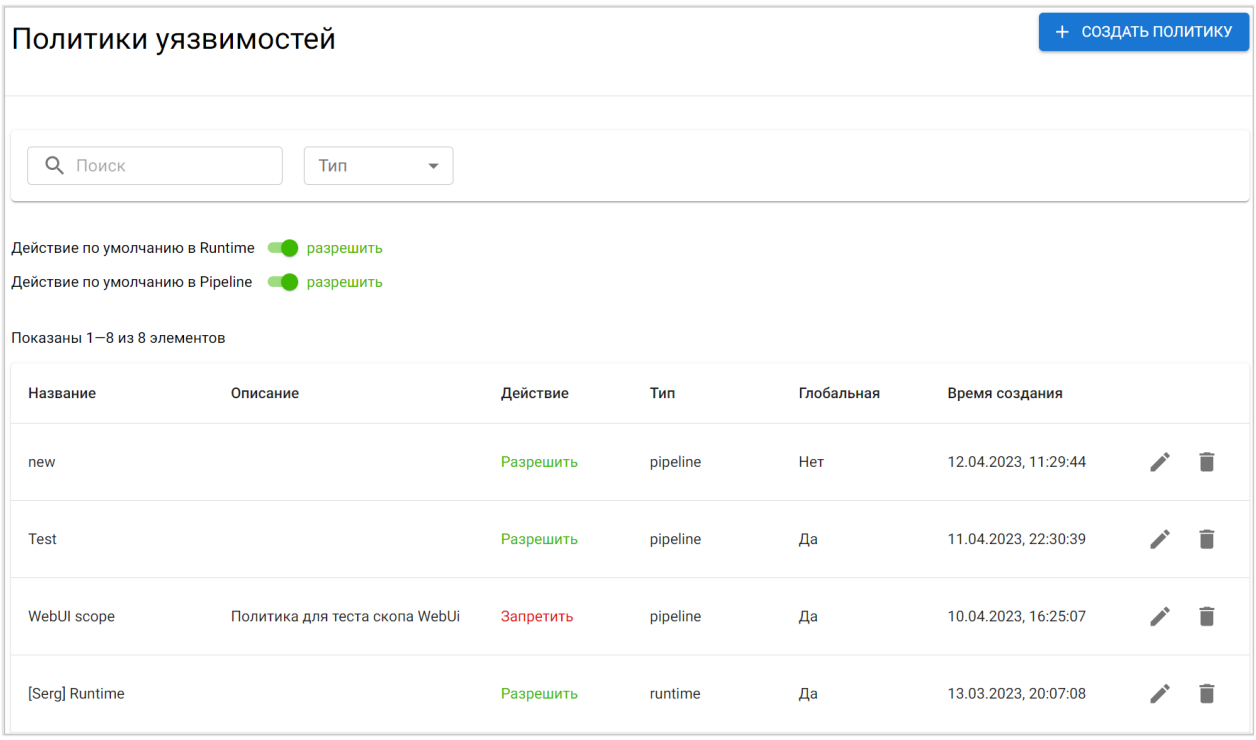

Рисунок 15 – Форма «Политики»

6.1 Наборы правил

Наборы правил сканирования используются для ограничения области поиска уязвимостей по их свойствам.

Наборы правил должны применяться к политикам уязвимостей.

При создании набора правил учитываются параметры:

- уровень угрозы;
- наличие эксплойта;
- дата обнаружения уязвимости.

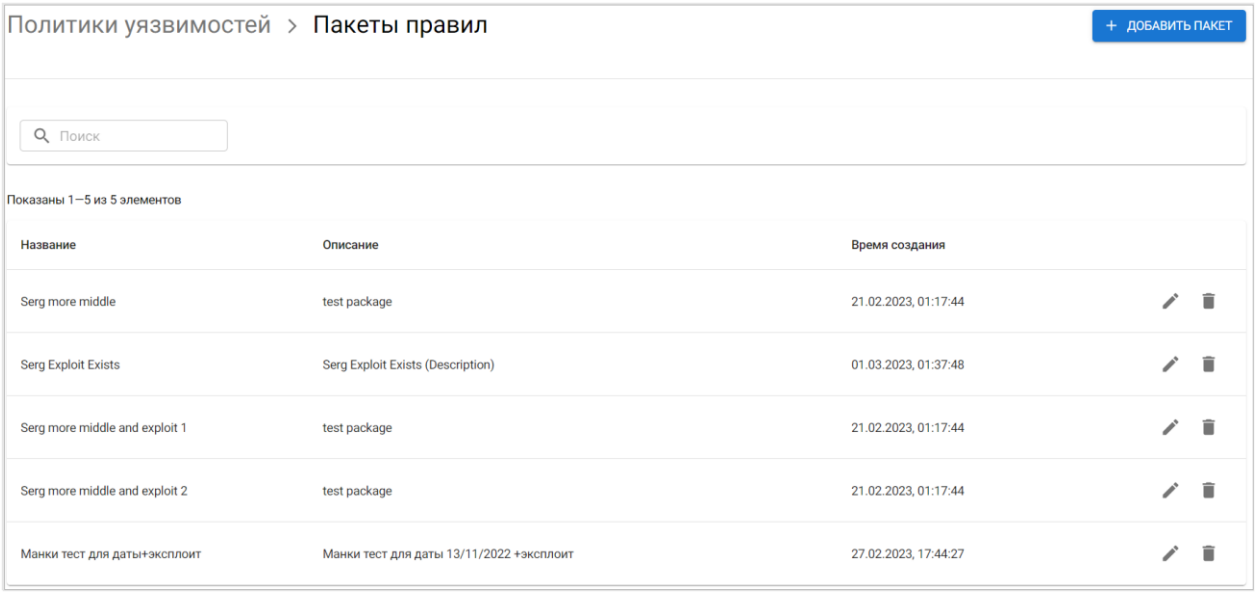

Рисунок 16 – Политики. Пакеты правил

6.2 Агенты

Создание API ключа для подключения сканирующего агента с применением политики обнаружения уязвимостей и указанием типа сканирования.

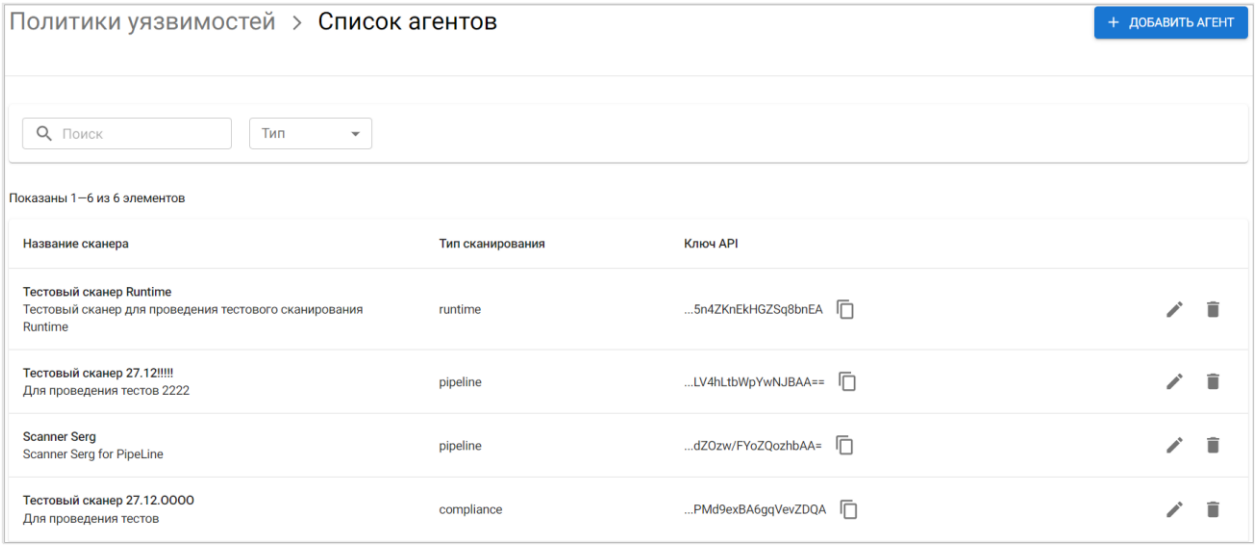

Рисунок 17 – Политики. Агенты

7 Отчетность

Реализует возможность параметризованной выгрузки отчетной информации за выбранные временные промежутки по результатам сканирований на наличие уязвимостей, а также иных функций, реализуемых Продуктов в составе ИС.

Выгрузка осуществляется в машиночитаемом структурированном формате с целью обеспечения возможности дальнейшей обработки во внешних системах.

8 Администрирование

8.1 Пользователи

Реализует возможности просмотра, редактирования и создания пользователей (операторов, администраторов) и назначения им соответствующих ролей в рамках Портала управления.

8.2 Роли

Реализует возможности просмотра, редактирования и создания ролей пользователей и назначения им соответствующих прав доступа в рамках Портала управления для применения ролевой модели.

Имеет следующие категории для применения модели чтения/записи:

- анализ уязвимостей;
- политики;
- отчётность;
- администрирование.

8.3 Лицензии

Реализует возможности управления доступными лицензиями.

8.4 Серверы аутентификации

Реализует возможность подключения к серверам LDAP и RADIUS.

ОГРН 1247700390288 ИНН 9728133771 КПП 772801001
117246, г. Москва, Научный проезд, д.12
почта: info@atomic-ds.ru
веб-сайт: https://atomic-sec.ru/

9 Перечень принятых сокращений

ИС	–	автоматизированная информационная система Заказчика
БД	–	база данных, управляемая реляционной СУБД
ПО	–	программное обеспечение
ПП	–	программная платформа
ПК	–	программный комплекс
СКЗИ	–	средство криптографической защиты информации
СУБД	–	система управления базами данных

ОГРН 1247700390288 ИНН 9728133771 КПП 772801001
117246, г. Москва, Научный проезд, д.12
почта: info@atomic-ds.ru
веб-сайт: https://atomic-sec.ru/

10 Перечень терминов и определений

Автоматизированная информационная система (ИС) – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций.

Администратор системный – лицо, ответственное за функционирование автоматизированной системы в установленном штатном режиме работы.

Администратор информационной безопасности – лицо, ответственное за защиту автоматизированной системы от несанкционированного доступа к информации.

Безопасность информации – состояние защищенности информации, характеризуемое способностью персонала, технических средств и информационных технологий обеспечивать конфиденциальность (сохранение в тайне от субъектов, не имеющих полномочий на ознакомление с ней), целостность и доступность информации при ее обработке техническими средствами.

Доступ к информации (доступ) – ознакомление с информацией, ее обработка, в частности, копирование, модификация или уничтожение информации.

Доступность (санкционированная доступность) информации – состояние информации, характеризуемое способностью технических средств и информационных технологий обеспечивать беспрепятственный доступ к информации субъектов, имеющих на это полномочия.

Защита информации от несанкционированного доступа (защита от НСД) **или воздействия** – деятельность, направленная на предотвращение получения информации заинтересованным субъектом (или воздействия на информацию) с нарушением установленных прав или правил.

Защищаемая информация – информация, являющаяся предметом собственности и подлежащая защите в соответствии с требованиями правовых документов или требованиями, устанавливаемыми собственником информации (ГОСТ Р 50922).

Информационная технология – приемы, способы и методы применения средств вычислительной техники при выполнении функций хранения, обработки, передачи и использования данных (ГОСТ 34.003).

ОГРН 1247700390288 ИНН 9728133771 КПП 772801001
117246, г. Москва, Научный проезд, д.12
почта: info@atomic-ds.ru
веб-сайт: https://atomic-sec.ru/

Информационные сети общего пользования – вычислительные (информационно-телекоммуникационные сети) открытые для пользования всем физическим и юридическим лицам, в услугах которых этим лицам не может быть отказано.

Конфиденциальная информация – документированная информация, доступ к которой ограничивается в соответствии с законодательством Российской Федерации.

Локальная вычислительная сеть – вычислительная сеть, поддерживающая в пределах ограниченной территории один или несколько высокоскоростных каналов передачи цифровой информации, предоставляемых подключаемым устройствам для кратковременного монопольного использования.

Несанкционированный доступ (несанкционированные действия) – доступ к информации или действия с информацией, нарушающие правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами.

Обработка информации – совокупность операций сбора, накопления, ввода, вывода, приема, передачи, записи, хранения, регистрации, уничтожения, преобразования, отображения, осуществляемых над информацией.

Продукт – программный комплекс **АТОМИК**, введенный в эксплуатацию в составе Информационной системы Заказчик.

Средство защиты информации – техническое, программное средство, вещество и/или материал, предназначенные или используемые для защиты информации (ГОСТ Р 50922).

Целостность информации – устойчивость информации к несанкционированному или случайному воздействию на нее в процессе обработки техническими средствами, результатом которого может быть уничтожение и искажение информации.