



**Программное обеспечение для мониторинга и проверки  
контейнерных сред**

**АТОМИК**

**Руководство пользователя**

**На 26 листах**

**Москва  
2023**



## Содержание

1 Введение.....	5
2 Общие сведения.....	6
3 Аутентификация пользователя .....	8
3.1 Форма аутентификации пользователя.....	8
4 Главная страница.....	9
4.1 Форма «Главная».....	9
4.2 Навигационная панель .....	9
5 Анализ уязвимостей .....	12
5.1 Сканирования Pipeline.....	13
5.2 Сканирования Runtime .....	13
5.3 Образ .....	14
5.4 Обзор .....	15
5.5 Уязвимости .....	15
5.6 Список ПО .....	17
5.7 Политика сканирования .....	19
5.8 Метаданные .....	20
5.9 История сканирований .....	21
6 Политики.....	22
6.1 Наборы правил.....	23
6.2 Агенты.....	23
7 Отчетность .....	25
8 Администрирование .....	26
8.1 Пользователи .....	26
8.2 Роли.....	26
8.3 Лицензии.....	26
8.4 Серверы аутентификации.....	26
9 Перечень принятых сокращений .....	27
10 Перечень терминов и определений.....	28

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



## Список таблиц

Табл. 1 – Перечень разделов и форм Портала управления.....	6
--	---



## Список рисунков

Рисунок 1 – Форма аутентификации пользователя.....	8
Рисунок 2 – Форма «Главная» .....	9
Рисунок 3 – Навигационная панель .....	10
Рисунок 4 – Форма «Анализ уязвимостей» .....	12
Рисунок 5 – Форма «Сканирования Pipeline» .....	13
Рисунок 6 – Форма «Сканирования Runtime».....	14
Рисунок 7 – Сканирование. Обзор .....	15
Рисунок 8 – Сканирование. Уязвимости .....	16
Рисунок 9 – Сканирование. Сведения об уязвимости.....	17
Рисунок 10 – Сканирование. Список ПО .....	18
Рисунок 11 – Сканирование. Сведения о пакете ПО .....	19
Рисунок 12 – Сканирование. Политика сканирования .....	20
Рисунок 13 – Сканирование. Метаданные .....	20
Рисунок 14 – Сканирование. История сканирований .....	21
Рисунок 15 – Форма «Политики» .....	22
Рисунок 16 – Политики. Пакеты правил .....	23
Рисунок 17 – Политики. Агенты .....	24



## **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).



## 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.



## 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**.

The image shows a login form titled "Вход" (Login). It consists of two text input fields: "Имя \*" (Name) and "Пароль \*" (Password). Below the fields is a blue button with the text "ВОЙТИ" (Login).

**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.





## 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

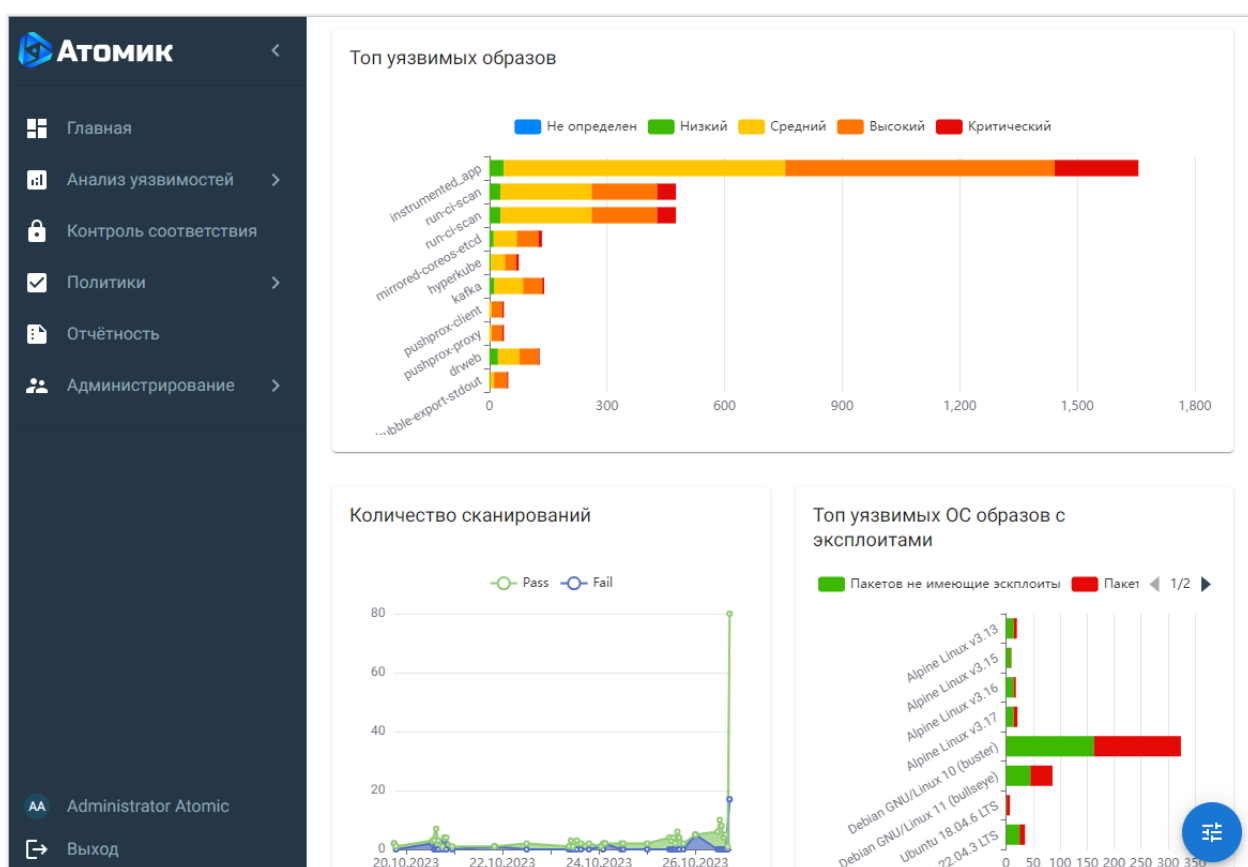


Рисунок 2 – Форма «Главная»

Для удобства отображения имеется ограничитель количества графиков.

### 4.2 Навигационная панель

Позволяет просматривать и переходить в доступные разделы системы.

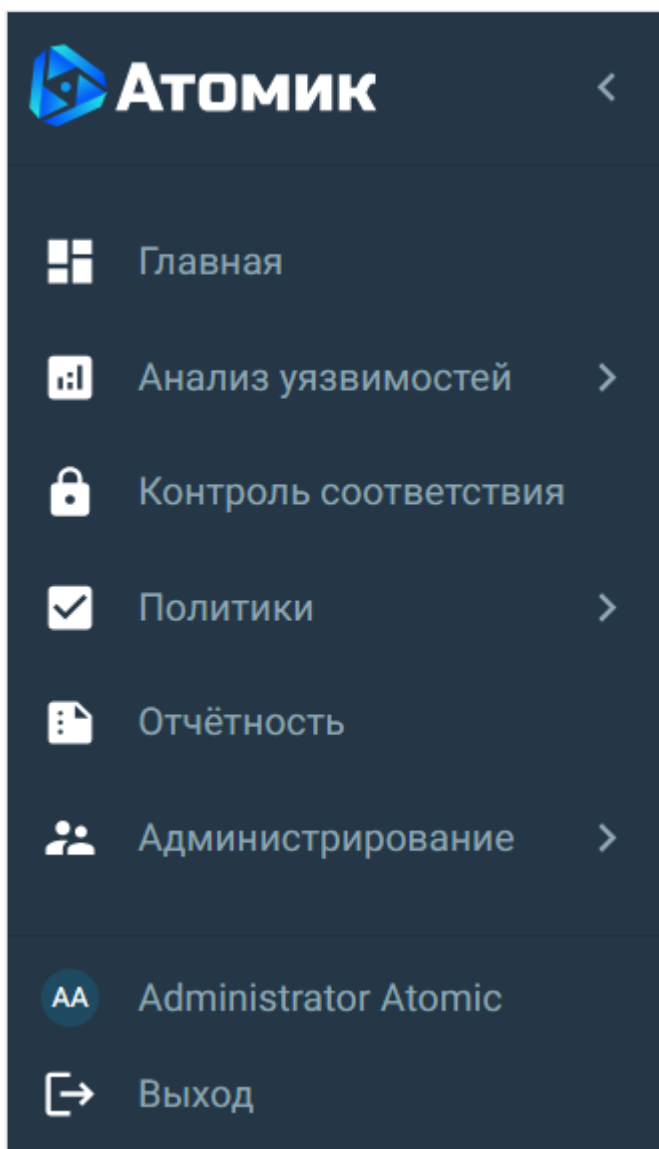
Для удобства панель можно скрыть нажатием на функциональную стрелку.



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](mailto: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.

Сканирование	Образ	ID образа	Уязвимость	Вердикт
runtime	rancher/mirrored-pause (3.7)	221177c6082	- - - - -	Успешный
runtime	rancher/mirrored-cluster-proportional-autoscaler (1.8.6)	ed4a19fb5fc	- - - - -	Успешный
runtime	rancher/mirrored-coredns-coredns (1.9.4)	a81c2ec4e94	- - - - -	Успешный
runtime	rancher/mirrored-coreos-etcd (v3.5.6)	094bf003646	- 11 59 55 9	Успешный

Рисунок 4 – Форма «Анализ уязвимостей»

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



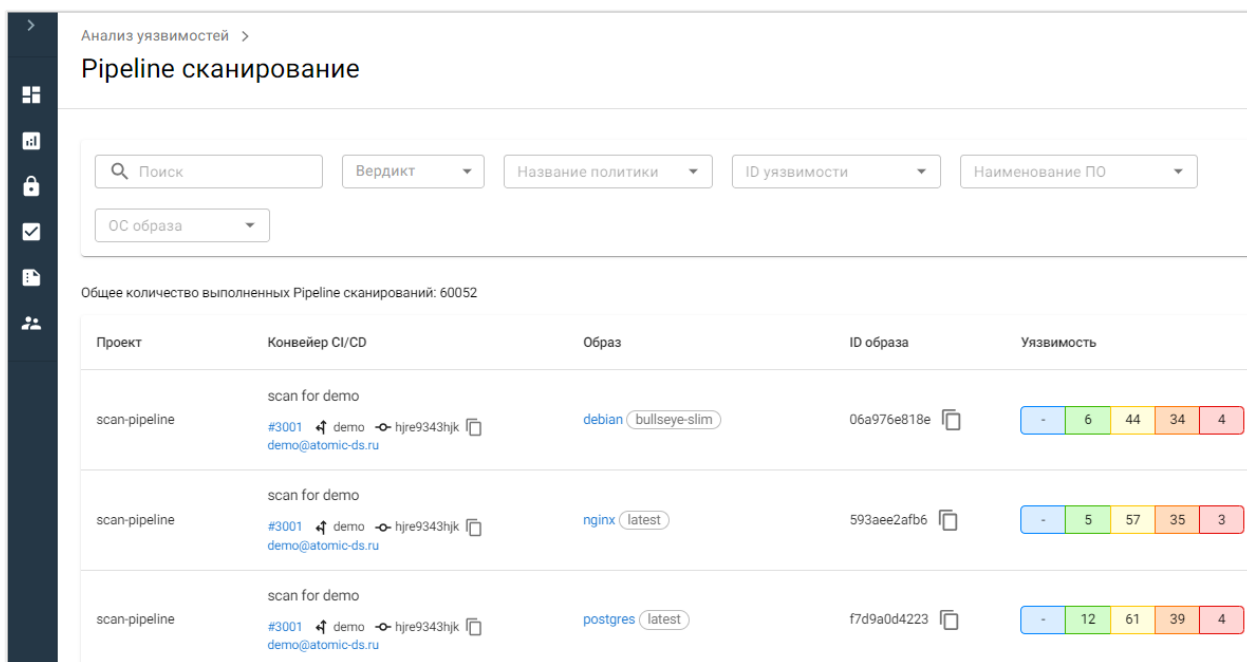
Для перехода в просмотр найденных уязвимостей образа нажать указателем на значение в столбце Уязвимость.

## 5.1 Сканирования Pipeline

Позволяет просматривать список результатов всех сканирований Pipeline образов.

Отображает общее количество выполненных Pipeline сканирований.

Управление просмотром аналогично разделу Анализ уязвимостей.



Проект	Конвейер CI/CD	Образ	ID образа	Уязвимость
scan-pipeline	scan for demo #3001 demo hjre9343hjk demo@atomic-ds.ru	debian bullseye-slim	06a976e818e	6 44 34 4
scan-pipeline	scan for demo #3001 demo hjre9343hjk demo@atomic-ds.ru	nginx latest	593aee2afb6	5 57 35 3
scan-pipeline	scan for demo #3001 demo hjre9343hjk demo@atomic-ds.ru	postgres latest	f7d9a0d4223	12 61 39 4

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;



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

Кластер	Namespace	Приложение	Тип	Образы	Уязвимость
demo-agent-atomic-cluster	ingress-nginx	ingress-nginx-admission-patch	J	■	- - - - -
demo-agent-atomic-cluster	ingress-nginx	nginx-ingress-controller	DS	■	- 2 18 10 -
demo-agent-atomic-cluster	ingress-nginx	ingress-nginx-admission-create	J	■	- - - - -
demo-agent-atomic-cluster	kube-system	rke-metrics-addon-deploy-job	J	■	- 4 36 28 7
demo-agent-atomic-cluster	kube-system	metrics-server	D	■	- - - - -

**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.

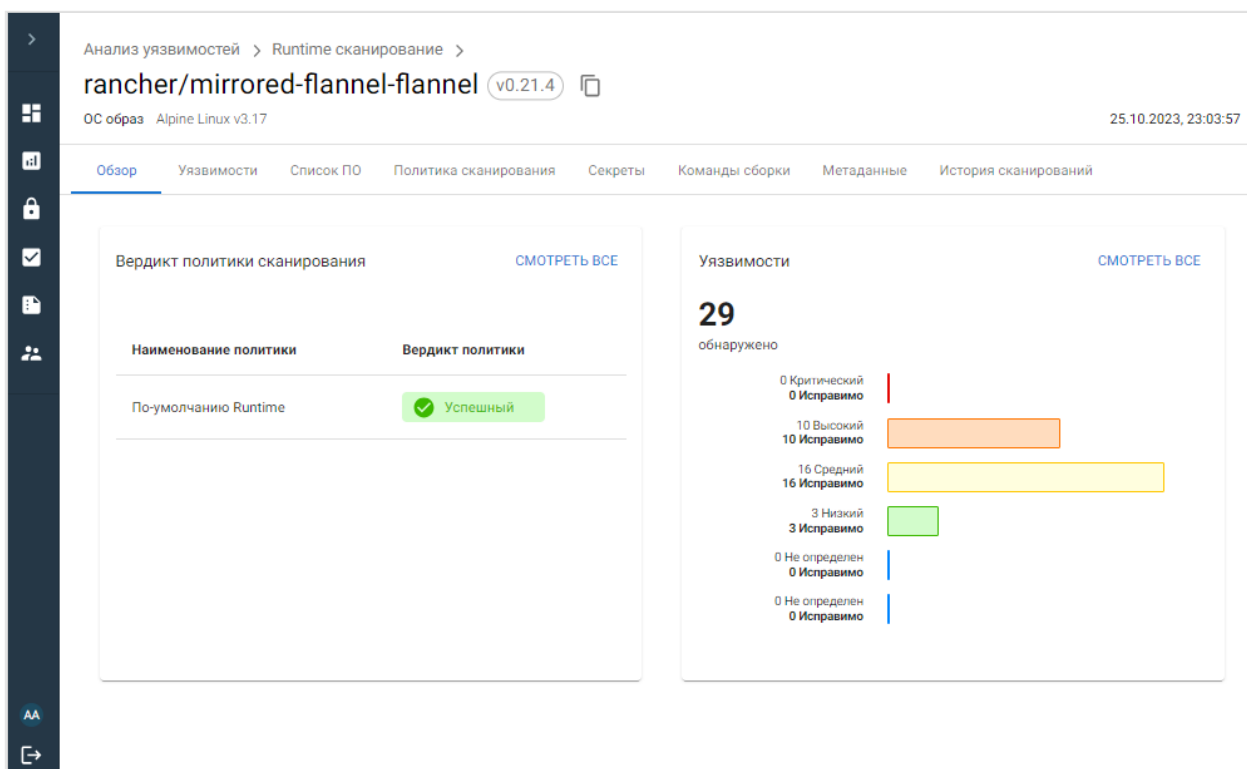


Рисунок 7 – Сканирование. Обзор

## 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.

Анализ уязвимостей > Runtime сканирование >

rancher/mirrored-flannel-flannel v0.21.4

ОС образ Alpine Linux v3.17 25.10.2023, 23:03:57

Обзор **Уязвимости** Список ПО Политика сканирования Секреты Команды сборки Метаданные История сканирований

Поиск Уровень опасности CVSS оценка ≥ Значение Тип источника

ОЧИСТИТЬ ФИЛЬТРЫ

Показаны 1–7 из 7 элементов

Уязвимость	Уровень	CVSS ↓	Пакет и версия	Тип источника
CVE-2023-29491	Высокий	7.8 V3	ncurses 6.3_p20221119-r0	Образ контейнера
CVE-2023-2603	Высокий	7.8 V3	libcap 2.66-r0	Образ контейнера
CVE-2023-28319	Высокий	7.5 V3	curl 7.88.1-r1	Образ контейнера
CVE-2023-28320	Средний	5.9 V3	curl 7.88.1-r1	Образ контейнера

### 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;





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

Метрика	Значение
Базовая оценка	10 <b>Критический</b>
Влияние факторов	6.05
Влияние эксплоитов	3.89
<b>Эксплуатируемость</b>	
Вектор атаки (AV)	NETWORK
Сложность атаки (AC)	LOW
Требуемые привилегии (PR)	NONE
Взаимодействие с пользователем (UI)	NONE
Сфера (S)	CHANGED
<b>Влияние</b>	
Конфиденциальность (C)	HIGH
Целостность (I)	HIGH
Доступность (A)	HIGH

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.

Анализ уязвимостей > Runtime сканирование >  
**rancher/mirrored-flannel-flannel** v0.21.4

ОС образ Alpine Linux v3.17 25.10.2023, 23:03:57

Обзор Уязвимости **Список ПО** Политика сканирования Секреты Команды сборки Метаданные История сканирований

Поиск  Уровень опасности  Тип источника

Показаны 1–10 из 101 элементов

Пакет	Тип	Уязвимость ↓	Тип источника
curl 7.88.1-r1	alpine		Образ контейнера
openssl 3.0.8-r0	alpine		Образ контейнера
ncurses 6.3_p20221119-r0	alpine		Образ контейнера
nghttp2 1.51.0-r0	alpine		Образ контейнера

### Рисунок 10 – Сканирование. Список ПО

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



The screenshot displays the Atomic Security interface. The main window shows a list of packages under the heading 'rancher/mirrored-flannel-flannel v0.21.4'. The 'curl' package is selected, and a detailed view is shown on the right. The detailed view includes the package name 'curl 7.88.1-r1 ALPINE' and a severity score of 2. Below this, a list of vulnerabilities is shown, including CVE-2023-28321, CVE-2023-28320, CVE-2023-38546, and CVE-2023-28322.

Пакет	Тип	Уязвим
curl 7.88.1-r1	alpine	-
openssl 3.0.8-r0	alpine	-
ncurses 6.3_p20221119-r0	alpine	-
nghttp2 1.51.0-r0	alpine	-
libcap 2.66-r0	alpine	-

**Уязвимость**

- Высокий
- Средний
  - CVE-2023-28321
  - CVE-2023-28320
- Низкий
  - CVE-2023-38546
  - CVE-2023-28322

Рисунок 11 – Сканирование. Сведения о пакете ПО

## 5.7 Политика сканирования

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



Обзор Уязвимости Список ПО **Политика сканирования** Метаданные История сканирований

Общий вердикт ✔ Запрещено

Общее количество политик сканирования: 3 ☐ Скрыть успешно пройденные

Вердикт	Политика
<span style="color: red;">✔ Запрещено</span>	WebUI scope
<span style="color: orange;">⊖ Не соответствует</span>	data111
<span style="color: orange;">⊖ Не соответствует</span>	[Serg] more low

Наименование правил	Результат проверки
⊖ Угрозы в программных пакетах	<span style="color: orange;">⊖ Не соответствует</span>
⊖ Критические уязвимости программных пакетов	<span style="color: blue;">✔ Соответствует</span>
⊖ Критические угрозы в программных пакетах	<span style="color: blue;">✔ Соответствует</span>
⊖ Уязвимости программных пакетов	<span style="color: orange;">⊖ Не соответствует</span>

Рисунок 12 – Сканирование. Политика сканирования

## 5.8 Метаданные

Отображает дополнительную информацию текущего образа.

Обзор Уязвимости Список ПО Политика сканирования **Метаданные** История сканирований

ID образа	sha256:5a708b9456fcb46a5c4ab2d425755b0727ae9ac1959a7c2fda6edc0ae86ba77e
Контрольная сумма	Не определено
Автор	Не определено
Ярлыки Docker	Не определено
Размер	205MB
Дата	25.02.2023
Операционная система	Debian GNU/Linux 11 (bullseye)
Архитектура	amd64
Тип образа	Docker

Рисунок 13 – Сканирование. Метаданные



## 5.9 История сканирований

Отображает список всех сканирований текущего образа в Runtime и Pipeline.

Анализ уязвимостей > Runtime сканирование > rancher/mirrored-flannel-flannel v0.21.4

OS образ Alpine Linux v3.17 26.10.2023, 17:52:10

Обзор Уязвимости Список ПО Политика сканирования Секреты Команды сборки Метаданные История сканирований

Поиск Статус Вердикт

Показаны 1–1 из 1 элементов

Сканирование	Образ	ID образа	Уязвимость	Вердикт	Дата ↓
runtime	rancher/mirrored-flannel-flannel v0.21.4	11ae74319a2	2 17 10	Успешный	26.10.2023, 17:52:10

**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.

Политики уязвимостей						<a href="#">+ СОЗДАТЬ ПОЛИТИКУ</a>
<input type="text" value="Поиск"/>		Тип <span>▼</span>				
Действие по умолчанию в Runtime <span>●</span> разрешить						
Действие по умолчанию в Pipeline <span>●</span> разрешить						
Показаны 1–8 из 8 элементов						
Название	Описание	Действие	Тип	Глобальная	Время создания	
new		Разрешить	pipeline	Нет	12.04.2023, 11:29:44	
Test		Разрешить	pipeline	Да	11.04.2023, 22:30:39	
WebUI scope	Политика для теста скопа WebUi	Запретить	pipeline	Да	10.04.2023, 16:25:07	
[Serg] Runtime		Разрешить	runtime	Да	13.03.2023, 20:07:08	

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.

Название	Описание	Время создания	
Serg more middle	test package	21.02.2023, 01:17:44	
Serg Exploit Exists	Serg Exploit Exists (Description)	01.03.2023, 01:37:48	
Serg more middle and exploit 1	test package	21.02.2023, 01:17:44	
Serg more middle and exploit 2	test package	21.02.2023, 01:17:44	
Манки тест для даты+эксплоит	Манки тест для даты 13/11/2022 +эксплоит	27.02.2023, 17:44:27	

Рисунок 16 – Политики. Пакеты правил

## 6.2 Агенты

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



Политики уязвимостей > Список агентов + ДОБАВИТЬ АГЕНТ

Поиск  Тип

Показаны 1–6 из 6 элементов

Название сканера	Тип сканирования	Ключ API	
<b>Тестовый сканер Runtime</b> Тестовый сканер для проведения тестового сканирования Runtime	runtime	...5n4ZKnEkHGZSq8bnEA	
<b>Тестовый сканер 27.12!!!!</b> Для проведения тестов 2222	pipeline	...LV4hLtbWpYwNJBAA==	
<b>Scanner Serg</b> Scanner Serg for PipeLine	pipeline	...dZOzw/FYoZQozhbAA=	
<b>Тестовый сканер 27.12.0000</b> Для проведения тестов	compliance	...PMd9exBA6gqVevZDQA	

**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.



## 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



## 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, характеризующееся 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, характеризующееся 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).



**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.