



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

АТОМИК

Описание функциональных характеристик

На 23 листах

**Москва
2024**



Содержание

1 Введение.....	5
2 Общие сведения.....	6
3 Функциональные характеристики	7
3.1 Пользовательский интерфейс	7
3.2 Панель мониторинга.....	7
3.3 Анализ уязвимостей	7
3.4 Наборы правил сканирования.....	13
3.5 Политики уязвимостей.....	13
3.6 Агенты сканирования.....	13
3.7 Отчетность	14
3.8 Разграничение прав пользователей по ролям.....	14
4 Требования к среде развертывания.....	15
5 Системные требования	16
6 Перечень принятых сокращений	17
7 Перечень терминов и определений.....	18



Список таблиц

Табл. 1 – Требования к среде развертывания.....	15
Табл. 2 – Системные требования	16



Список рисунков

Рисунок 1 – Форма «Панель мониторинга»	7
Рисунок 2 – Форма «Сканирование Runtime»	8
Рисунок 3 – Сканирование. Обзор	9
Рисунок 4 – Сканирование. Уязвимости	9
Рисунок 5 – Сканирование. Сведения об уязвимости	10
Рисунок 6 – Сканирование. Список ПО	11
Рисунок 7 – Сканирование. Сведения о пакете ПО	12
Рисунок 8 – Политики. Пакеты правил	13
Рисунок 9 – Политики. Список агентов	14

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 описание содержит информацию об основных функциональных характеристиках продукта АТОМИК (далее по тексту - Продукт).



2 Общие сведения

АТОМИК - программное обеспечение для сканирования контейнерных информационных систем и приложений в них с целью обнаружения уязвимостей в процессах разработки и эксплуатации.

АТОМИК интегрируется в контейнерную среду для получения данных о ее структуре и приложениях.



3 Функциональные характеристики

3.1 Пользовательский интерфейс

АТОМИК реализует собственный Web-интерфейс управления с поддержкой Web-браузеров: Yandex Browser, Google Chrome, Edge, Mozilla Firefox. Для получения доступа к функциям управления Web-интерфейса требуется ввести данные учетной записи пользователя.

3.2 Панель мониторинга

Поддерживается отображение статистических метрик результатов работы Продукта в текстовом и графическом отображении.

Поддерживается возможность добавлять, редактировать отображение и размещение метрик в удобном порядке.

Наглядное отображение статистики анализа уязвимостей представлено ниже.

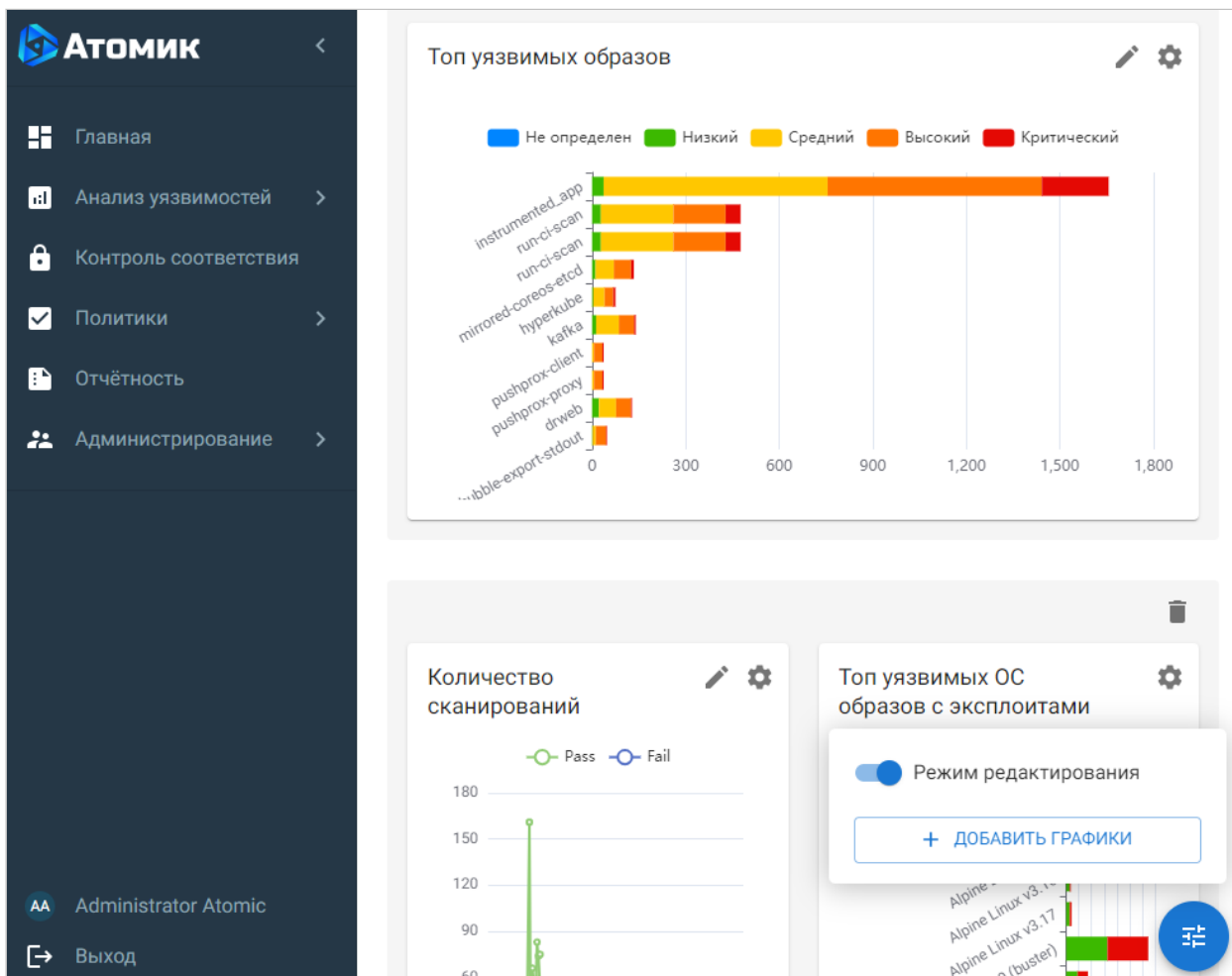


Рисунок 1 – Форма «Панель мониторинга»

3.3 Анализ уязвимостей

Поддерживается проведение сканирования следующими методами:

- встраивание кода сканирования в pipeline;
- интеграция агента сканирования в runtime среде;
- выборочное сканирование Docker-образов.

Используя перечисленные методы поддерживается анализ сканируемых приложений, включает в себя следующие функциональные особенности:

- обнаружение уязвимостей с эксплоитами;
- обнаружение возможности исправления уязвимостей;
- обнаружение секретов в образах и исходном коде приложений;
- обнаружение вирусов в образах и исходном коде приложений;



- представление подробной информации о контейнерной среде, включает в себя детализацию по принадлежности к кластеру, по namespace, по образу, по приложению;
- предоставление подробной информации о каждом просканированном образе: ОС, архитектура, тип образа, список установленного ПО, размер;
- анализ контейнерной среды об уязвимостях в виде: общего количества и списка уязвимостей, с детализацией по критичности, в разрезе количества уязвимостей в каждом установленном программном пакете, с пометкой о наличии эксплойта и/или исправления;
- ведение истории сканирований с вердиктом успешности или неуспешности сканирования;
- детальное определение уровня опасности каждой уязвимости по оценке CVSS;
- предоставление ссылки на уязвимости в базе CVE;

Просмотр просканированных приложений:

Анализ уязвимостей >
Runtime сканирование

Поиск: [Поиск] Кластер: 1 x Namespace: 2 x Тип: [Тип] Название политики: [Название политики]

Статус: [Статус] ID уязвимости: [ID уязвимости] Наименование ПО: [Наименование ПО] ОС образа: [ОС образа] ОЧИСТИТЬ ФИЛЬТРЫ

Образов в runtime: 74 Интервал обновления: 15 секунд

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 2 – Форма «Сканирований Runtime»



Просмотр определенного контейнера:

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

Вердикт политики сканирования

СМОТРЕТЬ ВСЕ

Наименование политики	Вердикт политики
По-умолчанию Runtime	Успешный

Уязвимости

СМОТРЕТЬ ВСЕ

29 обнаружено

- 0 Критический 0 Исправимо
- 10 Высокий 10 Исправимо
- 16 Средний 16 Исправимо
- 3 Низкий 3 Исправимо
- 0 Не определен 0 Исправимо
- 0 Не определен 0 Исправимо

Рисунок 3 – Сканирование. Обзор



Просмотр списка уязвимостей определенного контейнера:

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 ≥ Тип источника

ОЧИСТИТЬ ФИЛЬТРЫ

Показаны 1–7 из 7 элементов

Уязвимость	Уровень	CVSS ↓	Пакет и версия	Тип источника
CVE-2023-29491 <input type="button" value="📄"/>	Высокий	7.8 V3	ncurses 6.3_p20221119-r0 <input type="button" value="📄"/>	Образ контейнера
CVE-2023-2603 <input type="button" value="📄"/>	Высокий	7.8 V3	libcap 2.66-r0 <input type="button" value="📄"/>	Образ контейнера
CVE-2023-28319 <input type="button" value="📄"/>	Высокий	7.5 V3	curl 7.88.1-r1 <input type="button" value="📄"/>	Образ контейнера
CVE-2023-28320 <input type="button" value="📄"/>	Средний	5.9 V3	curl 7.88.1-r1 <input type="button" value="📄"/>	Образ контейнера

Рисунок 4 – Сканирование. Уязвимости



Просмотр определенной уязвимости:

CVE-2022-32207 ✕

Уровень Критический Reported by [nvd](#)

Пакет [libcurl 7.80.0-r0](#) ALPINE

Исправленная версия: 7.80.0-r2

Оценка уязвимости Дата 07.07.2022

Источник выбран для расчета баллов

NVD	7.5 V2	AV:N/AC:L/Au:N/C:P/I:P/A:P
Посмотреть больше	9.8 V3	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:...

О других уязвимостях также сообщаем

REDHAT	9.8 V3	CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:...
Посмотреть больше		

Описание
curl: Unpreserved file permissions



Рисунок 5 – Сканирование. Сведения об уязвимости

Просмотр списка ПО определенного контейнера:

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	- 2 2 3 -	Образ контейнера
openssl 3.0.8-r0	alpine	- - 14 2 -	Образ контейнера
ncurses 6.3_p20221119-r0	alpine	- - - 2 -	Образ контейнера
nghttp2 1.51.0-r0	alpine	- - - 2 -	Образ контейнера

Рисунок 6 – Сканирование. Список ПО



Просмотр уязвимостей определенного программного пакета:

The screenshot displays the Atomic Security interface. The main window shows a list of packages under the heading 'Анализ уязвимостей > Runtime сканирование > rancher/mirrored-flannel-flannel v0.21.4'. The 'Уязвимости' tab is active, showing a search bar and a dropdown for 'Уровень опасности'. Below the search bar, it indicates 'Показаны 1–10 из 101 элементов'. A table lists packages with columns for 'Пакет', 'Тип', and 'Уязвимости'. The 'curl' package is highlighted, and a detailed view is shown on the right. This view includes the package name 'curl 7.88.1-r1 ALPINE' and a vulnerability score represented by colored bars: 2 (green), 2 (yellow), 3 (orange), and 1 (red). Below the score, a list of vulnerabilities is shown, including CVE-2023-28321, CVE-2023-28320, CVE-2023-38546, and CVE-2023-28322, each with a severity level (High, Medium, Low) and a status icon.

Рисунок 7 – Сканирование. Сведения о пакете ПО

3.4 Контроль соответствия

Поддерживается контроль соответствия серверов контейнерного оркестратора Kubernetes стандартам защиты от распространенных уязвимостей и неправильных конфигураций, включает в себя следующие функциональные особенности:

- создание собственных политик контроля соответствия;
- обнаружение соответствий стандартам по каждому отдельному правилу;
- подробное описание причины неуспешных результатов проверок;
- подробная детализация выполняемых действий во время проверок в неуспешных проверках;
- ведение истории проверок.

3.5 Политики безопасности

Поддерживается создание и применение политик безопасности с указанием нескольких наборов правил сканирования, имеет следующие функции:



- создание собственных политик;
- возможность блокировки сборки образа при отрицательном вердикте политики;
- возможность получения уведомлений о применении политик;
- возможность ограничения действия политик по основным тегам образа;
- применение политик к одному из типов сканирования: pipeline, runtime или registry (только одного);
- применение политик к отдельным агентам или ко всем;
- применение политик согласно выбранным наборам правил обнаружения уязвимостей;
- применение политик согласно найденным секретам;
- применение политик согласно найденным вирусам.

3.6 Наборы правил сканирования

Поддерживается создание определенных наборов правил обнаружения уязвимостей для их применения в политиках безопасности, включает в себя следующие функциональные особенности:

- создание нескольких правил проверок уязвимостей образа в одном наборе;
- проверки уязвимостей на наличие эксплойта;
- проверки уязвимостей по скорингу CVSS V2/V3;
- проверки уровня критичности уязвимостей;
- проверки даты публикации уязвимостей;
- проверки наличия исправления уязвимостей;
- проверки по конкретным id уязвимостей;
- проверки используемых команд сборки образов Docker.

Набор правил сканирования:



Правила

Уязвимости

Уязвимости
Проверка уязвимостей образа

Команды сборки образа

Docker
Команды сборки образа Docker

ИЛИ

Уязвимости
Уязвимости

Проверка уязвимостей образа

- Наличие эксплоита Выберите
- Скоринг CVSS V2 = Выберите
- Скоринг CVSS V3 = Выберите
- Уровень уязвимости = Выберите
- Дата публикации уязвимости = Выберите дату
- Доступно исправление Выберите
- Уязвимости (один либо несколько id) = Выберите

Рисунок 8 – Политики. Пакеты правил

3.7 Агенты сканирования

Поддерживается создание множественных API ключей для интеграции агента в системе контейнерной оркестрации, позволяет проводить поиск уязвимостей и применять блокирующие политики безопасности.

Поддерживается применение политики без блокировки.

Поддерживается разделение отличающихся политик путем создания нескольких агентов и применения к ним соответствующей политики.



Список агентов:

Политики уязвимостей >

Список агентов

+ ДОБАВИТЬ АГЕНТ

Поиск Тип

Показаны 1–10 из 18 элементов

Название сканера	Тип сканирования	Ключ API		
3242 234	watcher	...ButZWDFGJ6XKB0aU0A		
Scanner Serg1 Scanner Serg for PipeLine	pipeline	...dZOzw/FYoZQozhbAA=		
Тестовый сканер 27.12.0000 Для проведения тестов	watcher	...PMd9exBA6gqVevZDQA		

Рисунок 9 – Политики. Список агентов

3.8 Отчетность

Поддерживается выгрузка отчетов по данным об уязвимостях в формате NDJSON, поддерживается возможность выбора периода выгрузки, поддерживается отправка отчетов по расписанию.

3.9 Ролевой доступ пользователей. LDAP

Поддерживается интеграция со службами каталогов с использованием SSL шифрования.

Системой поддерживается разграничение доступа пользователей по ролям и группам доступа в соответствии с группами LDAP.



4 Требования к среде развертывания

Перечень основных требований к среде развертывания приведен в Табл.1

Табл. 1 – Требования к среде развертывания

Тип	Наименование
Операционная система	Поддержка eBPF: Linux Kernel 4.16+; Поддержка BTF: Linux Kernel 5.1+
Программное обеспечение для автоматизации развёртывания и управления приложениями	Docker, Kubernetes
СУБД	PostgreSQL, ClickHouse
Брокер сообщений	Apache Kafka
Балансировщик	Nginx Ingress



5 Системные требования

Перечень минимальных системных требований для работы основных компонентов Продукта приведен в Табл.2

Табл. 2 – Системные требования

Количество процессоров:	4
Оперативная память:	16 Гб
Жесткий диск:	80 Гб свободного места



6 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



7 Перечень терминов и определений

CI/CD - технология автоматизации тестирования и доставки новых модулей разрабатываемого программного обеспечения заинтересованным сторонам (разработчики, аналитики, инженеры качества, конечные пользователи и др.);

Pipeline - процесс, который ведет разработку программного обеспечения путем создания, тестирования и развертывания кода, также известного как CI / CD;

Runtime – процесс в контейнерной среде содержащий разработанное программное обеспечение с целью его использования;

Namespace – группа ресурсов в пределах одного кластера;

CVE - база данных общеизвестных уязвимостей информационной безопасности;

CVSS - открытый стандарт, используемый для расчета количественных оценок уязвимости в информационной безопасности.

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).

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.