

# Платформа для управления уязвимостями и обеспечения безопасности в процессах разработки и DevSecOps "TRON.ASOC v.1.2"

Руководство пользователя

Апрель 2025

# Содержание

Введение	4
1. Термины и определения	5
2. Общие сведения	7
3. Начало работы в системе	9
4. Описание интерфейса и функционала	12
4.1. Настройки главного меню	13
4.2. Настройки элементов рабочей области	13
4.2.1. Настройки отображения данных	13
4.3. Информационная панель	15
4.3.1. Расчеты основных метрик	18
4.3.2. Настройки виджетов	20
4.4. Проекты	21
4.4.1. Создание нового проекта	23
4.4.2. Редактирование проекта	23
4.4.3. Отчеты по проектам	25
4.4.4. Обзор проекта	27
4.5. Конвейеры безопасности и проверки безопасности	28
4.5.1. Создание конвейера безопасности	29
4.5.2. Создание проверки безопасности	30
4.5.3. Запуск конвейера безопасности	33
4.5.4. Запуск проверки безопасности	33
4.5.5. Остановка сканирования	34
4.5.6. Загрузка внешнего отчета	34
4.5.7. Использование CLI-инструментов	37
4.5.8. Интеграция в CI процесс	39
4.5.8.1. Описание переменных	39
4.5.8.2. Пример отправки результата сканирования CLI-инструмента TRON ASOC в рамках CI	в 40
4.5.9. Результаты сканирований	41
4.5.10. Контроль качества проекта	42
4.6. Проблемы безопасности	44
4.7. Библиотека зависимостей	47
4.8. Контроль качества	48
4.8.1. Добавление нового контроля качества	49
4.9. Правила безопасности	51
4.9.1. Создание правила безопасности	52
4.10. Правила дедупликации	53
4.10.1. Поиск дубликатов	53
4.10.2. Создание правил дубликатов	54

4.11. Правила реагирования	54
4.11.1. Создание правила реагирования	54
5. Отчеты	58
6. Журнал событий	59
7. Конструктор полей	60
8. Требования к аппаратным и программным характеристикам рабочего мес	та
пользователя	62

# Введение

Настоящий документ представляет собой руководство пользователя программного комплекса TRON.ASOC.

В роли пользователей могут быть разработчики, тестировщики, инженеры безопасности, специалисты техподдержки различных ИТ-систем, и другие участники процесса DevSecOps.

С целью более детального описания доступного функционала, данный документ был составлен для пользователя с полными правами доступа ко всем функциям системы. Видимость некоторых функций отдельного пользователя может быть ограничена в соответствии с назначенной ролью. При необходимости расширить права доступа к определенному функционалу рекомендуется обратиться к администратору системы.

# 1. Термины и определения

Термин/аббревиатура	Определение
ΠΟ	Программное обеспечение
ASOC (Application Security Orchestration and Correlation)	Платформы или решения для оркестрации и корреляции безопасности приложений - платформы, предназначенные для управления и координации безопасностью приложений, позволяют автоматизировать процессы обнаружения, анализа и реагирования на угрозы
DAST (Dynamic Application Security Testing)	Динамический анализ кода — анализ программного обеспечения без доступа к исходному коду, реализуемый при помощи выполнения программ. Процесс тестирования приложений, имитирующий вредоносные внешние атаки, пытающиеся использовать распространенные уязвимости.
DevSecOps (Development Security Operations)	Процесс безопасной разработки - методология разработки программного обеспечения, которая интегрирует практики безопасности (Sec) в процессы разработки и поставки программного обеспечения (DevOps).
OSA (Open Source Analysis)	Анализ открытого программного обеспечения - анализ библиотек и компонентов с открытым исходным кодом, которые входят в периметр разработки программного обеспечения, а также уже используются в качестве артефактов в приложении. Анализ проводится с точки зрения известных уязвимостей безопасности и нарушений лицензий.
SCA (Software Composition Analysis)	Анализ структуры программного обеспечения - позволяет определять состав программного обеспечения для выявления и управления компонентами с открытым исходным кодом и их уязвимостями.

Термин/аббревиатура	Определение
SAST (Static Application Security Testing)	Статическое тестирование безопасности приложений - это процесс тестирования приложения на наличие ошибок и уязвимостей в исходном коде с применением статического анализа. Статический анализ может применяться для поиска кода, потенциально содержащего уязвимости.
IaC (Infrastructure-as-Code)	Инфраструктура как код - это подход к созданию и управлению инфраструктурой через использование кода, например, конфигурационных файлов или скриптов.
Container Security	Безопасность контейнеров - подход к защите и безопасной настройке систем контейнеризации, общее понятие, охватывающее набор различных инструментов и методов для защиты контейнеров от возможных угроз и атак.
Проект	Проект - это сущность, которая создается авторизованным пользователем, чтобы логически объединить весь набор связанных приложений или компонентов, которые разрабатываются и поддерживаются в рамках одной команды или организации, и который нужно проверять на соответствие политикам безопасности компании и качество.
AST (Application Security Testing)	Тестирование безопасности приложений
Интеграция	Интеграция - обмен данными между системами с возможной последующей обработкой.
AD (Active Directory)	Службы каталогов – совокупности программных сервисов и баз данных (на базе Microsoft) для иерархического представления информационных ресурсов в сети и настройки доступа к ним.
LDAP (Lightweight Directory Access Protocol)	Легковесный протокол доступа к каталогам

# 2. Общие сведения

«TRON.ASOC» - программный продукт, платформа для обнаружения и управления уязвимостями, а также обеспечения безопасности в процессах разработки и DevSecOps.

- интегрируется с внешними сканерами безопасности, такими как статический анализатор исходного кода **PT Application Inspector** и анализатор безопасности контейнеров **Kaspersky Container Security**.
- интегрируется со статическим анализатором кода приложений Solar AppScreener (не только исходного, но и бинарного кода) на наличие уязвимостей и НДВ.
- взаимодействует с решениями композиционного анализа программных продуктов CodeScoring и OWASP Dependency Track.
- интегрируется с платформой **JFrog**, предназначенной для управления и развертывания программных пакетов.
- может принимать и анализировать отчеты, обрабатывать полученные результаты от следующих инструментов:
  - Trivy сканер уязвимостей с открытым исходным кодом, разработанный для контейнерных сред,
  - Grype эффективный сканер контейнеров, Docker-образов и файловых систем на наличие уязвимостей,
  - **KICS** (Kaspersky Industrial CyberSecurity) решение для централизованного управления безопасностью,
  - о Semgrep статический сканер безопасности приложений,
  - Aqua решение, обеспечивающее комплексную нативную защиту контейнеров.
- позволяет добавлять уязвимости вручную (**Manual**) для построения комплексных метрик.
- предоставляет возможность управлять проверками исходного кода и образов контейнеров на известные уязвимости, ошибки конфигурации, секреты, а также работать с результатами этих проверок в едином интерфейсе. Интеграция с инструментами позволяет настраивать сканирования, запускать проверки, консолидировать, анализировать и обрабатывать результаты, а также производить мониторинг состояния безопасности разрабатываемых продуктов.
- помогает группировать, исследовать и устранять уязвимости из различных источников, обеспечивая тем самым безопасный процесс разработки.
- упрощает работу с найденными проблемами и уязвимостями, проводя их анализ и группировку для более эффективного управления безопасностью.

- позволяет оценивать влияние уязвимостей, изменять их статусы и приоритизировать для последующих шагов, управлять исключениями. Таким образом, продукт позволяет управлять уязвимостями ПО и защитой приложений на всех этапах разработки.
- позволяет оставлять комментарии к уязвимостям и просматривать комментарии от других пользователей.
- позволяет создавать и настраивать точки контроля качества ПО для каждого ИБ-пайплайна, иметь способ организации критериев качества каждого сканирования. На основе критериев контроля качества система решает, успешно ли завершилась работа конвейера проверок безопасности и позволяет определить, может ли продукт перейти на следующий этап разработки или выпуска на основе заданных критериев качества.
- предоставляет возможность внесения исключений в результаты отработки, получаемые от сканеров, в ASOC, что позволяет не подсвечивать уже обработанные и принятые проблемы безопасности. Время действия и область применения правил исключений можно настраивать.
- является единым источником данных об уязвимостях в ПО от инструментов с разными типами проверок (SAST, Container Security, OSA/SCA, DAST) и, таким образом, может стать единым инструментом контроля качества ПО.
- предлагает использовать дашборды, отчеты и метрики внутри продукта, которые предоставляют гибкие формы отчетности и аналитические данные для оценки текущего состояния безопасности проектов, прогнозирования рисков и принятия решений. С помощью визуализации данных платформа предоставляет пользователям наглядную информацию о состоянии безопасности их проектов.
- внедряет безопасность и управление рисками в непрерывные процессы разработки, при этом не требует для работы внешних CI-конвейеров
- предлагает удобный пользовательский интерфейс, доступный в современных браузерах на движке Chromium (Google Chrome, Яндекс Браузер, Edge, Safari и т.д.) и Firefox.
- поддерживает создание гибкой ролевой модели, позволяя настроить различные уровни доступа и разрешений для пользователей, что способствует более эффективному и безопасному управлению проектами.
- поддерживает интеграцию с LDAP и AD.
- предоставляет возможности для управления сканированиями, включая настройку параметров сканирования, планирование запусков и мониторинг выполнения сканирований.
- позволяет выгружать отчеты по результатам сканирований в разных форматах, что обеспечивает удобство интеграции с другими системами и инструментами анализа данных.

# 3. Начало работы в системе

Для начала работы в системе TRON.ASOC необходимо запросить доступ у администратора, который после настройки учетной записи предоставит ссылку для входа и первичные данные учетной записи. По ссылке осуществляется переход на страницу авторизации в системе.

Для успешной авторизации необходимо выполнить следующие шаги:

1. Перейти на страницу авторизации (Рис. 1).

TRÓN ASOC	Here nonsociarians* Here nonsociarians Here nonsociarians  Tapona* Beggirte nanona  tabains  yseafire donuale o fron ABOC (2)



- 3. Далее ввести Имя пользователя и Пароль от учетной записи.
- 4. Нажать на кнопку Войти.

При первом входе, а также по запросу, потребуется изменить пароль к учетной записи, следуя указанным рекомендациям к новому паролю (Рис. 2), и нажать на кнопку **Изменить**.

изменить пароль	⊕ Ru
Новый пароль*	
	0
Тароль должен содержать:	
• Не менее 8 символов	
<ul> <li>Хотя бы одну цифру</li> </ul>	
<ul> <li>Прописную букву</li> </ul>	
<ul> <li>Строчную букву</li> </ul>	
<ul> <li>Хотя бы один специальный символ</li> </ul>	
Тодтвердите пароль <b>*</b>	
	0
Изменить	

При успешной авторизации откроется Информационная панель (Рис. 3).

≡ ⊕	Информационная панель		
	Весь период Год Квартал Месяц Неделя День 27.02.2025 2	7032025 🗙	🔒 Создать отчет 🛛 🛃 Настроить расположение
<ul> <li>Виндориационная паниль</li> <li>Проекти</li> <li>Полобным безопалостия</li> <li>Вобизотая замисникастия</li> <li>Колгроль качества</li> </ul> Possent Possent Q Правила безопалостия Правила дедугликация Q Правила дедугликация Д Правила дедугликация	Накопительный график ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ; ;	Уязвимости : Кого указанска 2850 Сандовани 201 6 критноский 37 6 Нослой 207 1977 19	Открытые уязвимости         :           СwE-476         194         CwE-119         52           CwE-478         200         CwE-647         46           CwE-125         65         CwE-122         46           CwE-190         58         CwE-170         38
Адиниистрирования (5) Управления доступкая (6) Интеграция (7) Онтеграция (7) Управления (7) Полощика (7) Конструктор полебя Параметри порслочения	Выбрать метрику V Гриненить Выберите метрику и нажилте «Применить», чтобы ужидеть её динамический график	Наиболее критичные уязымости         ;           [ CVF-2024-3737]         10         OVF-2023-5641 CWF-187, 2           [ CVF-2024-32002 CWF-59, 2         CVF-2023-46865 CWF-190, 2         2           [ CVF-2024-45849 CWF-190, 2         CVF-2023-46865 CWF-190, 2         2           [ CVF-2024-45840 CWF-100, 2         CVF-2023-46865 CWF-190, 2         1           [ CVF-2024-45840 CWF-100, 2         CVF-2021-234465 CWF-101, 1         1           [ CVF-2024-45840 CWF-100, 2         CVF-2021-234465 CWF-101, 1         1           [ CVF-2021-234465 CWF-100, 2         CVF-2021-234465 CWF-101, 1         1           [ CVF-2021-234465 CWF-100, 2         CVF-2021-234465 CWF-101, 1         1	HaufGonee yssausue npoektu         :           TESTCAV1         274         297           TESTCAV1         274         297           KOSSTATUS7         53         6           TESTCO1         1         1           TESTCO2         1         1           Juce Shop OWASP         1         1           Nose Shop OWASP         1         1           Nose Shop OWASP         1         1
ල 0 nporpamme  ඨ admin		Метрики © Плотность риска 0	

Рис. 3

В случае ввода неверных учетных данных на экране отобразится сообщение "*Неверный логин и/или пароль*". При превышении числа попыток аутентификации с неверным паролем аккаунт будет временно заблокирован. Количество попыток аутентификации и продолжительность блокировки устанавливается администратором системы (по умолчанию лимит попыток входа — 3, срок блокировки — 1 минута). При возникновении других проблем с входом в систему, необходимо обратиться к администратору.

В случае успешной настройки системы со стороны администратора (созданы необходимые учетные записи, назначены роли и доступы пользователям, внесены требуемые изменения в настройки системы, подключены инструменты безопасности, источники сканирования, инструменты уведомлений, трекеры) пользователям для начала предлагается следующий алгоритм работы с системой:

- 1. Необходимо создать проекты в системе, проекты должны иметь понятное название, краткое описание (см. <u>Создание нового проекта</u>).
- 2. Далее по каждому из проектов необходимо:
  - 1. Перейти в Обзор проекта.
  - 2. Добавить Конвейеры безопасности.
  - 3. Добавить Проверки безопасности.
  - 4. Добавить <u>Контроль качества</u> (при необходимости, возможно добавить позднее, при наличии достаточного количества проверок).
  - 5. Также добавить <u>Правила безопасности</u>, <u>Правила дедупликации</u> в отношении проекта (при необходимости, возможно добавить позднее, при наличии достаточного количества проверок).
  - 6. Далее Запустить сканирование (Конвейер безопасности).
  - 7. Ознакомиться с <u>результатами сканирования</u>. По результатам рекомендуется предпринять шаги по устранению выявленных уязвимостей, <u>создать задачи в трекере</u> при необходимости, и далее отслеживать исправление уязвимости, и также запускать новые сканирования для проверки.
  - 8. Добавить необходимые Правила реагирования.
  - 9. По требованию создать необходимые отчеты.
- 3. Дальнейшие действия зависят от индивидуальных потребностей, в рамках предложенного функционала (см. инструкцию ниже).

# 4. Описание интерфейса и функционала

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:
  - Информационная панель
  - Проекты
  - Проблемы безопасности
  - Библиотека зависимостей
  - Контроль качества
  - Правила безопасности
  - Правила дедупликации
  - Правила реагирования
  - Блок Администрирования
    - Управление доступом
    - Интеграции
    - Отчеты
    - Журнал событий
    - Помощник

Раздел Помощник будет доступен в следующих релизах.

- Конструктор полей
- Параметры подключения

Разделы блока **Администрирование** доступны администраторам системы. Подробнее о разделах см. Руководство администратора.

- О программе общая информация о системе
- Учетная запись данные профиля учетной записи

Видимость разделов главного меню зависит от набора привилегий и прав роли пользователя.

Для расширения доступа к системе необходимо согласовать изменения и обратиться к администратору для перенастройки ролей.

• Рабочая область. Информация и элементы управления в рабочей области зависят от выбранного раздела или подраздела.

## 4.1. Настройки главного меню

Предусмотрены следующие настройки главного меню:

• Выбор языка интерфейса (русский или английский). Для этого

необходимо нажать на кнопку 
и в раскрывшемся списке выбрать необходимый язык.

• Возможность свернуть/развернуть главное меню. Для этого необходимо нажать на кнопку

## 4.2. Настройки элементов рабочей области

#### 4.2.1. Настройки отображения данных

Для табличных представлений в интерфейсе TRON.ASOC предусмотрены следующие настройки отображения данных:

 Поиск. Выполнить поиск по отображаемым данных возможно с помощью поля Поиск..., расположенного над таблицей (Рис. 4).



• Настройка полей таблицы. Для настройки видимости полей таблицы

необходимо нажать на кнопку и в открывшейся форме скорректировать видимость полей (Рис. 5). Поля различаются в зависимости от данных таблицы и выбранного раздела.

Проблемы бе	зопасности						н	астройки таблицы		×
Проблемы безопасности И	роблемы безопасности Исключенные проблемы безопасности							Сбросить интерфейс		Î
+ Создать правило безопас	ности 🛛 🖸 Создать задач	и из проблем						ID уязвимости		
П уязвимости ∨ 	Категория v Use of Hard-coded Passw	Уровень критичности  > Низкий  >	Обнаружено с помо v PT Application Inspector	CWE ~ 		Статус ~ • Новый ~		Категория		
	ord							Уровень критичности		
С КССС-16	Use of Hard-coded Passw ord	Средний 🗸	PT Application Inspector	CWE-259		<ul> <li>В работе ∨</li> </ul>		Обнаружено с помощью		
🗆 кссс-38 🗇	Use of Hard-coded Passw ord	Низкий 🗸	PT Application Inspector	CWE-259		• Новый ∨		CWE		
С кссс-53 Ф	Use of Hard-coded Passw	Низкий 🗸	PT Application Inspector	CWE-259		• Новый ∨		CVE		
	Use of Hard-coded Passw	likovuči 🗸	PT Application Inspector	CWE-259		• Новый у		Статус	0	
─ KCCC-26 U	ord							Сканируемый объект		
С кссс-23	Use of Hard-coded Passw ord	Низкий 🗸	PT Application Inspector	CWE-259		● Новый ∨		TIPUEKI		
КССС-33 О	Use of Hard-coded Passw ord	Низкий ∨	PT Application Inspector	CWE-259		• Новый ∨				
С кссс-6 С	Use of Hard-coded Passw ord	Низкий ∨	PT Application Inspector	CWE-259		• Новый ∨				
C KCCC-41	Use of Hard-coded Passw ord	Низкий ∨	PT Application Inspector	CWE-259		• Новый ∨	n	Отмена		

Рис. 5

• Фильтрация. Для настройки фильтрации необходимо нажать на значок

фильтра и в открывшейся форме справа указать необходимые фильтры (Рис. 6). Фильтры различаются в зависимости от данных таблицы и выбранного раздела.

П	роблемы безопасности Ис	ВОПАСНОСТИ ключенные проблемы безоп.	асности					<b>Фильтрь</b> Найдено элеме	I ентов: 168124	×
+ Создать правило безопасности 🕑 Создать задания из проблем										
	ID уязвимости 🗸	Категория 🗸	Уровень критичности 🗸	Обнаружено с помо 🗸	CWE ~	CVE ~	Статус 🗸	Категория	Все значения	<b>`</b>
0	кссс-52 🗇	Use of Hard-coded Passw ord	Низкий ∨	PT Application Inspector	CWE-259		• Новый ∨	Уровень критичности	Все значения	
	**************************************	Use of Hard-coded Passw	Средний 🗸	PT Application Inspector	CWE-259		• В работе 🗸	Обнаружено с помощью	Все значения	~
	KUUL-10 U	ord						CWE	Все значения	~
	кссс-за	Use of Hard-coded Passw ord	Низкий ∨	PT Application Inspector	CWE-259		• Новый ∨	CVE	Все значения	~
								Статус	Новый × В работе ×	××
	кссс-53 🗇	Use of Hard-coded Passw ord	Низкий ∨	PT Application Inspector	CWE-259		● Новый ∨		Ложноположител × Подтверждено × Исправлено × Исключено × Вручную ×	
	кссс-26	Use of Hard-coded Passw ord	Низкий ∨	PT Application Inspector	CWE-259		• Новый 🗸	Сканируемый объект	Все значения	~
	кссс-23	Use of Hard-coded Passw ord	Низкий ∨	PT Application Inspector	CWE-259		• Новый ~	Проект	Все значения	~
	кссс-33 🗇	Use of Hard-coded Passw ord	Низкий ∨	PT Application Inspector	CWE-259		• Новый ~			
	кссс-6	Use of Hard-coded Passw ord	Низкий ∨	PT Application Inspector	CWE-259		• Новый 🗸			
	кссс-41 🗇	Use of Hard-coded Passw	Низкий 🗸	PT Application Inspector	CWE-259		• Новый ∨	Применить	Отмена	

Рис. 6

 Сортировка по возрастанию или убыванию. Табличный вид позволяет сортировать список данных по выбранному столбцу с помощью раскрывающегося списка при нажатии на выбранный столбец таблицы (Рис. 7).



Рис. 7

## 4.3. Информационная панель

Информационная панель представлена в виде сводных графиков (виджетов) по уязвимостям за установленный период (Рис. 3), она предоставляет возможность отследить наиболее важные метрики по доступным пользователю проектам в разработке. Значения накопительных графиков обновляются раз в сутки.

Доступны следующие виджеты (в зависимости от прав доступа):

 Накопительный график по выявлению уязвимостей за выбранный период времени (Рис. 8)



Рис. 8

• Уязвимости (Рис. 9)



Рис. 9

• Открытые уязвимости (Рис. 10)

открытые уязвимости	
CWE-476	400
CWE-416	269
CWE-200	180
CWE-787	166
CWE-125	136
Всего открытых уязвимостей	1693

Рис. 10

• Наиболее критичные уязвимости (Рис. 11)



Рис. 11

• Наиболее уязвимые проекты (Рис. 12)



Рис. 12

• Среднее время выявления дефекта ИБ (Рис. 13)





• Метрики (Рис. 14)

Метрики	ŝ
Плотность риска	
Частота проведения сканирования	
Коэффициент частоты сканирования	0.12
Количество дубликатов уязвимостей	
Процент устраненных уязвимостей (%)	
Среднее время выполнения сканирования (мин.)	1.88
Количество security rules	
Количество проблем, подпавших под security rules	
Интегральный риск-индекс	2.58
Среднее время в статусе «Новый» (час.)	
Среднее время в статусе «В работе» (час.)	
Среднее время в статусе «Подтверждено» (час.)	223.34
Среднее время в статусе «Исправлено» (час.)	622.43
Среднее время в статусе «Вручную» (час.)	0.21
Среднее время в статусе «Ложноположительный» (час.)	1.90
Среднее время в статусе «Дубликат» (час.)	
Среднее время в статусе «Исключено» (час.)	

Рис. 14

По данным метрикам предусмотрены отдельные виджеты для большей наглядности (в линейном виде):

- Коэффициент частоты сканирования
- Количество уязвимостей
- Среднее время жизни дефекта ИБ
- Процент устраненных уязвимостей
- Количество дубликатов уязвимостей

- Среднее время исправления дефекта ИБ
- Плотность риска
- Интегральный риск-индекс

#### 4.3.1. Расчеты основных метрик

Процент покрытия имеющихся информационных систем/приложений практиками безопасной разработки рассчитывается по следующей формуле:

 $Coverage\% = \frac{\text{Количество систем с применением практик}}{Oбщее количество систем} \times 100$ 

Среднее время жизни дефекта ИБ (Lead Time) рассчитывается, как медианное время жизни дефекта, т.е. от статуса Новый (New) до любого закрытого статуса (Suppress, Fixed и т.д.).

#### Среднее время идентификации дефектов ИБ (Mean-Time-To-Detect)

рассчитывается, как медианное время идентификации дефектов в проекте/проектах. Под идентификацией дефекта подразумевается изменение статуса от Новый (New) до любого другого следующего статуса.

#### Среднее время исправления дефектов ИБ (Mean-Time-To-Resolve)

рассчитывается, как медианное время от открытого статуса, отличного от Новый (New) до закрытого статуса.

Плотность риска (М) рассчитывается по следующей формуле:

$$M = \frac{C_{\rm Крит} \cdot W_{\rm Крит} + C_{\rm Xa\"{i}} \cdot W_{\rm Xa\widecheck{i}} + C_{\rm Meдиум} \cdot W_{\rm Meдиум} + C_{\rm лоу} \cdot W_{\rm лоу} + C_{\rm Heonpeden} \cdot W_{\rm Heonpeden}}{C_{\rm BCe}}$$

где:

- Скрит количество критичных уязвимостей в проекте.
- Схай количество уязвимостей высокого уровня в проекте.
- Смеднум количество уязвимостей среднего уровня в проекте.
- Слоу количество уязвимостей низкого уровня в проекте.
- С<sub>неопредел</sub> количество уязвимостей с неопределённым уровнем критичности в проекте.
- W<sub>крит</sub>, W<sub>хай</sub>, W<sub>медиум</sub>, W<sub>лоу</sub>, W<sub>неопредел</sub> весовые коэффициенты для каждого уровня критичности. Например:
  - $W_{
    m KpHT} = 1.0$  (самый высокий вес).
  - $W_{\text{хай}} = 0.8.$
  - $W_{\text{медиум}} = 0.5.$
  - $W_{\text{noy}} = 0.2$ .

- $W_{
  m Heonpegen} = 0.3$  (средний вес, так как неизвестный уровень критичности все же имеет некоторую значимость).
- Свсе общее количество уязвимостей в проекте:

$$C_{\text{все}} = C_{\text{крит}} + C_{\text{хай}} + C_{\text{медиум}} + C_{\text{лоу}} + C_{\text{неопредел}}$$

Среднее время сканирования рассчитывает среднее время сканирования.

Процент устраненных уязвимостей рассчитывается, как отношение количества закрытых уязвимостей к общему числу уязвимостей в проекте. Среднее время нахождения в определенном статусе рассчитывается, как медианное время нахождения в каждом статусе в целочисленном формате часов.

**Интегральный риск-индекс** в разрезе систем/сервисов/приложений рассчитывается по следующей формуле:

$$R = \sqrt[3]{H \cdot V \cdot L}$$

где:

- Н плотность риска
- V коэффициент частоты сканирования
- L коэффициент времени исправления и идентификации дефектов.

Коэффициент V (коэффициент частоты сканирования) рассчитывается по следующей формуле:

V = (Максимальная частота сканирования – Минимальная частота сканирования) / (Частота сканирования в проекте–Минимальная частота сканирования)

Данная формула нормирует частоту сканирования в проекте относительно минимальной и максимальной частоты сканирования по всем проектам. Это гарантирует, что Коэффициент V будет находиться в диапазоне от 0 до 1 и будет положительным.

#### Коэффициент времени исправления и идентификации дефектов L

оценивает скорость устранения уязвимостей относительно медианного значения, рассчитывается по следующей формуле:

$$L = rac{\mathrm{MTTR}_{\mathrm{текущая}} + \mathrm{MTTD}_{\mathrm{текущая}}}{\mathrm{MTTR}_{\mathrm{медианная}} + \mathrm{MTTD}_{\mathrm{медианная}}}$$

где:

- MTTR<sub>текушая</sub> среднее время исправления уязвимости (Mean-Time-To-Resolve).
- MTTD<sub>текущая</sub> среднее время обнаружения уязвимости (Mean-Time-To-Detect).
- MTTR<sub>медианная</sub>, MTTD<sub>медианная</sub> медианные значения этих времён по всем проектам.

L отражает отклонение времени обработки дефектов от медианных значений. Чем быстрее проект исправляет дефекты и идентифицирует их, тем меньше значение L.

Остальные используемые метрики рассчитываются на основе перечисленных выше метрик, подсчета количества значений по заданным параметрам, и используют простейшие операции вычисления.

#### 4.3.2. Настройки виджетов

Виджеты можно настроить по необходимости. Для этого необходимо перейти в режим редактирования расположения (Рис. 15) с помощью кнопки вверху справа **Настроить расположение** (Рис. 3).

≡ ⊕	Информационная панель			
	+ Добавить виджет		Отмена Сохранить измене	сния
<ul> <li>В Информационная панель</li> <li>Проекты</li> </ul>	Накопительный график	Уязвимости	<ul> <li>Метрики</li> </ul>	0
Проблемы безопасности П Библиотека зависимостей	100K	Crasuppeasunit		
Контроль качества Правила		6017 Контический		
<ul> <li>Правила безопасности</li> <li>Правила дедупликации</li> </ul>	07 апр. 2025 00 апр. 2025 09 апр. 2025	Низкий		
Ц Правила реагирования Администрирование	Коэффициент частоты сканирования ①	∺ Количество уязвимостей ⊙	Интегральный риск-индекс	
© Интеграции В Отчеты	0.36		Среднее время в статусе «В работе» (час.)      Среднее время в статусе «Подтверждено» (час.)      Среднее время в статусе «Подтверждено» (час.)      Среднее время в статусе «Исправлено» (час.)      Соеднее время в статусе «Исправлено» (час.)	
<ul> <li>В Журнал событий</li> <li>Конструктор полей</li> </ul>	0.24 0.15 0.12		764         Среднее время в статусе «Врученую» (час.)         0           573         Среднее время в статусе «Ложноположительной» (час.)         1           0         3/2         Среднее время в статусе «Ложноположительной» (час.)         1	
Параметры Параметры подключения				
() O nporpamme	Пореднее время жизни дефекта ИБ о	Процент устраненных уязвимостей ⊙	<ul> <li>Количество дубликатов уязвимостей о</li> </ul>	
ి admin				

Рис. 15

В режиме редактирования расположения доступны следующие настройки виджетов:

 Добавление новых виджетов с помощью кнопки Добавить виджет, в том случае, когда ранее были удалены из видимости какие-либо из представленных выше виджетов. 2. Перемещение виджетов в рамках рабочей области с помощью кнопки

Û

Интегральный риск-ин,	декс 🕠	Û

3. Удаление виджетов с помощью кнопки

на каждом из виджетов.

на каждом из виджетов.

4. Увеличение длины виджета (Рис. 16).

Рис. 16

После настройки расположения необходимо нажать на кнопку Сохранить изменения

Также на некоторых виджетах в режиме просмотра (Рис. 3) предусмотрена возможность изменения типа виджета (Рис. 17). Предлагаются на выбор следующие типы виджетов:

- Столбчатая диаграмма
- Круговая диаграмма
- Карточка

...



Рис. 17

## 4.4. Проекты

Раздел Проекты включает список доступных проектов, которые проверяются на соответствие политикам безопасности компании и качеству (Рис. 18). Каждый проект может иметь свои параметры безопасности и настройки. Пользователи

могут настроить как один, так и несколько проектов. Также есть возможность просматривать сводную информацию по проектам, удалять, редактировать проекты в зависимости от прав доступа.

≡ ⊕	Проекты						
	+ Добавить проект 📗 🗅 Создать	отчет				Поиск	Q & 7
	Имя проекта 🗸	Дата добавления 🚍	Дата обновления 🗸	Теги ч	Код проекта 🗸	Инструменты	
		26/03/2025 14:52	26/03/2025 14:52		JUICE		/ û
щ проолема оезопасности ш Библиотека зависимостей т.:	TESTDAY12	26/03/2025 01:22	30/03/2025 21:01		TESTDAY1	<b>○ ●</b>	0 0
Контроль качества Правила	TESTDAY	26/03/2025 01:09	27/03/2025 16:30	testday	TESTDAY	0	0 Û
Правила безопасности	TEST001	25/03/2025 10:28	25/03/2025 10:28		TEST001	en 🕑	0
<ul> <li>Правила дедупликации</li> <li>Правила реагирования</li> </ul>	TESTCVSS	25/03/2025 10:14	26/03/2025 00:36	cvss	TESTCVSS	📀 🙀 🗑	0 0
Администрирование	C test	13/12/2024 13:02	15/01/2025 13:43	newtag newtag_6 notags proverkatags	TEST	Θ 🕷	0 û
З Управление доступом	ISSUETERTIN020241212T141920 002Z	12/12/2024 17:19	12/12/2024 17:19	qaload	ISSUETESTING20241212T14192	08	0 Û
<ul> <li>Отчеты</li> <li>Журнал событий</li> </ul>		12/12/2024 17:17	12/12/2024 17:17	qa:load	ISSUETESTING20241212T14173	◎ ⑥	0
// Помощник		12/12/2024 17:14	12/12/2024 17:14	qacload	ISSUETESTING20241212T14140	•	0 0
Параметры		11/12/2024 14:00	05/02/2025 14:49	notags			0
<ul> <li>Вараметры подключения</li> <li>О программе</li> </ul>	Bcero 58					< 1 2 3 _ 6 >	10/страница 🗸
ය admin							

Рис. 18

Список проектов представлен в виде таблицы со следующими полями:

- Имя проекта
- Дата создания
- Дата обновления
- Теги
- Код проекта
- Инструменты

Также доступна настройка полей таблицы. Для этого необходимо нажать на

кнопку

и настроить видимость полей (Рис. 19).

≡ ⊕	Проекты					(	На	астройки таблицы	×
	+ Добавить проект 🛛 🖒 Создати						00	бросить интерфейс	
88 Информационная панель	Имя проекта  ~	Дата добавления = -	Дата обновления  ~	Теги ~	Код проекта ~	Инст		Имя проекта	
🗅 Проекты	TESTSUPRESS	07/04/2025 21:51	07/04/2025 21:51		TESTSUPRESS	Θ			
ф Проблемы безопасности	C TEST1	07/04/2025 12:13	07/04/2025 12:13		TEST1		-	Дата добавления	
<ul> <li>Библиотека зависимостей</li> <li>Контроль качества</li> </ul>	Сервисный проект команды DevS ecOps	06/04/2025 22:40	06/04/2025 22:40		DEVSECOPS		#	Дата обновления	
Правила	TESTGATE	06/04/2025 21:45	06/04/2025 21:45		TESTGATE		#	Теги	
О Правила безопасности Правила дедупликации	ASOC16444454	03/04/2025 21:02	03/04/2025 21:02		ASOC16444454	۲	#	Код проекта	
Ф Правила реагирования	ASOC37648939	03/04/2025 20:53	03/04/2025 20:53		ASOC37648939		#	Инструменты	
Администрирование	<ul> <li>Big data</li> </ul>	03/04/2025 14:38	03/04/2025 14-38		1113	0			
🗘 Интеграции	MARINA	02/04/2025 17:17	02/04/2025 17:17		MARINA				
🕒 Отчеты	TESTISSUES1	01/04/2025 20:49	02/04/2025 17:19		TESTISSUES	0			
Е Журнал событий						۲			
[] Конструктор полей						000			
Параметры Параметры подключения	□ MAGO	31/03/2025 16:33	31/03/2025 16:33		MAGO	0			
③ O nporpamme									
						000			
음 admin	Bcero 68						Пр	именить Отмена	

Рис. 19

В таблице проектов доступны следующие действия:

- Поиск по названию проекта.
- Фильтрация списка проектов по тегам.
- Сортировка списка по имени, тегу или коду проекта.
- Просмотр подробной информации о проекте при нажатии на имя проекта (см. раздел Обзор проекта).

#### 4.4.1. Создание нового проекта

Чтобы создать новый проект, выполните следующие шаги:

- 1. Нажмите на кнопку Добавить проект на странице Проекты.
- 2. В открывшейся форме создания проекта (Рис. 20) заполните обязательные поля **Код проекта**, **Название проекта**, а также другие поля, при необходимости.

Проекты						Создать проект	×
+ Добавить проект 🕞 Создат	гь отчет					Код проекта* 🛈	Â
🗌 Имя проекта 🗸	Дата добавления 🖃	Дата обновления 🗸	Теги ч	Код проекта 🗸	Инст	Код проекта	
TESTSUPRESS	07/04/2025 21:51	07/04/2025 21:51		TESTSUPRESS	0	Название проекта* 🛈	
C TEST1	07/04/2025 12:13	07/04/2025 12:13		TEST1		Описание Ф	
<ul> <li>Сервисный проект команды DevS ecOps</li> </ul>	06/04/2025 22:40	06/04/2025 22:40		DEVSECOPS		Описание	
TESTGATE	06/04/2025 21:45	06/04/2025 21:45		TESTGATE	6	Теги ①	_6
ASOC16444454	03/04/2025 21:02	03/04/2025 21:02		ASOC16444454	۲	Выберите из списка	~
ASOC37648939	03/04/2025 20:53	03/04/2025 20:53		ASOC37648939		Дата старта проекта	_
Big data	03/04/2025 14:38	03/04/2025 14:38		1113	O	Дата окончания проекта	
	02/04/2025 17:17	02/04/2025 17:17		MARINA			
TESTISSUES1	01/04/2025 20:49	02/04/2025 17:19		TESTISSUES	o	Владелец проекта	-
					<b>(</b>	Ссылка на Confluence	
MAGO	31/03/2025 16:33	31/03/2025 16:33		MAGO	0	Соблюдение Compliance О AppSec	
Bcero 68						Создать Отмена	

Рис. 20

Рекомендации к заполнению некоторых полей отмечены знаком 0.

3. Далее нажмите кнопку Создать.

#### 4.4.2. Редактирование проекта

Для редактирования проекта необходимо нажать на кнопку напротив выбранного проекта (Рис. 18). После этого откроется форма редактирования проекта (Рис. 21).

Π	роекты					Редактировать проект ×
H	- Добавить проект 📗 🕒 Создать (					Код проекта* ()
0		Дата добавления ~	Дата обновления ~	Теги ч	Код проекта - И	ISSUETESTING20241106T092721661Z
	661Z ISSUETESTING20241212T141406	12/12/2024 17:14	12/12/2024 17:14	qa:load	ISSUETESTING20241212T14140	ISSUETESTING20241106T092721661Z
	613Z ISSUETESTING20241212T141731 439Z	12/12/2024 17:17	12/12/2024 17:17	qa:load	ISSUETESTING20241212T14173	Project ISSUETESTING20241106T092721661Z for load test
	ISSUETESTING20241212T141920 002Z	12/12/2024 17:19	12/12/2024 17:19	qa:load	ISSUETESTING20241212T14192	Teru ()
	Juice Shop OWASP	26/03/2025 14:52	01/04/2025 18:28	owasp	JUICE	Дата старта проекта
	косс	22/07/2024 17:31	22/07/2024 17:31		кссс	Дата окончания проекта
	KCSSTATUS	11/12/2024 11:00	11/12/2024 11:00		KCSSTATUS	Владелец проекта
	KCSSTATUS2	11/12/2024 11:58	11/12/2024 11:58		KCSSTATUS2	· · · · · · · · · · · · · · · · · · ·
	KCSSTATUS3	11/12/2024 12:04	11/12/2024 12:04		KCSSTATUS3	Ссылка на Confluence
	KCSSTATUS4	11/12/2024 12:49	11/12/2024 12:49		KCSSTATUS4	Соблюдение Compliance
Bce	ro 68					Аррбес

Рис. 21

После завершения редактирования, необходимо нажать на кнопку Сохранить.

Также, чтобы отредактировать проект, можно перейти на страницу проекта. Для этого необходимо выполнить следующие шаги:

- 1. На странице **Проекты** нажать на имя проекта, выделенное синим цветом (Рис. 30).
- 2. Перейти на вкладку Параметры проекта (Рис. 22).
- 3. Далее нажать на кнопку Редактировать проект (Рис. 22).



Рис. 22

4. Отредактировать параметры проекта (Рис. 21) и нажать на кнопку Сохранить.

#### 4.4.3. Отчеты по проектам

В системе предусмотрены Сводный и Детализированный отчеты по проектам.

Для создания сводного отчета по проектам, необходимо выполнить следующие шаги:

1. В разделе **Проекты** выбрать проект или несколько проектов. Для этого поставить галочки в чекбоксах рядом с названиями выбранных проектов

П	роекты									
	+ Добавить проект D Создать	отчет					Поиск		۹	\$ ₹
•	Имя проекта 🚊	Дата добавления 🗸	Дата обновления 🗸	Теги ү	Код проекта 🗸	Инструменть	·			
	ISSUETESTING20241106T092721 661Z	06/11/2024 12:27	06/11/2024 12:27	qaload	ISSUETESTING20241106T09272	00	200	0	Û	
۵	ISSUETESTING20241212T141406 613Z	12/12/2024 17:14	12/12/2024 17:14	qaload	ISSUETESTING20241212T14140	0		O	Û	
۲	ISSUETESTING20241212T141731 439Z	12/12/2024 17:17	12/12/2024 17:17	qatload	ISSUETESTING20241212T14173	0		0	Û	
	ISSUETESTING20241212T141920 002Z	12/12/2024 17:19	12/12/2024 17:19	qaload	ISSUETESTING20241212T14192	0		0	Û	
	Juice Shop OWASP	26/03/2025 14:52	01/04/2025 18:28	owasp	JUICE	00	ා 📦 📦	0	Û	
						800 <b>(</b>	4			
	KCCC	22/07/2024 17:31	22/07/2024 17:31		KCCC	00		0	Û	
	KCSSTATUS	11/12/2024 11:00	11/12/2024 11:00		KCSSTATUS			0	Û	
	KCSSTATUS2	11/12/2024 11:58	11/12/2024 11:58		KCSSTATUS2			O	Û	
	KCSSTATUS3	11/12/2024 12:04	11/12/2024 12:04		KCSSTATUS3			O	Û	
	KCSSTATUS4	11/12/2024 12:49	11/12/2024 12:49		KCSSTATUS4			0	Û	
Bc	ro 68					< 1	2 3 4 7 >	1	0 / стр	аница 🗸

2. Далее нажать на кнопку Создать отчет (Рис. 23).

Рис. 23

 В открывшейся форме Создать сводный отчет заполнить параметры и необходимые фильтры отчета, при этом рекомендуется сократить количество обнаруженных проблем до 80 (количество указано в поле Всего проблем), чтобы загрузка отчета не занимала много времени (Рис. 24).

П	роекты				Создать сводны	й отчет ×
H	- Добавить проект 🌔 Создать	отчет			Название отчета*	Введите название
•	Имя проекта 😑	Дата добавления 🗸	Дата обновления 🗸	Теги ~	Период отчета*	Весь период
0	ISSUETESTING20241106T092721 661Z	06/11/2024 12:27	06/11/2024 12:27	qaload	Выбранные проекты*	ISSUETESTING20241× × ×
۲	ISSUETESTING20241212T141406	12/12/2024 17:14	12/12/2024 17:14	qa:load		При выборе более 10 проектов загрузка PDF-отчета будет недоступна
	0132 ISSUETESTING20241212T141731	12/12/2024 17:17	12/12/2024 17:17	astand	Фильтр	Всего проблем: 24 512 ①
	439Z			darioad	Поле	Фильтр
	ISSUETESTING20241212T141920 002Z	12/12/2024 17:19	12/12/2024 17:19	qa:load	Категория	Все значения 🗸
	Juice Shop OWASP	26/03/2025 14:52	01/04/2025 18:28	owasp	Уровень критичности	Все значения 🗸
					Обнаружено с помощью	Все значения 🗸
	косс	22/07/2024 17:31	22/07/2024 17:31		CWE	Все значения 🗸
	KCSSTATUS	11/12/2024 11:00	11/12/2024 11:00		CVE	Все значения 🗸
	KCSSTATUS2	11/12/2024 11:58	11/12/2024 11:58		Статус	Все значения
	KCSSTATUS3	11/12/2024 12:04	11/12/2024 12:04		Сканируемый объект	Все значения ч
	KCSSTATUS4	11/12/2024 12:49	11/12/2024 12:49			
Bce	ro 68					
					Создать отчет Отмена	

Рис. 24

 Нажать на кнопку Создать отчет. При успешном создании пользователь увидит всплывающую нотификацию (Рис. 25). Отчет будет доступен в разделе Отчеты → Сводные.



Рис. 25

Детализированный отчет доступен отдельно по проекту. Для создания данного отчета необходимо выполнить следующие шаги:

1. Перейти в <u>Обзор проекта</u>, нажать на кнопку **Создать отчет** и выбрать **Детализированный** (Рис. 26).



Рис. 26

 В открывшемся окне заполнить поле Название отчета и добавить необходимые фильтры по полям отчета (Рис. 27), при этом рекомендуется сократить количество обнаруженных проблем до 80 (количество указано в поле Всего проблем), чтобы загрузка отчета не занимала много времени (Рис. 28).

Проекты > TESTISSUES1 > Обзор		Создать детали:	зированный отчет ×
Обзор Конвейеры безопасности Результаты сканирования Контроль качеств	а Проблемы безопасности Библиотека зависимосте	Название отчета*	Введите название
Весь период Год Квартал Месяц Неделя День 14.04.2024 14	04.2025 ×	Фильтр	Всего проблем: 13 188 ()
		Поле	Фильтр
Накопительный график	Уязвимости	Категория	Все значения 🗸
ТК	Сканирова	Уровень критичности	Все значения
10	7258	Обнаружено с помощью	Все значения
0 0 0	Высокий Средний	CWE	Все значения 🗸
8 8 4 5 4 8 8 8 8 8 8 8 8 8 8 8 8 8 8 8	Низкий	CVE	Все значения 🗸
	•	Статус	Все значения 🗸
Инструменты безопасности	Метрики	Сканируемый объект	Все значения 🗸
14	Среднее время в статусе «Исключено» (час.)		
12	Среднее время в статусе «Вручную» (час.)		
10	Плотность риска		
8	Частота проведения сканирования		
4	Среднее время выполнения сканирования (мин.)		
	Количество дубликатов уязвимостей		
0	Процент устраненных уязвимостей (%)		
	Количество security rules		
	Количество проблем, подпавших под security rules	Создать отчет Отмена	
Наиболее критициые ударимости	Интегральный риск-индекс		

Рис. 27

Фильтр		Всего проблем: 215 ①
Поле	Фильтр	Сократите количество проблем в отчете до 80, используя указанный фильтр. В
Категория	Все значения	противном случае создание РОН-отчета займет значительное количество времени.
Уровень критичности	Критический ×	×
Обнаружено с помощью	Все значения	~

Рис. 28

3. Далее нажать на кнопку **Создать отчет**. При успешном создании пользователь увидит всплывающую нотификацию (Рис. 25). Отчет будет доступен в разделе **Отчеты** → **Детализированные**.

#### 4.4.4. Обзор проекта

Подраздел **Обзор** (Рис. 29) предоставляет возможность просмотра Дашборда с информацией по часто встречающимся уязвимостям с параметрами критичности, источникам обнаружения и рейтингом наиболее критичных уязвимостей в рамках одного проекта. Значения накопительных графиков обновляются раз в сутки.

E ⊕	Проекты         TESTISSUES1         >           Обзор         Конеейеры безопасности         Результаты сканирования         >           Вето-перееле         Гот. Конеен         Нелеен         Вето-	Обзор Контроль качества Проблемы безопасности Библиот па па годов, па па годов	ка зависимостей Параметры проекта	A possible order v ) Althermore approximate
88 Информационная панель	The second secon			
Проекты	Накопительный график	Уязвимости		Открытые уязвимости
П Библиотока зависимостой				
		1K	Всего уязвимостей 9604	1032
		10	Сканирований 100	CWE-476
Правила		0		4124 CWE-416 345
<ul> <li>Правила оезопасности</li> </ul>	3 43 43 43 43 43 43 43 43 43 43 43 43 43	5 <sup>th</sup> 15 <sup>th</sup>	Критический 168	CWE-200 312
Правила дедупликации	Satt att att att att att att att att att	3.007	Высокий 3249	CWE-200,CWE-1022 243
Д Правила реагирования	Ησεινά 👧 Β πρήστε 💼 Πρητροηγησιμο 👼 Βηγιμγιο		Среднии 4175 О пизкии 1987     Неопределенный 25	CWE-125
Администрирование	a noosa a passio a natropationa a optimita			
83 Управление доступом				
🗘 Интеграции	Инструменты безопасности	Метрики	\$	Всего уязвимостей
)) Отчеты		14 Среднее время нахождения уязвими	сти в статусе Исключено (час.)	10.2K
🗄 Журнал событий		12 Среднее время нахождения уязвими	сти в статусе Вручную (час.)	8.16K 6.12K
]. Конструктор полей		Плотность риска	0.57	4.08K
араметры		4астота проведения сканирования		2.04K
🖇 Параметры подключения		4 Среднее время выполнения сканиро	вания (мин.)	03-08 03-15 03-22 03-29 03-31 04-05 04-07
🔊 О программе		2 Количество дубликатов уязвимостей 0		10120 mm 0604 mm 100
	31 мар. 2025 07 anp. 2025	<ul> <li>Процент устраненных уязвимостей ( Корицертов ресультацие)</li> </ul>	6)	окрытах АОЛ4 сканибования ТОО
		Количество зесилту rules		
පී admin		количество прослем, подпавших под	accurry runs	

Рис. 29

Чтобы перейти к подразделу необходимо в разделе **Проекты** выбрать один из доступных проектов и нажать на имя проекта, выделенное синим цветом (Рис. 30).

$\Box$	Имя проекта 🗸
	TESTSUPRESS
0	TEST1

Рис. 30

Функционал настроек виджетов идентичен с настройками виджетов Информационной панели (подробнее см. <u>Настройки виджетов</u>).

## 4.5. Конвейеры безопасности и проверки безопасности

Конвейер безопасности (пайплайн) - это группирующая сущность для Проверок безопасности. У пользователя есть возможность создания новых и настройки доступных, в соответствии с назначенной ролью, ранее созданных Конвейеров безопасности.

В TRON.ASOC каждый Конвейер безопасности привязан к проекту.

Для того, чтобы начать работу с Конвейерами безопасности, необходимо перейти в раздел **Проекты**, найти необходимый проект, открыть его обзор, после чего перейти на вкладку **Конвейеры безопасности** (Рис. 31).

≡ ⊕	Проекты > TESTISSU	роекты  → TESTISSUES1  → Конвейеры безопасности									
	Обзор Конвейеры безопасности Результаты о	боор Коневёры безопасности Результаты сканерования Контроль качества. Проблемы безопасности. Библиотека зависимостей. Параметры проекта									
器 Информационная панель	+ Добавить конвейер безопасности										
Проекты Троблемы безопасности	appscreener Контроль пройдон Результаты сканирования		Последний	запуск пайплайна 07/04/	2025 09:24	Начать новое сканирован	ние + Добавить провер	ку безопасности	🕆 Удалить конвейер		
П Библиотека зависимостей	Название источника	Инструмент	Тип	Последний запуск	Статус	Статус проверки	Результаты сканирования	SBOM			
<ul> <li>Контроль качества</li> <li>Позвила</li> </ul>	issuesharbor https://harbor.tronsec.ru/	Scoring01 http://code.int.ximi.group:8095/	Ручной	07/04/2025 18:14	• Не выполн	эн	Результаты сканирования	<ul> <li>Ожидает загрузки</li> </ul>	🖞 Смотреть 📄		
О Правила безопасности	nosqlinjectionvulnapp https://github.com/vulnerable-apps/nosql-injection-vu	PT AI -2 https://158.160.74.198/	Ручной	07/04/2025 17:08	• Не выполни	эн	Результаты сканирования	<ul> <li>Не поддерживается</li> </ul>	🛱 Смотреть 📼		
Правила дедупликации Д Правила реагирования	issuesharbor https://harbor.tronsec.ru/	Scoring01 http://code.int.ximi.group:8095/	Ручной	07/04/2025 18:02	• Не выполн	вн	Результаты сканирования	<ul> <li>Ожидает загрузки</li> </ul>	ф Смотреть 🖂		
Администрирование 85 Управление доступом	issuesnexus http://nexus.int.ximi.group:8081	Scoring01 http://code.int.ximi.group:8095/	Ручной	08/04/2025 10:46	• Не выполн	ен • Контроль не пройден	Результаты сканирования	<ul> <li>Ожидает загрузки</li> </ul>	ф Смотреть 🖂		
О Интеграции	asocCore https://ximilab.gitlab.yandexcloud.net/ximidev/tron-asi	Scoring01 http://code.int.ximi.group:8095/	Ручной		• Новый		Результаты сканирования О	<ul> <li>Ожидает загрузки</li> </ul>	🖞 Смотреть 🚍		
<ul> <li>В Журнал событий</li> </ul>	asocCore https://ximilab.gitlab.yandexcloud.net/ximidev/tron-asi	Scoring01 http://code.int.ximi.group:8095/	Ручной		• Новый		Результаты сканирования ©	• Ожидает загрузки	🖞 Смотреть 🚍		
С. Конструктор полей	issuesgitcore https://ximilab.gitlab.yandexcloud.net/ximidev/tron-asi	Scoring01 http://code.int.ximi.group:8095/	Ручной	07/04/2025 14:18	• Не выполн	эн	Результаты сканирования	<ul> <li>Ожидает загрузки</li> </ul>	🖞 Смотреть 🔛		
Параметры подключения	issuesgitcore https://ximilab.gitlab.yandexcloud.net/ximidev/tron-asi	issuescodescoring http://code.int.ximi.group:8095/	Ручной	07/04/2025 14:17	• Не выполн	вн	Результаты сканирования	<ul> <li>Ожидает загрузки</li> </ul>	ф Смотреть 🖂		
⑦ О программе	issuesgitcore https://ximilab.gitlab.yandexcloud.net/ximidev/tron-asi	Scoring01 http://code.int.ximi.group:8095/	Ручной	07/04/2025 14:16	• Не выполн	эн	Результаты сканирования	<ul> <li>Ожидает загрузки</li> </ul>	∰ Смотреть 📄		
 ది admin	issuesgitcore https://ximilab.gitlab.yandexcloud.net/ximidev/tron-asi	Scoring01 http://code.int.ximi.group:8095/	Ручной	07/04/2025 14:16	• Не выполн	вн	Результаты сканирования	• Ожидает загрузки	ф Смотреть 🖂		

Рис. 31

Каждый Конвейер безопасности представлен отдельной строкой, которая содержит название и описание конвейера, ссылку на результаты сканирования, содержащиеся внутри конвейера проверки безопасности.

Также отображены данные проверки безопасности (название каждой проверки безопасности в конвейере, используемые в проверке инструменты безопасности и источники, тип проверки (ручной или автоматический), время последнего запуска, статус последнего успешного сканирования, ссылка на результаты сканирования (Рис. 31).

#### 4.5.1. Создание конвейера безопасности

Чтобы создать новый Конвейер безопасности, необходимо выполнить следующие шаги:

- 1. В разделе **Проекты** найти необходимый проект и перейти на страницу данного проекта (Обзор проекта)
- 2. Перейти на вкладку Конвейер безопасности
- 3. Нажать на кнопку Добавить конвейер безопасности (Рис. 32).

Проекты · TESTISSUES1 · Конвейеры безопасности Результаты сканирования Контроль качества Проблемы безопасности Библиотека зависимостей Па + Добавить конвейер безопасности

Рис. 32

4. На странице создания конвейера безопасности (Рис. 33) заполнить обязательное поле **Имя**, а также дополнительные поля **Описание** и **Шаблон** при необходимости.

В данном случае, в роли шаблона может быть любой другой конвейер безопасности, созданный ранее. Для добавления шаблона необходимо в поле **Шаблон** ввести название конвейера безопасности, который необходимо переиспользовать. По умолчанию список шаблонов появляется при вводе символов в поле **Шаблон** (Рис. 33).

Проекты → TESTISSU	<b>ES1</b> → Конвейер	ы безопасн	ности				Создать конвейер безопасности
Обзор Конвейеры безопасности Результаты с	жанирования Контроль качества	Проблемы безопасности	и Библиотека зависимо	остей Параметры	проекта		
+ Добавить конвейер безопасности							ими: О Имя конвейера
appscreener Контроль пройден Результаты сканирования		Последний	запуск пайплайна 07/04/	2025 09:24 🔘 H	ачать новое сканирован	ше	Описание
Название источника	Инструмент	Тип	Последний запуск	Статус	Статус проверки	Резуль	Шаблон
issuesharbor https://harbor.tronsec.ru/	Scoring01 http://code.int.ximi.group:8095/	Ручной	07/04/2025 18:14	• Не выполнен		Резуль	Выберите шаблон 🗸
nosqlinjectionvulnapp https://github.com/vulnerable-apps/nosql-injection-vu	PT AI -2 https://158.160.74.198/	Ручной	07/04/2025 17:08	• Не выполнен		Резуль	
issuesharbor https://harbor.tronsec.ru/	Scoring01 http://code.int.ximi.group:8095/	Ручной	07/04/2025 18:02	• Не выполнен		Резуль	
issuesnexus http://nexus.int.ximi.group:8081	Scoring01 http://code.int.ximi.group:8095/	Ручной	08/04/2025 10:46	• Не выполнен	<ul> <li>Контроль не пройден</li> </ul>	Резуль	
asocCore https://ximilab.gitlab.yandexcloud.net/ximidev/tron-ase	Scoring01 http://code.int.ximi.group:8095/	Ручной		• Новый		Резуль ()	
asocCore https://ximilab.gitlab.yandexcloud.net/ximidev/tron-aso	Scoring01 http://code.int.ximi.group:8095/	Ручной		• Новый		Резуль ①	
issuesgitcore https://ximilab.gitlab.yandexcloud.net/ximidev/tron-ase	Scoring01 http://code.int.ximi.group:8095/	Ручной	07/04/2025 14:18	• Не выполнен		Резуль	
issuesgitcore https://ximilab.gitlab.yandexcloud.net/ximidev/tron-asc	issuescodescoring http://code.int.ximi.group:8095/	Ручной	07/04/2025 14:17	• Не выполнен		Резуль	
issuesgitcore https://ximilab.gitlab.yandexcloud.net/ximidev/tron-asc	Scoring01 http://code.int.ximi.group:8095/	Ручной	07/04/2025 14:16	• Не выполнен		Резуль	
issuesgitcore https://ximilab.gitlab.yandexcloud.net/ximidev/tron-asc	Scoring01 http://code.int.ximi.group:8095/	Ручной	07/04/2025 14:16	• Не выполнен		Резуль	Создать Отмена

Рис. 33

5. Далее нажать на кнопку Создать.

После создания Конвейера безопасности необходимо добавить к нему <u>Проверку безопасности</u>.

#### 4.5.2. Создание проверки безопасности

**Проверка безопасности** - это сущность, которая может объединять в себе связку инструмента сканирования и источника. Она используется для запуска сканирования безопасности, а также для получения результатов сканирований.

Для того, чтобы добавить проверку безопасности, необходимо выполнить следующие шаги:

 В разделе Проекты → <Название проекта> → Конвейеры безопасности нажать на кнопку Добавить проверку безопасности (Рис. 34).

appscreener Контрольпройден Результаты сканирования		Последний за	пуск пайплайна 07/04/2	025 09:24 🔘 H	ачать новое сканирован	не + Добавить провер	ку безопасности	🖞 Удалить конвейер
Название источника issuesharbor https://harbor.tronsec.ru/	Инструмент Scoring01 http://code.int.ximi.group:8095/	Тип Ручной	Последний запуск	• Не выполнен	Статус проверки	Результаты сканирования Результаты сканирования	SBOM • Ожидает загрузки	🛱 Смотреть 📟
nosqlinjectionvulnapp https://github.com/vulnerable-apps/nosql-injection-vu	PT AI -2 https://158.160.74.198/	Ручной	07/04/2025 17:08	• Не выполнен		Результаты сканирования	<ul> <li>Не поддерживается</li> </ul>	🛱 Смотреть 😁

Рис. 34

2. Далее заполнить форму создания проверки безопасности (Рис. 35).

Проекты → TESTISSU	ES1 → Конвейер	ы безопасн	юсти		(	Создать прове	рку безопас	ности	×
Обзор Конвейеры безопасности Результаты с	канирования Контроль качества	Проблемы безопасности	Библиотека зависимо	остей Параметр	ы проекта				
						Инструмент*	AppScreener DAST (EN)	_Api Token_25102024_qamkr-27	<b>~</b>
+ Добавить конвейер безопасности						Источник*	App URL (http://www.itse	ecgames.com)   issuesappurl	•
appscreener Контроль пройден Результаты сканирования		Последний з	запуск пайплайна 07/04/	2025 09:24 💿	Начать но	Запуск задачи сканир	ования	Ручной Автоматически	Ä
Название источника	Инструмент	Тип	Последний запуск	Статус	Статус				
issuesharbor https://harbor.tronsec.ru/	Scoring01 http://code.int.ximi.group:8095/	Ручной	07/04/2025 18:14	<ul> <li>Не выполнен</li> </ul>					
nosqlinjectionvulnapp https://github.com/vulnerable-apps/nosql-injection-vu	PT AI -2 https://158.160.74.198/	Ручной	07/04/2025 17:08	• Не выполнен					
issuesharbor https://harbor.tronsec.ru/	Scoring01 http://code.int.ximi.group:8095/	Ручной	07/04/2025 18:02	• Не выполнен					
issuesnexus http://nexus.int.ximi.group:8081	Scoring01 http://code.int.ximi.group:8095/	Ручной	08/04/2025 10:46	• Не выполнен	<ul> <li>Кон про</li> </ul>				
asocCore https://ximilab.gitlab.yandexcloud.net/ximidev/tron-asi	Scoring01 http://code.int.ximi.group:8095/	Ручной		• Новый					
asocCore https://ximilab.gitlab.yandexcloud.net/ximidev/tron-asi	Scoring01 http://code.int.ximi.group:8095/	Ручной		• Новый					
issuesgitcore https://ximilab.gitlab.yandexcloud.net/ximidev/tron-asr	Scoring01 http://code.int.ximi.group:8095/	Ручной	07/04/2025 14:18	• Не выполнен					
issuesgitcore https://ximilab.gitlab.yandexcloud.net/ximidev/tron-asr	issuescodescoring http://code.int.ximi.group:8095/	Ручной	07/04/2025 14:17	• Не выполнен					
issuesgitcore https://ximilab.gitlab.yandexcloud.net/ximidev/tron-asc	Scoring01 http://code.int.ximi.group:8095/	Ручной	07/04/2025 14:16	• Не выполнен					
issuesgitcore https://ximilab.gitlab.yandexcloud.net/ximidev/tron-ask	Scoring01 http://code.int.ximi.group:8095/	Ручной	07/04/2025 14:16	• Не выполнен		Создать Отмена			

Рис. 35

Для настройки проверки безопасности выбор инструмента безопасности является обязательным (Рис. 35). Выбрать возможно только инструмент, ранее добавленный администратором в разделе Интеграции. Поля формы зависят от выбранных полей **Источник** и **Инструмент**.

3. Нажать на кнопку Создать.

Если при создании интеграции с инструментом безопасности администратор не указал метод аутентификации, то при добавлении инструмента в **Проверку безопасности** поле выбора метода аутентификации является обязательным для заполнения. При выборе метода аутентификации на этапе создания проверки безопасности, необходимо ввести данные для аутентификации в соответствующие поля (могут меняться в зависимости от метода: **Токен АРI**, **Логин/Пароль**).

Если при создании интеграции с источником сканирования администратор не указал метод аутентификации, то при добавлении источника в **Проверку безопасности** заполнение поля выбора метода аутентификации является обязательным. При выборе метода аутентификации на этапе создания проверки безопасности, необходимо ввести данные для аутентификации в соответствующие поля (Рис. 36).

	ерку безоп	асности
Инструмент*	AppScreener SAST	(EN)_25102024_w/o auth settings_qa 🗸 🗸
Метод аутентификации	Токен АРІ	× v
Токен АРІ*		٥
Источник*	Git Repository (http	://111.11.11.11)   dsfgsdfsdbabinban 🗸
Название ветки или тега*	Введите название	
Запуск задачи скани	оования	Ручной Автоматический

Рис. 36

Также для некоторых инструментов предусмотрена возможность выбора типа запуска сканирования (ручной или автоматический), периодичность и время запуска сканирования при выборе автоматического запуска.

После заполнения всех необходимых полей (инструмент безопасности, источник, методы аутентификации) предлагается проверить соединение с инструментами. Для этого необходимо нажать на кнопку **Проверить соединение** (в случае, если она активна).

В проверках безопасности также предусмотрена загрузка (импорт) результатов сканирования от внешних инструментов (Рис. 37) в зависимости от выбранного инструмента безопасности. Эта опция доступна не для всех инструментов безопасности.

				ей параметры	Ipoekia			
+ Добавить конвейер безопасности								
stsupress				(	Начать новое сканирован	ние + Добавить провер	рку безопасности	🖞 Удалить конвей
зультаты сканирования								
азвание источника	Инструмент	Тип	Последний запуск	Статус	Статус проверки	Результаты сканирования	SBOM	
suesappurl	dastauth http://apps.int.tronasoc.ru/app/api/v1	Ручной	08/04/2025 15:16	• Выполнен		Результаты сканирования	<ul> <li>Не поддерживается</li> </ul>	∰ Смотреть
p://www.itsecgames.com								
tp://www.itsecgames.com							Начать	новое сканировани

Рис. 37

#### 4.5.3. Запуск конвейера безопасности

Для того, чтобы запустить конвейер безопасности необходимо выполнить следующее:

1. В разделе **Проекты** → *<Название проекта>* → **Конвейеры безопасности** нажать кнопку **Начать новое сканирование** (Рис. 38).

Проекты · TESTSUPRESS · Конвейеры безопасности										
Обзор Конвейеры безопасности Результаты си	канирования Контроль качества Про	блемы безопасности	Библиотека зависимосте	ай Параметры проекта						
+ Добавить конвейер безопасности										
testsupress Результаты сканирования				🛞 Начать новое ска	нирование + Добавить провер	ку безопасности	🖞 Удалить конвейер			
Название источника	Инструмент	Тип	Последний запуск	Статус Статус провер	Результаты сканирования	SBOM				
issuesappurl http://www.itsecgames.com	dastauth http://apps.int.tronasoc.ru/app/api/v1	Ручной	08/04/2025 15:16	• Выполнен	Результаты сканирования	• Не поддерживается	🛱 Смотреть 🖂			

Рис. 38

Данное действие приведет к запуску всех проверок безопасности в конвейере.

#### 4.5.4. Запуск проверки безопасности

Для того, чтобы запустить отдельную проверку безопасности необходимо выполнить следующее:

1. В разделе **Проекты** → *<Название проекта>* → **Конвейеры безопасности** найти в списке необходимую проверку безопасности и

раскрыть список действий по данной проверке с помощью кнопки

2. В списке действий выбрать Начать новое сканирование (Рис. 39).

		Биолиотека зависимосте	еи Параметры	проекта			
			0	Э Начать новое сканирован	ие + Добавить провер	оку безопасности	🖞 Удалить конвейс
Инструмент	Тип	Последний запуск	Статус	Статус проверки	Результаты сканирования	SBOM	
dastauth http://apps.int.tronasoc.ru/app/api/v1	Ручной	08/04/2025 15:16	• Выполнен		Результаты сканирования	• Не поддерживается	🛱 Смотреті 📻
						<ul> <li>Начат</li> <li>Просм</li> </ul>	ь новое сканирование мотреть проверку
						0. 10.000	
	Инструмент dastauth http://apps.int.tronasoc.ru/app/api/v1	Инструмент Тип dastauth http://apps.int.tronasoc.ru/app/api/v1 Ручной	Инструмент Тип Последний запуск dastauth http://apps.inttronasoc.ru/app/api/v1 Ручной 08/04/2025 15:16	Инструмент         Тип         Последний запуск         Статус           dastauth http://apps.int.tronasoc.ru/app/api/v1         Ручной         08/04/2025 15:16         ● Выполнен	Инструмент         Тип         Последний запуск         Статус         Статус проверки           datauth http://apps.inttronasoc.ru/spp/api/v1         Ручной         08/04/2025 15:16               Выполнен	Инструмент         Тип         Последний запуск         Статус         Статус проверки         Результаты сканирования           dastauth http://apps.inttronasoc.ru/app/api/v1         Ручной         08/04/2025 15:16         • Выполнен         Результаты сканирования	Инструмент         Тип         Последний запуск         Статус         Статус проверки         Результаты сканирования         SBOM           datauth http://apps.inttronasoc.ru/app/apl/v1         Ручной         08/04/2025 15:16         • Выполнен         Результаты сканирования         SBOM

Рис. 39

При запуске проверки безопасности меняется ее статус на **В работе**. После успешного завершения проверка переходит в статус **Выполнено**. Общее максимальное время работы цикла сканирования - по умолчанию 1 час. Если цикл достиг максимального времени работы, то проверка переходит в статус **Не выполнено** и процесс завершается. Статус **Не выполнено** также назначается, если возникли ошибки на каком-либо из этапов сканирования.

#### 4.5.5. Остановка сканирования

Сканирование со статусом *В процессе* возможно принудительно остановить. Для этого в разделе Проекты → *<Название проекта>* → Конвейеры безопасности в соответствующей Проверке безопасности необходимо нажать на кнопку Остановить сканирование.

#### 4.5.6. Загрузка внешнего отчета

Загрузка внешнего отчета может быть произведена вручную. Для загрузки необходимо выполнить следующие шаги:

 В разделе Проекты → <Название проекта> → Конвейеры безопасности нажать на кнопку Импортировать результаты в меню справа (Рис. 40).

Проекты > Т	ESTISSUES	1 У Коне	ейеры безопас	ности					
Обзор Конвейеры безопасно	Результаты скани	рования Контроль ка	ачества Проблемы безопаснос	сти Библиотека завис	имостей Параметры проек	га			
+ Добавить конвейер безопа	сности								
appscreener Контроль пройден Результаты сканирования	I		Последни	ій запуск пайплайна 07,	/04/2025 09:24 🔘 Начать	новое сканирование + Добав	ить проверку безог	асности	🕆 Удалить конвейер
Название источника	Инструмент	Тип	Последний запуск	Статус	Статус проверки	Результаты сканирования	SBOM		
issuespath https://jfrog.tronsec.ru	Scoring01 http://code.int.ximi.grc	Ручной	08/04/2025 17:25	• Не выполнен		Результаты сканирования	• Ожида	ает загрузки	🏦 Смотреть 🖂
issuesnexus http://nexus.int.ximi.group:8081	Scoring01 http://code.int.ximi.gro	Ручной	08/04/2025 17:24	• Не выполнен		Результаты сканирования	• Ожида	<ul> <li>Начать</li> <li>Просмо</li> </ul>	новое сканирование
issuesharbor https://harbor.tronsec.ru/	Scoring01 http://code.int.ximi.gro	Ручной	07/04/2025 18:14	• Не выполнен		Результаты сканирования	• Ожид	С. Импорт С. Импорт	ировать результаты ировать SBOM
nosqlinjectionvulnapp https://github.com/vulnerable-app	PT AI -2 https://158.160.74.19	Ручной	07/04/2025 17:08	• Не выполнен		Результаты сканирования	<ul> <li>Не подде</li> </ul>	Удалить     рживается	проверку

Рис. 40

2. Далее загрузить JSON-файл с результатами (Рис. 41).

Проекты > Т	ESTISSUES	1 → Коне	ейеры безопас	ности			Импорти	оовать результаты	×
Обзор Конвейеры безопасно	сти Результаты скани	рования Контроль к	ачества Проблемы безопаснос	сти Библиотека завис	имостей Параметры проект	a			
+ Добавить конвейер безопан appscreener Контроль пройден Результаты сканирования	ности		Последни	ий запуск пайплайна 07,	/04/2025 09:24 💿 Начать н	ювое сканирование	J	Перетащите файл Вы можете загрузить не более одного файла JSON	
Название источника	Инструмент	Тип	Последний запуск	Статус	Статус проверки	Результаты сканирован			
issuespath https://jfrog.tronsec.ru	Scoring01 http://code.int.ximi.grc	Ручной	08/04/2025 17:25	• Не выполнен		Результаты сканировани			
issuesnexus http://nexus.int.ximi.group:8081	Scoring01 http://code.int.ximi.grc	Ручной	08/04/2025 17:24	• Не выполнен		Результаты сканировани			
issuesharbor https://harbor.tronsec.ru/	Scoring01 http://code.int.ximi.grc	Ручной	07/04/2025 18:14	• Не выполнен		Результаты сканировани			
nosqlinjectionvulnapp https://github.com/vulnerable-app	PT AI -2 https://158.160.74.19	Ручной	07/04/2025 17:08	• Не выполнен		Результаты сканировани			
issuesharbor https://harbor.tronsec.ru/	Scoring01 http://code.int.ximi.grc	Ручной	07/04/2025 18:02	• Не выполнен		Результаты сканировани			
issuesnexus http://nexus.int.ximi.group:8081	Scoring01 http://code.int.ximi.grc	Ручной	08/04/2025 10:46	• Не выполнен	• Контроль не пройден	Результаты сканировани			
asocCore https://ximilab.gitlab.yandexcloud.	Scoring01 http://code.int.ximi.grc	Ручной		• Новый		Результаты сканировани			
asocCore https://ximilab.gitlab.yandexcloud.	Scoring01 http://code.int.ximi.grc	Ручной		• Новый		Результаты сканировани			
issuesgitcore https://ximilab.gitlab.yandexcloud.r	Scoring01 http://code.int.ximi.grc	Ручной	07/04/2025 14:18	• Не выполнен		Результаты сканировани			
issuesgitcore https://ximilab.gitlab.yandexcloud.i	issuescodescoring http://code.int.ximi.grc	Ручной	07/04/2025 14:17	• Не выполнен		Результаты сканировани	Сохранить	Отмена	

Рис. 41

3. Нажать на кнопку Сохранить.

Требования к JSON-файлу:

```
{
"properties": {
  "issues": {
    "type": "array",
    "items": {
      "type": "object",
      "properties": {
         "category": { "type": "string" },
         "severity": {
          "type": "string",
           "enum": ["critical", "high", "medium", "low", "undefined"]
         },
         "id": { "type": "string" },
         "cwe": { "type": "string" },
         "cve": { "type": "string" },
         "line": { "type": "integer", "minimum": 1 },
         "code": { "type": "string" },
         "libraryName": { "type": "string" },
         "libraryVersion": { "type": "string" },
         "file": { "type": "string" },
         "links": {
          "type": "array",
          "items": { "type": "string", "format": "uri" }
         },
         "description": { "type": "string" },
         "recommendation": { "type": "string" },
         "fixedVersion": { "type": "string" },
```

```
"ratings": {
           "type": "array",
           "items": {
             "type": "object",
             "properties": {
               "metric": { "type": "string" },
               "score": { "type": "number", "minimum": 0, "maximum":
10 }
             },
             "required": ["metric", "score"]
           }
         },
         "path": {
           "type": "array",
           "items": { "type": "string" }
         }
       },
       "required": ["category", "severity"]
    }
  }
},
"required": ["issues"]
}
```

#### Пример тела запроса:

```
[
{
   "category": "OS dependency vulnerability",
   "severity": "high",
   "scan object": "jfrog.tronsec.ru/tron/event-broker:1.1.2-patch",
   "cwe": "CWE-79",
   "cve": "CVE-2023-1234",
   "tool type name": "KCS",
   "lib name": "example-library",
   "lib version": "1.2.3",
   "info links": ["https://example.com/cve-2023-1234",],
   "description": "This is a vulnerability description.",
   "recommendations": "Sanitize user input before executing
commands.",
   "fixed version": "1.2.4",
   "ratings": "CVSS: 9.1 (Critical)",
   "path": "/src/controllers/userController.js",
   "exploit": "Proof-of-concept exploit code here."
 },
```

Кроме того, при использовании внешних скриптов и в зависимости от выбранного инструмента сканирования (например, CLI-инструмента) у проверки безопасности может быть доступна опция получения результатов сканирования извне путём http-запроса от внешнего инструмента на эндпоинт TRON.ASOC.

Предусмотрена возможность загрузки не более одного файла в формате JSON.

#### 4.5.7. Использование CLI-инструментов

Для того, чтобы получить возможность отправки результатов от CLI-инструмента (Command Line Interface), предварительно необходимо добавить его в список доступных инструментов безопасности в разделе Интеграции → Источники безопасности, при этом необходимо заполнить поля Название, Описание и выбрать один из представленных инструментов (Рис. 42):

- Trivy
- Crype
- OWASP Dependency Track
- Semgrep
- Aqua
- CodeScoring
- Kaspersky Container Security
- KICS
- PT Application Inspector
- Solar Appscreener
- Manual сторонний инструмент, из которого можно загрузить результаты сканирований в систему, которые будут учитываться при дальнейшей обработке данных. Результаты загружаются в формате JSON с теми же требованиями, что представлены в разделе выше <u>Загрузка внешнего</u> <u>отчета</u>.

	Интеграции				Добавить и	инструмент безопасности	×
	Инструменты безопасности Источники скани	рования Инструменты уведомлений Трекеры з	адач		Название*	12334	
	+ Добавить инструмент безопасности					От 4 до 255 симеолов - Бухвы, цифры, пробелы	
25 Информационная панель					Описание*	Instrument	
🗅 Проекты	Название ч	Инструмент =	Описание ~	Статус пров			
1 Проблемы безопасности	KICS_RG2_qamkr-51	KICS	KICS_RG2_qamkr			От 4 до 255 симеолов - Буквы, цифры, пробелы	6
П риблиотека зависимостей					Инструмент*	Manual	×
⊙ Контроль качества	issueskiks	KICS	issueskiks				
Правила	test kcs-42	KICS	test kcs		Конечная точка	АРІ проверки безопасности	>
О Правила безопасности	Manual	Manual	Check	_			
💭 Правила дедупликации							
Ф Правила реагирования	issuesmanual	Manual	issuesmanual				
Администрирование	Issuesowasp	OWASP Dependency Track	issuesowasp				
8 Управление доступом		OWIND Design days of Tarak		_			
🗘 Интеграции	testowasp	GWASP Dependency mack	testowasp				
🕒 Отчеты	test1245	PT Application Inspector	000000	🛛 Успешн			
🗊 Журнал событий				01.04.20;			
🗋 Конструктор полей				URL инструм			
				Метод аутен			
Параметры	PTAI (EN)_RG2_qamkr-48	PT Application Inspector	PTAI (EN)_RG2_qamkr	🛛 Успеши			
Параметры подключения				31.10.20			
③ О программе				URL инструк			
				ane rog sy res			
යි admin	PT AI (RU)_Login/Paasword_25102024_qamkr-26	PT Application Inspector	PT AI (RU)_Login/Paasword_25102024_qamkr	Успешн 25.10.20;	Создать Отме	на	

Рис. 42

После добавления инструмента необходимо добавить новый источник сканирования. Для этого необходимо выполнить следующие шаги:

- 1. В разделе Интеграции → Источники сканирования нажать на кнопку Добавить источник сканирования.
- 2. В открывшейся форме заполнить поля **Имя**, **Описание**, указать значение поля **Источник =** *CLI Tool Custom Source* (Рис. 43).

Для CLI-инструментов источником может быть любая ссылка: репозиторий, база знаний и т.д.

≡ ⊕	Интеграции				Добавить исто	очник сканирования	×
	Инструменты безопасности Источники сканир	ования Инструменты уведомлений Трекеры з	адач		Имя*		
99 Информационная ранель	+ Добавить источник сканирования					От 4 до 255 символов - Букаы, цифры, пробелы	
🗅 Проекты	Название 🗉	Источник ч	Описание ч	Статус прог	Описание*		
道(Проблемы безопасности	AppURL itsecgames	App URL	AppURL itsecgames_25102024_qamkr	🛛 Успешн		От 4 до 255 симеолов - Букаы, цифры, пробелы	6
Библиотека зависимостей				25.10.20; URL источни	Источник"	CLI Tool Custom Source	~
<ul> <li>Контроль качества</li> </ul>	asocCore	Git Repository	asocCore	🛛 Успешн	URL с полезной	Пример: https://your.link.com	
Правила О Правила безопасности				31.03.20; URL источни	информациеи о процессе сканирования		
💭 Правила дедупликации	asocFront	Git Repository	asocFront	Успешн			
Ф Правила реагирования				30.03.20			
Администрирование	CI ICustomSource 20241028T1356150667 mb3c	Ci LTopi Custom Source	CHCustomSource 20241028T1356150667 mb3				
управление доступом О Интеграции	02004000000202420201200020000200002		CERCURNING _ 024102011000100002_1100	27.03.20;			
🔁 Отчеты				URL источни			
🗄 Журнал событий	CLICustomSource_202604031180129610Z_xowyyx	CLI Tool Custom Source	CLICustomSource_20260403T180129610Z_xow	Ошибка 03.04.20;			
[, Конструктор полей				URL источни			
Параметры Параметры полключения	CLISourceRG2	CLI Tool Custom Source	CLI_SOURCE_RG2_qamkr	Успешн 27.03.20;			
<ol> <li>О программе</li> </ol>				URL источни			
	CLITC Source	CLI Tool Custom Source	CLITC Source_25102024_qamkr	Успешн 25.10.201			
송 admin				URL источни	Создать Отмена	⊳ Прове	рить соединение

Рис. 43

3. Нажать на кнопку Создать.

Далее требуется создать проверку безопасности в конвейере безопасности соответствующего проекта. Для этого необходимо выполнить следующие шаги:

- 1. В разделе **Проекты** → <*Название проекта*> → Конвейеры безопасности нажать на кнопку Добавить проверку безопасности.
- 2. В открывшейся форме создания проверки указать ранее созданные инструмент сканирования и источник сканирования соответственно в полях **Инструмент** и **Источник** (Рис. 44).

Проекты > TESTISSU	ES1 → Конвейе	ры безопасн	ости		(	Создать прове	ерку безопасности	×
Обзор Конвейеры безопасности Результаты с	канирования Контроль качества	Проблемы безопасности	Библиотека зависим	остей Параметр	ы проекта	Инструмент*	Manual   Check	~
+ Добавить конвейер безопасности						Источник*	CLI Tool Custom Source (http://dev.a	soc.ximi.group/)   Cl 🗸
appscreener Контрольпройден Результаты сканирования		Последний з	апуск пайплайна 07/04/	2025 09:24 🔘	Начать но	Запуск задачи сканир	ования	Ручной
Название источника	Инструмент	Тип	Последний запуск	Статус	Статус			
issuespath https://jfrog.tronsec.ru	Scoring01 http://code.int.ximi.group:8095/	Ручной	08/04/2025 17:25	• Не выполнен				
issuesnexus http://nexus.int.ximi.group:8081	Scoring01 http://code.int.ximi.group:8095/	Ручной	08/04/2025 17:24	• Не выполнен				
issuesharbor https://harbor.tronsec.ru/	Scoring01 http://code.int.ximi.group:8095/	Ручной	07/04/2025 18:14	• Не выполнен				
nosqlinjectionvulnapp https://github.com/vulnerable-apps/nosql-injection-vu	PT AI -2 https://158.160.74.198/	Ручной	07/04/2025 17:08	• Не выполнен				
issuesharbor https://harbor.tronsec.ru/	Scoring01 http://code.int.ximi.group:8095/	Ручной	07/04/2025 18:02	• Не выполнен				
issuesnexus http://nexus.int.ximi.group:8081	Scoring01 http://code.int.ximi.group:8095/	Ручной	08/04/2025 10:46	• Не выполнен	• Кон про			
asocCore https://ximilab.gitlab.yandexcloud.net/ximidev/tron-ase	Scoring01 http://code.int.ximi.group:8095/	Ручной		• Новый				
asocCore https://ximilab.gitlab.yandexcloud.net/ximidev/tron-aso	Scoring01 http://code.int.ximi.group:8095/	Ручной		• Новый				
issuesgitcore https://ximilab.gitlab.yandexcloud.net/ximidev/tron-ase	Scoring01 http://code.int.ximi.group:8095/	Ручной	07/04/2025 14:18	• Не выполнен				
issuesgitcore https://ximilab.gitlab.yandexcloud.net/ximidev/tron-ase	issuescodescoring http://code.int.ximi.group:8095/	Ручной	07/04/2025 14:17	• Не выполнен		Создать Отмена		



3. Нажать на кнопку **Создать.** После успешного создания проверки будет доступен запуск сканирования данной проверки, а также всех созданных проверок выбранного проекта.

#### 4.5.8. Интеграция в CI процесс

В системе предусмотрена возможность интегрировать сканирование уязвимостей в CI-пайплайн GitLab, используя различные инструменты для сканирования, и отправлять результаты сканирования в ASOC.

#### 4.5.8.1. Описание переменных

Для правильной настройки скрипта необходимо использовать следующие переменные:

- IMAGE\_TO\_SCAN: yourimagename/latest образ Docker, который будет сканироваться.
- REPORT\_FILE: trivy-report.json имя файла, в который будет сохранен отчет сканирования.
- API\_URL: http://your-tronasoc-url/api/v1/check/{check\_id}/external - appec API.
- API\_TOKEN: asoc-your\_api\_token\_here API токен TRON.ASOC.

Данные переменные необходимо задать в разделе variables в файле gitlab-ci.yml.

# 4.5.8.2. Пример отправки результата сканирования CLI-инструмента в TRON.ASOC в рамках CI

Пример включает две стадии — scan и upload. Скрипт сначала выполняет сканирование, а затем загружает результат.

```
stages:
 - scan
  - upload
variables:
  IMAGE TO SCAN: anaisurlichs/cns-website:0.0.6 # Ofpas Docker,
который будет сканироваться.
 REPORT FILE: trivy-report.json # Имя файла, в который будет сохранен
отчет сканирования.
 API URL:
http://example.asoc.ximi.group/api/v1/check/{check id}/external #
адрес API. {CheckID} становится доступным после создания Проверки
безопасности.
API TOKEN: asoc-exampletoken # API токен TRON.ASOC.
scan image:
 stage: scan
 image: aquasec/trivy:latest # Docker-образ, который будет
использоваться для выполнения задачи, в зависимости от инструмента.
script:
    # Скрипт запускает trivy для сканирования указанного Docker-образа
и сохраняет результат в переменную $REPORT FILE.
    - trivy image -- format json -- output $REPORT FILE $IMAGE TO SCAN
    - echo "Scan completed, report saved to $REPORT FILE"
   # Артефакты, которые будут сохраняться в GitLab.
 artifacts:
   paths:
      - $REPORT FILE
    when: always # Обеспечивает сохранение артефакта независимо от
успешного или неуспешного выполнения задачи.
upload report:
 stage: upload
 image: curlimages/curl:latest # Минимальный образ на базе Alpine с
предустановленным curl.
 script:
    # Содержит команду curl для отправки POST-запроса на адрес API,
используя --data для передачи содержимого файла отчета сканирования.
    - echo "Uploading report $REPORT FILE to $API URL"
    - 1
     curl --location $API URL --header "x-api-token: $API TOKEN"
--header "content-type: application/json" --data @$REPORT FILE
```

```
# Задает зависимость от задачи scan_image, чтобы upload_report имел
доступ к артефактам в этой задаче.
dependencies:
- scan_image
```

Пример использует Trivy в качестве сканера и предназначен для GitlabCI. Также предлагается использовать любой инструмент, изменив образ и команды стадии stage.

Если уже есть результат сканирования - рекомендуется использовать стадию upload для отправки результатов (артефакта). Ниже приведен пример для Grype:

```
scan_image:
image: anchore/grype:latest
stage: scan
script:
    - echo "Scanning image $IMAGE_TO_SCAN"
    - grype $IMAGE_TO_SCAN -o json > $REPORT_FILE
    - echo "Scan completed, report saved to $REPORT_FILE"
artifacts:
    paths:
        - $REPORT_FILE
when: always
```

#### 4.5.9. Результаты сканирований

Результат успешного сканирования можно просмотреть как для отдельного конвейера безопасности во вкладке **Проекты** → *<Название проекта>* → **Результаты сканирований**, так и для отдельной проверки безопасности (Рис. 45).

Проекты · TESTSUPRESS · Конвейеры безопасности									
Обзор Конвейеры безопасности Результаты с	канирования Контролькачества Про	блемы безопасности	Библиотека зависимосте	хстей Параметры проекта					
+ Добавить конвейер безопасности									
testsupress Результаты сканирования				<ul> <li>Начать новое сканирование</li> <li>+Добавить проверку безопасности</li> <li>Д' Удалить конвейс</li> </ul>	ер				
Название источника	Инструмент	Тип	Последний запуск	Статус Статус проверки Результаты сканирования SBOM					
issuesappurl http://www.itsecgames.com	dastauth http://apps.int.tronasoc.ru/app/api/v1	Ручной	08/04/2025 15:16	• Выполнен Результаты сканирования • Не поддерживается ф Смотреть 🖨	3				
Bcero 1				< 1 > 10/страница	~				

Рис. 45

Результаты сканирования (Рис. 46) содержат информацию о конвейере безопасности, источнике, использованном инструменте безопасности, дате начала, количестве найденных проблем безопасности, статусе сканирования.

≡ ⊕	Проекты > ТЕЗ	STISSUES1 → Резулі	ьтаты сканирования	4		
	Обзор Конвейеры безопасности	Результаты сканирования Контроль качес	тва Проблемы безопасности Библи	отека зависимостей Параметры проекта		
8 Информационная панель					Поиск	Q 🕸 🛛
	Конвейер безопасности	Название источника	Инструмент	Дата начала	Всего уязвимостей	Статус
(Д) Проблемы безопасности	appscreener	issuespath	Scoring01	08/04/2025 17:25		• Не выполнен
Библиотека зависимостей			nttp://code.int.ximi.group:8095/			<ul> <li>Ошибка: ASOC-1067: CodeScori &gt;</li> </ul>
⊘ Контроль качества	200000000	Inclusion	Scoring01	09/04/2025 17:23		
Правила	apporteeller	10000010000	http://code.int.ximi.group:8095/	00/04/2020 17-20		• Не выполнен
Правила безопасности						Ошибка: ASOC-1075: CodeScori >
Правила дедупликации	appscreener	issuesnexus	Scoring01	08/04/2025 15:23		• Не выполнен
Д Правила реагирования			http://code.inc.tim.group.co+o/			Ошибка: ASOC-1075: CodeScori >
Администрирование	appscreener	issuesnexus	Scoring01	08/04/2025 15:07		• Не выполнен
С Митеграние доступом			http://code.int.ximi.group:8095/			Outerfire: ASOC-1075: CodeScori
В Журнал событий	appscreener	asocCore	Scoring01 http://code.int.ximi.group:8095/	08/04/2025 15:02	128	• Выполнен 👌 Скачать 🖻
С. Конструктор полей	appscreener	issuesnexus	Scoring01 http://code.int.ximi.group:8095/	08/04/2025 14:50		• Не выполнен
						Ошибка: ASOC-1075: CodeScori >
Параметры подключения	appscreener	issuesnexus	Scoring01	08/04/2025 14:47		• Не выполнен
⑦ О программе			indergroups and an independent of			Ошибка: Get "http://code.int.ximi>
	appscreener	issuesnexus	Scoring01	08/04/2025 14:46		• Не выполнен
송 admin			http://code.intxinfl.group.8096/			

Рис. 46

Когда выполнение проверки безопасности завершается, результаты проверки импортируются из инструментов AST. Результаты сканирования безопасности собираются и упорядочиваются. Каждый инструмент AST создает отчет по безопасности во время каждого запуска тестирования безопасности. Система позволяет выгружать отчеты по результатам сканирований в формате JSON, что обеспечивает удобство интеграции с другими системами и инструментами анализа данных. Выполненный отчет можно скачать с помощью кнопки Скачать (Рис. 47).

Проекты  → TESTISSUES1  → Результаты сканирования										
Обзор Конвейеры безопасности Р	езультаты сканирования Контроль качест	ва Проблемы безопасности Библиотен	ка зависимостей Параметры проекта							
					Поиск		۹	\$ V		
Конвейер безопасности	Название источника	Инструмент	Дата начала	Всего уязвимостей		Статус				
appscreener	issuespath	Scoring01 http://code.int.ximi.group:8095/	08/04/2025 17:25			• Не выполнен		E	)	
						Ошибка: ASOC-1067: CodeScori >>				
appscreener	issuesnexus	Scoring01 http://code.int.ximi.group:8095/	08/04/2025 17:23			• Не выполнен		E	)	
						Ошибка: ASOC-1075	5: CodeS	cori >>		
appscreener	issuesnexus	Scoring01 http://code.int.ximi.group:8095/	08/04/2025 15:23			• Не выполнен		E	)	
						Ошибка: ASOC-1075	5: CodeS	cori >>		
appscreener	issuesnexus	Scoring01 http://code.int.ximi.group:8095/	08/04/2025 15:07			• Не выполнен		E	)	
						Ошибка: ASOC-1075	5: CodeS	cori >>		
appscreener	asocCore	Scoring01 http://code.int.ximi.group:8095/	08/04/2025 15:02	128		• Выполнен	坐 Скач	ать	)	

Рис. 47

#### 4.5.10. Контроль качества проекта

Конвейеры безопасности и проверки безопасности могут содержать один или несколько Контролей качества, информация о которых представлена в разделе **Проекты** → *<Название проекта>* → **Контроль качества** (Рис. 48).

≡ ⊕	Проекты → TESTISSU	ES1 → Контроль качества		
	Обзор Конвейеры безопасности Результаты (	сканирования Контроль качества Проблемы безопасности Библиотека зависимостей Параметры проекта		
89 Информационная панель			Поиск	۹ 🕸 🛛
🗅 Проекты	Конвейер безопасности	Имя шаблона		
(Д) Проблемы безопасности	appscreener	Добавить контроль		
<ul> <li>Библиотека зависимостей</li> <li>Контроль качества</li> </ul>	testAnxolerd https://github.com/anxolerd/dvpwa	Добавить котроль		
Правила О Правила безопасности	scaauth http://appsint.tronasoc.ru/app/api/v1			
<ul> <li>Правила дедупликации</li> </ul>	testAnxolerd https://github.com/anxolerd/dvpwa	<b>Добавить</b> контроль		
Д. Правила реагирования	scaauth http://apps.int.tronasoc.ru/app/api/v1			
Администрирование & Управление доступом	issuesappurl http://www.itsecgames.com	Дрбавить контроль		
🗘 Интеграции 🕒 Отчеты	dastauth http://apps.int.tronasoc.ru/app/api/v1			
🗄 Журнал событий	issuesgitcore https://ximilab.gitlab.yandexcloud.net/ximidev/tron	Добавить контроль		
С. Конструктор полей	issuescodescoring			
Параметры 🛞 Параметры подключения	asocCore	Добавить контроль		
⑦ О программе	issuescodescoring http://code.int.ximi.group.8095/	·		
දී admin	asocCore https://ximilab.gitlab.yandexcloud.net/ximidev/tron	+ Добавить контроль		

Рис. 48

На данной вкладке доступно управление привязкой контролей качества к пайплайну и чеку с возможностью установить правило действия выбранного контроля (информационное оповещение о провале гейта или блокирование merge-request'a до устранения ошибок).

Для того, чтобы добавить Контроля качества, необходимо выполнить следующие шаги:

- 1. В разделе **Проекты** → *<Название проекта>* → **Контроль качества** нажать на кнопку **Добавить контроль.**
- 2. В раскрывшемся списке (Рис. 49) выбрать требуемый контроль или нажать на кнопку **Создать новый контроль качества** (в данном случае, откроется форма создания нового контроля (Рис. 50)).

Проекты > TESTISSUES1 > Контроль качества Обзор Конведеры безопасности Результаты сканирования Контроль качества Проблемы безопасности Библиотека зависимостей Параметры проекта									
Corpuserts S Ormeea									
Конвейер безопасности	Имя шаблона								
appscreener	Выберите из списка		^						
testAnxolerd https://github.com/anxolerd/dvpwa scaauth http://apps.inttronasoc.ru/app/api/v1 testAnxolerd https://github.com/anxolerd/dvpwa scaauth http://apps.inttronasoc.ru/app/api/v1 issuesapput	123123 12345 123456 222222 2223123132 52565 56565 56566								
dastauth http://apps.int.tronasoc.ru/app/api/v1	Создать новый контроль качества								

Рис. 49

Проекты → TESTISSUES1 → Контроль качества	Создать контроль качества ×
Обзор Конвейеры безопасности Результаты сканирования Контроль качества Проблемы безопасности Библиотека зависимосте	Hassauve แลก็กาษа <b>*</b> ()
🛱 Сохранять 🔊 Отмена	
Конвейер безопасности Имя шаблона	
аppscreener Добажить контроль	
testAnxolerd https://github.com/anxolerd/dvpwa	
scaauth http://apps.int.tronasoc.ru/app/api/v1	
testAnxolerd <u>Aofaauna kompona</u> https://github.com/anxolerd/dvpwa	
scaauth http://apps.int.tronasoc.ru/app/api/v1	
Issuesappurl Actions Kompone http://www.issecgames.com	
dastauth http://apps.int.tronasoc.ru/app/api/v1	
issuesgitcore Actions https://ximilab.gitlab.yandexcloud.net/ximidev/tron	
issuescodescoring http://code.int.ximi.group:8095/	
asocCore Actions Action	
Issuescodescoring http://code.int.ximi.group:8095/	
asocCore + [	Создать Отмена

Рис. 50

3. Нажать на кнопку Сохранить.

Результаты прохождения Контролей качества можно отследить в проекте в конвейерах и проверках безопасности.

## 4.6. Проблемы безопасности

В разделе **Проекты** → *<Название проекта>* → **Проблемы безопасности** (Рис. 51) (или в разделе **Проблемы безопасности** из главного меню слева) отображаются все найденные в проекте уязвимости, их уровень критичности и дополнительная информация (каким инструментом и где найдены, CWE и CVE, статусы проблем безопасности и примененные правила).

≡⊕	Проекты 🔿 🗋	TESTISSUES1	<ul> <li>Проблем</li> </ul>	ы безопасно	сти				
	Обзор Конвейеры безопаса	ности Результаты сканирова	ния Контроль качества	Проблемы безопасности	Библиотека зависимостей	Параметры проекта			
응 Информационная панель	+ Создать правило безопас	ности 🛛 🖸 Создать задачи	из проблем					Поиск	९ 🔹 🗸
🗅 Проекты	<ul> <li>ID уязвимости ~</li> </ul>	Категория 🗸	Уровень критичности   ~	Обнаружено с помощ 🗸	CWE ~	CVE ~	Статус 🗸	Правило безопасности 🗸	Сканируемый объект 🗸
() Проблемы безопасности		Container os misconfigurat	Низкий 🗸	Kaspersky Container Secu			• Новый ∨		nexus.int.ximi.group:8083/a soc-core:develop
<ul> <li>Библиотека зависимостей</li> <li>Контроль качества</li> </ul>	TESTISSUES-100	Container os misconfigurat ion	Высокий 🗸	Kaspersky Container Secu			• Новый ~		nexus.int.ximi.group:8083/a soc-core:develop
Правила О Правила безопасности	TESTISSUES-136	Container os dependency vulnerability	Средний 🗸	Kaspersky Container Secu		CVE-2025-22866	• Новый ∨		nexus.int.ximi.group:8083/a soc-core:develop
Правила дедупликации	TESTISSUES-34	Container os dependency vulnerability	Средний 🗸	Kaspersky Container Secu		CVE-2024-45341	• Новый 🗸		nexus.int.ximi.group:8083/a soc-core:develop
Администрирование		Container os dependency vulnerability	Средний 🗸	Kaspersky Container Secu		CVE-2024-45336	• Новый ~		nexus.int.ximi.group:8083/a soc-core:develop
83 Управление доступом О Интеграции	TESTISSUES-69	Container os dependency vulnerability	Средний 🗸	Kaspersky Container Secu	CWE-674	CVE-2024-34158	• Новый 🗸		nexus.int.ximi.group:8083/a soc-core:develop
В Отчеты	TESTISSUES-116	Container os dependency vulnerability	Средний 🗸	Kaspersky Container Secu		CVE-2024-34155	• Новый ~		nexus.int.ximi.group:8083/a soc-core:develop
<ul> <li>Е) Журнал событий</li> <li>С. Конструктор полей</li> </ul>		Container os dependency vulnerability	Средний 🗸	Kaspersky Container Secu		CVE-2024-24791	• Новый 🗸		nexus.int.ximi.group:8083/a soc-core:develop
Параметры Параметры подключения		Container os dependency vulnerability	Средний 🗸	Kaspersky Container Secu		CVE-2024-24789	• Новый ~		nexus.int.ximi.group:8083/a soc-core:develop
⑦ О программе	TESTISSUES-25	Container os dependency vulnerability	Средний 🗸	Kaspersky Container Secu		CVE-2024-24785	<ul> <li>Новый ∨</li> </ul>		nexus.int.ximi.group:8083/a soc-core:develop
admin	Всего 10248 / Выбрано 0						<	1 2 3 1025	> 10/страница ч

Рис. 51

По каждой найденной проблеме предусмотрена возможность получить дополнительную информацию в окне детального просмотра уязвимости (Рис. 52). Для просмотра необходимо нажать на **ID уязвимости**.

Проекты · TESTISSUES1 · Пробл Container os misconfiguration ×								
Обзор Конвейеры безопас	ности Результаты сканировани	ия Контроль каче	Информация Описание	История Дубликаты Библиотека зависимостей Созданные задачи				
+ Создать правило безопас	сности 📔 🖸 Создать задачи и	із проблем	ID уязвимости Категория	TESTISSUES-100 🗇 Container os misconfiguration				
П уязвимости ч	Категория 🗸	Уровень критичност	Статус	• Новый 🗸				
	Container os misconfigurat	Низкий 🗸	Уровень критичности	Высокий 🗸				
TESTISSUES-100	Container os misconfigurat	Высокий 🗸	Обнаружено с помощью Сканируемый объект –	Kaspersky Container Security nexus.int.ximi.group:8083/asoc-core:develop				
TESTISSUES-136	Container os dependency vulnerability	Сродний 🗸	Проект Действия	Создать правило безопасности				
TESTISSUES-34 D	Container os dependency vulnerability	Средний 🗸						
	Container os dependency vulnerability	Средний 🗸			Пока нет комментариев			
TESTISSUES-69	Container os dependency vulnerability	Средний 🗸						
TESTISSUES-116	Container os dependency vulnerability	Средний 🗸						
TESTISSUES-115 O	Container os dependency vulnerability	Средний 🗸						
TESTISSUES-52	Container os dependency vulnerability	Средний 🗸						
TESTISSUES-25	Container os dependency vulnerability	Средний 🗸						
Всего 10248 / Выбрано 0					Введите комментарий			

Рис. 52

Также предусмотрены следующие возможности:

- Возможность оставлять комментарии, просматривать комментарии других пользователей. Раздел комментариев находится в окне детального просмотра проблемы безопасности
- Видимость статусов проблем безопасности (Новый, В работе, Ложноположительный, Подтвержденный, Исправлено, Исключено, Вручную, Дубликат). Статусы можно изменять при просмотре списка найденных проблем, а также в окне детального просмотра.
- Фильтрация по доступным атрибутам. Для настройки необходимо нажать

на кнопку 🚺 и выбрать требуемые настройки фильтрации (Рис. 53).

Проекты > 1	Проекты  · TESTISSUES1 · Проблемы безопасности							Фильтры Найдено элементов: 10248	
Обзор Конвейеры безопасн	юсти Результаты сканирова	ния Контроль качества	Проблемы безопасности	Библиотека зависимостей	Параметры проекта				
+ Создать правило безопас	+ Создать правило безопасности 🛛 🕑 Создать задачи из проблем								
<ul> <li>ID уязвимости ~</li> </ul>	Категория 🗸	Уровень критичности 🗸	Обнаружено с помощ 🗸	CWE ~	CVE v	Статус ~	Категория	Все значения	
	Container os misconfigurat ion	Низкий 🗸	Kaspersky Container Secu			• Новый ~	Уровень критичности	Все значения	<b>`</b>
TESTISSUES-100	Container os misconfigurat ion	Высокий 🗸	Kaspersky Container Secu			• Новый 🗸	Обнаружено с помощью	Все значения	<b>`</b>
TESTISSUES-136	Container os dependency vulnerability	Средний 🗸	Kaspersky Container Secu		CVE-2025-22866	• Новый ∨	CWE	Все значения	~
TESTISSUES-34	Container os dependency	Средний 🗸	Kaspersky Container Secu		CVE-2024-45341	• Новый ~	CVE	Все значения	×
TESTISSUES-18	Container os dependency vulnerability	Средний 🗸	Kaspersky Container Secu		CVE-2024-45336	• Новый ∨	Правило	Все значения	×
TESTISSUES-69	Container os dependency vulnerability	Средний 🗸	Kaspersky Container Secu	CWE-674	CVE-2024-34158	• Новый ∨	сканируемый	Все значения	~
TESTISSUES-116	Container os dependency vulnerability	Средний 🗸	Kaspersky Container Secu		CVE-2024-34155	• Новый ~	OUDERT		
TESTISSUES-115	Container os dependency vulnerability	Сродний 🗸	Kaspersky Container Secu		CVE-2024-24791	• Новый ~			
TESTISSUES-52	Container os dependency vulnerability	Средний 🗸	Kaspersky Container Secu		CVE-2024-24789	• Новый ∨			
TESTISSUES-25	Container os dependency vulnerability	Средний 🗸	Kaspersky Container Secu		CVE-2024-24785	• Новый ∨			
Всего 10248 / Выбрано 0							Применить	Отмена	

Рис. 53

- Возможность создания задач в трекере на основе выявленных проблем безопасности. Для создания задач необходимо выполнить следующие шаги:
  - а. В разделе Проекты → <Название проекта> → Проблемы
     безопасности или в разделе Проблемы безопасности из
     главного меню слева выбрать уязвимости из списка с помощью

чекбоксов	$\Box$	(Рис.	54	).
-----------	--------	-------	----	----

Пр	Проекты · TESTISSUES1 · Проблемы безопасности											
Oốs	Обзор Конвейеры безопасности Результаты сканирования Контроль качества Проблемы безопасности Библиотека зависимостей Параметры проекта											
+	+ Создать правило безопасности 🛛 Создать задачи из проблем											
۰	ID уязвимости ∨	Категория 🗸	Уровень критичности 🗸	Обнаружено с помощ 🗸	CWE ~	CVE v	Статус 🗸					
	TESTISSUES-55 O	Container os misconfigurat ion	Низкий ∨	Kaspersky Container Secu			• Новый ∨					
	TESTISSUES-100	Container os misconfigurat ion	Высокий 🗸	Kaspersky Container Secu			• Новый ∨					
	TESTISSUES-136	Container os dependency vulnerability	Средний 🗸	Kaspersky Container Secu		CVE-2025-22866	• Новый ∨					
0	TESTISSUES-34	Container os dependency vulnerability	Средний 🗸	Kaspersky Container Secu		CVE-2024-45341	• Новый ∨					



- b. Далее нажать на кнопку Создать задачи из проблем.
- с. В открывшемся окне выбрать Трекер задач (Инструкцию по созданию трекера см. Руководство администратора) и заполнить поле Название задачи (Или Префикс задач, в зависимости от настроек трекера задач), и выбрать Тип задачи (Рис. 55).

Проблем	ы безопасности		Создать задачи из проблем					
Проблемы безопа	сности Исключенные проблемы безог	асности	Выбранные проблемы	2 Показать списком				
+ Создать прав	ило безопасности 🛛 🖸 Создать задач	ни из проблем	Трекер задач*	Jira tracker	~			
ID уязвимости	I – Категория –	Уровень критичности  ~	Обнаружено с помо 👻	CWE ~	CVE ~		Все выбранные проблемы безопасности будут объединены в общую задачу	
С кссс-52 С	Use of Hard-coded Passw ord	Низкий 🗸	PT Application Inspector	CWE-259		Название задачи*	Введите название	
🛛 кссс-16 🗇	Use of Hard-coded Passw ord	Средний 🗸	PT Application Inspector	CWE-259		Тип задачи*	Тип задачи по умолчанию	~
кссс-за П	Use of Hard-coded Passw ord	Низкий 🗸	PT Application Inspector	CWE-259				
С кссс-53 Ф	Use of Hard-coded Passw ord	Низкий ∨	PT Application Inspector	CWE-259				
С кссс-26	Use of Hard-coded Passw ord	Низкий ∨	PT Application Inspector	CWE-259				
С кссс-23	Use of Hard-coded Passw ord	Низкий ∨	PT Application Inspector	CWE-259				
С кссс-33	Use of Hard-coded Passw ord	Низкий ∨	PT Application Inspector	CWE-259				
С кссс-6 Ф	Use of Hard-coded Passw ord	Низкий 🗸	PT Application Inspector	CWE-259				
О кссс-41 Ф	Use of Hard-coded Passw	Низкий ∨	PT Application Inspector	CWE-259		Создать Отмена		

Рис. 55

d. Нажать на кнопку Создать.

## 4.7. Библиотека зависимостей

Раздел Библиотека зависимостей представляет информацию по зависимостям в проектах (Рис. 56).

≡ ⊕	Библиотека завис	имостей								
						Поиск		۹	\$ 7	7
00.16	Название	Версия	Тип	Происхождение	Проблемы безопасности	~	Проект			
С Проекты	abbrev	111	Библиотека	Code	0					
троблемы безопасности	accepts	1.3.7	Библиотека	Code	0					
Библиотека зависимостей	acom	4.0.13	Библиотека	Code	0					
<ul> <li>Контроль качества</li> </ul>	acom	7.3.1	Библиотека	Code	0					
Правила	acom	3.3.0	Библиотека	Code	0					
О Правила безопасности	acom-globais	3.1.0	Библиотека	Code	0					
😐 Правила дедупликации	acom-node	1.8.2	Библиотека	Code	0					
Ф. Правила реагирования	acom-walk	7.2.0	Библиотека	Code	0					
Администрирование	after	0.8.2	Библиотека	Code	0					
83 Управление доступом	ajv	6.12.3	Библиотека	Code	0					
🗘 Интеграции	Boero 1003					( 1 2	3 101 >	10 / ctp	аница 🗸	
р отчеты В Уляция собщий										
<ul> <li>Домошник</li> </ul>										
(). Конструктор полей										
Папаметры										
Параметры подключения										
④ О программе										
≗ admin										

Рис. 56

Предусмотрена возможность просмотра детализированной информации по зависимостям (Рис. 57).

Рис. 57

## 4.8. Контроль качества

Платформа позволяет создавать и настраивать точки контроля качества ПО для каждого конвейера безопасности и проверки безопасности. Раздел **Контроль качества** позволяет пользователям управлять шаблонами контроля качества и отслеживать метрики, которые применяются для оценки качества программного обеспечения и выявления возможных отклонений от норм. К каждому конвейеру и проверке безопасности можно добавить один или несколько контролей качества, если это необходимо в рамках проекта.

≡ ⊕	Контроль качества					
	+ Добавить контроль качества 🌐 Удалить				Поиск	Q 🏶 🕅
29 Информационная панель	Название шаблона	Количество метрик 🗸	Проекты	Автор		
Сі Проекты	123123	1	<ul> <li>Привязанные проекты отсутствуют</li> </ul>	testproject	O	Û
Д Проблемы безопасности	12345	1	Привязанные проекты отсутствуют	testproject	0	Û
<ul> <li>Библиотека зависимостей</li> <li>Контроль качества</li> </ul>	123455	0	<ol> <li>Привязанные проекты отсутствуют</li> </ol>	testproject	Ø	Û
Правила	222222	0	TESTDAY1, ISSUETESTING20241212T141731439 Z, MAGO	admin	D	Û
<ul> <li>Правила безопасности</li> <li>Правила дедупликации</li> </ul>	22223123132	1	Привязанные проекты отсутствуют	admin	0	Û
Д Правила реагирования	52555	0	Привязанные проекты отсутствуют	testproject	0	Û
Администрирование 85 Управление доступом	5555	0	<ul> <li>Привязанные проекты отсутствуют</li> </ul>	admin	0	Û
🗘 Интеграции	565656	0	<ul> <li>Привязанные проекты отсутствуют</li> </ul>	admin	0	Û
Отчеты Е Журнал событий	basic	2	TESTDAY1, ISSUETESTING20241212T141731439 Z, QARG2	admin	D	Û
(). Конструктор полей	<ul> <li>by appscreener</li> </ul>	0	<ul> <li>Привязанные проекты отсутствуют</li> </ul>	admin	0	D
Параметры இ Параметры подключения	Всего 35 / Выбрано 0				< 1 2 3 4 >	10/страница 🗸
⑦ О программе						
은 admin						

Рис. 58

Таблица шаблонов контролей качества (Рис. 58) содержит список шаблонов, которые уже созданы и используются в системе. Поля таблицы следующие:

- Название шаблона это имя шаблона контроля качества.
- Количество метрик показывает количество метрик, которые используются в данном шаблоне контроля качества.
- Проекты список проектов, к которым привязан данный шаблон.
   Щелкнув по View, можно увидеть проекты, к которым применен этот шаблон.
- Автор отображает имя пользователя, который создал данный шаблон.

В таблице доступна сортировка шаблонов по количеству метрик, названию или автору. Также возможно редактировать контроли качества. Для этого

необходимо нажать на кнопку редактирования 🦉 и внести изменения в открывшейся форме (Рис. 59).

K	Контроль качества			Редактировать контроль качества ×					
+	- Добавить контроль качества 📋 Удалить			Название шаблона* 🛈					
	Название шаблона	Количество метрик 🗸	Проекты	123123					
	123123	1	<ul> <li>Привязанные проекты отсутству</li> </ul>	тві Метрика ()		Пороговое значение			
	12345	1	Привязанные проекты отсутству	Уровень критичности/Высоки 🗸	Не меньше 🗸	123123			
0	123455	0	Привязанные проекты отсутству	Добавить метрику					
0	222222	0	TESTDAY1, ISSUETESTING2024121: Z, MAGO						
0	22223123132	1	Привязанные проекты отсутству						
0	52555	0	Привязанные проекты отсутству						
0	5555	0	Привязанные проекты отсутству						
0	565656	0	Привязанные проекты отсутству						
0	basic	2	TESTDAY1, ISSUETESTING2024121: Z, QARG2						
0	by appscreener	0	Привязанные проекты отсутству						
Bce	го 35 / Выбрано О								
				Сохранить Отмена					

Рис. 59

#### 4.8.1. Добавление нового контроля качества

Чтобы добавить новый шаблон контроля качества, необходимо нажать кнопку **Добавить контроль качества** и в открывшейся форме указать название шаблона (Рис. 60).

Контроль качества	L. C.		Создать контроль качества
+ Добавить контроль качества			Название шаблона* ()
Название шаблона	Количество метрик 🗸	Проекты	
123123	1	<ul> <li>Привязанные проекты отсутству</li> </ul>	
12345	1	Привязанные проекты отсутству	
123455	0	<ol> <li>Привязанные проекты отсутству</li> </ol>	
222222	0	TESTDAY1, ISSUETESTING2024121: Z, MAGO	
22223123132	1	Привязанные проекты отсутству	
52555	0	Привязанные проекты отсутству	
5555	0	Привязанные проекты отсутству	
565656	0	Привязанные проекты отсутству	
basic	2	TESTDAY1, ISSUETESTING2024121: Z, QARG2	
by appscreener	0	Привязанные проекты отсутству	
Всего 35 / Выбрано О			
			Создать Отмена

Рис. 60

Созданный шаблон необходимо отредактировать с помощью кнопки

редактирования 🧖, задать необходимые метрики для отслеживания качества и сохранить шаблон (Рис. 59).

Удаление шаблонов производится с помощью кнопки удаления 🔟 в списке шаблонов.

## 4.9. Правила безопасности

Система предоставляет возможность создания правил исключения для работы с результатами в продукте. Страница **Правила безопасности** предназначена для управления правилами безопасности, которые применяются к уязвимостям и другим проблемам безопасности в проектах (Рис. 61). Это позволяет временно или постоянно игнорировать определенные типы проблем, исходя из их приоритета или иных критериев. Логика работы с правилами позволяет настраивать время действия правила (на заданное время или навсегда), а также область действия (по проектам).

E ⊕	Правила бе + добавить правило б	ЗОПАСНОСТИ езопасности	I						Поиск	Q	\$	V
	Название ч	Категория ч	Компонент ч	CVE ~	CWE ~	Статус 🗸	Число применений 🗸	Время истечения с.	🗸 Область 🗸			
22 Информационная панель	test1	Container os dependen	CLICustomSource_202	CVE-2021-32256	CWE-787	• Не активен	0		Просмотреть	0	Û	
ф Проблемы безопасности	TESTSUPRESS	X-Content-Type-Optio				• Активен	210	2025-04-09	Просмотреть	0	0	
П Библиотека зависимостей	TESTSUPRESS1	X-Content-Type-Optio				• Активен	252	2025-04-09	Просмотреть	-	-	
Контроль качества										U		
Правила	p787	Container os dependen	nexus.int.ximi.group:80	CVE-2020-19186	CWE-787	<ul> <li>Не активен</li> </ul>	1		Просмотреть	0	Û	
Правила безопасности	Suppress Rule for project = ae4a0ac6-4910-4739-a	Log Forging				• Не активен	90		Просмотреть	O	Û	
О Правила дедупликации	eac-dd8e0bd6e025											
	правило	Ssl parameter				• Не активен	0		Просмотреть	O	Û	
Администрирование & Управление доступом	555	Use of Hard-coded Pas				• Не активен	0		Просмотреть	0	٥	
💭 Интеграции	Cynnpecc KCS Container	Container os dependen	nexus.int.ximi.group:80	CVE-2024-24790		• Не активен	3	2024-10-29	Просмотреть	0	0	
🔒 Отчеты	os Critical CVE20242479 0 stdlib									-	-	
<ul> <li>Е) Журнал событий</li> <li>С. Конструктор полей</li> </ul>	Suppress Rule5 for projec t = ISSUETESTING202412	Container os dependen			CWE-476	• Не активен	0		Просмотреть	0	Û	
Параметры В Параметры подключения	Suppress Rule3 for projec t = ISSUETESTING202412 12T142220998Z	Empty Default Exceptio				• Не активен	0		Просмотреть	0	Û	
	Bcero 53							<	1 2 3 6 >	10/cT	раница	~
≗ admin												

Рис. 61

Столбцы таблицы правил безопасности (Рис. 61):

- Название название или идентификатор правила безопасности.
- Категория категория проблемы, к которой применяется правило безопасности.
- Компонент компонент системы или путь к репозиторию
- СVE уникальный идентификатор уязвимости в базе данных CVE.
- СWE код CWE (Common Weakness Enumeration), который описывает тип уязвимости.
- Статус статус активности правила.
- Число применений количество проблем, к которым данное правило было применено.
- Время истечения срока действия срок действия правила.
- Область область проектов.

#### 4.9.1. Создание правила безопасности

Создание правила безопасности происходит на основании указанных параметров. Набор параметров зависит от типа проблемы безопасности. При помощи правил безопасности можно также централизованно управлять статусами обнаруженных проблем безопасности, которые будут подчиняться этому правилу.

Для создания нового правила необходимо выполнить следующие шаги:

- 1. В разделе Правила безопасности нажать на кнопку Добавить правило.
- 2. В открывшейся форме (Рис. 62) ввести необходимые данные:
  - а. Уникальное название для создаваемого правила безопасности.
  - b. Тип проблемы безопасности
  - с. Инструмент, использованный для обнаружения проблемы безопасности.
  - d. Выбрать категорию проблемы безопасности.
  - е. Компонент системы или путь, где была обнаружена проблема.
  - f. Идентификатор уязвимости из базы данных CVE
  - g. CWE для описания конкретного типа уязвимости.
  - h. Путь к файлу или директории в репозитории, где была найдена проблема.
  - і. Источник обнаружения
  - ј. Период, в течение которого правило безопасности будет активно.
     Это может быть фиксированная дата окончания действия правила, или оно может быть бессрочным.
  - к. Статус проблемы безопасности
  - I. Область применения (проекты)

Правила бе	зопасности	Создать правило безопасности						
+ Добавить правило б	езопасности							Название* 🛈
Название ~	Категория 🗸	Компонент ~	CVE ~	CWE ~	Статус 🗸	Число применений 🗸	Время и	
test1	Container os dependen	CLICustomSource_202	CVE-2021-32256	CWE-787	• Не активен	0		Тип проверки безопасности
TESTSUPRESS	X-Content-Type-Optio				• Активен	210	2025-04	Инструмент ()
TESTSUPRESS1	X-Content-Type-Optio				• Активен	252	2025-04	· · ·
p787	Container os dependen	nexus.int.ximi.group:80	CVE-2020-19186	CWE-787	• Не активен	1		Категория*
Suppress Rule for project = ae4a0ac6-4910-4739-a eac-dd8e0bd6e025	Log Forging				• Не активен	90		Компонент
правило	Ssi parameter				• Не активен	0		CVE
555	Use of Hard-coded Pas				• Не активен	0		CWE
Cynnpecc KCS Container os Critical CVE20242479 0 stdlib	Container os dependen	nexus.int.ximi.group:80	CVE-2024-24790		• Не активен	3	2024-10	Путь
Suppress Rule5 for projec t = ISSUETESTING202412 12T142220998Z	Container os dependen			CWE-476	• Не активен	0		Код уязвимости
Suppress Rule3 for projec t = ISSUETESTING202412 12T142220998Z	Empty Default Exceptio				• Не активен	0		Статус проблемы безопасности*
Bcero 53								Создать Отмена

Рис. 62

3. После заполнения нажать на кнопку Создать.

## 4.10. Правила дедупликации

Правила дедупликации предназначены для работы над объединением и удалением дубликатов записей в системе путем настройки правил сравнения данных. Он позволяет автоматически находить и объединять повторяющиеся записи, снижая количество избыточной информации.

≡ ⊕	Правила дедупликации				
	+ Добавить правило дедупликации			Поиск	Q 🕸 🛛
90 Мифоризиионизе приель	Название =	Метод	Статус ~		
С Проекты	123	По комбинированным полям	• Не активен	0	
Проблемы безопасности	aunder	По комбинированным полям	• Не активен	Ø Û	
<ul> <li>Библиотека зависимостей</li> <li>Контроль качества</li> </ul>	autocomplit	С помощью правил сопоставления	Не активен	Ø Û	
Правила	DD QARG2 2	С помощью правил сопоставления	• Не активен	0 0	
О Правила безопасности	DD RG KCS	По комбинированным полям	• Не активен	0 0	
<ul> <li>Правила дедупликации</li> <li>Правила реагирования</li> </ul>	DDRULE1 QATEST	По комбинированным полям	• Не активен	0 0	
Администрирование	DDrule2	С помощью правил сопоставления	• Не активен	0 0	
85 Управление доступом Онтеграции	DEDUBLICATION70	С помощью правил сопоставления	• Не активен	0 0	
🛯 Отчеты	DEFAULT	По комбинированным полям	• Не активен	0 0	
Е Журнал событий	ISSUETESTING20241106T091754941Z12256	На основе существующей проблемы безопасности	<ul> <li>Не активен</li> </ul>	0	
	Bcero 30			< 1 2 3 >	10/страница 🗸
இ Параметры подключения					
⑦ О программе					
은 admin					

Рис. 63

Таблица (Рис. 63) содержит список существующих правил дедупликации с возможностью сортировки и просмотра подробной информации, содержит следующие параметры:

- Название имя правила.
- Метод способ дедупликации. Возможные методы:
  - С помощью правил сопоставления дедупликация выполняется на основе предварительно заданных критериев сопоставления.
  - По комбинированным полям дедупликация выполняется по набору полей, таких как CVE, CWE или другие параметры.
  - На основе существующей проблемы безопасности
- Статус указывает, активно ли правило в данный момент.

#### 4.10.1. Поиск дубликатов

Дубликаты возможно посмотреть в разделе **Проблемы безопасности**. Для этого необходимо выполнить следующие шаги:

- 1. Перейти в **Проекты** → <*Название проекта*> → **Проблемы безопасности**.
- 2. Найти и открыть проблему безопасности, к которой может относиться дедупликация.
- 3. В открывшемся окне выбрать вкладку Дубликаты.

В списке отобразятся записи, отмеченные как дубликаты, с их ID, названием правила и статусом.

Также возможно добавить дубликат вручную или отменить дедупликацию, используя соответствующие кнопки внизу страницы.

#### 4.10.2. Создание правил дубликатов

Для создания нового правила необходимо выполнить следующие шаги:

- 1. В разделе **Правила дедупликации** нажать на кнопку **Добавить правило дедупликации**.
- 2. В открывшейся форме (Рис. 64) необходимо указать метод дедупликации, категорию полей для сопоставления и дополнительные параметры, зависящие от выбранного метода.

Правила дедупликации	Создать правило дедупликации				
+ Добавить правило дедупликации			Имя правила* ①		
Название 💷	Метод	Статус 🗸	Метод*	Выберите метод	~
123	По комбинированным полям	• Не активен	Сгруппированные проекты	Выберите проект	~
aunder	По комбинированным полям	• Не активен			
autocomplit	С помощью правил сопоставления	• Не активен			
DD QARG2 2	С помощью правил сопоставления	• Не активен			
DD RG KCS	По комбинированным полям	• Не активен			
DDRULE1 QATEST	По комбинированным полям	• Не активен			
DDrule2	С помощью правил сопоставления	• Не активен			
DEDUBLICATION70	С помощью правил сопоставления	• Не активен			
DEFAULT	По комбинированным полям	• Не активен			
ISSUETESTING20241106T091754941Z12256	На основе существующей проблемы безопасности	• Не активен			
Bcero 30					
			Создать Отмена		

Рис. 64

3. Нажать на кнопку Создать.

## 4.11. Правила реагирования

Правила реагирования необходимы для настройки конкретных уведомлений и отправки их в соответствующие инструменты. В данном инструменте возможно автоматизировать отправку проблем безопасности в уже созданную интеграцию с трекером задач. Также возможно настроить автоматическую отправку событий на адрес электронной почты группе лиц.

#### 4.11.1. Создание правила реагирования

Для создания правила реагирования, необходимо выполнить следующие шаги:

1. Перейти в раздел Правила реагирования.

≡ ⊕	Правила реаги	рования									
	+ Добавить правило реагирова	эния					Поиск		۹	\$ 1	V
90 Mutonusuuse asuaa	Название правила 😑	Статус	Тип реагирования	Инструмент	Проекты	Автор					
<ul> <li>Проекты</li> </ul>	responceRule	Не активен	Ф Оповещение	testNotifier	TESTOVSS	ədmin		0	Û		
∰ Проблемы безопасности Ш Библиотека зависимостей	responceRule1	💽 Активен	Ф Оповещение	testNotifier	Все проекты	admin		0	Û		
⊘ Контроль качества	test12	Не активен	Ф Опсвещение	testNotifier	Все проекты	admin		0	Û		
Правила О Правила безопасности	test121	Не активен	Ф Оповещение	testNotifier	Все проекты	admin		0	Û		
<ul> <li>Правила дедупликации</li> <li>Правила реалирования</li> </ul>	testTask	💽 Активен	🖸 Создание задач	testTracker	TESTSUPRESS	admin		0	Û		
Администрирование	tracker88	Не активен	Создание задач	Jira tracker	DEDUBLICATION	admin		0	Û		
35 Управление доступом О Интеграции	еуыеі	Пе активен	Ф Оповещение	testNotifier	Все проекты	admin		0	Û		
<ul> <li>Отчеты</li> <li>Журнал событий</li> </ul>	Bcero 7						< 1	· [	10 / стр	зница м	~
🕻 Конструктор полей											
Параметры (© Параметры подключения											
⑦ О программе											
≗ admin											

2. Далее нажать на кнопку Добавить правило реагирования (Рис. 65).

Рис. 65

- 3. Далее в открывшейся форме (Рис. 66) необходимо заполнить следующие поля:
  - Имя проекта
  - Описание (опционально)
  - Проекты в рамках каких проектов будут собираться события или проблемы безопасности
  - Тип реагирования выбор типа реагирования

Правила реаг	Правила реагирования					Создать правило реагирования ×			
+ Добавить правило реагир	оования				Hannaurol	Rearing upper uppe			
Название правила 🚊	Статус	Тип реагирования	Инструмент	Проекты	пазвание	Введите название Название должно содержать от 4 до 255 символо только буквы (латинские или кириллические), циф	в и может включать иры и пробелы.		
responceRule	Не активен	Ф Оповещение	testNotifier	TESTCVSS	Описание	Введите описание			
responceRule1	Активен	Ф. Оповещение	testNotifier	Все проекты	Проекты	Выберите проект	~		
test12	Не активен	Ф Оповещение	testNotifier	Все проекты	Тип реагирования*	Ф Оповещение	оздание задач		
test121	Не активен	0.0000000000	testNotifier	Все проекты	События*	Выберите события			
		AL ONOBELLENIE			Инструмент	Выберите инструмент	~		
testTask	🚺 Активен	🖾 Создание задач	testTracker	TESTSUPRESS	оповещения				
tracker88	Не активен		Jira tracker		Добавление получ	чателей 🛈			
		El contanue antes		DEDUBLICATION	Пользователи	Выберите из списка	~		
еуые1	Не активен	Ф. Оповещение	testNotifier	Все проекты	Роли	Выберите из списка	~		
					Внешние адреса	example@example.com			
Bcero 7					SH. HOHE	Нажимайте ENTER после каждого адреса	,		
					Создать Отмена	)			

Рис. 66

• Если выбран тип **Оповещение** необходимо дополнить значениями следующих полей:

- События множественный выбор из списка событий системы
- Инструмент оповещения выбор из созданных интеграций Notify tool

Блок **Добавление получателей** заполняется при необходимости добавить больше получателей. Предусмотрено добавление конкретных пользователей (с помощью указанной почты в профиле), ролей (события будут отправляться пользователям с данной ролью). Также возможно добавить конкретные адреса электронной почты через в поле **Внешние адреса эл. почты** (Рис. 67).

Правила реаг	Правила реагирования					Создать правило реагирования ×				
+ Добавить правило реаги	рования				Hannaura					
Название правила 😑	Статус	Тип реагирования	Инструмент	Проекты	название*	Название должно содержать от 4 до только буквы (латинские или кипил	255 символов и может включать			
responceRule	Не активен	Ф Оповещение	testNotifier	TESTCVSS	Описание	Введите описание				
responceRule1	Активен	Ф Оловещение	testNotifier	Все проекты	Проекты	Выберите проект	#			
test12	Не активен	Ф. Оповещение	testNotifier	Все проекты	Тип реагирования•	Ф Оповещение	🛛 Создание задач			
test121	Не активен	О оповешение	testNotifier	Все проекты	События*	Выберите события				
testTask	С Активен	Создание задач	testTracker	TESTSUPPESS	Инструмент оповещения	• Выберите инструмент	~			
				1201001 11200	Добавление полу	учателей 🛈				
tracker88	Не активен	🕑 Создание задач	Jira tracker	DEDUBLICATION	Пользователи	Выберите из списка	~			
еуые1	Не активен	Оповещение	testNotifier	Все проекты	Роли	Выберите из списка	~			
					Внешние адреса	example@example.com				
Bcero 7						Нажимайте ENTER после каждого ад	peca			
					Создать Отмена	а				

Рис. 67

- Если выбран тип **Создание задач** (Рис. 68) необходимо дополнить значениями следующих полей:
  - Трекер задач выбор из созданных интеграций
  - Фильтры условия фильтрации для проблем безопасности.

Правила реагирования				Создать правило реагирования				
+ Добавить правило реагирования					Название* Введите название			
Название правила 😑	Статус	Тип реагирования	Инструмент	Проекты		Название должно содержать от 4 до 255 символов и может включать только буквы (латинские или кириллические), цифры и пробелы.		
responceRule	Не активен	Ф Оповещение	testNotifier	TESTOVSS	Описание	Введите описание		
responceRule1	С Активен	Ф. Оповещение	testNotifier	Все проекты	Проекты	Выберите проект 🗸		
test12	Не активен	Ф Оповещение	testNotifier	Все проекты	Тип реагирования*	Ф Оповещение	🕑 Создание задач	
test121	Не активен	Оповещение	testNotifier	Все проекты	Трекер задач*	Выберите трекер задач	~	
testTask	Активен	Создание задач	testTracker	TESTSUPRESS	Фильтры	due a		
tracker88	Не активен	Создание задач	Jira tracker	DEDUBLICATION	Категория	Все значения	•	
					Уровень критичности	Все значения	~	
еуые1	Не активен	Ф Оповещение	testNotifier	Все проекты	Обнаружено с помощы	все значения	~	
Bcero 7					CWE	Все значения	~	
					CVE	Все значения	~	
					Статус	Все значения	~	
					Сканируемый объект	Все значения	~	
					Создать Отмена	a		

Рис. 68

Данный тип реагирования позволяет гибко настроить отправку необходимых проблем безопасности в область трекера задач.

После заполнения формы создания правил реагирования необходимо нажать на кнопку Создать.

# 5. Отчеты

Страница **Отчеты** предназначена для управления и просмотра отчетов, содержащих данные о проектах и найденных в них уязвимостях. Отчеты отображаются в таблицах **Сводные** и **Детализированные**, в которых можно увидеть основную информацию и дату создания.

Также доступна сортировка по названию, дате создания. Для этого необходимо щелкнуть на заголовок соответствующего столбца (Название отчета или Создан).

Для каждого отчета доступны три формата скачивания: **PDF** (до трех проектов в одном отчете), **JSON** и **CSV**. Для загрузки отчета необходимо нажать на соответствующую кнопку рядом с отчетом (Рис. 69).

Чтобы удалить отчет, необходимо нажать на кнопку 🛄 и в открывшемся окне нажать Удалить.

Отчеты ASOC Сводные Дета Скачат testday1 30/03/2025 23:24 PDF U JSON U CSV 30/03/2025 23:22 (4) PDF (4) JSON (4) CSV 29/03/2025 16:25 (L) PDF (L) JSON (L) CSV 29/03/2025 16:21 (JJSON (J) CSV 05/11/2024 13:20 Û Report (29 projects) 08-07-2024 11-05-2024 (4) PDF (4) JSON (4) CSV ort (10 projects)\_10-28-2024\_11-05-2024 05/11/2024 13:20 (4) PDF (4) JSON (4) CSV ort (2 projects) 01-01-2000 10-31-2024 31/10/2024 13:35 H PDF JSON CSV n n Report 08-07-2024 10-31-2024 DEMO 31/10/2024 13:20 (4) PDF (4) JSON (4) CSV ort (3 projects)\_10-24-2024\_10-30-2024 30/10/2024 15:21 n (1) PDF (1) JSON (1) CSV ry Report (20 projects)\_10-24-2024\_10-30-2024 30/10/2024 11:19 n H PDF H JSON H CSV < 1 2 > 10/страница ~ Bcero 19

Рис. 69

# 6. Журнал событий

Раздел **Журнал событий** позволяет просматривать административные и функциональные события, которые совершают пользователи в системе, а также скачивать отчеты за выбранный период в формате CSV (Рис. 70). Для этого необходимо выполнить следующие шаги:

1. В разделе **Журнал событий** выбрать вкладку **Администрирование** или **Функциональные события**, в зависимости от требования.

≡⊕	Журнал событий						
	Администрирование Функциональные собития						
8 Информационная панель	Весь период Месяц Неделя День					🛓 Скачать отчет	г в формате CSV
🗅 Проекты	🗙 Сбросить фильтры					Поиск	۹
Проблемы безопасности	Дата события 🗐	IP Appec ~	Код события 🗸	Г Описание	Уровень критичности		т
Библиотека зависимостей	30/03/2025 23:24	10.150.132.6	ADM-4001	User admin created a report testdav1	3		
Контроль качества			Create Report				
Правила	30/03/2025 23:22	10.150.132.6	ADM-4001 Greate Report	User admin created a report testday	3		
Правила безопасности	30/03/2025 21:01	10.150.132.6	ADM-8002	User admin edited the project data	5		
Правила дедупликации			Project Data Edited	TESTDAY1.			
Ц Правила реагирования	30/03/2025 21:01	10.150.132.6	ADM-8002 Broket Data Edited	User admin edited the project data TESTDAY1	5		
Администрирование	30/03/2025 21:01	10 150 132 6	ADM-8002	User admin edited the project data	5		
О Интеграции			Project Data Edited	TESTDAY1.			
🗋 Отчеты	30/03/2025 21:00	10.150.132.6	ADM-8002 Project Data Edited	User admin edited the project data TESTDAY1.	5		
🗄 Журнал событий	30/03/2025 21:00	10.150.132.6	ADM-8002	User admin edited the project data	Б		
Э. Помощник			Project Data Edited	TESTDAY1.			
Конструктор полей	30/03/2025 20:58	10.150.132.6	ADM-8002 Project Data Edited	User admin edited the project data TESTDAY1.	5		
Параметры	30/03/2025 20:46	10.150.132.6	ADM-2008	Source testAnxolerd full settings	9		
Параметры подключения			Source full settings were viewed by user	viewed by admin			
④ О программе	30/03/2025 20:46	10.150.132.6	ADM-2007 Tool full settings were viewed by user	Tool appscreenerSCA full settings viewed by admin	9		
යි admin	Bcero 497				< 1 2	3 50 > 1	0/страница 🗸 🖣

Рис. 70

- 2. Выберите необходимый период, за который требуется построить отчет.
- 3. Нажмите кнопку **Скачать отчет в формате CSV**. После этого отчет автоматически загрузится локально на ПК.

# 7. Конструктор полей

Раздел Конструктор полей позволяет настроить пользовательские поля проектов (Рис. 71).

≡	Конструктор полей
	Konerpykrop IIonen
	Проект
	Системные поля
88 Информационная панель	Kon npoekta* 🕢
🗅 Проекты	Код проекта
та Проблемы безопасности	
Библиотека зависимостей	
Контроль качества	
Правила	Описание 🛈
О Правила безопасности	
💭 Правила дедупликации	
Д Правила реагирования	Теги Ф
Алимиистрипороцие	Выберите из списка 🗸 🗸
8 Управление доступом	
🗘 Интеграции	Пользовательские поля
В Отчеты	Дата старта проекта
🕄 Журнал событий	
— //: Помощник	Дата окончания проекта
🗋 Конструктор полей	
	Владелец проекта
Параметры	~
ез параметры подключения	Ссылка на Confluence
() O hpor pawwe	
≗ admin	Соблюдение Compliance

Рис. 71

Для настройки необходимо выполнить следующие шаги:

- 1. На странице Конструктор полей нажать кнопку Редактировать поля.
- В открывшемся окне справа (Рис. 72) скорректировать (добавить/удалить) представленный набор полей с помощью кнопок

Добавить поле и 👘.

	Название поля	Тип	Обяза	тельно
	Дата старта проекта	Дата	<b>v</b>	
	Дата окончания проекта	Дата	<b>v</b>	
	Владелец проекта	Список пользователей	•	
8	Ссылка на Confluence	Ссылка	•	
8	Соблюдение Compliance	Чекбокс	<b>v</b>	
	AppSec	Список пользователей	~ 0	

Рис. 72

- 3. Заполнить поля Название поля, Тип и Обязательное поле.
- 4. Далее нажать кнопку Создать.

# 8. Требования к аппаратным и программным характеристикам рабочего места пользователя

Характеристика	Минимальное значение	Рекомендуемое значение		
Процессор	4 ядра	8 ядер и более		
Оперативная память	16 ГБ	32 ГБ и более		
Жесткий диск	500 ГБ свободного места	Рекомендуется использование SSD для повышения производительности		
Сетевое соединение	Высокоскоростное интернет-соединение, минимум 1 Гбит/с			
Операционная система	<ul> <li>macOS: macOS 10.14 или более поздние версии.</li> <li>Linux: Современные дистрибутивы с поддержкой необходимых версий браузеров.</li> <li>Windows: Windows 10 или более поздние версии.</li> </ul>			
База данных	PostgreSQL 13 или более поздние версии	Рекомендуется настроить резервное копирование и восстановление данных.		
Браузер	Сhromium (Google Chrome, Edge, Safari и т. д.) и Firefox.			