

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

Руководство администратора

Апрель 2025

Содержание

Введение	4
1. Термины и определения	5
2. Общие сведения	7
3. Установка решения	9
3.1. Установка с помощью Docker Compose	9
3.2. Установка с помощью Helm Chart	10
4. Обновление решения	11
5. Удаление решения	11
6. Авторизация администратора	11
7. Описание интерфейса и функционала	14
7.1. Информационная панель	14
7.2. Проекты	15
7.3. Проблемы безопасности	15
7.4. Библиотека зависимостей	16
7.5. Контроль качества	16
7.6. Правила безопасности	17
7.7. Правила дедупликации	17
7.8. Правила реагирования	18
8. Настройки системы	19
8.1. Настройки правил авторизации пользователей	19
8.2. Управление пользователями и ролями	19
8.2.1. Добавление нового пользователя	20
8.2.2. Редактирование пользователя	21
8.2.3. Удаление пользователя	21
8.2.4. Сброс пароля	22
8.2.5. Настройка ролей	22
8.2.6. Добавление новой роли	23
8.2.7. Добавление группы пользователей	24
8.2.8. Аутентификация в LDAP	26
8.2.9. Метод аутентификации	27
9. Настройки интеграций	29
9.1. Инструменты безопасности	29
9.1.1. Подключение инструментов безопасности	29
9.1.2. Редактирование инструмента	30
9.1.3. Удаление инструмента	30
9.1.4. Примеры интеграций с инструментами	31
9.1.4.1. Добавление в раздел Интеграции РТ Application Inspector	31
9.1.4.2. Добавление в раздел Интеграции KCS	32
9.2. Источники сканирования	32

9.2.1. Подключение источника сканирования	33
9.2.2. Редактирование источника сканирования	34
9.2.3. Удаление источника сканирования	34
9.3. Инструменты уведомлений	35
9.4. Трекеры задач	36
9.4.1. Добавление трекера задач	37
10. Отчеты	41
11. Журнал событий	42
12. Конструктор полей	43
13. Требования к аппаратным и программным характеристикам рабочего в	места
пользователя	45

Введение

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

В роли администраторов могут быть разработчики, администраторы, специалисты, отвечающие за развертывание и сопровождение инфраструктуры и системного программного обеспечения (операционные системы, сервера приложений, базы данных и т.п.), необходимых для непрерывной работы системы, а также отвечающих за создание и управление учетными записями, ролями и доступами пользователей, внесение изменений в настройки, контроль лицензии, подключение инструментов безопасности и источников сканирования.

1. Термины и определения

Термин/аббревиатура	Определение
ПО	Программное обеспечение
ASOC (Application Security Orchestration and Correlation)	Платформы или решения для оркестрации и корреляции безопасности приложений - это платформы, предназначенные для управления и координации безопасностью приложений, позволяют автоматизировать процессы обнаружения, анализа и реагирования на угрозы безопасности, связанные с приложениями.
DAST (Dynamic Application Security Testing)	Динамический анализ кода - это 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 - это 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 - это 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 - это 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	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	Обмен данными между системами с возможной последующей обработкой
AD (Active Directory)	Службы каталогов - это 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

Платформа «TRON.ASOC» осуществляет комплексный контроль информационной безопасности разрабатываемых проектов, обеспечивая надежную защиту на всех этапах разработки:

- 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,
 - 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. Установка решения

3.1. Установка с помощью Docker Compose

Решение поставляется в виде образов контейнеров. Для установки необходимо выполнить следующие шаги:

- 1. Установить компоненты. Для этого необходимо:
 - а. Скачать архив *docker-compose-v1.2.zip.*
 - b. Задать значение для переменной ASOC_DOMAIN, которая содержит зарезервированное доменное имя для графического интерфейса ASOC. В случае пилотного проекта, необходимо на DNS-сервере добавить А-запись для хоста, где запускается docker-compose.
 - c. Далее для корректной локальной работы необходимо исправить/добавить в /etc/hosts следующую строку (значение из переменной ASOC_DOMAIN):

127.0.0.1 localhost asoc.testdomain.ximi

- d. Проверить актуальность значений переменных: ASOC_IMG_FRONT, ASOC IMG CORE в соответствии с нужной версией сборки.
- e. Запустить скрипт show.sh, который выведет значения переменных из файла *docker-compose.yaml* для проверки:

./show.sh

f. Выполнить вход в реестр, позволяющий получить доступ к образам контейнеров ASOC (с помощью username от учетной записи harbor):

```
docker login harbor.tronsec.ru
```

g. Далее выполнить следующую команду:

docker-compose up -d

h. Проверить статус контейнеров:

docker ps

Корректный статус в данном случае - Running *или* Up About a minute.

 Проверить в любом браузере загрузку web-интерфейса решения по ip-адресу http://<ASOC_DOMAIN> (например, http://asoc.testdomain.ximi или http://localhost), и выполнить вход в систему по инструкции ниже Авторизация администратора.

3.2. Установка с помощью Helm Chart

Чтобы установить решение с помощью **Helm Chart**, необходимо выполнить следующие шаги:

- 1. Обеспечить наличие следующих компонентов и доступов:
 - Доступ к реестру harbor.tronsec.ru
 - Установленные утилиты kubectl и helm
 - Доступ к kubeconfig для целевого кластера с правами к namespace для ASOC
- 2. Подготовить Helm Chart. Для этого необходимо подключить Helm-репозиторий производителя, где находится пакет Helm Chart, а именно, выполнить следующие команды:

```
export CHART_URL=xxxxxx
export CHART_USERNAME=xxxxxx
export CHART_PASSWORD=xxxxxx
export VERSION=xxxxxx
helm repo add asoc \
https://$CHART_URL/repository/public-charts/ \
--username $CHART_USERNAME \
--password $CHART_PASSWORD
helm repo update
helm pull asoc/asoc --version $VERSION
tar xvf asoc-$VERSION.tgz
```

Значения CHART_URL, CHART_USERNAME, CHART_PASSWORD, VERSION предоставляются производителем.

 Подготовить values-config.yaml. Для этого необходимо создать и заполнить файл с параметрами установки (asoc/values.yaml), в которых указать следующие значения:

```
default.domain="example.com"
default.networkPolicies.ingressControllerNamespaces="ing
ress-nginx"
```

4. Далее выполнить установку чарта:

```
cd asoc/
helm upgrade --install asoc-release \
--namespace asoc \
--create-namespace \
--values values.yaml \
```

4. Обновление решения

При выходе новой версии решения, рекомендуется выполнить обновление. Для успешного обновления необходимо выполнить установку, используя данные новых образов и чартов (подробнее см. <u>Установка решения</u>).

5. Удаление решения

В случае удаления решения с помощью Docker Compose, необходимо выполнить следующие шаги:

- 1. Запустить папку установленного ранее архива docker-compose-v1.2.zip.
- 2. Остановить контейнеры ASOC из манифеста docker-compose.yaml:

docker-compose down

3. При необходимости удалить данные БД:

docker-compose down --volumes

Для удаления через Helm Chart необходимо выполнить следующее:

helm uninstall <RELEASE NAME> -n <namespace>

При удалении через Helm Chart сохраняется secret poll-secret и pv.

6. Авторизация администратора

Для успешной авторизации необходимо выполнить следующие шаги:

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



- 3. Далее ввести Имя пользователя и Пароль от учетной записи администратора.

 При первом входе в систему необходимо использовать следующие данные учетной записи администратора: Имя пользователя - admin 									
• пароль - аспіп Также необходимо ознакомиться и принять Согласие с	EULA (Рис. 2).								
Согласие с EULA ⊕ R									
законодательством Российской Федерации без учета принципов коллизионного права.									
Все споры и разногласия разрешаются на основании действующего законодательства Российской Федерации в судебном порядке.									
За нарушение авторских и исключительных прав Лицензиара на Программное обеспечение Вы несете гражданскую, административную или уголовную ответственность в соответствии с законодательством Российской Федерации.									
000 «КСИМИ ДАТА»									
Соглашаюсь Не соглашаюсь									
Рис. 2									
Далее потребуется изменить пароль к данной учетной з	записи, следуя								

указанным требованиям к новому паролю (Рис. 3) и нажать кнопку **Изменить**.

Изменить пароль	⊕ Ru ~
Новый пароль*	
	0
Пароль должен содержать:	
 Не менее 8 символов 	
 Хотя бы одну цифру 	
 Прописную букву 	
 Строчную букву 	
 Хотя бы один специальный символ 	
Подтвердите пароль*	
	Ø
Изменить	

4. Нажать Войти.

При успешной авторизации откроется Информационная панель (Рис. 4).

■ При возникновении проблем с первым входом в систему, необходимо обратиться в техподдержку TRON.ASOC.

≡ ⊕	Информационная панель		
ASOC	Весь период Год Квартал Месяц Неделя День 27.02.2025 2	27.03.2025 ×	🔒 Создать отчет
89 Информационная панель	Накопительный график	Уязвимости	Открытые уязвимости
Проблемы безопасности	100K	Всего укавимостей 2850	CWE-476 194 CWE-119 52 CWE-416 126 CWE-667 46
Библиотека зависимостей	1K 10	Сканирований 201	CWE-787
Правила	50° 50° 50° 50° 50° 50° 50° 50° 50° 50°	Критический 37	CWE-190 56 CWE-770 38
🔿 Правила безопасности	The Sher Charles and the terms of the state	 Высокий 396 (Средний 1797) Низкий 607 	Всего отколтых узвенностей 742
 Правила дедупликации Ф. Правила реагирования 	🧧 Новый 🛃 В работе 💿 Подтверждено 🛃 Вручную	Неопределенный 13	,42
Администрирование	Выбрать метрику 🗸 Примонить	Наиболее критичные уязвимости	Наиболее уязвимые проекты
 О Интеграции 		CVE-2024-37371 10 CVE-2023-5841 CWE-787; 2 CVE-2024-32002 CWE-59; 2 CWE-122	TESTDAY1 2746 399
В Отчеты Мотира соби лий		CWE-22; CWE-434 CVE-2023-45855 CWE-190	KCSSTATUS7 53 6
 Журнал собалии Ломощник 	Выберите метрику и нажмите «Применить», чтобы увидеть её динамический график	CVE-2024-45490 CWE-611 2 CWE-20 CVE-2024-45491 CWE-190 2 CVE-2021-23463 CWE-611 1	TESTON
С. Конструктор полей		······	Juice Shop OWASP
Параметры Параметры подключения			Новые 2850 Критические и Уязвимости высокого 433 уровня
⑦ О программе		Метрики	
å admin		Плотность риска	

Рис. 4

7. 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
 - Управление доступом
 - Интеграции
 - Отчеты
 - Журнал событий
 - Помощник

Раздел Помощник будет доступен в следующих релизах.

- Конструктор полей
- Параметры подключения
- О программе общая информация о системе
- Учетная запись данные профиля учетной записи
- Рабочая область. Информация и элементы управления в рабочей области зависят от выбранного раздела или подраздела.

7.1. Информационная панель

Информационная панель представлена в виде сводных графиков (виджетов) по уязвимостям за установленный период (Рис. 4). Данные виджеты можно настроить по усмотрению, с помощью кнопки **Настроить расположение**. Доступны следующие настройки виджетов:

- 1. Добавление новых виджетов с помощью кнопки Добавить виджет.
- 2. Перемещение виджетов в рамках рабочей области с помощью кнопки

на каждом из виджетов.

3. Удаление виджетов с помощью кнопки 🛄 на каждом из виджетов.

Подробнее о разделе, см. Руководство пользователя.

7.2. Проекты

Раздел **Проекты** включает список созданных проектов, которые проверяются на соответствие политикам безопасности компании и качеству (Рис. 5). 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	OTHET				Поиск	Q & 7
10 Mutanuauuauuaa aayaa	Имя проекта 🗸	Дата добавления 🚍	Дата обновления 🗸	Теги ч	Код проекта 🗸	Инструменты	
Проекты		26/03/2025 14:52	26/03/2025 14:52		JUICE		0 Û
проблемы безопасности						···· 🕲 🖷	
Библиотека зависимостей	TESTDAY12	26/03/2025 01:22	30/03/2025 21:01		TESTDAY1	O 🔹	0 0
Правила	TESTDAY	26/03/2025 01:09	27/03/2025 16:30	testday	TESTDAY	•	0 Û
О Правила безопасности	D TESTOD1	25/03/2025 10:28	25/03/2025 10:28		TEST001	(m) 🕐	0 Û
 Правила дедупликации Правила реагирования 	TESTCVSS	25/03/2025 10:14	26/03/2025 00:36	cvss	TESTCVSS	💿 🗑 🕱	0 û
Администрирование	🔿 test	13/12/2024 13:02	15/01/2025 13:43	newtag newtag_6 notags proverkatags	TEST	0	0 Û
8 Управление доступом Э Интеграции	ISSUETESTING20241212T141920 002Z	12/12/2024 17:19	12/12/2024 17:19	qatioad	ISSUETESTING20241212T14192	0	ı î
Отчеты П Журная событий		12/12/2024 17:17	12/12/2024 17:17	qalload	ISSUETESTING20241212T14173	O (b)	0 Č
Ломощник		12/12/2024 17:14	12/12/2024 17:14	qatload	ISSUETESTING20241212T14140	0	0 0
С Конструктор полей		11/12/2024 14:00	05/02/2025 14:49	notags			0
 Параметры подключения 	Bcero 58					< 1 2 3 _ 6 >	10/страница 🗸
 ⑦ О программе å admin 							
ے admin							

Рис. 5



7.3. Проблемы безопасности

Раздел **Проблемы безопасности** состоит из подразделов **Проблемы безопасност**и и **Исключенные проблемы безопасности**. Данный раздел демонстрирует все найденные уязвимости и основную информацию по ним (Рис. 6).

≡ ⊕	Проблемы бе	зопасности									
	Проблемы безопасности	Проблемы безопасности Исслоченные проблемы безопасности									
В Информационная панель	+ Создать правило безопа	сности 🛛 🖸 Создать задач	и из проблем					Поиск	c	\$	₽,
🗅 Проекты	 ID уязвимости ч 	Категория 🗸	Уровень критичности ~	Обнаружено с помо 🗸	CWE ~	CVE ~	Статус 🗸	Сканируемый объект 🗸	Проект ч		
 Проблемы безопасности Библиотека зависимостей 	D KCCC-52 🗗	Use of Hard-coded Passw ord	Низкий ∨	PT Application Inspector	CWE-259		• Новый ∨	https://dmilab.gltlab.yand excloud.net/dmidev/tron- asoc/core	KCCC		
⊘ Контроль качества Правила	O KCCC-16 D	Use of Hard-coded Passw ord	Средний 🗸				• В работе 🗸				
 Правила безопасности Правила дедупликации 	О косс-за 🗗	Use of Hard-coded Passw ord	Низкий ∨				• Новый ~				
ц правила реагирования Администрирование 8. Управление поступом	О косс-53 🗗	Use of Hard-coded Passw ord	Низкий 🗸				• Новый ∨				
© Интеграции © Отчеты	CCC-26	Use of Hard-coded Passw ord	Низкий ∨				• Новый ∨				
Е Журнал событий	CCCC-23	Use of Hard-coded Passw ord	Низкий ∨				• Новый ∨				
С Конструктор полей Параметры	O KOCC-33 🗗	Use of Hard-coded Passw ord	Низкий ∨	PT Application Inspector			• Новый ∨				
 Параметры подключения О программе 	O KOOCHS 🗗	Use of Hard-coded Passw ord	Низкий ∨				• Новый ~				
ది ədmin	O KOCO-41 D	Use of Hard-coded Passw ord	Низкий 🗸				• Новый ∨				

Рис. 6

Подробнее о разделе, см. Руководство пользователя.

7.4. Библиотека зависимостей

Раздел Библиотека зависимостей представляет информацию по зависимостям в проектах (Рис. 7).

≡ ⊕	Библиотека завис	имостей								
						Поиск		٩	\$	7
00 Mutopupulauna caupa	Название	Версия	Тип	Происхождение	Проблемы безопасности	~	Проект			
П Проекты	abbrev	1.1.1	Библиотека	Code	0					
троблемы безопасности	accepts	1.3.7	Библиотека	Code	0					
Библиотека зависимостей	acom	4.0.13	Библиотека	Code	0					
💬 Контроль качества	acom	7.3.1	Библиотека	Code	0					
Правила	acom	3.3.0	Библиотека	Code	0					
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					
8 Управление доступом	8jv	6.12.3	Библиотека	Code	0					
С Интеграции	Bcero 1003					< 1 2	3 101 >	10/стр	аница –	~
El Wanuan cofu mai										
 Журнал созатий Журнал созатий 										
(). Конструктор полей										
Параметри										
Параметры подключения										
⑦ О программе										
్రీ admin										

Рис. 7

Подробнее о разделе, см. Руководство пользователя.

7.5. Контроль качества

Раздел Контроль качества содержит список шаблонов контроля качества (Рис. 8) с возможностью добавления новых, удаления и редактирования существующих шаблонов в зависимости от потребностей безопасности.

= ⊕	Контроль качества					
	+ Добавить контроль качества 📋 Удалить				Поиск	Q 🕸 🛛
00 14-1	Название шаблона	Количество метрик 🗸	Проекты	Автор		
 Проекты 	12321312	2	Просмотреть	admin	0	Û
() Проблемы безопасности	222222	0	Просмотреть	admin	0	Û
 Библиотека зависимостей Контроль качества 	basic	2	Просмотреть	ədmin	0	Û
Правила	by Check	0	Просмотреть	ədmin	0	Û
 Правила безопасности Правила ледупликации 	dtfed	0	Просмотреть	admin	0	Û
ф. Правила реагирования		0	Просмотреть	admin	0	Û
Администрирование	00000	1	Просмотреть	admin	0	Û
 В Управление доступом Онтеграции 	QARGGSDCHECKKCS	2	Просмотреть	maxkrasnovetskiy	0	Û
🔒 Отчеты	QARGGSDCHECKPTAI	1	Просмотреть	maxkrasnovetskiy	0	Û
Е Журнал событий	QARGGSDCHECKSAST	4	Просмотреть	maxkrasnovetskiy	0	Û
Конструктор полей	Bcero 12				< 1 2 >	10/страница 🗸
Параметры Параметры подключения						
⑦ О программе						
్రీ admin						

Рис. 8

Подробнее о разделе, см. Руководство пользователя.

7.6. Правила безопасности

Раздел **Правила безопасности** состоит из набора правил, с помощью которых производятся проверки безопасности (Рис. 9). Данные правила можно настраивать исходя из потребностей безопасности.

	Правила бе:	Травила безопасности										
	+ Добавить правило бе	+ Добекть правило безопасности — X Сбросоть фильтры										٩
였 Информационная панель	Название ч	Категория ч Т	Компонент ч Т	CVE v	₩ CWE	⊤ Статус ∨	т Число ч	Время истечения с У	Область ч			
🗅 Проекты		Container os dependen	naxus int ximi,group :808			• Не активен	1		Все проекты		0	Û
Проблемы безопасности						• Не активен	90		Просмотреть		0	Û
Библиотека зависимостей												
 Контроль качества 	правило	Ssl parameter				• Не активен	0		Просмотреть		O	Û
Правила О Правила безопасности						• Не активен	0		Просмотреть		0	Û
 Правила дедупликации Правила реагирования 		Container os dependen	nosus intximi.group:808			Не активен	3	2024-10-29	Просмотреть		0	Û
Администрирование В Управление доступом		Container os dependen				• Активен	0		Просмотреть		0	Û
🗘 Интеграции 🕒 Отчеты		Empty Default Exceptio				• Активен	0		Просмотреть		0	Û
 Е Журнал событий Э: Помощник 		DOM Modification HTM				Не активен	0		Просмотреть		0	Û
[] Конструктор полей 			nexus int ximi.grou p:808			Не активен	19		Просмотреть		0	Û
Параметры Ф Параметры подключения			Gittlab_tron_core			• Не активен	416	2024-10-28	Просмотреть		0	Û
⑦ О программе	Bcero 50								< 1 2	3 4 5 >	10/стр	заница 🗸
음 admin												

Рис. 9

Подробнее о разделе, см. Руководство пользователя.

7.7. Правила дедупликации

Раздел Правила дедупликации содержит информацию о правилах, методах дедупликации (Рис. 10).

€ ⊕	Правила дедупликации				
	+ Добавить правило дедупликации 🛛 🗙 Сбросить фильтры			Поиск	٩
	Название =_	Метод	т Статус ч	Ψ	
ы информационная панель ⊡ Проекты	123	По комбинированным полям	• Не активен		/ 0
∰ Проблемы безопасности	aunder	По комбинированным полям	Не активен		0 0
 Библиотека зависимостей Контроль качества 	autocomplit	С помощью правил сопоставления	• Не активен		0
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
💭 Правила дедупликации	DDRULE1 OATEST	По комбинированным полям	• Не активен		
Ф Правила реагирования					0
Администрирование	DDrule2	С помощью правил сопоставления	• Не активен		0 0
В Управление доступом О Интеграции	DEDUBLICATION70	С помощью правил сопоставления	• Не активен		0 0
С Отчеты	DEFAULT	По комбинированным полям	 Не активен 		0 0
Курнал событий	ISSUETESTING20241106T091754941Z12256	На основе существующей проблемы безопасности	• Не активен		0 0
Помощник Конструктор полей	Bran 20				10/cmausia ×
Параметры подключения					
⑦ О программе					
ది admin					

Рис. 10

Подробнее о разделе, см. Руководство пользователя.

7.8. Правила реагирования

Раздел Правила реагирования содержит список правил реагирования на появление уязвимостей в системах и приложениях в рамках существующих проектов (Рис. 11).

	Правила реагир	ования							
	+ Добавить правило реагирован	ия					Поиск	Q \$	∇
응 Информационная панель	Название правила <u>—</u> responceRule	Статус	Тип реагирования	Инструмент уведомления	Проекты	Автор admin		 Û	
Проблемы безопасности	Bcero 1				TEOTOROS) / страница	a v]
© Контроль качества									
Правила О Правила безопасности									
 Правила дедупликации Правила реагирования 									
Администрирование В Управление доступом									
🗘 Интеграции									
🕑 Журнал событий 🎉 Помощник									
() Конструктор полей Параметры									
Параметры подключения • О программе									
å admin									

Рис. 11

Подробнее о разделе, см. Руководство пользователя.

8. Настройки системы

8.1. Настройки правил авторизации пользователей

На вкладке Параметры подключения (Рис.12) предусмотрены следующие возможности:

- настройка параметров требований к паролю,
- максимальная продолжительность сеанса,
- время выхода из системы после периода неактивности,
- количество попыток ввода пароля до временной блокировки,
- длительность временной блокировки.

≡ ⊕		
	Параметры подключения	
	Требования к паролю	Сохранить
	3 ក៏អ្នកថារ ស្លាករដាម។ ឧត្តរដ្ឋារដាម រសារ ស៊ីស ល្អអម្ យុមមុទ្រ។	
88 Информационная панель	Tapon, pointer coppensaria toria du opine autrananya in cupier provenya dy expressione de la companya de la com de la companya de la co	
🗅 Проекты		
∰ Проблемы безопасности		
Библиотека зависимостей	Аутентификация	
 Контроль качества 	Makciwanalisa npogonkintenision: ceasica 9 4. O	
Правила		
О Правила дедупликации	Chemical to carciteses increases increases and the second se	
Д Правила реагирования	Количество попиток ввода пароля до временной блокировал 3	
	Период временной бложировки 1 мин. ()	
83 Управление доступом		
🗘 Интеграции		
🔓 Отчеты		
🗄 Журнал событий		
Помощник		
С Конструктор полей		
Параметры		
Параметры подключения		
() O the barware		
å admin		

Рис. 12

Для настройки параметров подключения администратору необходимо выбрать нужные требования и нажать на кнопку **Сохранить**. После чего все пользователи принудительно должны изменить пароль при следующей авторизации в системе.

8.2. Управление пользователями и ролями

Раздел Управление доступом позволяет администраторам управлять пользователями и их ролями в системе (Рис. 13). Данный раздел включает четыре ключевых подраздела:

- Пользователи
- Роли
- Группы
- LDAP

≡ ⊕	Управление доступом				
	Метод аутентификации Переключение доступно после настройки параметров маплинга	как минимум для 1 группы		~	Переключить
89 Информационная панель					
🗅 Проекты	Tonesson Form Typing Lord				
🛱 Проблемы безопасности	+ Добавить пользователя 🔅 Сброс пароля 📋 Удалить	1		Поиск	٩
Библиотека зависимостей					
😔 Контроль качества	Имя пользователя =	Отображаемое имя 🗸	Назначенные роли	т Сброс пароля	T
Правила	admin	admin	isadm	Нет	Θ
Правила безопасности	adminchik	adminchik	asocadm, chf, dev, isadm, isaud, isoff	Нет	Θ
Правила дедупликации					
Ф Правила реагирования		demaigneev	0ev	Нет	8
Администрирование	Idap_recovery	Idap_recovery	Isauth	Нет	
83 Управление доступом	maxkrasnovetskiy	maxkrasnovetskiy	qamkr	Нет	
🗘 Интеграции		-			0
🕒 Отчеты	petya	Petya	asocadm	Нет	
Е Журнал событий	qatestuser	Пользователь QAuser	qamkr	Нет	
 Ломощник Констриктор полой 	atestuser1	gatestuser12	gamkr	Uez	
C KONCIDINITOPHONEM				nei	
Параметры	qatestuser3		qamkr	Да	
 О программе 	gatestuseró	qatestuseró	testnumber	Нет	
ి ədmin	Всего 21 / Выбрано О			< 1 2 3 >	10/страница 🗸

Рис. 13

Подраздел Пользователи предоставляет список со следующей информацией о пользователях:

- **Имя пользователя** уникальный логин или идентификатор пользователя.
- Отображаемое имя имя, которое видят другие пользователи.
- Назначенные роли перечень ролей, которые присвоены пользователю. Роли определяют права доступа пользователя к различным функциям системы.
- Сброс пароля индикатор того, требуется ли пользователю сброс пароля. Значение *Да* означает, что пользователь должен изменить свой пароль при следующем входе в систему.

8.2.1. Добавление нового пользователя

Для добавления нового пользователя, необходимо выполнить следующие шаги:

- 1. В разделе **Управление доступом** нажать на кнопку **Добавить пользователя.**
- В открывшемся окне Создать пользователя (Рис. 14) заполнить поля Имя пользователя, его Отображаемое имя (не обязательно), Электронная почта.

≡●	Управление доступом · Пользователи · Создать пользователя	î
	Общая информация	Отмена Создать
89 Информационная панель		
🗅 Проекты	Отображаемое имя ()	
🖞 Проблемы безопасности		
Библиотека зависимостей	Злектроная почта*	
⊙ Контроль качества		
Правила	Hoseviii napone*	
О Правила безопасности	Введите новый пароль 👁	
💭 Правила дедупликации	Reports answer capparate:	
Ф Правила реагирования	tendence culturation Xone for conversion	
Администрирование	Inconceyo 6yiay Conceyo 6yiay Conceyo 6yiay	
83 Управление доступом	• Хотя бы саим специальный силиоп	
🗘 Интеграции	Подтеврдите пароль*	
🔓 Отчеты	Подтвердите пароль Ф	
🗄 Журнал событий		
): Помощник	Cred Trades a sole a stressor	
[] Конструктор полей	Роли для назначения	
Параметры	TROOK. Q	
🕸 Параметры подключения	ASOC Administrator	
⑦ О программе	_ chief	
	Developer	
å admin	IS Administrator	

Рис. 14

- 3. Ввести пароль, соответствующий правилам авторизации, в поле **Новый** пароль и подтвердить его в поле **Повторите пароль**.
- Далее при необходимости назначить пользователю одну или несколько ролей, которые определят его права доступа, с помощью поиска в блоке Роли для назначения (подробнее см. <u>Настройка ролей</u>).
- 5. Также при необходимости включить опцию сброса пароля.
- 6. Далее нажать на кнопку Создать.

8.2.2. Редактирование пользователя

Для того, чтобы отредактировать права доступа пользователя, необходимо выполнить следующие шаги:

- 1. В разделе **Управление доступом** найти пользователя в списке и нажать на его имя.
- 2. На открывшейся странице редактирования изменить данные пользователя (кроме имени), включая его роли и требование сброса пароля (при необходимости).
- 3. Нажать кнопку на Сохранить.

8.2.3. Удаление пользователя

Для того, чтобы удалить пользователя, необходимо выполнить следующее:

• В разделе Управление доступом отметить галочкой слева выбранного пользователя в списке и нажать на кнопку Удалить.

Обратите внимание, что удаление пользователя может быть необратимым.

8.2.4. Сброс пароля

Для того, чтобы инициировать сброс пароля необходимо выполнить следующее:

• В разделе **Управление доступом** найти нужного пользователя и изменить значение **Сброс пароля** на **Да**. При следующем входе пользователь должен будет принудительно изменить пароль.

Очистить сессии пользователя и сбросить пароль можно также в пунктах подменю в списке пользователей.

8.2.5. Настройка ролей

В подразделе **Роли** (Рис.15) отображаются все роли, которые назначены пользователям системы с указанием количества пользователей, которым они принадлежат.

В системе предусмотрены следующие базовые роли пользователей:

- Администратор (*isadm*) роль с полными правами, при установке продукта присваиваются все существующие права. Предназначена для пользователей, отвечающих за развертывание и сопровождение инфраструктуры и системного программного обеспечения, необходимых для работы решения (например, операционные системы, сервера приложений, базы данных), а также отвечающих за создание и управление учетными записями, ролями и доступами пользователей, внесение изменений в настройки, контроль лицензии, подключение инструментов безопасности и источников сканирования.
- Аудитор (*isaud*) роль предназначена для контроля за безопасностью данных и систем, мониторинга действий пользователей и операций системы, анализа журналов событий, контроля результатов сканирования и соответствия Контролям качества.
- Инженер ИБ (*isoff*) роль предназначена для контроля и обеспечения информационной безопасности разрабатываемых проектов, настройки правил безопасности и мониторинга угроз, управление инструментами безопасности, сканированиями.
- Разработчик (dev)- минимальная базовая роль, предназначена для пользователей, осуществляющих проверку на соответствие стандартам, просмотр результатов сканирования, исключенных проблем.

Данные роли, кроме Администратора, можно удалить. Роль Администратора можно только заблокировать.

≡ ⊕	Управление доступом				
	Метод аутентификации Переключение доступно после настройки пар	аметров маппинга как минимум для 1 группы			• Переклочить
🔀 Информационная панель 🗅 Проекты	Пользователи Роли Группы LDAP				
Проблемы безопасности	+ Создать роль				Поиск Q 🕸
Библиотека зависимостей	Идентификатор роли =	Название роли 🗸	Описание	Пользователи ~	
 Контроль качества 	asocadm	ASOC Administrator	-	2	
Правила () Правила безопасности	chf	chief	boss	1	0 0
 Правила дедупликации Ф. Правила реагирования 	dev	Developer		3	/ 0
Администрирование	isadm	IS Administrator		4	0 D
В Управление доступом О Интеграции	Isaud	IS Auditor		2	Ø Û
🔁 Отчеты	isauth	IS Authentication Manager		1	ℓ û
Е Журнал событий	isoff	IS Officer		2	0
[] Конструктор полей	qamkr	qamkr	Роль для предрелизного тестирование (Краснов	5	ℓ û
Параметры	testnumber	test1	testitestitestitestitestitestitestitest	2	0 Û
रह Параметры подключения () О программе	testrolea	testrolea		0	0
్రీ admin	Bcero 13				< 1 2 > 10/страница >

Рис. 15

Поля таблицы следующие:

- **Идентификатор роли** уникальное имя роли в системе. Например, *activerole, argentgf, asocadm*.
- Название роли название, отображаемое в интерфейсе.
- **Группы Active Directory** если используется интеграция с AD, здесь отображены группы, с которыми связана роль.
- Пользователи количество пользователей, которым назначена данная роль.

8.2.6. Добавление новой роли

При добавлении новых пользователей рекомендуется назначить минимальную базовую роль (например, роль Разработчика (dev)), а настройку дополнительных узконаправленных прав добавлять с помощью новых групп, так как права по ролям и группам суммируются (подробнее см. <u>Добавление</u> <u>группы пользователей</u>).

Чтобы добавить новую роль выполните следующие шаги:

- 1. В подразделе **Управление доступом Роли** нажмите **Создать роль**.
- 2. В открывшемся окне справа (Рис. 16) заполните **ID Роли**, **Название роли** и **Описание.**

Управление доступом	L. C.			Создать	роль ×
Метод аутентификации Переключение доступно после настройки пар	аметров маппинга как минимум для 1 группы			ID роли*	Введите ID роли
Пользователи Роли Группы LDAP				Название роли*	Введите название роли
+ Создать роль				Описание	Введите описание
Идентификатор роли 😑	Название роли 🗸	Описание	Пользователи 🗸		От 4 до 255 символов
asocadm	ASOC Administrator		2	Разрешения	Разрешить всё
chf	chief	boss	1	Поиск по раздел	nam Q
dev	Developer		3	Проекты	Выбрать все
isadm	IS Administrator		4		 Просмотр проектов Создание и редактирование проектов
isaud	IS Auditor		2		Удаление проектов
isauth	IS Authentication Manager		1		Управление тегами
isoff	IS Officer		2	Конвейеры безопа	всности Выбрать все
qamkr	qamkr	Роль для предрелизного тестирование (Краснов	5		 Просмотр конвейеров и загрузка результатов
testnumber	testi	testitestitestitestitestitestitestitest	2		Создание и редактирование конвейеров
testrolea	testrolea		0		
Bcero 13				Создать	тмена

Рис.16

- 3. Далее настройте доступ к проектам и конвейеру безопасности в блоке **Разрешения**. Для этого поставьте галочки в нужных чекбоксах
 - Просмотр проектов
 - Создание и редактирование проектов
 - Удаление проектов
 - Конструктор полей
 - Управление тегами
 - Просмотр конвейеров и загрузка результатов
 - Создание и редактирование конвейеров
 - Запуск конвейеров
- 4. Нажмите кнопку Создать.

8.2.7. Добавление группы пользователей

Подраздел **Группы** позволяет создавать группы пользователей (Рис. 17), редактировать и удалять их, добавлять в них пользователей.

При добавлении новых пользователей в группу указанные в группе дополнительные права суммируются с правами роли пользователя.

≡ ⊕	Управление доступом	I				
	Метод аутентификации Переключение доступно после настройки пар	аметров маплинга как минимум для 1 группы				Переключить
Ниформационная панель	Пользователи Роли Группы LDAP					
🗅 Проекты						
Проблемы безопасности	+ Создать группу				Поиск	Q ⊜ 7
Библиотека зависимостей		-				
Контроль качества	название группы 🗸	Теги проектов 🗸	назначенные роли 🗸	Пользователи ~		
Правила	projectDAY	testday	1	1	0	Û
Правила безопасности	projectDAY1	testday1	1	1	0	0
Правила дедупликации	project@VRR		1	1		-
Правила реагирования	pojeccovos	CVES	A.	*	0	0
Администрирование	officerproject	cvss	1	2	0	Û
83 Управление доступом	develop		1	1	Π	0
🗘 Интеграции					ν	0
🔓 Отчеты	officer		1	2	0	Û
Журнал событий	admin		1	1	0	Û
Э. Помощник						
с конструктор полеи	Bcero 7				< 1 >	10/страница 🗸
Параметры						
Параметры подключения						
(•) О программе						
송 admin						

Рис. 17

Для того, чтобы добавить группу, необходимо выполнить следующее:

- 1. В подразделе **Управление доступом** → **Группы** нажать на кнопку **Создать группу.**
- 2. В открывшемся окне (Рис. 18) заполнить поля формы:
 - Название группы
 - Добавить роли
 - Теги проектов
 - Добавить пользователей

Также предусмотрено добавление связи с группой LDAP/AD в блоке **Маппинг с LDAP**. Для того, чтобы добавить группу LDAP, необходимо добавить интеграцию с LDAP/AD (см. <u>Аутентификация в LDAP</u>), после чего группа LDAP/AD появится в списке групп блока **Маппинг с LDAP**.

€	Управление до	оступом		Создать группу ×
	Метод аутентификации Переключение доступно пос	ле настройки параметров маппин	га как минимум для 1 группы	Название группы* 🕥 Введите название
器 Информационная панель С Проекты	Пользователи Роли Групп	ы LDAP		Добавить роли* Выберите из списка У
🛱 Проблемы безопасности	+ Создать группу			Теги проектов 🛈
Библиотека зависимостей			Toru angouran	Выберите из списка 🗸
 Контроль качества 	Название группы 🗸			Добавить пользователей
Правила	testgroup1			Выберите из списка 🗸
Правила безопасности	testgroup1	1		Manager of DAP
Правила дедупликации Правила реагирования	testgroupadmin	1		Укажите название группы LDAP, которая должна соответствовать текущей группе
Администрирование	testcvss			Введите название
89 Управление доступом	TestGroupUsers	2	event1	
🗘 Интеграции				
🔓 Отчеты —	1test1	1	qa-load	
Е Журнал событий	testLdap	1	aicopilot business_analyst_f	
 Ломощник Конструктор полей 	groupfornewrole	1	aicopilot	
Параметры	testisadm	2	event1	
🕸 Параметры подключения	Группа 413	5	aicopilot ai_forecast	
ది admin			business_analyst_f	Создать Отмена

Рис. 18

3. Далее нажать на кнопку Создать.

8.2.8. Аутентификация в LDAP

Подраздел LDAP предназначен для удобного и безопасного управления пользователями и их доступом, используя интеграцию с LDAP или AD (Рис. 19).

Stringenering of the string of the strin			
Meropa ayreentruóµksauµu Descoserene Point Pyrint LDAP Intercente Point Pyrint Pyrint LDAP Intercente Point Pyrint Pyrint LDAP Intercente Point Pyrint Pyri	⊕ }	правление досту	лом
Normal Normal Normal Important Important <th></th> <th>Метод аутентификации Переключение доступно после настр</th> <th>ройки параметров маплинга как минимум для 1 группы</th>		Метод аутентификации Переключение доступно после настр	ройки параметров маплинга как минимум для 1 группы
Normal Morenal Morenal Morenal Morenal Morenal Morenal Mary Methicol Bannocu Morenal	ационная панель	Тользователи Роли Группы LDA	AP
ANCY ADDCTORD CTI ADDCTORD ADDCT	ы —		
Normal Import Import Apprentrup/ukaquum B LOAP URL copeopol More More More More More More </th <th>лемы безопасности</th> <th></th> <th></th>	лемы безопасности		
I Banaman gan LDM Banaman gan LDM AyrentruфukaLuka B LDAP ULL compose* ULL co	отека зависимостей	Пресеты	💭 Отменить и сбросить поля
CM Ayrentruéµukauµa B LDAP URL copeopor* Bataine cauny VM URL copeopor* Dapora ywénnoù aanoca Immeri CM Dapora ywénnoù aanoca CM Dapora ywénnoù aanoca CM Dapora ywénnoù aanoca Esaooos ywoatawoo sna* Topmer: CM Dapora ywénnoù aanoca Esaooos ywoatawoo sna* Topmer: CH(Intra SaQIA MAACCount) kame-fakij(koljet:Class-person)) Immer: CH(Intra SaQIA MAACCount) kame-fakij(koljet:Class-top) Immer: CHURT Dapora ywennoù sanoca Dipure: Churt pinonaozarene* Dipure: Churt pinonaoza	16 качества	Заполнить для LDAP Заполнить д	una Active Directory
KIT AyrentruфukaLugus B LDAP VIII. copuspus* Betaarse counny VIII. copuspus* Pamaer Biscoore yuwaanaoe suus* Pamaer: VIII. (Information Status) Counny Ownunp nonaoasren* Pamaer: VIII. (Information Status) Counny Ownunp nonaoasren* Pamaer: VIII. (Information Status) Counny Ownunp nonaoasren* Pamaer: VIII. (Information Status) Counny Octuoe Hactporiku Counny			
Ayrentrugkukagus B LDAP URL copiepa* Bichaare coanny Wax velmoid samuci Imports velmoid samuci ON Tipports velmoid samuci Bisbore yuwaamucie xxx* Ppumeer DC-tronneer_DC-viscal Ownary P nonaccarent* Cpumeer (Afformenter-f-sky(ningumeenter-	а безопасности		
VIEL. copiespoir* Estature county Max Max yelfmoil samocin Immediate Max Tapons-yelfmoil samocin Immediate Max Tapons-yelfmoil samocin Immediate Escosor yewatnuos max* Tapens- Escosor yewatnuos max* Tapens- Escosor yewatnuos max* Ownup Trobusostmen* Tapens- Escosor yewatnuos max* Tapens- Escosor yewatnuos max* Ochostes Hactportkut Tapens- Escosor yewatnuos max* Tapens- Escosor yewatnuos max*	релуппикации	Аутентификация в LDA	P
New veltificiol annuci Imagents Data Tagonts yeltificiol annuci Data Tagonts yeltificiol annuci Easone yevantucio stati Tipmeng: Easone yevantucio stati Tipmeng: Eductore yevantucio Tipmenge:	020400000000	URL cepsepa*	Вставьте ссылку
Nexts Color Out Diportury vietnosis associa Diportury vietnosis associa Improver: DC-istorase; DC-istorase; Easonoos yvvacatavooi stua* Tippaver: DC-istorase; DC-istorase; Outvoirip nonaloasaren** Eginase; Outvoirip nonaloasaren** Eginase; Outvoirip nonaloasaren* Eginase; <t< td=""><td>ареатирования</td><td>เป็นสารเลลีรมณ์ การเหตุม</td><td></td></t<>	ареатирования	เป็นสารเลลีรมณ์ การเหตุม	
Not Pipons ywłania amucii Impons ywłania amucii Biadele ywłania wie kwi* Pipowseg DC-tronsec DC-slocal Ownarp Pionaccentrat* Pipowseg DC-tronsec Children Ownarp Piprima* Pipowseg DC-tronsec Children Ownarp Piprima* Pipowseg TC-tronsec Children Ochobshue Hactppöňku Pipowseg	оинсаодих	VININ J TO LITION SOLITION	
Bacedood ywwathwee Hwat* Tipuweg: DC-troonsec.DC-foocal Gwrau*p nonuccearem* Tipuweg: Cd-(intr-Ka)(AAAACcountName=Ka)(SobjectClass=person)) Cd-(intr-Ma)(AAAACcountName=Ka)(SobjectClass=person)) Cd-(intr-Ma)(AAAACcountName=Ka)(SobjectClass=person)) Cd-(intr-Ma)(AAAACcountName=Ka)(SobjectClass=person)) Cd-(intr-Ma)(AAAACcountName=Ka)(SobjectClass=person)) Cd-(intr-Ma)(AAAAACcountName=Ka)(SobjectClass=person)) Cd-(intr-Ma)(AAAAACcountName=Ka)(SobjectClass=person)) Cd-(intr-Ma)(AAAAACcountName=Ka)(SobjectClass=person)) Cd-(intr-Ma)(AAAAACcountName=Ka)(SobjectClass=person)) Cd-(intr-Ma)(AAAAACcountName=Ka)(SobjectClass=person)) Cd-(intr-Ma)(AAAAACcountName=Ka)(SobjectClass=person)) Cd-(intr-Ma)(AAAAACcountName=Ka)(SobjectClass=person)) Cd-(intr-Ma)(AAAAACcountName=Ka)(SobjectClass=person)) Cd-(intr-Ma)(AAAAACcountName=Ka)(SobjectClass=person)) Cd-(intr-Ma)(AAAAACcountName=Ka)(SobjectClass=person)) Cd-(intr-Ma)(AAAAACcountName=Ka)(SobjectClass=person)) Cd-(intr-Ma)(AAAAAACcountName=Ka)(SobjectClass=person)) Cd-(intr-Ma)(AAAAAACcountName=Ka)(SobjectClass=person)) Cd-(intr-Ma)(AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA	не доступом	Пароль учётной записи	••••••
Websity nonsolateren* Пример: Q4[(n=r-Ka](AdAAccountName=Ka](ObjectClass=person)) A Websity provintia* Пример: (AdjectClass=person)) A Websity provintia* Пример: (dpientDer=Ka](x)(objectClass=top) (objectClass=group)) A Network OchoBHNE HacTpoÑku	ции	Базовое уникальное имя*	Downer: DC=transec DC=local
OchoBHNE Hactpoñku Inpake: (A(Inv:As)(AAAAccountName-Sk)(x)detClass=perion)) // // // // // // // // // // // // //			
Филіцір группы* Филіцір группы* Филіцір группы* Фолонарти Мацинальни маральни марал Сементи маральни м маральни маральни ма	событий	Фильтр пользователя*	Пример: (&((cn=%s)(s&M&ccountName=%s)YobjectClass=person))
Website Tpomesex (d,d(member=%s)(x)(objectClass=top)) (objectClass=group))) COCHOBHNUE HactpoЙKИ	ник		(-(()
чения чения Основные настройки	ктор полей	dun to councut	Remmer
мения ((objectClass=group)))/		ownerp r pyriner	(&([(member=%s)(uniquemember=%s))([(objectClass=top)
Основные настройхи			(objectClass=group)))
Основные настройки	201010		
основные настроики		0	
Ословните поло атрибитами, ноторы на опродолжет изследника		основные настроики	

Рис. 19

Для настройки интеграции необходимо выполнить следующие шаги:

- 1. В подразделе **Управление доступом** → **LDAP** в блоке **Пресеты** выбрать один из предложенных вариантов предзаполнения данных:
 - о Заполнить для LDAP

- Заполнить для Active Directory
- 2. Далее заполнить поля соответствующими данными и атрибутами из LDAP/AD.
 - о URL сервера
 - Имя учетной записи имя учетной записи, используемой для аутентификации при подключении к LDAP-серверу
 - Пароль учетной записи пароль учетной записи LDAP.
 - Базовое уникально имя основной контекстный путь (Base Distinguished Name), где будут выполняться запросы LDAP.
 - Фильтр пользователя фильтр поиска пользователя
 - Фильтр группы фильтр поиска группы
 - Название орг.единицы атрибут, который определяет организационную единицу пользователя
 - Уникальное имя атрибут, который определяет дистинктивное имя (DN) пользователя или группы
 - Имя пользователя
 - Фамилия пользователя
 - Название группы
 - Логин пользователя
 - Email пользователя
 - Член группы
 - Группы пользователя
- 3. После заполнения необходимо убедиться, что все параметры LDAP настроены правильно и система сможет успешно подключиться к серверу LDAP. Для этого необходимо нажать на кнопку **Проверить соединение**.
- 4. В случае успешной проверки необходимо сохранить настройки с помощью кнопки **Сохранить**.

8.2.9. Метод аутентификации

После настройки интеграции с LDAP/AD рекомендуется выбрать метод аутентификации. Для этого необходимо выполнить следующее:

- В разделе Управление доступом → Группы добавить хотя бы одну группу (или отредактировать существующую) с настроенной связью с LDAP-группой (блок Маппинг с LDAP).
- 2. Далее в блоке **Метод аутентификации** выбрать один из представленных методов аутентификации:
 - Внутренняя модель и LDAP
 - о Только LDAP
 - о LDAP отключен
- 3. Далее необходимо убедиться в правильности введенных данных и нажать кнопку **Переключить**.

Ва сесси осуще	ажно! При смене метода аутентификации произойдет закрытие ии у всех пользователей, и дальнейшая авторизация будет ествляться в соответствии с выбранным методом (Рис. 20).	
	() Переключить метод аутентификации? ×	
	Все текущие сессии будут завершены, и пользователям придётся авторизоваться снова, используя новые учётные данные	
	Переключить метод аутентификации Отменить	
	Рис. 20	

9. Настройки интеграций

9.1. Инструменты безопасности

Просмотр всех подключенных инструментов безопасности доступен в разделе **Интеграции** → **Инструменты безопасности** (Рис. 21). Функционал позволяет также добавлять новые инструменты, редактировать и удалять существующие.

Поддерживаемые инструменты безопасности:

- PT Application Inspector
- Kaspersky Container Security
- Solar AppScreener
- Aqua
- CodeScoring
- Grype
- KICS
- OWASP Dependency Track
- Trivy
- Semgrep

≡●	Интеграции						í
	Инструменты безопасности Источники сканир	ования Инструменты уведомлений Трекеры з	здач				[
85 Информационная панель	+ Добавить инструмент безопасности 🛛 🗙	Сбросить фильтры			Поиск		٩
🗅 Проекты	Название 🚞	Инструмент ч	Описание ч	Статус проверки соединения			
☆ Проблемы безопасности □ Библиотека зависимостей ○ Колтороновичиства	AppScreener DAST (EN)_25102024_w/o auth settin	Solar AppScreener DAST	AppScreener DAST (EN)_25102024_w/o auth settings_qamkr	Henposepen 25.10.2024, 13:45 URL инструмента: http://appa.int.tronasoc.ru/ap.	0	Û	
Контроль качества Правила Правила безопасности Правила депулликации	 AppScreener DAST (EN)_Api Token_25102024_gam	Solar AppScreener DAST	AppScreener DAST (EN)_Api Token_25102024_qamkr	Ycneшно 25.10.2024, 15:14 ИК инструмента: http://apps.int.tronasoc.ru/ap Метод аучентификации: Api Token	0	Û	
Д Правила реагирования Администрирование	AppScreenerDAST_RG2_qamkr-52	Solar AppScreener DAST	AppScreenerDAST_RG2_qamkr	Ycneuwo 31.10.2024, 12:56 URL, wwcTpysierra: http://appa.int.tronssoc.ru/sp	0	Ċ	
В Управление доступом О Интеграции				Метод аутентификации: Api Token			
 Отчеты Журнал событий 	AppScreener DAST (RU)_25102024_w/o auth settin	Solar AppScreener DAST	AppScreener DAST (RU)_26102024_w/o auth settings_qamkr	 Ошибка: ABUG-835: AppSicreener tool se >> 25.10.2024, 13:42 URLинструмента: http://appa.int.tronasoc.ru/ap 	0	Û	
 Помощник Конструктор полей 	AppScreener DAST (RU)_Api Token_25102024_qam	Solar AppScreener DAST	AppScreener DAST (RU)_Api Token_25102024_qamkr	 Успешно 25.10.2024,15:15 	0	Û	
Параметры Параметры подключения				чисстино путими на поридири Internation data in the second s			
⑦ О программе	AppScreener SAST (EN)_25102024_w/o auth settin	Solar AppScreener SAST	AppScreener SAST (EN)_25102024_w/o auth settings_qamkr	 Ошибка: ASOC-833: ApriScreener tool se >> 25:10:2024, 13:46 URL инструмента: http://apps.int.tronasoc.ru/ap 	0	Û	
Å admin	AppParaapar PART (EA)) Api Takap 2E102024 aam	Polar AppParoppar PAPT	AppCorpoper CACT (EN) Ani	0.1/1			

Рис. 21

9.1.1. Подключение инструментов безопасности

Чтобы добавить новый инструмент безопасности, необходимо выполнить следующее:

- 1. В разделе Интеграции → Инструменты безопасности нажмите кнопку Добавить инструмент безопасности.
- 2. В открывшемся окне заполнить поля **Название**, **Описание** и добавить **Инструмент**.

3. В зависимости от выбранного инструмента необходимо заполнить дополнительные поля (описание инструмента и URL, язык результатов сканирования). Выбор метода аутентификации на этом шаге не является обязательным, но без заполнения метода аутентификации нельзя проверить соединение с инструментом. Поля для заполнения далее могут отличаться в зависимости от выбора метода аутентификации. Если метод указан и выбрана аутентификация по API -токену, нужно заполнить поле API Токен, если выбран метод аутентификации по логину и паролю, нужно заполнить поля Логин и Пароль.

Для инструмента **CodeScoring** могут использоваться уже существующие данные аутентификации.

Чтобы сделать проверку соединения, нажмите **Проверить соединение**. Система отправит запрос на соединение с инструментом и в верхнем правом углу пользовательского интерфейса отобразится соответствующее уведомление.

4. Далее нажать на кнопку Создать.

9.1.2. Редактирование инструмента

Редактирование инструмента производится по клику на кнопку в списке соответствующем инструменте безопасности. Форма редактирования аналогична форме добавления, но поля заполнены текущими данными (Рис. 22).

≡	Интеграции				Редактирова	ть интергацию с инструментом б
	Инструменты безопасности Источники сканирования Инструменты уведомлений Трекеры задач					AnnScreener D&ST (FN) 25102024 w/o auth settings namk
	+ Добавить инструмент безопасности 🛛 🖂					От 4 до 255 символов - Буквы, цифры, пробелы
В Информационная панель Проекты	Название 🚊	Инструмент ч	Описание ч	Статус пр	Описание*	AppScreener DAST (EN)_25102024_w/o auth settings_qamkr
Д Проблемы безопасности	AppScreener DAST (EN)_25102024_w/o auth settin	Solar AppScreener DAST	AppScreener DAST (EN)_25102024_w/o auth settings.gam/r	🛆 Непр		🖌 От 4 до 255 символов - Буквы, шлфры, пробелы
Библиотека зависимостей Контроль качества			occuBo_donua	25.10.2 URL инстр	Инструмент*	Solar AppScreener DAST 🗸
Правила	AppScreener DAST (EN)_Api Token_25102024_qam	Solar AppScreener DAST	AppScreener DAST (EN)_Api Token_25102024_qamkr	S Ycneu	URL инструмента*	http://apps.int.tronasoc.ru/app/api/v1
О Правила безопасности				URL инстр	Язык результатов сканирования*	English ~
 Правила дедупликации Правила реагирования 	AnnScreenerDAST RG2 namkr-52	Solar AppScreeper DAST	AppScreenerDAST RG2 namkr	Метод аут	Метод аутентификации	Выберите метод 🗸
Администрирование	Abbeneterererererererererererererererererer		Abbect certer pilot - Kotz_danier	31.10.2		
83 Управление доступом				Инстр Метод аут		
Отчеты	AppScreener DAST (RU)_25102024_w/o auth settin	Solar AppScreener DAST	AppScreener DAST (RU)_25102024_w/o auth settings_qamkr	Ошиб		
 Е) Журнал событий 				URL WHCTP		
Помощник	AppScreener DAST (RU)_Api Token_25102024_gam	Solar AppScreener DAST	AppScreener DAST (RU)_Api Token_25102024_qamkr	Ycneu 25.10.2		
Папаметры				URL инстр		
Параметры подключения	AppScreener SAST (EN)_25102024_w/o auth settin	Solar AppScreener SAST	AppScreener SAST (EN)_25102024_w/o auth	Ошиб		
⑦ О программе			settings_qamkr	25.10.2		
్రీ admin	AppScreener SAST (EN)_Api Token_25102024_gamk	Solar AppScreener SAST	AppScreener SAST (EN)_Api	♥ Ycneu	Сохранить Отмена	Проверить соединение

Рис. 22

9.1.3. Удаление инструмента

Удаление инструмента сканирования производится на странице Инструменты безопасности с помощью кнопки 🗊 в строке инструмента, который нужно

удалить (Рис. 21), после чего в открывшемся окне подтвердить удаление инструмента (Рис. 23).



Рис. 23

9.1.4. Примеры интеграций с инструментами

9.1.4.1. Добавление в раздел Интеграции РТ Application Inspector

Раздел Интеграции - это перечень адаптеров и параметров к ним, которые требуются для конфигурации интеграции с инструментом.

Для добавления инструмента на платформу, необходимо выполнить следующие шаги:

- 1. Перейти в раздел **Интеграции** и нажать на кнопку **Добавить инструмент безопасности** и в появившейся форме заполнить поля:
 - Название интеграции например, Инспектор. Имя должно быть уникальным.
 - Описание для удобства идентификации, например, Позитивный инспектор.
 - Инструмент выбор инструмента из выпадающего списка.
- 2. Далее необходимо настроить параметры подключения:
 - Ввести адрес API PT Application Inspector. Например: https://your.company.ptsecurity/api/v1.
 - Выбрать язык результатов сканирования.
 - Выбрать метод аутентификации (этот шаг на данном этапе не является обязательным, если метод аутентификации не указать при создании интеграции, его можно будет указать на этапе добавления новой проверки безопасности)
 - Login/Password (если используется по логину и паролю).
 - API Token (если используется токен доступа)
 - Если выбран метод Login/Password, заполните соответствующие поля логина и пароля.
 - Для API Token вставьте токен в выделенное поле.
- 3. Далее нажать на кнопку **Проверить соединение**. При правильно заполненных полях статус проверки должен быть успешным. Если

соединение не установлено, нужно проверить корректность введенных данных и повторить попытку.

4. После успешной проверки соединения нажать на кнопку **Сохранить**, интеграция появится в общем списке инструментов безопасности.

9.1.4.2. Добавление в раздел Интеграции КСЅ

Для добавления необходимо выполнить следующие шаги:

- 1. В разделе Интеграции → Инструменты безопасности необходимо нажать на кнопку Добавить инструмент безопасности.
- 2. В появившейся форме необходимо заполнить следующие обязательные поля:
 - а. Название
 - b. Описание (добавить краткое описание для инструмента)
 - с. Инструмент (Kaspersky Container Security из выпадающего списка)
- 3. Далее добавить дополнительные параметры инструмента:
 - a. Указать **URL инструмента** Kaspersky Container Security (Например: *https://your.company.kcs/api/v1*)
 - b. Выбрать язык результатов сканирования
 - с. **Метод аутентификации** (в этом инструменте для авторизации используется API Token) и вставить токен в поле **Токен API**

Выбор метода аутентификации на данном этапе не является обязательным. Если метод аутентификации не указать при создании интеграции, его можно будет указать на этапе добавления новой проверки безопасности.

9.2. Источники сканирования

Просмотр всех подключенных источников сканирования доступен в разделе Интеграции → Источники сканирования (Рис. 24). Также предусмотрена возможность отсортировать по названию, типу источника, описанию, перейти к добавлению, редактированию или удалению источников сканирования.

Поддерживаемые источники сканирования:

- GitLab
- Nexus
- CLI Tool
- Jfrog
- Harbor
- AppUrl

	Интеграции Инструменты безопасности Источники сканиро	езния Инструменты уведомлений Трекеры зад	94			
器 Информационная панель	+ Добавить источник сканирования × Сбр	росить фильтры		Поиск		۹
🗋 Проекты	Название 三	Источник ч	Описание ~	Статус проверки соединения		
∰ Проблемы безопасности ∰ Библиотека зависимостей	AppURL itsecgames	App URL	AppURL itsecgames_25102024_qamkr	Успешно 25.10.2024, 16:35	0	Û
\bigotimes Контроль качества	asocCore	Git Repository	asocCore	 Успешно 26.03.2025, 01:14 	0	Ċ
Правила О Правила безопасности	CLICustomSource_20241028T135615066Z_mb3c2a	CLI Tool Custom Source	CLICustomSource_20241028T135615066Z_mb3c2a	Ошибка: ASOC-428: Scan sources test co >> 27.03.2025, 13:45	0	Û
 Правила дедупликации Правила реагирования 	CLISourceRG2	CLI Tool Custom Source	CLI_SOURCE_RG2_gamkr	Успешно 27.03.2025, 14:04	0	Û
Администрирование 83. Управление доступом	CLITC Source	CLI Tool Custom Source	CLITC Source_25102024_gamkr	Успешно 25.10.2024, 15:35	0	Û
© Интеграции	CLI without url	CLI Tool Custom Source	CLI without url	Успешно 30.10.2024, 18:39	0	٥
ы отчеты Е Журнал событий	dsfgsdfsd	Git Repository		Oшибка: ASOC-436: Authentication requi >> 31.10.2024, 16:48	0	Û
 Помощник Конструктор полей 	dsfgsdfsdaawnaanwaan	Git Repository		Ошибка: ASOC-436: Authentication requi >> 31.10.2024, 16:51	0	Û
Параметры ЯК Параметры полключения	DWVA	Git Repository		Успешно 31.10.2024,11:28	0	Û
О программе	Git_30second	Git Repository		∆ Не проверен	0	Û
ළි admin	Bcero 185			< 1 2 3 _ 19 >	10 / стр	аница 🗸

Рис.24

9.2.1. Подключение источника сканирования

Чтобы подключить источник сканирования, необходимо выполнить следующие шаги:

- 1. Перейти в раздел Интеграции Источники сканирования.
- 2. Нажать кнопку Добавить источник сканирования.
- В открывшейся форме добавления источника сканирования (Рис. 25) заполнить поля Имя, Описание, в раскрывающемся меню поля Источник выбрать источник сканирования.

	Интеграции			Добавить исто	очник сканирования ×
	Инструменты безопасности Источники сканирования Инструменты уведомлений Трекеры задач			Имя"	
89 Информационная панель	+ Добавить источник сканирования 🛛 🗙 Сбр			Описание*	От 4 до 255 симеолов - Бухвы, цифры, пробелы
🗅 Проекты	Название =	Источник ч	Описание ч		
🛱 Проблемы безопасности	AppURL itsecgames	App URL	AppURL itsecgames_25102024_qamkr		Ст 4 до 255 символов - Бухвы, шифры, пробелы
Библиотека зависимостей				Источник*	Выбрать
⊙ Контроль качества					
Правила	asocCore	Git Repository	asocCore		
Правила безопасности					
💭 Правила дедупликации	seor Eront	Git Panository	searErant		
Ф. Правила реагирования					
Администрирование					
83 Управление доступом	CLICustomSource_20241028T135615066Z_mb3c2a	CLI Tool Custom Source	CLICustomSource_20241028T135615066Z_mb3c2a		
💭 Интеграции					
🔓 Отчеты					
🗉 Журнал событий	CLISourceRG2	CLI Tool Custom Source	CLI_SOURCE_RG2_qamkr		
Э: Помощник					
(). Конструктор полей	CLITC Source	CLI Tool Custom Source	CLITC Source_25102024_gamkr		
Параметры					
🕸 Параметры подключения					
④ О программе	CLI without url	CLI Tool Custom Source	CLI without url		
				Создать Отмена	
ے admin				United and the second s	

Рис. 25

- После выбора источника инструмента необходимо заполнить дополнительные поля, специфичные выбранному на предыдущем шаге инструменту:
 - а. URL источника.

- b. **Метод аутентификации** Заполнение поля на этом этапе не является обязательным, но без него нельзя будет осуществить проверку соединения с источником сканирования.
- с. Далее поля для заполнения далее могут отличаться в зависимости от выбора метода аутентификации. Если метод указан и выбрана аутентификация по API - токену, необходимо заполнить поле **Токен API**, если выбран метод аутентификации по логину и паролю, нужно заполнить поля **Логин/Пароль**. Для проверки соединения, нажать кнопку **Проверить соединение**.

Система отправит запрос на соединение с источником и в верхнем правом углу пользовательского интерфейса отобразится соответствующее уведомление.

5. Далее нажать на кнопку Создать.

9.2.2. Редактирование источника сканирования

Редактирование источника производится с помощью кнопки в соответствующем источнике сканирования. Форма редактирования аналогична форме добавления, но поля заполнены текущими данными (Рис. 26).

≡	Интеграции			Редактироват	ь интеграцию с источником скаї
	Инструменты безопасности Источники сканирования Инструменты уведомлений Трекеры задач				Anni IRI ittacramat
	+ Добавить источник сканирования 🛛 🗙 Сб			NINDH -	Аррокстсякоданняя От 4 до 255 симаолов - Бухаы, цифры, пробелы
 Проекты 	Название 🚍	Источник ч	Описание 🗸	Описание*	AppURL itsecgames_25102024_qamkr
∰ Проблемы безопасности	AppURLitsecgames	App URL	AppURL itsecgames_25102024_qamkr		Ст 4 до 255 симеолов - Бухвы, цифры, пробелы
Библиотека зависимостей				Источник*	App URL V
💮 Контроль качества					
Правила	asocCore	Git Repository	asocCore	ORE NCIONHUKA	http://www.rsecgames.com
Правила безопасности					
Правила дедупликации	asocFront	Git Repository	asocFront		
Ф Правила реагирования					
Администрирование					
8 Управление доступом	CLICustomSource_20241028T135615066Z_mb3c2a	CLI Tool Custom Source	CLICustomSource_20241028T135615066Z_mb3c2a		
🗘 Интеграции					
🖸 Отчеты	CLISourceRG2	CLI Tool Custom Source	CLI SOURCE RG2 namin		
🗄 Журнал событий					
;): Помощник					
[]. Конструктор полей	CLITC Source	CLI Tool Custom Source	CLITC Source_25102024_qamkr		
Параметры					
Параметры подключения					
⑦ О программе	CLI without url	CLI Tool Custom Source	CLI without url		
≗ admin				Сохранить Отмена	р Проверить соединение

Рис. 26

9.2.3. Удаление источника сканирования

Чтобы удалить источник сканирования, перейдите в раздел Интеграции —

Источники сканирования, нажмите на кнопку сканирования, который нужно удалить (Рис. 25), после чего в открывшемся окне подтвердить удаление источника (Рис. 27).



Рис. 27

9.3. Инструменты уведомлений

Подраздел Инструменты уведомлений позволяет настроить интеграцию уведомлений об уязвимостях, например, на электронную почту (Рис. 28).

≡	Интеграции				
	Инструменты безопасности Источники сканирования Ин	струменты уведомлений Трекеры задач			
89 Информационная панель	+ Добавить инструмент уведомления			Поиск	Q 🏶 🕅
🗅 Проекты	Название =	Инструмент 🗸	Статус проверки соединения		
(Д) Проблемы безопасности	testNotifier	Электронная почта	🖉 Успешно	/ 1 🖸	
Библиотека зависимостей			27.03.2025, 10:21		
Контроль качества	Bcero 1			$\langle 1 \rangle$	10/страница 🗸
Правила					
Правила безопасности					
Правила дедупликации					
Ф Правила реагирования					
Администрирование					
83 Управление доступом					
💭 Интеграции					
🔓 Отчеты					
🗄 Журнал событий					
Э: Помощник					
С. Конструктор полей					
Параметры					
Параметры подключения					
⑦ О программе					
ి ədmin					

Рис. 28

Для создания инструмента уведомлений необходимо выполнить следующие шаги:

- 1. В разделе Интеграции → Инструменты уведомлений нажать на кнопку Добавить инструмент уведомлений.
- 2. В открывшемся окне (Рис. 29) заполнить следующие поля
 - Название
 - Инструмент выбрать Электронная почта
 - SMTP-сервер
 - о Порт
 - Имя пользователя
 - Пароль
 - Отправитель
 - При необходимости добавить адреса электронных почт конкретных получателей в поле Получатели

Интеграции			Добавить инс	трумент уве	едомлен	× RN
Инструменты безопасности Источники сканирования Ин	струменты уведомлений Трекеры задач		Название*	Введите название		
+ Добавить инструмент уведомления			Инструмент*	Электронная почта	nea, unqua, nuovena	· ·
Haseakue = TestNotifier	инструмент ч Электронная почта	Статус проверки соединения Успешно	SMTP-cepsep*			
testMailtogo1	Электронная почта	 Успешно 10.04.2025, 14:26 	Порт•	Не выбрано	SSL	TLS
test112	Электронная почта	Успешно 10.04.2025, 14:27		Некоторые SMTP-серверь шифрования. Если при под выбрать соответствующий	и требуют явного ука (ключении возникае) і тип шифрования (SS	зания режима г ошибка, попробуйте SL/TLS).
223231	Электронная почта	Ошибка: ASOC-1018: notifier too 10.04.2025, 14:26	Имя пользователя* Пароль*			۲
Bcero 4			Отправитель*			
			Получатели			~
			Создать Отмена		⊳ Про	верить соединение

Рис. 29

3. При необходимости проверить соединение с помощью кнопки **Проверить** соединение.

Если при подключении возникает ошибка, попробуйте выбрать соответствующий тип шифрования (SSL/TLS).

4. Нажать на кнопку Создать.

9.4. Трекеры задач

В подразделе **Трекеры задач** есть возможность настроить интеграции с трекерами задач (Рис. 30).

≡ ⊕ TRON ASOC	Интеграции Инструменты безопасности Источники сканирования Ин + добавить тремер задач	струменты уведомлений Трекеры заден		
В Информационная панель				
🗋 Проекты	Название ч	Статус	кол-во задач >	Действия
∰ Проблемы безопасности	Jira tracker	Пе активен	2	🙏 Проверить соединение 🥒 📋
Библиотека зависимостей	testTracker	О Активен	9	🖧 Проверить соединение 🥢 📋
Контроль качества				
Правила				
Правила безопасности				
💭 Правила дедупликации				
Правила реагирования				
Администрирование 83 Управление доступом				
💭 Интеграции				
🔒 Отчеты				
🗄 Журнал событий				
Помощник				
(). Конструктор полей				
Параметры © Параметры подключения				
⑦ О программе				
å admin				

Рис. 30

9.4.1. Добавление трекера задач

Для добавления трекера задач необходимо выполнить следующие шаги:

- 1. В разделе Интеграции Трекеры задач нажать на кнопку Добавить трекер задач.
- 2. В открывшемся окне (Рис. 31) заполнить следующие параметры подключения:
 - Название интеграции (например, *Jira Tracker*)
 - URL-адрес рабочей области
 - АРІ-токен аутентификации
 - Логин для аутентификации

Интеграции			Добавить трекер задач ×
Инструменты безопасности Источники сканирования Ин	струменты уведомлений Трекеры задач		1 Подключение — 2 Параметры задач — 3 Маплинг данных — 4 Настройки сикоронизации
+ Добавить трекер задач			Reprint uses uses
Название ч	Статус	Кол-во зада	и URL-адрес рабочей области* Вставить съюжи
Jira tracker	П Не активен	2	
testTracker	Пе активен	9	Аутентификация
			АРІ-токен* Вставьте токен Ф
			Логин* Электронная почта или имя пользователя
			Создать Отмена

Рис. 31

- 3. После заполнения всех полей нажать на кнопку Создать.
- 4. Далее заполнить следующие параметры задач (Рис. 32):
 - Проект
 - Тип задачи
 - Формат отправки задач (как Несколько отдельных задач или Одну общую задачу)

Подключение — (2) Параметры задач — (3) Маллинг данных — (4) Настройки синхронизации						
Укажите параметры по умолчанию,	которые будут применяться к задачам в трек	ере задач				
Проект*		~				
Тип задачи*	Task	~				
Отправлять задачи как	Несколько отдельных задач	Одну общую задачу				
Сохранить Отмена						

Рис. 32

- 5. После заполнения нажать на кнопку Сохранить.
- Далее заполнить необходимые параметры маппинга задач (Рис. 33). Доступен выбор предзаполненных данных с помощью кнопки Применить пресет.

В блоке **Поля** необходимо указать соответствие полей в ASOC с полями в трекере. Для успешного маппинга важно указать все обязательные поля из трекера. По умолчанию обязательные поля указаны в Пресетах, но они могут отличатся от настроек трекера.

В блоке **Статусы** необходимо указать соответствие статусов ASOC со статусами трекера.

Подключение — Параметры задач — Маппинг данных — Настройки синхронизации						
Поля Сопоставьте поля ASOC с полями трекера за	адач					
+ Добавить поле 🛛 🕃 Применить пр	ресет 🖓 Отменить пресет и очистить поля					
Поля ASOC	Поля трекера задач					
Issue ID × View ID × Category × Severity × Tool Type Name × CWE × CVE ×	Х У					
View ID × Category × Severity × Статусы	Х У Резюме					
Сопоставьте статусы ASOC со статусами тре	екера задач					
+ Добавить статус 🛛 🕃 Применить п	пресет 📿 Отменить пресет и очистить поля					
Статусы ASOC	Статусы трекера задач					
в работе	В работе Х У Х					
Ложноположительный	Готово 🗙 🗸					
Подтверждено	Готово х ч х					
Исправлено	(
Сохранить Отмена						

Рис. 33

- 7. Нажать на кнопку Сохранить.
- 8. Далее в случае необходимости обратной отправки изменений из трекера в ASOC (данное действие избавит от потребности ручного отслеживания состояния задач в трекере и обновления данных в ASOC), перевести в активное состояние **Отправку изменений, представленных в трекере задач, в ASOC** (Рис. 34) и нажать на кнопку **Сохранить**.



Рис. 34

После этого в случае успешного соединения трекер будет отображен в списке трекеров в статусе *Активен*.

Также при необходимости доступна возможность проверки соединения с помощью кнопки **Проверить соединение**, и отключение трекера с помощью перевода его **Статуса** в *Не активен* (Рис. 35).

Интеграции			
Инструменты безопасности Источники сканирования Ин	струменты уведомлений Трекеры задач		
+ Добавить трекер задач			
Название 🗸	Статус	Кол-во задач 🗸	Действия
Jira tracker	Пе активен	2	🖧 Проверить соединение 🧷 🖞
testTracker	Пе активен	9	🖧 Проверить соединение 🧷 📋

Рис. 35

Для редактирования/удаления трекера необходимо нажать на соответствующую кнопку действий (Рис. 35).

10. 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. 36).

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

Отчеты Сводные Дета Скачат testday1 30/03/2025 23:24 (1) PDF (1) JSON (1) CSV 30/03/2025 23:22 (4) PDF (4) JSON (4) CSV 29/03/2025 16:25 Le PDF Le JSON Le 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 (+) PDF (+) JSON (+) 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 H PDF H JSON H CSV ñ < 1 2 > 10/страница ~ Bcero 19

Рис. 36

11. 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. 37). Для этого необходимо выполнить следующие шаги:

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

¥	журнал событии						
	Администрирование Функциональные сог	бытия					
8 Информационная панель	Весь период Месяц Неделя День					🛃 Скачать отчет в	формате CSV
🗅 Проекты	🗙 Сбросить фильтры					Поиск	۹
Проблемы безопасности		ID Annec 14	Kon cofferma y	00000000	Voonous kontrassoona		
🖽 Библиотека зависимостей	Ana coonna -				-		<u> </u>
Контроль качества	30/03/2025 23:24	10.150.132.6	ADM-4001 Create Report	User admin created a report testday1	3		
Правила	30/03/2025 23:22	10.150.132.6	ADM-4001 Create Report	User admin created a report testday	3		
Правила дедупликации	30/03/2025 21:01	10.150.132.6	ADM-8002 Project Data Edited	User admin edited the project data TESTDAY1.	5		
Д Правила реагирования	30/03/2025 21:01	10.150.132.6	ADM-8002 Project Data Edited	User admin edited the project data TESTDAY1.	5		
Администрирование В Управление доступом	30/03/2025 21:01	10.150.132.6	ADM-8002	User admin edited the project data	5		
🗘 Интеграции			Project Data Edited	TESTDATI.			
🗋 Отчеты	30/03/2025 21:00	10.150.132.6	ADM-8002 Project Data Edited	User admin edited the project data TESTDAY1.	5		
 В Журнал событий Помощник 	30/03/2025 21:00	10.150.132.6	ADM-8002 Project Data Edited	User admin edited the project data TESTDAY1.	5		
С 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 Параметры подключения	30/03/2025 20:46	10.150.132.6	ADM-2008 Source full settings were viewed by user	Source testAnxolerd full settings viewed by admin	9		
⑦ 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		
ది admin	Bcero 497				< 1 2	3 50 > 10/	страница 🗸

Рис. 37

- 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.

12. Конструктор полей

Раздел Конструктор полей позволяет настроить пользовательские поля проектов (Рис. 38).

≡ ⊕	Конструктор полей
	Проект
ASOC	
99 Информационная ранель	Системные поля
Проекты	Код проекта* 🛈
Проблемы безопасности	Код проекта
Библиотека зависимостей	Название проекта 🛈
Ю Контроль качества	название проекта
Правила	Описание ()
О Правила безопасности	
💭 Правила дедупликации	1
Ф Правила реагирования	Теги 🛈
	- anophile in children -
В Управление доступом	Пользовательские поля
О Интеграции	Дата старта проекта
В Уурнал событий	8
Элурнын созынын	Дата окончания проекта
С. Конструктор полей	
Вараметры	Владелец проекта
🕸 Параметры подключения	~
⑦ О программе	Ссылка на Confluence
	Соблюдение Compliance

Рис. 38

Для настройки необходимо выполнить следующие шаги:

- 1. На странице Конструктор полей нажать кнопку Редактировать поля.
- 2. В открывшемся окне справа (Рис. 39) скорректировать (добавить/удалить) представленный набор полей с помощью кнопок

Добавить поле и	Û	
-----------------	---	--

	Название поля	Тип	Обяз	ательно
8	Дата старта проекта	Дата	~	
8	Дата окончания проекта	Дата	~	
8	Владелец проекта	Список пользователей	~	
H	Ссылка на Confluence	Ссылка	~	
H	Соблюдение Compliance	Чекбокс	~	
8	AppSec	Список пользователей	~	

Рис. 39

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

13. 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	ое соединение Высокоскоростное интернет-соединение, минимум 1 Гбит/с		
Операционная система	 macOS: macOS 10.14 или более поздние версии. Linux: Современные дистрибутивы с поддержкой необходимых версий браузеров. Windows: Windows 10 или более поздние версии. 		
База данных	PostgreSQL 13 или более поздние версии	Рекомендуется настроить резервное копирование и восстановление данных.	
Браузер	Chromium (Google Chrome, Edge, Safari и т. д.) и Firefox.		