

ПК «SAFEERP CS EM»
Руководство администратора

Аннотация

Данный документ представляет собой руководство администратора для работы с программным комплексом «SAFEERP Code Security Extension Module» (далее – ПК «SAFEERP CS EM»).

Настоящее руководство состоит из информационной части (аннотации и листа содержания) и разделов основной части, включающих в себя:

- сведения о назначении ПК «SAFEERP CS EM»;
- общая схема работы ПК «SAFEERP CS EM»;
- описание разделов веб-интерфейса ПК «SAFEERP CS EM»;
- парольная политика ПК «SAFEERP CS EM».

Все примеры в данном документе приведены для ПК «SAFEERP CS EM» версии 4.9.11.

Содержание

1	Назначение ПК «SAFEERP CS EM»	6
1.1	Краткое описание возможностей ПК «SAFEERP CS EM»	6
1.2	Уровень подготовки администратора ПК «SAFEERP CS EM»	6
2	Общая схема работы ПК «SAFEERP CS EM»	8
2.1	Запуск веб-интерфейса ПК «SAFEERP CS EM»	8
2.2	Интеграция с CI/CD	8
2.2.1	Настройка параметров запуска скрипта	8
2.2.2	Настройка пайплайна	8
3	Описание веб-интерфейса ПК «SAFEERP CS EM»	10
3.1	Раздел «Статический анализ»	10
3.1.1	Подраздел «Проекты»	10
3.1.1.1	Создание проектов	12
3.1.1.2	Настройка проекта	18
3.1.1.3	Запуск и остановка сканирования проектов	19
3.1.1.4	Просмотр результатов сканирования	21
3.1.1.5	Выгрузка отчетов	23
3.1.1.6	Управление уязвимостями	26
3.1.1.7	Подключение почтовых уведомлений	33
3.1.1.8	Удаление проектов	41
3.1.2	Подраздел «Профили»	41
3.1.2.1	Просмотр профилей проверок	42
3.1.2.2	Создание профилей проверок	43
3.1.2.3	Редактирование профилей проверок	45
3.1.2.4	Копирование профилей проверок	46
3.1.2.5	Удаление профилей проверок	46
3.1.3	Подраздел «Проверки»	46
3.1.3.1	Добавление пользовательских проверок	46
3.1.3.2	Редактирование проверок	49
3.1.3.3	Удаление пользовательских проверок	49
3.2	Раздел «SCA»	49
3.2.1	Просмотр проекта	51
3.2.2	Добавление проекта	51

3.2.3	Настройка проекта	51
3.2.4	Запуск проекта и остановка сканирования.....	52
3.2.5	Просмотр результатов сканирования	53
3.2.6	Удаление проектов	55
3.3	Раздел «Цели сканирования»	55
3.3.1	Добавление цели сканирования	55
3.3.2	Редактирование цели сканирования.....	56
3.3.3	Удаление цели сканирования.....	56
3.3.4	Источники.....	56
3.3.4.1	Добавление источника типа «1С База данных»	57
3.3.4.2	Добавление источника типа «1С Клиент»	59
3.3.4.3	Добавление источника типа «SAP HANA»	61
3.3.4.4	Добавление источника типа «GIT»	62
3.3.4.5	Добавление источника типа «Файловая система»	66
3.3.4.6	Редактирование источника.....	67
3.3.4.7	Удаление источника.....	69
3.4	Раздел «Настройки»	70
3.4.1	Подраздел «Информация»	70
3.4.2	Подраздел «Лицензия»	72
3.4.2.1	Активация лицензии.....	73
3.4.2.2	Обновление лицензии.....	77
3.4.3	Подраздел «Jira».....	77
3.4.4	Подраздел «Пользователи»	78
3.4.4.1	Создание учётной записи	79
3.4.4.2	Удаление учётной записи	81
3.4.4.3	Изменение учётной записи	81
3.4.4.4	Сброс пароля УЗ	81
3.4.4.5	Блокировка и разблокировка учётной записи	82
3.4.4.6	Полномочия и роли	82
3.4.4.7	Пользовательские роли	84
3.4.4.8	Создание пользовательских ролей.....	84
3.4.4.9	Полномочия, назначаемые пользовательским ролям.....	85
3.4.4.10	Редактирование пользовательских ролей	89
3.4.4.11	Копирование ролей.....	90
3.4.4.12	Удаление пользовательских ролей	91
3.4.5	Подраздел «Журнал»	91

3.4.5.1	Просмотр журнала	94
3.4.5.2	Выгрузка журнала.....	94
3.5	Профиль пользователя.....	95
3.5.1	Просмотр данных текущего пользователя	95
3.5.2	Смена пароля	95
3.5.3	Просмотр списка активных подписок	95
3.5.4	Отмена почтовых подписок.....	96
4	Парольная политика.....	97
	Список сокращений	98

1 Назначение ПК «SAFEERP CS EM»

ПК «SAFEERP CS EM» предназначен:

- для анализа исходного кода различных языков программирования и технологий методом статического анализа;
- для анализа сторонних компонентов и библиотек с открытым исходным кодом (Open Source), используемых в ПО, для выявления уязвимостей и проблем с лицензиями.

Областью контроля ПК «SAFEERP CS EM» являются программные коды следующих языков программирования:

- 1C;
- Dockerfile;
- SQLScript;
- JavaScript;
- Python;
- C#;
- Java;
- XSJS;
- XS;
- файлов XAML и XML.

1.1 Краткое описание возможностей ПК «SAFEERP CS EM»

Функции ПК «SAFEERP CS EM», реализованные для администратора ПК в веб-интерфейсе:

- создание и редактирование проектов для анализа;
- запуск сканирования проектов для проведения процедур анализа кода контролируемых систем;
- подключение почтовых уведомлений по проекту;
- мониторинг результатов анализа во время выполнения итерации;
- выгрузка отчётов по результатам анализа в форматах pdf или xlsx;
- проверка статусов доступности ранее подключенных источников данных;
- администрирование пользователей и их ролей;
- подключение, редактирование, удаление источников данных;
- создание и редактирование профилей сканирования;
- создание новых пользовательских проверок;
- активация и удаление лицензий;
- просмотр и загрузка журнала событий.

1.2 Уровень подготовки администратора ПК «SAFEERP CS EM»

Администрирующий персонал ПК «SAFEERP CS EM» включает следующие роли:

- администратор ПК;

— администратор информационной безопасности.

Данный документ предназначен для администратора ПК «SAFEERP CS EM».

Квалификация и знания администратора ПК «SAFEERP CS EM» (АПК) должны быть достаточными для выполнения всех действий, предусмотренных данным документом, и должны определяться его опытом и стажем выполнения соответствующих работ.

2 Общая схема работы ПК «SAFEERP CS EM»

2.1 Запуск веб-интерфейса ПК «SAFEERP CS EM»

Доступ к веб-интерфейсу ПК «SAFEERP CS EM» осуществляется через веб-браузер по адресу, заданному при установке или настройке комплекса.

Примечание. После установки ПК «SAFEERP CS EM» первичная авторизация осуществляется с помощью пользователя `system` с заданным паролем `System__12`. После авторизации необходимо сменить пароль пользователю `system` согласно пункту 4 данного руководства.

2.2 Интеграция с CI/CD

ПК «SAFEERP CS EM» может быть внедрён в процесс непрерывной интеграции и непрерывного развертывания (CI/CD) с помощью специального скрипта, который запускается через интерфейс командной строки (CLI). В рамках пайплайна GitLab CI/CD для выполнения задач используются различные раннеры, такие как Shell или Docker. Перед настройкой CI/CD процесса необходимо в SafeERP создать проект, выбрав источником данных архив

2.2.1 Настройка параметров запуска скрипта

Параметры скрипта `sast.py` представлены ниже:

- **-d** – адрес сервера, на котором развёрнут ПК «SAFEERP CS EM»;
- **-u** – логин от УЗ пользователя ПК «SAFEERP CS EM», у которого есть полномочия на создание и запуск сканирования проектов;
- **-p** – пароль от УЗ пользователя ПК «SAFEERP CS EM», который указан в параметре 2;
- **-n** – название проекта, создаваемого в ПК «SAFEERP CS EM» перед запуском пайплайна.

Примечания:

1. В создаваемом проекте источником данных должен являться архив (пиктограмма ).
2. Файлы, содержащие код для сканирования, должны быть расположены в репозитории GitLab, где запускается пайплайн.

2.2.2 Настройка пайплайна

Для каждого проекта GitLab, где используется CI/CD, необходимо наличие файла `.gitlab-ci.yml`, содержащего конфигурации для задач и настроек проекта. В случае использования ПК «SafeERP CS EM» данный файл выглядит следующим образом:

stages:

- sast

safeerp-check:

stage: sast

image:

```
name: sast_safeerp:latest
entrypoint: [""]
script:
  - set -e
  - test -f ci/sast.py || { echo "ci/sast.py не найден в репозитории"; exit 1; }
  - python -W ignore ci/sast.py -d $ADDR -u $SE_LOGIN -p $SE_PASS -n
$PROJECT_NAME
artifacts:
  when: always
  paths:
    - results/AnalysisResult*
    - results/
variables:
  SAVE_PDF: "1"
  SAVE_JSON: "1"
  SAVE_ASH: "1"
```

Для настройки скачивания отчетов необходимо в параметрах SAVE_PDF, SAVE_JSON, SAVE_ASH указать значения 1 или 0. 1 – формировать отчет в соответствующем формате, 0 – не формировать.

3 Описание веб-интерфейса ПК «SAFEERP CS EM»

ПК «SafeERP CS EM» содержит следующие разделы:

- «Статический анализ»;
- «SCA»;
- «Цели сканирования»;
- «Настройки».

3.1 Раздел «Статический анализ»

Раздел «Статический анализ» предназначен для анализа кода методом статического анализа.

Раздел «Статический анализ» содержит следующие функциональные подразделы:

- «Проекты»;
- «Профили»;
- «Проверки».

3.1.1 Подраздел «Проекты»

Основная рабочая область подраздела «Проекты» представлена на рис. 1 .

Проекты							⧻
Введите запрос для поиска							+ Добавить проект
Название	Статус	Последний запуск	Тип проекта	Профили	Языки	Всего итераций	⋮
	Отменено	28.05.2026 18:56:13		1 ▾	11 ▾	13	
	Отменено	28.05.2026 18:55:42		1 ▾	11 ▾	9	
	Завершено	28.05.2026 17:23:32		1 ▾	1 ▾	5	
	Завершено	28.05.2026 17:22:56		1 ▾	11 ▾	4	
	Завершено	28.05.2026 17:16:04		1 ▾	1 ▾	2	
	Завершено	28.05.2026 17:03:37		1 ▾	11 ▾	28	
	Завершено	28.05.2026 12:49:00		1 ▾	11 ▾	14	
	Ошибка	20.05.2026 10:07:31		1 ▾	11 ▾	1	
	Завершено	28.05.2026 09:08:00		1 ▾	11 ▾	14	
	Завершено	27.05.2026 14:52:42		1 ▾	11 ▾	1	

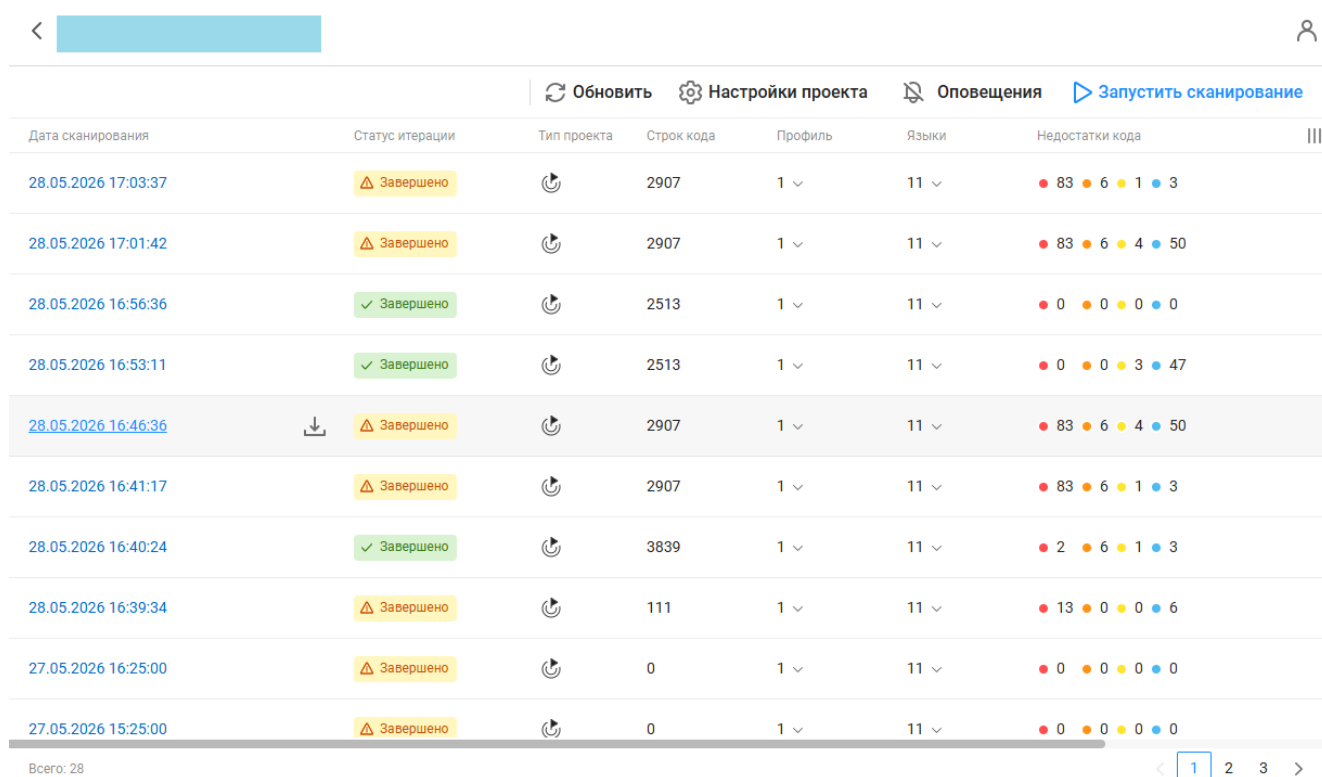
Всего: 135

Рисунок 1 – Основная рабочая область подраздела «Проекты»

Доступные действия в подразделе «Проекты» изложены в подпунктах 3.1.1.1 – 3.1.1.8 .
Для просмотра списка итераций проекта необходимо нажать на название проекта. В окне

показаны следующие столбцы (рис. 2):

- «Дата сканирования»;
- «Статус итерации»;
- «Тип проекта» – тип источника данных. Источники данных бывают следующих видов: архив и цели сканирования;
- «Строк кода» – количество проанализированных строк кода;
- «Профиль» – профили проверок, примененные к данной итерации;
- «Языки» – языки программирования проверок, используемых при анализе проекта;
- «Недостатки кода»;
- «Время сканирования».



Дата сканирования	Статус итерации	Тип проекта	Строк кода	Профиль	Языки	Недостатки кода	
28.05.2026 17:03:37	⚠ Завершено	🔄	2907	1 ▾	11 ▾	83 6 1 3	
28.05.2026 17:01:42	⚠ Завершено	🔄	2907	1 ▾	11 ▾	83 6 4 50	
28.05.2026 16:56:36	✓ Завершено	🔄	2513	1 ▾	11 ▾	0 0 0 0	
28.05.2026 16:53:11	✓ Завершено	🔄	2513	1 ▾	11 ▾	0 0 3 47	
28.05.2026 16:46:36	⬇ ⚠ Завершено	🔄	2907	1 ▾	11 ▾	83 6 4 50	
28.05.2026 16:41:17	⚠ Завершено	🔄	2907	1 ▾	11 ▾	83 6 1 3	
28.05.2026 16:40:24	✓ Завершено	🔄	3839	1 ▾	11 ▾	2 6 1 3	
28.05.2026 16:39:34	⚠ Завершено	🔄	111	1 ▾	11 ▾	13 0 0 6	
27.05.2026 16:25:00	⚠ Завершено	🔄	0	1 ▾	11 ▾	0 0 0 0	
27.05.2026 15:25:00	⚠ Завершено	🔄	0	1 ▾	11 ▾	0 0 0 0	

Всего: 28

Рисунок 2 – Список итераций проекта

Статусы проектов и итерации

Доступные статусы итераций и проектов представлены в таблице 1.

Таблица 1 – Статусы итераций и проектов

Статус	Значение
Нет сканирований	Проект создан. Сканирование не было запущено. Доступно для проектов
Выполняется (1%)	Запущен процесс сканирования
✓ Завершено	Сканирование завершено. Ошибки не обнаружены

 Завершено	Сканирование завершено. Обнаружены ошибки
 Ошибка	Сканирование было прервано из-за возникших ошибок
 Отменено	Сканирование было отменено пользователем

Недостатки кода

В таблице 2 представлены уровни критичности для недостатков кода.

Таблица 2 – Значения цветов для уровня критичности

Цвет	Значение
	Высокий
	Средний
	Низкий
	Информация

3.1.1.1 Создание проектов

Перед созданием проекта с источником данных «Цель сканирования» необходимо выполнить следующие действия:

- 1) Добавить цели сканирования. Подробное описание представлено в пункте 3.3.1 .
- 2) Добавить источник в цель сканирования. Подробное описание представлено в пункте 3.3.4 .

Для создания проекта необходимо выполнить следующие действия:

- 1) Выбрать подраздел «Проекты».
- 2) Нажать кнопку «+Добавить проект» (рис. 1).
- 3) Ввести название проекта, выбрать профиль или профили проверок, выбрать источник данных (рис. 3).
- 4) Выбрать цель сканирования (для проектов с одним источником данных типа «Цели сканирования» (рис. 4)) из выпадающего списка. Нажать кнопку «+Добавить источник». Выбрать тип источника, нажать кнопку «Применить» (рис. 5, 6, 7, 8, 9).
- 5) Выбрать тип запуска проекта.
- 6) Нажать кнопку «Добавить» (см. рис. 3 или рис. 4).

< Добавить проект

Название проекта

источник 1

Профили

Все проверки ×

Тип проекта



Добавить

Отменить

Сбросить

Рисунок 3 – Параметры создания нового проекта с типом источника данных «Архив»

< Добавить проект



Название проекта

Проект 1|

Профили

Все проверки ×

Тип проекта



Цель сканирования



Отложенный запуск

Выключен

Введите запрос для поиска

[+ Добавить источник](#)

Список пуст

Вы можете добавить источник при помощи кнопки ниже

Добавить источник

Добавить

Отменить

Сбросить

Рисунок 4 – Параметры создания проекта с источниками данных «Цель сканирования»

× Добавить источник

Источник данных	1C SAP HANA GIT Файловая система
Источник	
Объекты	

Добавить

Отменить

Рисунок 5 – Выбор источника данных типа 1C при создании проекта

× Добавить источник

Источник данных	1C SAP HANA Git Файловая система
Источник	
Объекты	

Добавить

Отменить

Рисунок 6 – Добавление источника типа SAP HANA

× Добавить источник

Источник данных	1C SAP HANA Git Файловая система
Источник	GIT Kate2 Extensions ▼
Коммит	07b9c5c8: Update code.Cs ▼
Объекты	GIT Kate2 Extensions × ▼
Режим сравнения с коммитом	Выкл. Из прошлой итерации Из источника

Добавить

Отменить

Рисунок 7 – Добавление источника типа Git без режима сравнения

× Добавить источник

Источник данных	1C SAP HANA Git Файловая система
Источник	test_repo_gf-gitflic 815565 ▼
Коммит	8456e687: минус s02 ▼
Объекты	test_repo_gf-gitflic 815565 × ▼
Режим сравнения с коммитом	Выкл. Из прошлой итерации Из источника

Добавить

Отменить

Рисунок 8 – Добавление источника с режимом сравнения с коммитом «Из прошлой итерации»

× Добавить источник

Источник данных	1С SAP HANA Git Файловая система
Источник	test_repo_gf-gitflic 815565
Коммит	403135fd: изменен s_onec_005
Объекты	test_repo_gf-gitflic 815565 ×
Режим сравнения с коммитом	Выкл. Из прошлой итерации Из источника
Источник для сравнения	cs_git_testexamples_OK
Коммит для сравнения	9676380e: Поправил отступы в тестовых пр...

Добавить

Отменить

Рисунок 9 – Добавление источника с режимом сравнения с коммитом «Из источника»

Примечания:

1. В проектах доступен отложенный запуск. Доступны следующие варианты отложенного запуска:
 - однократный отложенный запуск;
 - многократный отложенный запуск.

При выборе однократного отложенного запуска необходимо задать только дату и время, в которое будет запущено сканирование. При выборе многократного отложенного запуска необходимо задать период, во время которого будут производиться запуски сканирований, а также выбрать периодичность запуска сканирований. При выборе периодичности запуска сканирований существует два варианта:

- а) запуск сканирований с определённым интервалом (интервал в минутах или часах);
 - б) запуск сканирований по расписанию (каждый день, неделю или месяц в назначенное время).
2. Если источником данных является «1С база данных», то доступно сканирование редактируемых модулей. Для сканирования редактируемых модулей необходимо выбрать элемент «Редактируемые модули» в области «Сканировать», нажать кнопку «Применить» (см. рис. 5).

Примечание. При выборе элемента «Редактируемые модули» в ПК «SAFEERP CS EM» выгружаются файлы с кодом объектов, у которых правило поддержки установлено в значении: «Объект поставщика редактируется с сохранением поддержки» или «Объект поставщика снят с поддержки».

3. Если источником данных является 1С «База данных», то администратору или пользователю с правом на администрирование ПК «SAFEERP CS EM» доступен выбор объектов для сканирования. Для выбора объектов необходимо выбрать источник из списка, выбрать объекты в поле «Объекты», нажать кнопку «Применить» (см. рис. 5). Примечание. Внешние отчёты и обработки отделяются при выборе объекта сканирования
4. Если источником данных является «1С база данных», то доступно сканирование измененного кода, в который были внесены изменения с момента последнего сканирования. Для сканирования измененного кода необходимо следующее:

- источник сканирования должен быть один и тот же;
- хотя бы одна итерация проекта.

Для сканирования измененного кода необходимо установить флаг напротив «Только измененный» (см. рис. 5) в области «Сканировать», нажать кнопку «Применить».

В отчет по результатам сканирования выводится информация по дельте, не учитывая другой код.

5. Если источником данных выбран Git, то доступно сравнение двух источников типа git с целью сканирования измененного кода. Подробное описание см. в подпункте 3.1.1.1.1.

3.1.1.1.1 Сравнение двух источников типа git

В проектах доступно сравнение источников типа git. Данная функциональность доступна в проектах с источником данных типа git.

Доступны следующие режимы сравнения с коммитом:

- «Выкл» – сравнение источников отключено;
- «Из прошлой итерации» – сравнивается код с предыдущей итерацией;
- «Из источника» – сравнение кода с выбранным источником и коммитом.

При использовании функции сравнения кода необходимо указать два источника:

- источник – основной сканируемый источник, который будет проанализирован. Предполагается, что он содержит актуальную или расширенную версию кода;
- источник для сравнения – эталонный источник, с которым будет сопоставляться сканируемый источник. Ожидается, что он содержит более старую или меньшую версию кода.

В ПК «SAFEERP CS EM» анализируется сканируемый источник (основной источник) и определяет, какие файлы были изменены по сравнению с источником для сравнения (эталонным источником). В сканирование попадают только те файлы из сканируемого источника, которые:

- добавлены (есть в сканируемом источнике, но отсутствуют в источнике для

сравнения);

- изменены (различается содержимое файлов при сравнении);
- переименованы (изменилось имя файла или расширение);
- перемещены (изменился путь относительно корневой директории).

В результат сканирования выводятся только найденные уязвимости по коду, полученному в результате сравнения.

Добавление источника с сравниваемым кодом доступно на страницах:

- добавления проекта;
- настройки проекта.

Для сканирования источника необходимо выполнить следующие действия:

- 1) Нажать кнопку «+ *Добавить источник*».
- 2) Выбрать источник данных типа «Git».
- 3) Выбрать источник для сканирования в области «Источник». Выбрать объекты в области «Объекты».
- 4) Выбрать режим сравнения в поле «Режим сравнения с коммитом» (см. рис. 8 или 9).
Примечание. Для режима сравнения «С источником» необходимо выбрать источник для сравнения и коммит в полях «Источник для сравнения» и «Коммит для сравнения» (см. рис. 8).
- 5) Нажать кнопку «*Добавить*» (рис. 8).
- 6) Сохранить изменения в проекте.
- 7) Запустить сканирование проекта.

Примечание. Результаты сканирования будут доступны после запуска сканирования.

3.1.1.2 Настройка проекта

Для настройки проекта необходимо выполнить следующие действия:

- 1) Выбрать подраздел «Проекты».
- 2) Выбрать проект.
- 3) Нажать кнопку «*Настройки проекта*».
- 4) Внести изменения (название проекта, изменить профиль, добавить или удалить источники, включить или выключить отложенный запуск).
- 5) Нажать кнопку «*Сохранить*» (рис. 10).

< ST_Doc2

> Дополнительная информация

Название проекта

Профили Проверки 1С ×

Источник данных

Цель сканирования

Отложенный запуск Выключен

Введите запрос для поиска + Добавить источник

Название	Последнее состояние	Описание	Путь к источнику
	• Доступен		

Всего: 1

Сохранить Отменить Сбросить

Рисунок 10 – Настройки проекта

Примечания:

1. Для очищения введенных значений предусмотрена кнопка «Сбросить».
2. Для возврата на предыдущую страницу предусмотрена кнопка «Отменить».

3.1.1.3 Запуск и остановка сканирования проектов

Запуск сканирования осуществляется двумя способами:

- через контекстное меню;
- со страницы проекта.

Для запуска сканирования со страницы проекта необходимо выполнить следующие действия:

- 1) Выбрать подраздел «Проекты».
- 2) Выбрать проект.
- 3) Нажать кнопку «Запустить сканирование» (см. рис. 2).

Для запуска сканирования через контекстное меню необходимо выполнить следующие действия:

- 1) Выбрать подраздел «Проекты».
- 2) Нажать кнопку  в строке проекта, выбрать пункт «Запустить» в контекстном меню (рис. 11).

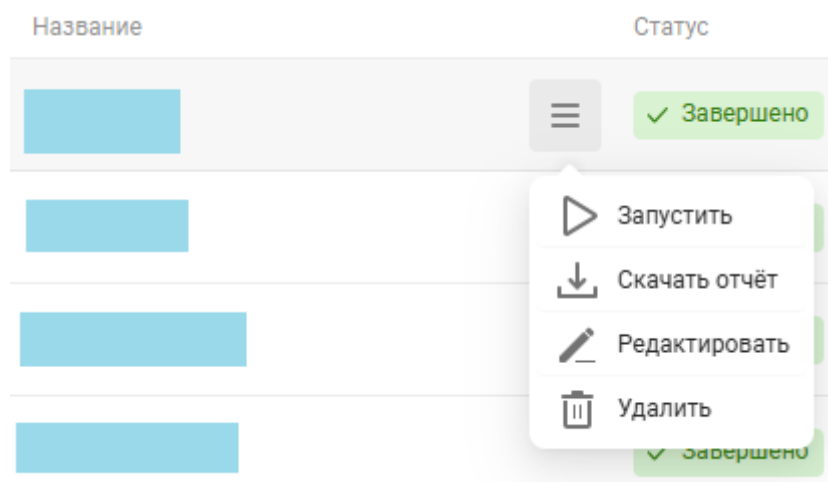


Рисунок 11 – Контекстное меню

Остановка сканирования

Остановка сканирования осуществляется следующими способами:

- через контекстное меню в строке проекта;
- со страницы проекта.

Для остановки сканирования со страницы проекта, необходимо выполнить следующие действия:

- 1) Выбрать подраздел «Проекты» .
- 2) Выбрать проект.
- 3) Нажать кнопку «Остановить сканирование».

Для остановки сканирования через контекстное меню необходимо выполнить следующие действия:

- 1) Выбрать пункт меню «Проекты».
- 2) Нажать кнопку  в строке проекта, выбрать пункт «Остановить» в контекстном меню.

Примечания:

1. Запуск сканирования проекта доступен только при наличии действующей лицензии на сервер управления соответствующего варианта исполнения (ПК «SafeERP CS EM» или ПК «SafeERP PS EM»). При истечении срока действия лицензии запуск сканирования блокируется до ее продления. Подробнее об условиях доступа см. в пункте 3.4.2.
2. При запуске сканирования проектов, в которых источником данных выбран архив , необходимо выбрать файл для анализа в следующих форматах:
 - zip;
 - cf;
 - cfe;
 - cfu;
 - erf;
 - epf;

- bsl;
- txt;
- js;
- js_;
- xsjs;
- dockerfile;
- xaml;
- ltp;
- ltw;
- xml;
- hdbprocedure;
- py;
- cs;
- java;
- xsaccess.

3.1.1.4 Просмотр результатов сканирования

При просмотре результатов сканирования доступно следующее:

- просмотр панели мониторинга по результатам итерации;
- просмотр результатов сканирования по результатам итерации;
- просмотр информации о найденной уязвимости.

Просмотр панели мониторинга

Для просмотра панели мониторинга необходимо выполнить следующие действия:

- 1) Выбрать проект.
- 2) Выбрать итерацию проекта.
- 3) Выбрать вкладку («Все результаты» или «Без исключенных уязвимостей»).

Данные панели мониторинга представлены на рис. 12. Доступен просмотр следующих областей:

- найденные уязвимости (количество и степень критичности найденных уязвимостей);
- динамика по уязвимостям (сравнение количества найденных уязвимостей с результатами предыдущего сканирования);
- соотношение уязвимостей (сравнение новых, сохранившихся и исправленных уязвимостей с результатами предыдущего сканирования);
- неблагополучный источник (указан источник с наибольшим количеством найденных уязвимостей и их критичность);
- наиболее часто срабатывающие проверки (топ-10 проверок с наибольшим количеством найденных уязвимостей).

Примечания:

1. При выборе панели мониторинга с заголовком «Без исключенных уязвимостей» отображаются уязвимости со статусами «Не устранена» и «В работе» (см. рис.

- 12).
2. При выборе панели мониторинга с заголовком «Все результаты» отображаются уязвимости со всеми статусами.

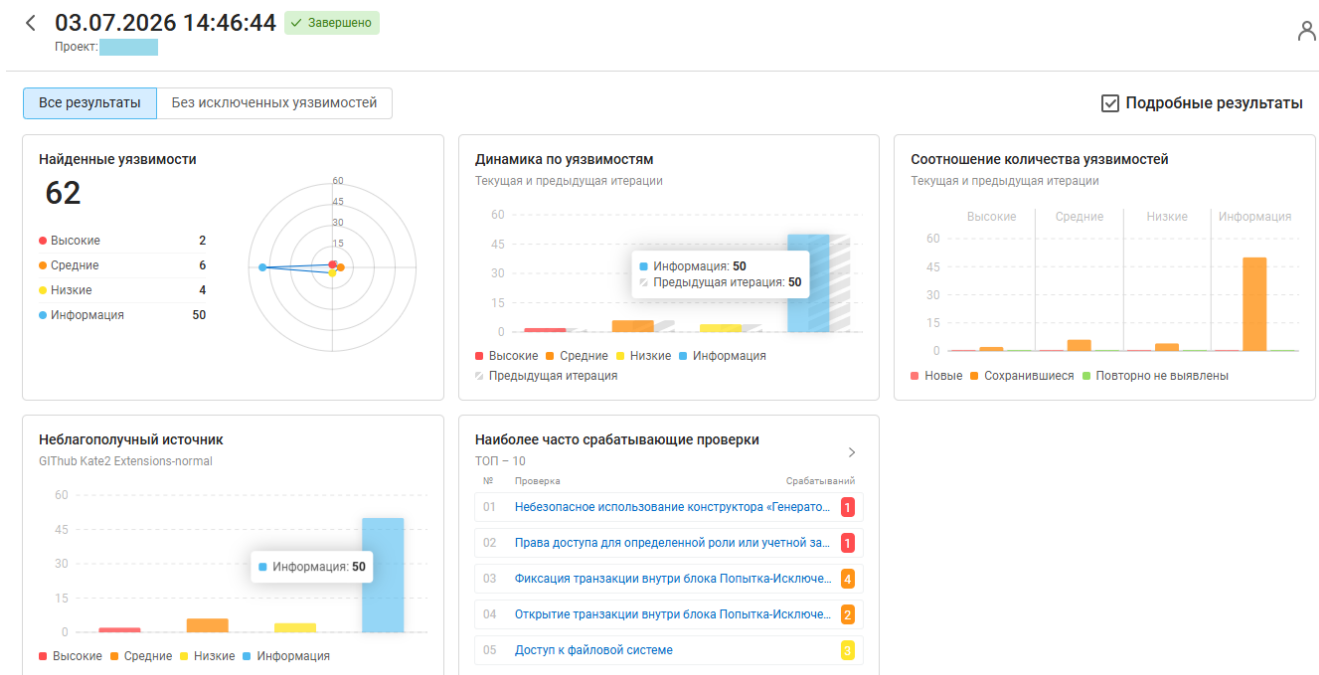


Рисунок 12 – Панель мониторинга по результатам итерации

Просмотр результатов итерации

Для просмотра результатов итерации необходимо выполнить следующие действия:

- 1) Выбрать проект.
- 2) Выбрать итерацию проекта.
- 3) Выбрать вкладку («Все результаты» или «Без исключенных уязвимостей»). Нажать кнопку «*Подробные результаты*».

Просмотр информации о найденной уязвимости

Для просмотра информации о найденной уязвимости необходимо выполнить следующие действия:

- 1) Выбрать проект.
- 2) Выбрать итерацию из списка, выбрать вкладку («Все результаты» или «Без исключенных уязвимостей»), нажать кнопку «*Подробные результаты*».
- 3) Выбрать проверку в дереве уязвимостей, выбрать уязвимость (рис. 13).

28.05.2026 09:21:00 ✓ Завершено

Проект:

Найденные уязвимости 21 | Исключенные уязвимости

Введите з...

Основная конфигурация/HTTPСервисы/MobileApp/Module.bsl

```
82
83 //Возвращает httpОтвет клиенту
84 //Параметры:
85 //Запрос - httpЗапрос с мобильного клиента, в котором содержатся параметры для сборки ответного сообщения
86 функция GetDataGET(Запрос)
87
88 УстановитьПривилегированныйРежим(Истина);
89
90 ПараметрыЗапроса = ПараметрыЗапроса(Запрос);
91
92 Если ТипЗнч(ПараметрыЗапроса) <> Тип("Соответствие") Тогда
93
```

Информация | Рекомендации | **Пример** | Ссылки | Управление уязвимостью | История

Пример кода с уязвимостью

```
1 функция ПроверитьСпособДоставки(Рассылка, Знач ПараметрыДоставки)
2     УстановитьПривилегированныйРежим(Истина);
3     ПараметрыЖурнала = Новый Структура;
4     ПараметрыЖурнала.Вставить("Метаданные", Метаданные.Справочники.РассылкиОтче
5     ПараметрыЖурнала.Вставить("МассивОшибок", Новый Массив);
6     ОпаснаяФункция();
7     КонецФункции
```

Пример кода без уязвимости

```
1 функция ПроверитьСпособДоставки(Рассылка, Знач ПараметрыДоставки)
2     УстановитьПривилегированныйРежим(Истина);
3     ПараметрыЖурнала = Новый Структура;
4     ПараметрыЖурнала.Вставить("Метаданные", Метаданные.Справочники.РассылкиОтчетов);
5     ПараметрыЖурнала.Вставить("МассивОшибок", Новый Массив);
6     УстановитьПривилегированныйРежим(Ложь);
7     ОпаснаяФункция();
8     КонецФункции
```

Всего проверок: 8 Выбранных уязвимостей: 0

Рисунок 13 – Строка с найденной уязвимостью

При просмотре результатов итерации пользователю доступны следующие действия (см. рис. 13):

- поиск уязвимости с помощью поисковой строки;
- управление уязвимостью (массовое и единичное);
- выгрузка отчетов;
- фильтрация результатов сканирования по источнику, состоянию уязвимости, языку программирования и уровню критичности уязвимости;
- свернуть/развернуть дерево уязвимостей;
- свернуть/развернуть область кода.

Примечание. Во вкладке «История» доступен просмотр изменений найденной уязвимости, а также добавление комментария.

3.1.1.5 Выгрузка отчетов

В подразделе «Проекты» доступна выгрузка отчетов по результатам сканирования.

Выгрузка отчёта доступна со следующих страниц:

- список проектов (рис. 14);
- списка итераций (рис. 15);
- страница подробных результатов – вкладки «Найденные уязвимости» и «Исключенные уязвимости» (рис. 16).

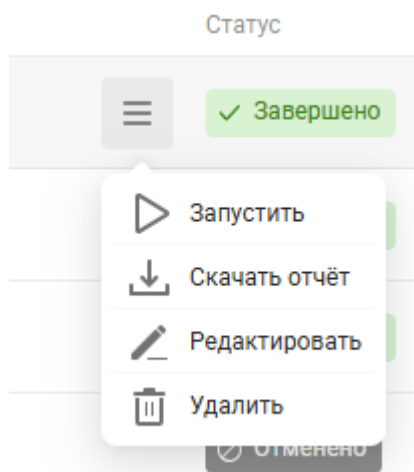


Рисунок 14 – Выгрузка отчета на странице списка проектов

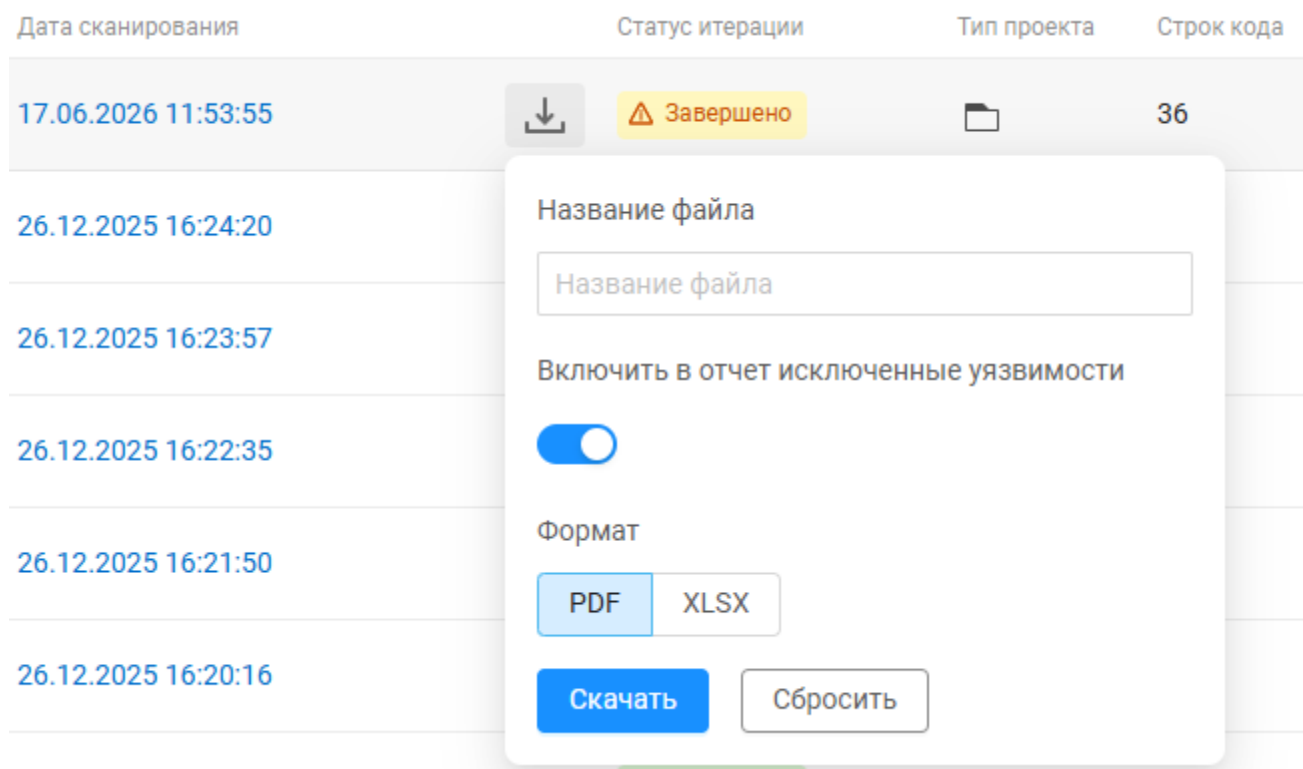


Рисунок 15 – Выгрузка отчета

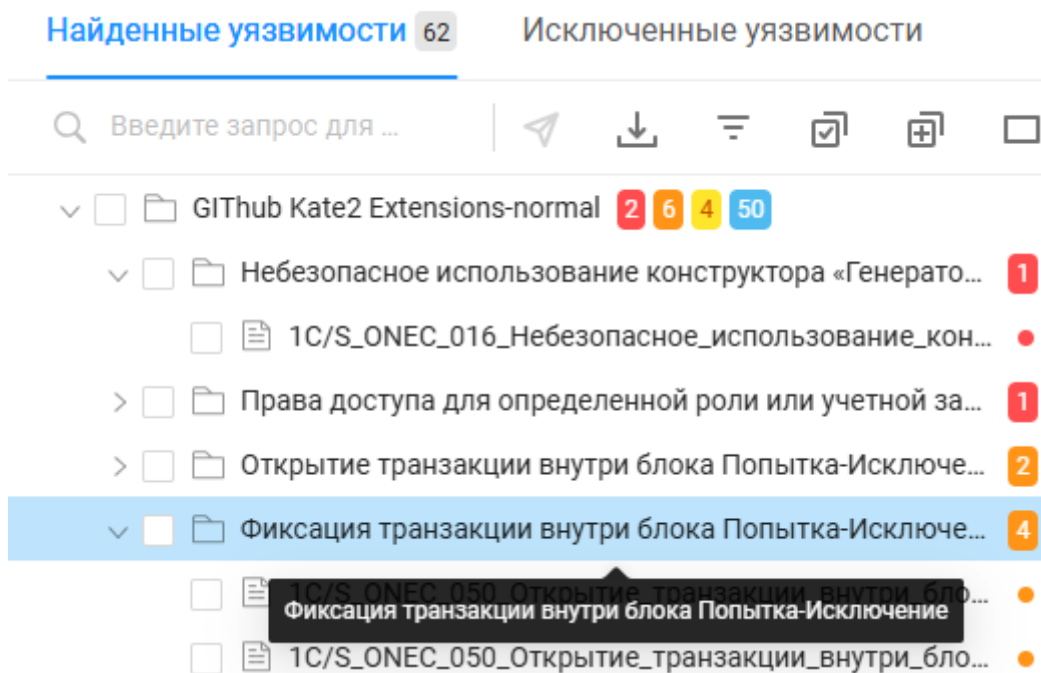


Рисунок 16 – Выгрузка отчета при просмотре дерева уязвимостей

Примечания:

1. Если оставить поле «Название файла» пустым, то файл архива с отчётом будет сохранён с названием, назначенным по умолчанию, в формате AnalysisResult_имя_проекта__дата_и_время_начала_сканирования.zip.
2. Файлы, которые войдут в архив, доступны в следующих форматах: PDF и XLSX.
3. Архив отчёта содержит файл «Общая информация», а также отдельные файлы по каждой проверке, в которых обнаружены уязвимости.
4. Максимальное количество отчётов, скачиваемых параллельно – два.
5. При формировании полного отчёта о сканировании, уязвимости, перенесённые в исключенные, в отчёт не попадают.

Выгрузка отчета со страницы списка проектов

На странице списка проектов доступно следующее:

- выгрузка полного отчета (включая исключенные уязвимости) - данный отчет выгружается по умолчанию;
- выгрузка отчета без исключенных уязвимостей - данный отчет содержит уязвимости, которые находятся во вкладке «Найденные уязвимости».

Выгрузка отчета со страницы списка итераций

На странице списка итераций доступна выгрузка отчета по результатам итераций (полный или без исключенных уязвимостей).

Выгрузка отчета со страницы подробных результатов

На странице дерева уязвимостей, как на вкладке «Найденные уязвимости», так и на вкладке «Исключенные уязвимости», доступна выгрузка отчёта в следующих вариантах:

- отчёт по умолчанию – выгружаются все уязвимости, если уязвимости в дереве не

- выбраны. Содержит информацию по всем уязвимостям вне зависимости от места загрузки отчёта;
- настраиваемый отчёт – выгружается по выбранным в дереве уязвимостям.

Если ни одна из уязвимостей не
выбрана, скачается отчет по всем
исключенным уязвимостям

Название файла

Название файла

Формат

PDF XLSX

Скачать Сбросить

Рисунок 17 – Окно сохранения отчета при выборе вкладки «Исключенные уязвимости»

XLSX отчет с информацией по сравнению двух итераций

В подразделе «Проекты» доступно сравнение итераций со статусом «Завершено» или «Предупреждение».

Сравнение итераций доступно:

- на странице списка проектов;
- на странице списка итераций;
- на странице подробных результатов во вкладке «Найденные уязвимости».

Для сравнения двух итераций необходимо выполнить следующие действия:

- 1) Нажать кнопку «Скачать отчет»;
- 2) Выбрать формат отчета *xlsx;
- 3) Выбрать итерацию для сравнения в поле «Итерация для сравнения».
- 4) Нажать кнопку «Скачать».

Примечание. Если итерация сравнения не выбрана, то сравнение по умолчанию идет с предыдущей успешной итерацией.

3.1.1.6 Управление уязвимостями

Управление уязвимостями осуществляется после проведения сканирования.

Администратору доступно следующее:

- единичное управление уязвимостью;
- массовое управление уязвимостью.

Найденные уязвимости принимают следующие статусы:

- «Не устранена» – данный статус присваивается уязвимости после обнаружения уязвимости;
- «В работе» – данный статус присваивается уязвимости администратором или пользователем с полномочиями на управление уязвимостями.

Исключенные уязвимости принимают следующие статусы:

- «Принята» – данный статус используется для обнаруженных уязвимостей, которые невозможно устранить оперативно, но которые должны быть исправлены в будущем;
- «Устранена» – данный статус используется для исключения исправленных уязвимостей;
- «Ложное срабатывание» – данный статус используется для исключения исправленных уязвимостей.

Для единичного управления уязвимостью необходимо выполнить следующие действия:

- 1) Выбрать проект.
- 2) Выбрать итерацию из списка. Нажать кнопку «*Подробные результаты*» (рис. 12).
- 3) Раскрыть проверку, выбрать уязвимость (рис. 18).

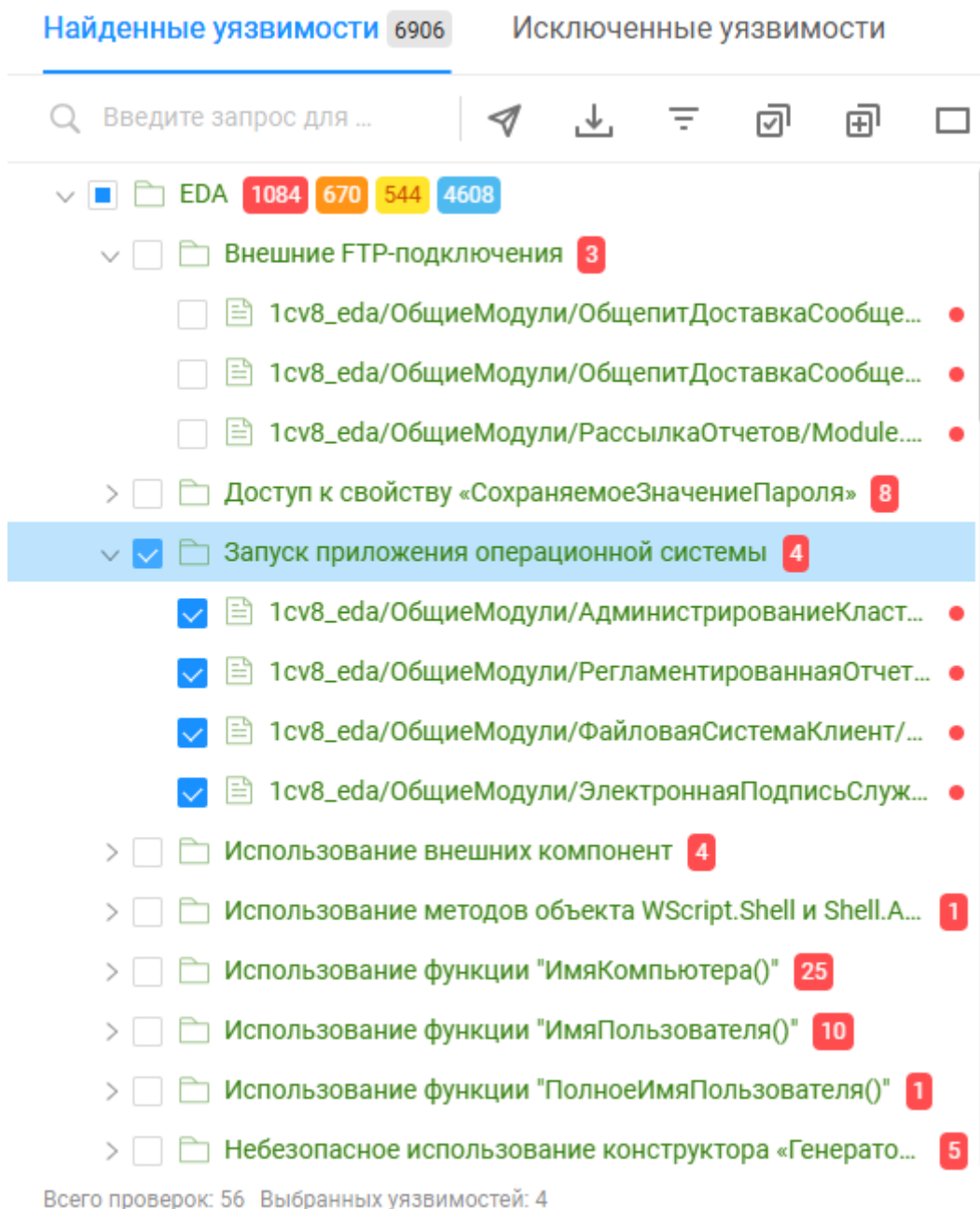


Рисунок 18 – Список обнаруженных недостатков кода

- 4) Выбрать выделенную строку. В открывшемся окне выбрать вкладку «Управление уязвимостью» (рис. 19).

[Информация](#) [Рекомендации](#) [Пример](#) [Ссылки](#) [Управление уязвимостью](#) [История](#)

Уровень критичности

Средняя

Статус уязвимости

Не устранена

Исполнитель

1 1

☒ Связать с задачей в Jira

Приоритет

Highest

Комментарий

Введите комментарий

Применить

Рисунок 19 – Окно для работы с уязвимостями

- 5) Указать статус уязвимости и уровень критичности (при необходимости), выбрать исполнителя, перевести переключатель «Связать с задачей в Jira» в активное положение (при необходимости), написать комментарий (при необходимости), нажать кнопку «Применить».

Примечания:

1. При единичном управлении уязвимостью доступно удаление привязки к системе отслеживания задач «Jira». Для удаления привязки необходимо выбрать проверку, выбрать уязвимость, выбрать вкладку «Управление уязвимостью», перевести переключатель «Связать с задачей в Jira» в неактивное положение. Задача в системе отслеживания задач «Jira» при этом не удаляется — удаляется только связь
2. При назначении исполнителя необходимо убедиться, что исполнитель подключен к системе отслеживания задач «Jira». Подробное описание приведено в подразделе 3.4.3.
3. Во вкладке «Управление уязвимостью» доступно изменение следующих параметров:
 - уровень критичность;
 - статус уязвимости;
 - исполнитель;
 - приоритет (доступно после выбора исполнителя и переключателя в активное положение «Связать с задачей в Jira»);
 - комментарий.

Изменение уровня критичности уязвимости доступно в следующих разделах:

- «Проекты». При изменении уровня критичности уязвимости в итерации. Изменения применяются в текущей и будущих итерациях. Изменения уровня критичности в подразделах «Проверки» или «Профили» не применяются.
- «Профили». При изменении уровня критичности проверки в пользовательском профиле, связанном с уязвимостью, изменения применяются только для будущих сканирований. Результаты прошлых итераций остаются без изменений.
- «Проверки». При изменении уровня критичности проверки, связанной с уязвимостью, в текущей и последующих итерациях изменения к результатам сканирования не применяются.

Массовое управление уязвимостями

Для массового управления уязвимостями необходимо выполнить следующие действия:

- 1) Выбрать проект.
- 2) Выбрать текущую итерацию проекта. Нажать кнопку «Подробные результаты» (рис. 12).
- 3) Раскрыть проверки, выбрать уязвимости (рис. 18).
- 4) Нажать кнопку «Управление уязвимостями».
- 5) Указать статус уязвимости и уровень критичности (при необходимости), выбрать исполнителя, перевести переключатель «Создать задачи в Jira» в активное положение (при необходимости), выбрать приоритет, написать комментарий (при необходимости), нажать кнопку «Применить» (рис. 20).

Управление уязвимостями



Уровень критичности

Средняя



Статус уязвимости

Принята



Исполнитель

1 1



▼ Связь с задачами в Jira ⓘ

ⓘ Уязвимостей выбрано: 2. С привязкой к Jira: 0



Создать задачи в Jira ⓘ

Приоритет

High



Комментарий

Введите комментарий

Применить

Отменить

Рисунок 20 – Окно «Управление уязвимостями»

Примечания:

1. Для уязвимостей, у которых уже создана задача в системе отслеживания «Jira», будет выполнено обновление параметров существующей задачи (статус уязвимости, критичность, исполнитель, приоритет, комментарий).
2. Для выделения всех найденных уязвимостей доступна кнопка «Выбрать все». Кнопка доступна в дереве найденных уязвимостей (см. рис. 13).
3. При массовом управлении уязвимости во вкладке «Исключенные уязвимости» доступны следующие статусы:
 - «В работе»;

- «Не устранена».
- 4. При массовом управлении уязвимости во вкладке «Найденные уязвимости» доступен следующий статус:
 - «Принята».
- 5. В окне «Управление уязвимостями» доступно изменение следующих параметров:
 - уровень критичность;
 - статус уязвимости;
 - исполнитель;
 - приоритет (доступно после выбора исполнителя и переключателя в активное положение «Связать с задачей в Jira»);
 - комментарий.

Перенос уязвимостей из списка, исключённых в список найденных

Для переноса уязвимости из списка исключённых уязвимостей в список найденных, необходимо:

- 1) Перейти к списку исключённых уязвимостей (см. рис. 18).
- 2) Выбрать уязвимости, которые необходимо вернуть, нажать на неё левой кнопкой мыши. В открывшемся окне выбрать вкладку «Управление уязвимостью» (см. рис. 19).
- 3) Выбрать уровень критичности и статус уязвимости.
- 4) Нажать кнопку «Применить».

Обновление уязвимости при изменении задачи в системе отслеживания «Jira»

При работе с системой отслеживания задач «Jira» необходимо учитывать следующее:

- 1) При изменении статуса задачи в системе отслеживания задач «Jira» изменяется статус уязвимости в ПК «SafeERP CS EM» на новое значение, соответствующее статусу задачи. Сопоставление статусов приведено в пункте 3.4.3.
- 2) При добавлении комментария в задаче в системе отслеживания задач «Jira» в уязвимости в истории изменений добавляется новая запись «Комментарий» от пользователя в ПК «SafeERP CS EM», соответствующего пользователю в системе отслеживания задач «Jira». Сопоставление статусов приведено в пункте 3.4.3.
- 3) При обновлении комментария в задаче в системе отслеживания задач «Jira» в уязвимости в истории изменений добавляется новая запись «Комментарий» от пользователя ПК «SafeERP CS EM», соответствующего пользователю в системе отслеживания задач «Jira». Настройка пользователя с системой отслеживания задач «Jira» приведена в подпунктах 3.4.4.1 и 3.4.4.3
- 4) Если не удалось обнаружить пользователя в ПК «SafeERP CS EM», соответствующего пользователю в системе отслеживания задач «Jira», то запись в истории будет от пользователя системы отслеживания задач «Jira» с пометкой «Jira».

3.1.1.7 Подключение почтовых уведомлений

В подразделе «Проекты» доступно подключение почтовых уведомлений по выбранному проекту.

Для настройки почтового сервиса необходимо обратиться к документу «Установка, обновление, удаление ПК «SAFEERP EM».

Для подключения почтовых уведомлений необходимо выполнить следующие действия:

- 1) Выбрать проект.
- 2) Нажать кнопку «Оповещения» (рис. 21).

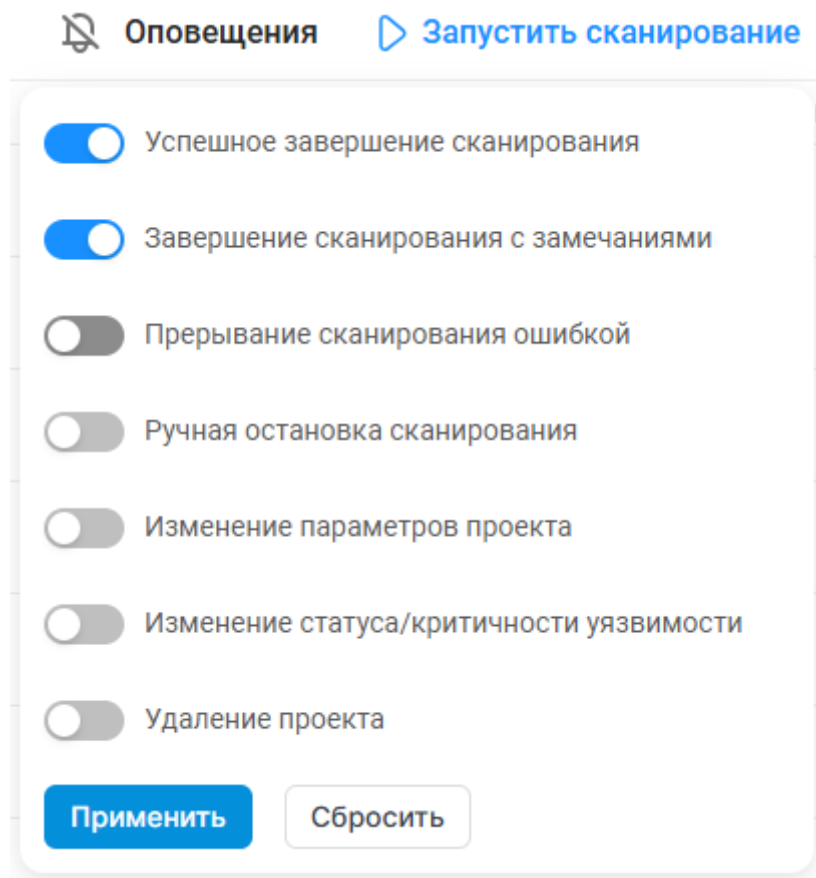


Рисунок 21 – Список событий (раздел «Статический анализ»)

- 3) Выбрать события окне (см. рис. 21).
- 4) Нажать кнопку «Применить».

Примечания:

1. Для корректной работы почтовых уведомлений необходимо убедиться, что в профиле пользователя указана электронная почта.
2. При единичном управлении уязвимостями в письмо выводить список изменений:
 - уровень критичности;
 - статус уязвимости;
 - ссылка на уязвимость.
3. При массовом управлении уязвимостями:
 - до 19 уязвимостей выводится следующий список изменений:
 - а) уровень критичности;

- б) статус уязвимости;
- в) ссылку на уязвимость;
- от 20 уязвимостей включительно и более выводится количество уязвимостей, которые были изменены.
- 4. При массовом управлении уязвимостями поступает одно письмо на все изменения.
- 5. Обработка большого количества событий при массовом управлении уязвимостями приводит к задержкам обработки почты.

Примеры почтовых уведомлений приведены на рисунках 22, 23, 24, 25, 26, 27, 28, 29.



Сканирование по проекту «К1 Источник» в модуле Статический анализ
завершено 15.06.2026 14:59:35

Всего обнаружено уязвимостей:	2000
Высокого уровня:	456
Среднего уровня:	325
Низкого уровня:	93
Информация:	1126

Перейти к детальной информации по итерации 15.06.2026 14:59:35

Рисунок 22 – Почтовое уведомление при выборе события «Успешное завершение сканирования»



Сканирование по проекту «[Проект Архив](#)» в модуле Статический анализ завершено 17.06.2026 11:54:05 с замечаниями: **«Анализ завершен с замечаниями: не удалось разобрать грамматикой следующее количество файлов - 14. Подробная информация в журнале или отчете».**

Всего обнаружено уязвимостей:	13
Высокого уровня:	13
Среднего уровня:	0
Низкого уровня:	0
Информация:	0

Перейти к детальной информации по итерации [17.06.2026 11:54:05](#)

Письмо автоматически сформировано SafeERP, пожалуйста, не отвечайте на него.

Рисунок 23 – Почтовое уведомление при выборе события «Завершение сканирования с замечаниями»



Сканирование по проекту «[Проект Источник](#)» в модуле Статический анализ прервано ошибкой:

Анализ прерван из-за ошибки: Подключение к источнику не установлено. Проверьте авторизационные данные источника.

Цель сканирования:

CS Goal

Источники:

1C DB Doc2 - 1

Перейти к детальной информации по итерации [17.06.2026 11:39:45](#)

Письмо автоматически сформировано SafeERP, пожалуйста, не отвечайте на него.

Рисунок 24 – Почтовое уведомление при выборе события «Прерывание сканирования ошибкой»



Сканирование по проекту «Проект Источник» в модуле Статический анализ было остановлено 17.06.2026 11:41:34 пользователем



Цель сканирования:	CS Goal
Источники:	1C DB Doc2 - 1
Уязвимостей на текущий момент:	398
Высокого уровня:	82
Среднего уровня:	9
Низкого уровня:	18
Информация:	289

Письмо автоматически сформировано SafeERP, пожалуйста, не отвечайте на него.

Рисунок 25 – Почтовое уведомление при выборе события «Ручная остановка сканирования»



В проекте «K6 1С Док21» в модуле Статический анализ были изменены параметры. Изменение произведено 11.06.2026 08:59:57

Были изменены параметры источников анализируемых данных:

1С DB Doc2 - 1

Список сканируемых объектов

[Расширения]

Все объекты

Письмо автоматически сформировано SafeERP, пожалуйста, не отвечайте на него.

Рисунок 26 – Почтовое уведомление при выборе события «Изменение параметров проекта»



В проекте «Проект Архив» в модуле Статический анализ были изменены параметры. Изменение произведено 17.06.2026 11:44:06

Всего изменено уязвимостей: 2

Статус уязвимостей был изменен:

~~Не устранена~~ / Принята

testexamples-master-1C/1C/S_ONEC_027_Использование_внешних_компонент_ERROR/
S_ONEC_027_Использование_внешних_компонент__2__2_0_0_0.bsl:5

~~Не устранена~~ / Принята

testexamples-master-1C/1C/
S_ONEC_030_Использование_методов_объекта_операционной_системы_ERROR/
S_ONEC_030_Использование_методов_объекта_операционной_системы__1__2_0_0_0.bsl:6

Критичность уязвимостей была изменена:

~~Высокая~~ / Низкая

testexamples-master-1C/1C/S_ONEC_027_Использование_внешних_компонент_ERROR/
S_ONEC_027_Использование_внешних_компонент__2__2_0_0_0.bsl:5

~~Высокая~~ / Низкая

testexamples-master-1C/1C/
S_ONEC_030_Использование_методов_объекта_операционной_системы_ERROR/
S_ONEC_030_Использование_методов_объекта_операционной_системы__1__2_0_0_0.bsl:6

Перейти к детальной информации по итерации 08.06.2026 09:07:03

Рисунок 27 – Почтовое уведомление при выборе события «Изменение статуса/критичности уязвимости»



В проекте «Проект Архив» в модуле Статический анализ были изменены параметры. Изменение произведено 17.06.2026 11:44:56

Всего изменено уязвимостей: 33

Перейти к детальной информации по итерации 08.06.2026 09:07:03

Письмо автоматически сформировано SafeERP, пожалуйста, не отвечайте на него.

Рисунок 28 – Почтовое уведомление при выборе события «Изменение статуса/критичности уязвимости» (при изменении больше 20 штук)



Проект «Проект Архив» в модуле Статический анализ был удален. Удаление произведено 17.06.2026 11:42:17

Письмо автоматически сформировано SafeERP, пожалуйста, не отвечайте на него.

Рисунок 29 – Почтовое уведомление при выборе события «Удаление проекта»

Просмотр активных подписок

Для просмотра списка активных подписок необходимо обратиться к подразделу 3.5

Отмена подписок

Отмена подписок осуществляется следующими способами:

- с помощью кнопки «Оповещения» при просмотре проекта.;
- с помощью кнопки «Отменить подписку по проекту» в профиле пользователя.

Подробная информация представлена в подразделе 3.5 .

Для отмены подписок необходимо выполнить следующие действия:

- 1) Выбрать проект.
- 2) Нажать кнопку «Оповещения».
- 3) Перевести переключатель в неактивное положение, нажать кнопку «Применить» (см. рис. 21).

3.1.1.8 Удаление проектов

Для удаления проекта необходимо выполнить следующие действия:

- 1) Выбрать проект (см. рис. 11).
- 2) Нажать кнопку «Удалить» в контекстном меню проекта (рис. 11).
- 3) Нажать кнопку **Да** в окне подтверждения (рис. 30).

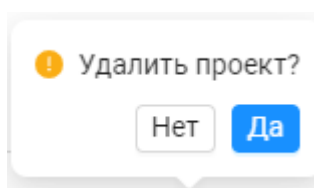


Рисунок 30 – Окно подтверждения удаления проекта

3.1.2 Подраздел «Профили»

Основная рабочая область подраздела «Профили» представлена на рис. 31.

Профили проверок						👤
🔍 Введите запрос для поиска						+ Добавить профиль
Название	Тип	Количество проверок	Языки	Кем добавлен	Когда добавлен	⋮
Все проверки	📁	184	11 ^	SECSEM	28.11.2025 15:17:41	
Проверки 1C	📁	76	1C C# XAML DOCKERFILE JAVA XML JS SQLSCRIPT XS XSJS PYTHON		28.11.2025 15:17:41	
Проверки C#	📁	10		SECSEM	28.11.2025 15:17:41	
Проверки Dockerfile	📁	20	1 v	SECSEM	28.11.2025 15:17:41	
Проверки Java	📁	6	1 v	SECSEM	28.11.2025 15:17:41	
Проверки JS	📁	12	1 v	SECSEM	28.11.2025 15:17:41	
Проверки Python	📁	10	1 v	SECSEM	28.11.2025 15:17:41	

Всего: 27

Рисунок 31 – Основная рабочая область подраздела «Профили»

Профили проверок – это группа проверок, объединённая по признаку (по языку программирования или списку задач).

Профили бывают стандартными (с предустановленным неизменяемым списком

проверок) и пользовательские (создает администратор ПК «SAFEERP CS EM» или пользователь, имеющий соответствующие права).

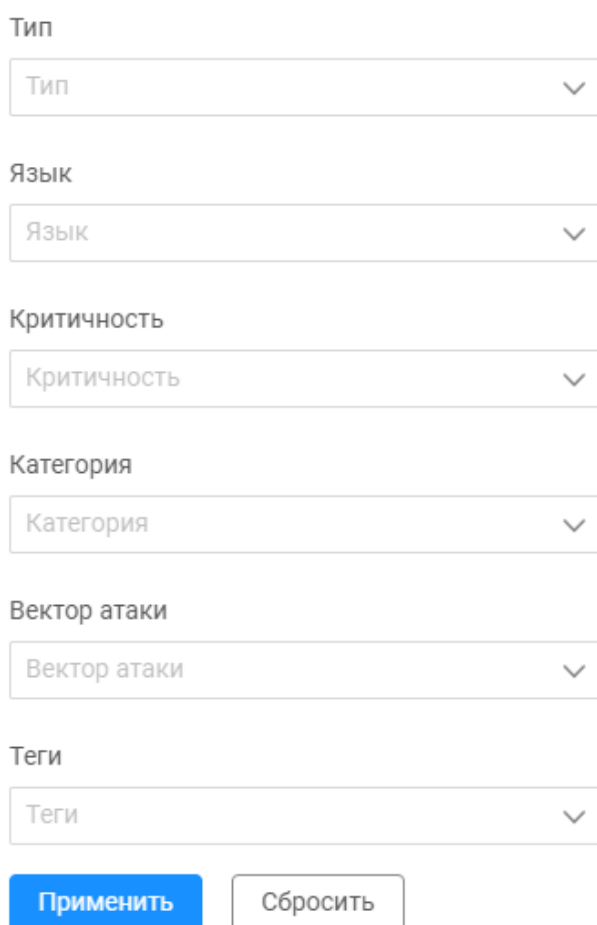
3.1.2.1 Просмотр профилей проверок

Для просмотра профиля, необходимо выполнить следующие действия:

- 1) Выбрать подраздел «Профили».
- 2) Выбрать профиль из списка.

Примечания:

1. Профиль «Owasp top 10 2025» является стандартным. В данный профиль входят проверки, которые срабатывают чаще согласно рейтингу Owasp.
2. При просмотре и редактировании профиля доступен поиск проверок с помощью кнопки «*Фильтр*». Доступен поиск по следующим параметрам (рис. 32):
 - тип;
 - язык;
 - критичность;
 - категория;
 - вектор атаки;
 - теги.



Тип

Тип

Язык

Язык

Критичность

Критичность

Категория

Категория

Вектор атаки

Вектор атаки

Теги

Теги

Применить

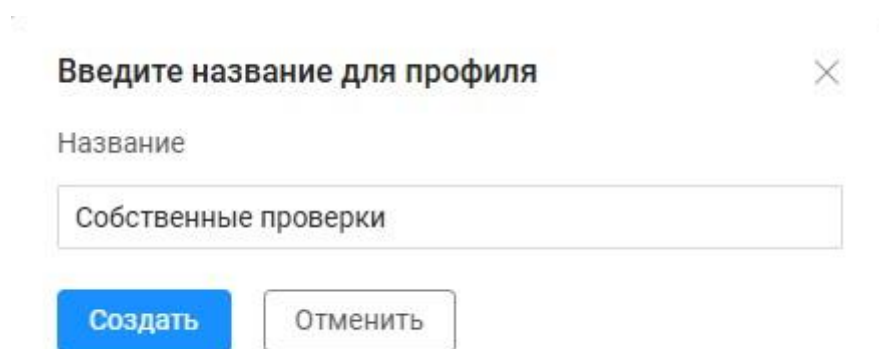
Сбросить

Рисунок 32 – Окно «Фильтр»

3.1.2.2 Создание профилей проверок

Для создания профиля, необходимо выполнить следующие действия:

- 1) Выбрать подраздел «Профили».
- 2) Нажать кнопку «+Добавить профиль» (см. рис. 31).
- 3) Ввести название профиля (рис. 33).
- 4) Нажать кнопку «Применить» (рис. 33).
- 5) Нажать кнопку «+Добавить проверки».
- 6) После установки флажков напротив проверок, которые необходимо добавить в профиль, нажать кнопку «Применить» (рис. 34).



Введите название для профиля

Название

Собственные проверки

Создать Отменить

Рисунок 33 – Название профиля

✕ Добавить проверки

☐	Название	Тип	Язык	Критичность	Категория	
☒	GET-запрос с использованием тела за...		1C	Средний	Надёжность	
☒	Внешние FTP-подключения		1C	Высокий	Безопасность	
☐	Выполнение команд операционной си...		1C	Высокий	Безопасность	
☐	Доступ к свойству «СохраняемоеЗнач...		1C	Высокий	Безопасность	
☐	Доступ к свойству «СохраняемоеЗначениеПароля»		1C	Низкий	Безопасность	
☐	Доступ к файловой системе		1C	Низкий	Безопасность	
☐	Запрос к БД в цикле		1C	Средний	Производительность	
☐	Запрос системной информации		1C	Низкий	Безопасность	
☐	Запуск внешнего отчета/обработки		1C	Низкий	Безопасность	

Всего: 194 Выбранных: 2

Рисунок 34 – Окно добавление проверок при создании профиля

Примечание. При добавлении проверок в профиль доступна кнопка «*Фильтр*». Доступен фильтр по следующим параметрам (рис. 35):

- тип (стандартный и пользовательский);
- язык (1C, Java Script, XSJS, XS, Python, XML, XAML, SQLScript, C#, JAVA, Dockerfile);
- критичность (высокая, средняя, низкая, информация);
- категория (производительность, надёжность, удобство сопровождения, безопасность);
- вектор атаки;
- теги.

Тип

Тип

Язык

Язык

Критичность

Критичность

Категория

Категория

Вектор атаки

Вектор атаки

Теги

Теги

Применить

Сбросить

Рисунок 35 – Окно «Фильтр»

3.1.2.3 Редактирование профилей проверок

В разделе «Профили» доступно редактирование следующих полей:

- проверки в профиле (добавление, удаление);
- критичность проверки.

Для редактирования профиля, необходимо выполнить следующие действия:

- 1) Выбрать подраздел «Профили».
- 2) Выбрать профиль.
- 3) Внести требуемые изменения.

Примечание. Профили, предоставляемые по умолчанию, редактировать нельзя.

Для того чтобы задать критичность проверки, необходимо выполнить следующие действия:

- 1) Выбрать подраздел «Профили».
- 2) Выбрать созданный или скопированный профиль.
- 3) Выбрать проверку.
- 4) Выбрать уровень критичности в выпадающем списке «Критичность».
- 5) Нажать кнопку «Сохранить».

Примечание. Изменение критичности проверки доступно только в пользовательских профилях проверок.

3.1.2.4 Копирование профилей проверок

Для копирования профилей проверок необходимо выполнить следующие действия:

- 1) Выбрать подраздел «Профили».
- 2) Выбрать профиль, который необходимо скопировать.
- 3) Нажать кнопку , выбрать пункт  Копировать профиль в раскрывшемся меню.
- 4) Указать название для скопированного профиля, подтвердить свой выбор, нажав кнопку «Создать копию».

3.1.2.5 Удаление профилей проверок

Для удаления профилей проверок необходимо выполнить следующие действия:

- 1) Выбрать подраздел «Профили».
- 2) Выбрать профиль, который необходимо удалить.
- 3) Нажать кнопку , выбрать пункт  Удалить профиль в раскрывшемся меню.
- 4) Нажать кнопку  в окне подтверждения.

Примечание. Профили, предоставляемые по умолчанию, удалить нельзя.

3.1.3 Подраздел «Проверки»

Основная рабочая область подраздела «Проверки» представлена на рис. 36.

Проверки							
Введите запрос для поиска							 Фильтр + Добавить проверку
Название	Тип	Язык	Критичность	Категория	Вектор атаки	Теги	
GET-запрос с использованием тела запроса		1С	Средний	Надёжность			
Внешние FTP-подключения		1С	Высокий	Безопасность		Соединение	
Выполнение команд операционной системы		1С	Высокий	Безопасность	1 ▾	ОС	
Доступ к свойству «СохраняемоеЗначениеПароля»		1С	Высокий	Безопасность	1 ▾	Секреты	
Доступ к файловой системе		1С	Низкий	Безопасность	1 ▾		
Запрос к БД в цикле		1С	Средний	Производительность		SQL-запрос	
Запрос системной информации		1С	Низкий	Безопасность	1 ▾		
Запуск внешнего отчета/обработки		1С	Низкий	Безопасность	1 ▾		
Запуск приложения операционной системы		1С	Высокий	Безопасность	1 ▾	ОС	
Извлечение лишних данных из БД		1С	Средний	Производительность		Запрос БД	

Всего: 194

Рисунок 36 – Основная рабочая область подраздела «Проверки»

3.1.3.1 Добавление пользовательских проверок

Добавление пользовательских проверок доступно для следующих языков

программирования:

- 1C;
- XAML;
- Java;
- XML;
- Python.

Примечания:

1. При создании пользовательской проверки необходимо заполнить следующие поля:
 - название;
 - язык;
 - шаблон проверки;
 - дополнительные поля, отображающиеся в зависимости от выбранного шаблона;
 - критичность.
2. После выбора параметра «Шаблон проверки» пользователю будут доступны всплывающие подсказки.
3. В поле «Вектор атаки» необходимо указать через что будет производиться атака.
4. Поле «Потенциальная уязвимость» – это флаг, который показывает, что срабатывание необходимо проверить вручную. В поле «Потенциальная уязвимость» необходимо указать «Да» или «Нет»

Для создания проверки необходимо выполнить следующие действия:

- 1) Выбрать подраздел «Проверки».
- 2) Нажать кнопку «+Новая проверка» (рис. 36).
- 3) Заполнить необходимые поля, добавить ссылку или ссылки на данную уязвимость (рис. 37).
- 4) Нажать кнопку «Добавить».

✕ Добавить проверку

Название	Введите название
Язык	Введите язык
Шаблон проверки	Выберите шаблон
Категория	Выберите категорию
Критичность	Выберите критичность
Вектор атаки	Выберите вектор атаки
Потенциальная уязвимость	☐
Описание	Введите описание
Влияние уязвимости	Введите влияние уязвимости
Рекомендации	Введите рекомендации
Пример кода с уязвимостью	Введите пример кода с уязвимостью
Пример кода без уязвимости	Введите пример кода без уязвимости
Теги	Выберите теги
Ссылки	+ Добавить ссылку

Рисунок 37 – Окно создания проверки

3.1.3.2 Редактирование проверок

Редактирование доступно только для пользовательских проверок. Для редактирования проверки, необходимо выполнить следующие действия:

- 1) Выбрать подраздел «Проверки».
- 2) Выбрать проверку, которую необходимо отредактировать.
- 3) Нажать кнопку «*Редактировать*».
- 4) Внести требуемые изменения.
- 5) Нажать кнопку «*Сохранить*».

3.1.3.3 Удаление пользовательских проверок

Доступно удаление только пользовательских проверок. Для удаления проверки, необходимо выполнить следующие действия:

- 1) Выбрать подраздел «Проверки».
- 2) Выбрать проверку, которую необходимо удалить.
- 3) Нажать кнопку «*Удалить*».
- 4) Нажать кнопку  в окне подтверждения.

3.2 Раздел «SCA»

Раздел «SCA» (Software Composition Analysis) предназначен для анализа файла спецификации с целью обнаружения встроенных компонентов и библиотек с открытым исходным кодом (Open Source), определения их актуальности, выявления уязвимостей и соответствий лицензионным требованиям.

Раздел «SCA» состоит из следующего подраздела:

- «Проекты».

Проекты



🔍 Введите запрос для поиска				+ Добавить проект
Название	Статус	Последний запуск	Выявленных угроз	III
	Предупреждение	25.05.2026 13:41:27	● 29 ● 165 ● 93 ● 13 ● 0	
	Предупреждение	14.05.2026 15:38:03	● 22 ● 83 ● 52 ● 4 ● 0	
	≡ Ошибка	05.05.2026 16:34:39	● 0 ● 0 ● 0 ● 0 ● 0	
	≡ Предупреждение	14.04.2026 10:46:59	● 32 ● 73 ● 55 ● 1 ● 0	
	Предупреждение	10.04.2026 16:54:24	● 5 ● 3 ● 11 ● 0 ● 0	
	Предупреждение	11.03.2026 11:57:37	● 35 ● 139 ● 79 ● 2 ● 0	
	Предупреждение	11.03.2026 09:02:46	● 5 ● 3 ● 11 ● 0 ● 0	
	Предупреждение	06.03.2026 08:59:47	● 49 ● 85 ● 71 ● 1 ● 0	
	Предупреждение	06.03.2026 07:13:18	● 49 ● 85 ● 71 ● 1 ● 0	

Рисунок 38 – Основная рабочая область подраздела «SCA»

Основная рабочая область подраздела «Проекты» состоит из следующих столбцов:

- «Название проекта»;
- «Статус» – статус последней итерации проекта;
- «Последний запуск» – дата и время последнего запуска;
- «Выявленных угроз» – количество и критичность выявленных угроз.

Статусы проектов и итерации

Доступные статусы итераций и проектов представлены в таблице 3.

Таблица 3 – Статусы итераций и проектов

Статус	Значение
Нет сканирований	Проект создан. Сканирование не было запущено. Доступно для проектов
Выполняется (1%)	Запущен процесс сканирования
Завершено	Сканирование завершено. Ошибки не обнаружены
Предупреждение	Сканирование завершено. Обнаружены угрозы
Ошибка	Сканирование было прервано из-за возникших ошибок

Индикация найденных уязвимостей приведена в таблице 4.

Таблица 4 – Статусы найденных угроз

Цвет	Значение
	Критичный
	Высокий
	Средний
	Низкий
	Не определен

3.2.1 Просмотр проекта

Для просмотра проекта необходимо выбрать проект из списка.

3.2.2 Добавление проекта

Для добавления проекта необходимо выполнить следующие действия:

- 1) Нажать кнопку «+ *Добавить проект*».
- 2) Заполнить необходимые поля.
- 3) Нажать кнопку «*Добавить*» (рис. 39).

× Добавить проект

Название проекта

Source 1

Описание проекта

Введите описание проекта

Добавить

Отменить

Рисунок 39 – Добавление проекта (раздел «SCA»)

3.2.3 Настройка проекта

Настройка проекта осуществляется следующими способами:

- через контекстное меню в строке проекта;
- через кнопку «*Настройки проекта*» при просмотре списка итераций.

Для настройки проекта через контекстное меню необходимо выполнить следующие действия:

- 1) Навести курсор на проект в столбце «Название».
- 2) Выбрать пункт «Редактировать» в контекстном меню.
- 3) Внести изменения (название проекта, описание проекта).

- 4) Нажать кнопку «Сохранить».

Для настройки проекта необходимо выполнить следующие действия:

- 1) Выбрать проект из списка.
- 2) Нажать кнопку «Настройки проекта».
- 3) Внести изменения (название проекта, описание проекта).
- 4) Нажать кнопку «Сохранить».

✕ Редактирование проекта

Название проекта	Новый проект
Описание проекта	Введите описание проекта

Рисунок 40 – Редактирование проекта

3.2.4 Запуск проекта и остановка сканирования

Запуск сканирования осуществляется следующими способами:

- через контекстное меню;
- со страницы проекта.

Для запуска сканирования через контекстное меню необходимо выполнить следующие действия:

- 1) Выбрать подраздел «Проекты».
- 2) Нажать кнопку  в строке проекта, выбрать пункт «Запустить» в контекстном меню.
- 3) Выбрать файл для сканирования. Нажать кнопку «Применить».

Для запуска сканирования со страницы проекта необходимо выполнить следующие действия:

- 1) Выбрать подраздел «Проекты».
- 2) Выбрать проект.
- 3) Нажать кнопку «Запустить сканирование».
- 4) Выбрать файл для сканирования. Нажать кнопку «Применить».

Примечания:

1. Для сканирования необходимо загружать файлы форматов JSON или XML,

которые соответствуют стандарту CycloneDX .

2. Для сканирования доступны файлы объемом не более 4095 Мбайт.
3. Запуск сканирования доступен только при наличии действующей лицензии на сервер управления соответствующего варианта исполнения (ПК «SafeERP CS EM» или ПК «SafeERP PS EM»). При истечении срока действия лицензии запуск сканирования блокируется до момента её продления. Подробнее об условиях доступа см. в пункте 3.4.2.

Остановка сканирования

Остановка сканирования осуществляется следующими способами:

- через контекстное меню;
- со страницы проекта.

Для остановки сканирования через контекстное меню необходимо выполнить следующие действия:

- 1) Выбрать пункт меню «Проекты».
- 2) Нажать кнопку  в строке проекта, выбрать пункт «Остановить» в контекстном меню.

Для остановки сканирования со страницы проекта необходимо выполнить следующие действия:

- 1) Выбрать подраздел «Проекты».
- 2) Выбрать проект.
- 3) Нажать кнопку «Остановить сканирование».

3.2.5 Просмотр результатов сканирования

Доступен просмотр результата сканирования. Для просмотра результата сканирования необходимо выбрать проект из списка, выбрать итерацию проекта.

При просмотре результата сканирования доступны следующие области:

- список компонентов с обнаруженными уязвимостями;
- список найденных уязвимостей.

Для просмотра результата сканирования необходимо выполнить следующее:

- 1) Выбрать проект (см. рис. 38).
- 2) Выбрать итерацию проекта.
- 3) Выбрать компонент из списка с обнаруженными уязвимостями.
- 4) Выбрать уязвимость из списка найденных уязвимостей.

< 25.05.2026 13:38:34

Предупреждение

Проект: 1

Введите запрос для поиска debug electron got lodash minimist Всего: 5	Введите запрос для поиска Наименование угрозы CVE-2026-4800 CVE-2021-23337 CVE-2020-28500 CVE-2025-13465 CVE-2026-2950 Статус угрозы Критичный Высокий Средний Средний Средний Фильтр III
---	--

Рисунок 41 – Список компонентов

Подробное описание уязвимости представлено на рис. 42.

× CVE-2024-11948

Информация о компоненте

Имя компонента

archiver

Группа компонента

Нет данных

Версия компонента

1.3.0

Информация об уязвимости

Источник

NVD

Описание

GFI Archiver Telerik Web UI Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of GFI Archiver. Authentication is not required to exploit this vulnerability.

The specific flaw exists within the product installer. The issue results from the use of a vulnerable version of Telerik Web UI. An attacker can leverage this vulnerability to execute code in the context of NETWORK SERVICE. Was ZDI-CAN-24041.

Статус угрозы

Критичный

Отменить

Рисунок 42 – Подробное описание уязвимости

3.2.6 Удаление проектов

Для удаления проектов необходимо нажать кнопку «Удалить» в контекстном меню, подтвердить действие.

Для удаления проекта необходимо выполнить следующие действия:

- 1) Навести курсор на проект в столбце «Название проекта».
- 2) Выбрать пункт «Удалить» в контекстном меню. Подтвердить действие.

3.3 Раздел «Цели сканирования»

Раздел «Цели сканирования» предназначен для ведения целей сканирования, а также для ведения источников.

Основная рабочая область представлена на рис. 43.

Цели сканирования				
🔍 Введите запрос для поиска				+ Цель сканирования
Название	Описание	Источники	Дата создания	⋮
		<code>/</code> Источники Демонстрация Клиента	25.12.2025 14:36:16	
		<code>/</code> Doc2 <code>/</code> Test_Repo_Public archive <code>/</code> cs_OK_db +12	19.12.2025 14:23:56	
		👍 1 👍 2 👍 3 👍 4	26.12.2025 07:28:55	
		<code>/</code> 1C Клиент Doc2 <code>/</code> GIT Kate2 little <code>/</code> GIT Kate2 little2 +6	17.12.2025 08:48:22	
			25.12.2025 16:58:10	
		Areent ERP Areent ERP2	05.12.2025 13:36:53	
			15.12.2025 14:45:33	
		<code>/</code> 1C DB UH new <code>/</code> UH <code>/</code> UH1	05.12.2025 12:19:41	
		<code>/</code> ext_1 <code>/</code> ext_2 <code>/</code> main <code>/</code> rep_1 👍 1	22.12.2025 09:20:37	

Рисунок 43 – Основная рабочая область раздела «Цели сканирования»

3.3.1 Добавление цели сканирования

Для добавления цели сканирования необходимо выполнить следующие действия:

- 1) Нажать кнопку «+Цель сканирования» (рис. 43).
- 2) Заполнить поля «Название», «Описание» (рис. 44).

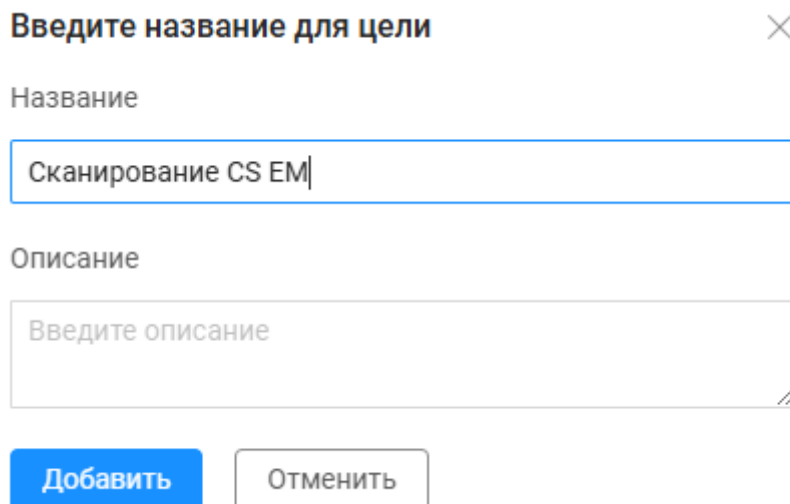


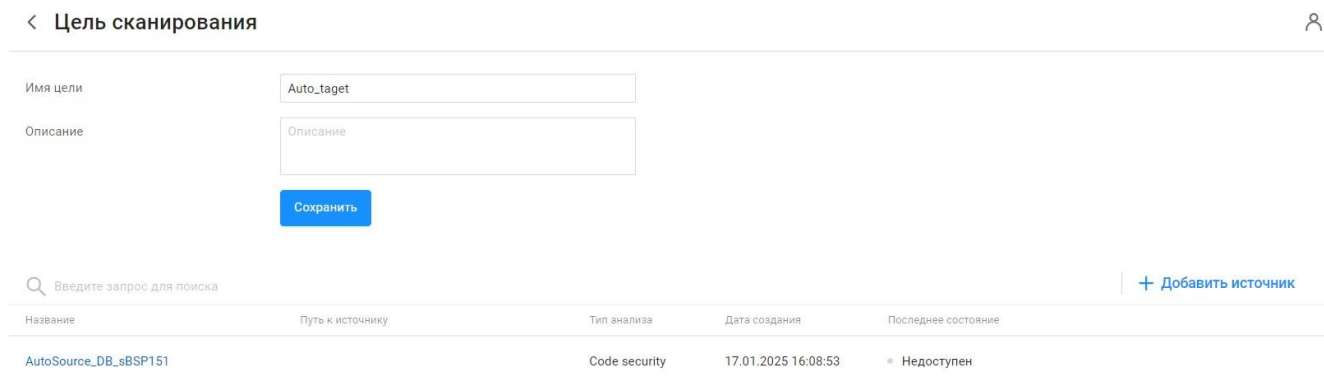
Рисунок 44 – Создание цели сканирования

3) Нажать кнопку «Добавить» (см. рис. 44).

3.3.2 Редактирование цели сканирования

Для редактирования цели необходимо выполнить следующие действия:

- 1) Выбрать цель из списка (рис.43).
- 2) Внести изменения (название, описание) (рис. 45).



Название	Путь к источнику	Тип анализа	Дата создания	Последнее состояние
AutoSource_DB_sBSP151		Code security	17.01.2025 16:08:53	* Недоступен

Рисунок 45 – Редактирование цели сканирования

3) Нажать кнопку «Сохранить» (рис. 45).

3.3.3 Удаление цели сканирования

Для удаления цели необходимо нажать кнопку «Удалить цель» в строке цели сканирования.

3.3.4 Источники

В проектах раздела «Статический анализ» применяются источники следующих типов:

- 1С База данных;
- 1С Клиент;

- SAP HANA;
- git;
- файловая система.

Примечание. Подключение источников в ПК «SafeERP CS EM» доступно только при наличии лицензии на подключение источников. При истечении срока действия лицензии создание источника блокируется до момента её продления. Подробнее об условиях доступа см. в пункте 3.4.2.

3.3.4.1 Добавление источника типа «1С База данных»

Для добавления источника типа «1С База данных» необходимо выполнить следующие действия:

- 1) Выбрать цель сканирования из списка или выполнить действия согласно пункту 3.3.1 .
- 2) Нажать кнопку «+Добавить источник».
- 3) Выбрать «Анализ кода» в поле «Тип анализа».
- 4) Выбрать «1С База данных» в поле «Тип источника».
- 5) Заполнить необходимые поля.
- 6) Нажать кнопку «Добавить» (рис. 46).

× Добавить источник

Тип анализа	Анализ кода
Название	Source
Описание	Введите описание источника
Тип источника	1С База данных
Путь к источнику	jdbc:postgresql://example_domain:5432/example_Database
Логин	admin
Пароль	

Добавить

Отменить

Рисунок 46 – Добавление источника типа «1С База данных» (БД Postgres)

× Добавить источник

Тип анализа	Анализ кода
Название	Source
Описание	Введите описание источника
Тип источника	1С База данных
Путь к источнику	<code>jdbc:sqlserver://192.168.1.10:1433;databaseName=example</code>
Логин	admin
Пароль	

ДобавитьОтменить

Рисунок 47 – Добавление источника типа «1С База данных» (БД MS SQL)

Примечания:

1. В поля «Логин» и «Пароль» необходимо ввести данные от проверяемой БД 1С. Учетная запись пользователя, проверяемой БД, должна иметь полномочия на чтение данной БД, а также пароль.
2. Путь к источнику (БД postgres) имеет следующий вид:
`jdbc:postgresql://<host>:<port>/<DatabaseName>`, где
— host – адрес сервера (DNS или IP);
— port – порт сервера postgres;
— DatabaseName – имя базы данных на сервере postgresql.
3. Путь к источнику (БД MS SQL) имеет следующий вид (рис. 47):
`jdbc:sqlserver://<host>:<port>;databaseName=<DatabaseName>`, и где
— host – адрес сервера (DNS или IP);
— port – порт сервера MS SQL;
— DatabaseName – имя базы данных на сервере MS SQL;
— integratedSecurity – использование аутентификация Windows. Принимает следующие значения: true и false;
— encrypt – процедура активации шифрования соединения. Принимает следующие

значения: true и false;

- trustServerCertificate – доверять сертификату сервера без проверки. Принимает следующие значения: true и false;
- authenticationScheme – в строке подключения JDBC к Microsoft SQL Server указывает, какой тип встроенной аутентификации используется приложением. Например, путь к источнику типа «1С База данных» выглядит следующим образом:
jdbc:sqlserver://192.168.1.10:1433;databaseName=example_DataBase;
authenticationScheme=SqlPassword;encrypt=true;trustServerCertificate=true

3.3.4.2 Добавление источника типа «1С Клиент»

Для добавления источника типа «1С Клиент» необходимо выполнить следующие действия:

- 1) Выбрать цель сканирования из списка или выполнить действия согласно пункту 3.3.1 .
- 2) Нажать кнопку «+Добавить источник».
- 3) Выбрать «Анализ кода» в поле «Тип анализа».
- 4) Выбрать «1С Клиент» в поле «Тип источника»
- 5) Выбрать в выпадающем списке «Тип базы» и «Версию клиента». Заполнить необходимые поля. Нажать кнопку «Добавить» (рис. 48).

× Добавить источник

Тип анализа	Анализ кода
Название	Source
Описание	Введите описание источника
Тип источника	1С Клиент
Тип базы	Серверный Файловый
Версия клиента	8.3.20.1674
Путь к источнику	example_domain:5432/example_Client
Логин	admin
Пароль	

Добавить

Отменить

Рисунок 48 – Добавление источника типа «1С Клиент»

Примечания:

1. Путь к источнику имеет следующий вид `<ДоменноеИмяКластера1С>:[port]/<ИмяБазы1С>` и состоит из:
 - `ДоменноеИмяКластера1С` – имя, которое отображается в консоли Администрирования серверов 1С;
 - `[port]` – номер используемого порта, если используется порт по умолчанию, то указать значение 1541;
 - `ИмяБазы1С` – имя базы сервера 1С так, как оно отображается в базах менеджера кластера или в настройках подключения клиентов 1С (рис. 49).

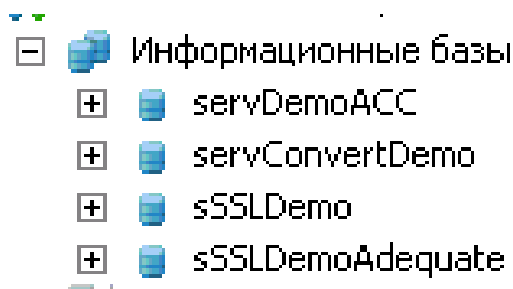


Рисунок 49 – Информационные базы 1С

2. В поля «Логин» и «Пароль» необходимо ввести имя и пароль от учетной записи пользователя.
3. Для корректного подключения источника типа «1С Клиент» с помощью толстого клиента необходимо обратиться к документу «Установка, обновление и удаление ПК SAFEERP EM».

3.3.4.3 Добавление источника типа «SAP HANA»

Для добавления источника типа «SAP HANA» необходимо выполнить следующие действия:

- 1) Выбрать цель сканирования из списка или выполнить действия согласно пункту 3.3.1 .
- 2) Нажать кнопку «*+Добавить источник*». Выбрать «Анализ кода» в поле «Тип анализа».
- 3) Выбрать «SAP HANA» в поле «Тип источника».
- 4) Заполнить необходимые поля. Нажать кнопку «*Добавить*» (рис. 50).

× Добавить источник

Тип анализа	Анализ кода
Название	Source
Описание	Введите описание источника
Тип источника	SAP HANA
Путь к источнику	http://0.0.0.0/safeerp-ems/support/cicd-test-repo.git
Логин	operator2
Пароль	

Добавить

Отменить

Рисунок 50 – Добавление источника типа SAP HANA

Примечания:

- Путь к источнику имеет следующий вид
<protocol>://<host>:<port>/_gazis_/SEHA/HANAAGENT.xsodata/ и состоит из:
 - protocol - принимает значения http:// или https:// ;
 - host – имя сервера;
 - port – порт сервера (диапазон 4300-4399 для https, 8000-8099 для http).
- Логин и пароль:
 - пароль от учётной записи в СУБД SAP HANA с присвоенной ей ролью «_gazis_.SEHA::SEHA»
 - создание роли «_gazis_.SEHA::SEHA» происходит автоматически при установке HANA-агента ПК SAFEERP и не требует дополнительных действий.

Для подключения ПК «SAFEERP CS EM» к агенту SAP HANA, необходимо установить HANA-агент SAFEERP. Подробное описание установки HANA-агента SAFEERP описано в документе «Установка, удаление ПК SAFEERP Security Suite».

3.3.4.4 Добавление источника типа «GIT»

Для добавления источника типа «GIT» необходимо выполнить следующие действия:

- 1) Выбрать цель сканирования из списка или выполнить действия согласно пункту 3.3.1 .
- 2) Нажать кнопку «+Добавить источник». Выбрать «Анализ кода» в поле «Тип анализа».
- 3) Выбрать «GIT» из выпадающего списка в поле «Тип источника».
- 4) Заполнить необходимые поля.
- 5) Нажать кнопку «Запросить» в поле «Список веток».
- 6) Выбрать ветку из выпадающего списка.
- 7) Нажать кнопку «Добавить» (рис. 51).

× Добавить источник

Тип анализа	Анализ кода
Название	Source
Описание	Введите описание источника
Тип источника	GIT
Способ аутентификации	Логин и пароль Токен доступа SSH-ключ
Путь к источнику	https://gitlab.gis/safeerp-ems/examples.git
Логин	admin
Пароль	
Список веток	Запросить

ДобавитьОтменить

Рисунок 51 – Добавление источника типа git со способом аутентификации «Логин и пароль»

× Добавить источник

Тип анализа	Анализ кода
Название	Source
Описание	Введите описание источника
Тип источника	GIT
Способ аутентификации	Логин и пароль Токен доступа SSH-ключ
Путь к источнику	https://gitlab.gis/safeerp-ems/examples.git
Токен доступа	
Список веток	Запросить

Добавить

Отменить

Рисунок 52 – Добавление источника типа git со способом аутентификации «Токен доступа»

✕ Добавить источник

Тип анализа	Анализ кода
Название	Источник 1
Описание	Введите описание источника
Тип источника	GIT
Способ аутентификации	Логин и пароль Токен доступа <input checked="" type="button" value="SSH-ключ"/>
Путь к источнику	https://gitlab.serp.dev.da.lan/safeerp-ems/testexamples.git
Ключ SSH	
Список веток	Запросить

Рисунок 53 – Добавление источника типа git со способом аутентификации «SSH-ключ»

Необходимые данные для подключения источников типа «GIT»

При подключении источника типа «GIT» доступны следующие способы аутентификации:

- логин и пароль;
- токен доступа;
- SSH-ключ.

Аутентификация с помощью логина и пароля

Путь к источнику имеет следующий вид (см. рис. 51):

<protocol>://<host >/<path>/<repository>.git и состоит из:

- protocol – принимает значения https:// или http:// ;
- host – имя сервера;

- path – путь к проекту, включая группу/организацию;
- project_name – имя репозитория с расширением git.

В поля «Логин» и «Пароль» необходимо ввести логин и пароль пользователя, имеющего доступ на чтение репозитория.

Примечание. Если источник является публичным, то ввод логина и пароля является необязательным.

Аутентификация с помощью токена доступа

Путь к источнику имеет следующий вид (см. рис. 52)

<protocol>://<host>/<path>/<repository>.git и состоит из:

- protocol – принимает значения https:// или http:// ;
- host – имя сервера;
- path – путь к проекту, включая группу/организацию;
- project_name – имя репозитория с расширением git.

В поле «Токен доступа» (см. рис. 52) необходимо ввести токен, который необходимо сгенерировать в хостинге кода. При генерации нужно будет выбрать доступ на чтение репозитория.

Аутентификация с помощью SSH-ключа

Путь к источнику (рис. 53) имеет следующий вид git@serviceurl:username/reponame.git и состоит из:

- serviceurl — URL сервиса, на котором размещён репозиторий (например, github.com или gitlab.com);
- username — логин или имя пользователя на сервисе, имеющего доступ на чтение репозитория;
- reponame — название репозитория.

Для настройки аутентификации по SSH-ключу необходимо выполнить следующие действия:

- 1) Сгенерировать пару ключей (публичный и приватный).
- 2) Добавить сгенерированный публичный ключ в настройки выбранного репозитория.
- 3) Ввести содержимое приватного ключа в поле «Ключ SSH» (см. рис. 53)

Примечания:

1. Генерацию SSH-ключей необходимо произвести самостоятельно.
2. Если источник типа git работает по протоколу https на основе самоподписанных сертификатов, то перед подключением необходимо выполнить следующие действия:
 - 1) Добавить публичный ssl-сертификат в каталог \$HOST_HOMEDIR/target_certs на сервере, где развернут «SAFEERP ПК CS EM».
 - 2) Перезапустить контейнеры с помощью команды:
docker-compose down && docker-compose up -d
 - 3) Дождаться полной загрузки сервисов перед добавлением источника.

3.3.4.5 Добавление источника типа «Файловая система»

Для корректного добавления источника необходимо произвести настройки согласно

документу «Установка, обновление и удаление ПК SAFEERP EM».

Для добавления источника типа «Файловая система» необходимо выполнить следующие действия:

- 1) Выполнить действия согласно пункту 3.3.1 или выбрать цель сканирования из списка.
- 2) Нажать кнопку «+Добавить источник». Выбрать «Анализ кода» в поле «Тип анализа».
- 3) Выбрать источник типа «Файловая система». Заполнить необходимые поля (рис. 54).
- 4) Выбрать директорию в поле «Путь к источнику». Выбрать «Анализ кода» в поле «Тип анализа».
- 5) Нажать кнопку «Добавить».

× Добавить источник

Тип анализа	Анализ кода
Название	Source
Описание	Введите описание источника
Тип источника	Файловая система
Путь к источнику	

Добавить

Отменить

Рисунок 54 – Добавление источника типа «Файловая система»

3.3.4.6 Редактирование источника

Для редактирования источника необходимо выполнить следующие действия:

- 1) Выбрать цель сканирования из списка (рис. 43).
- 2) Выбрать источник из списка (рис. 55).
- 3) Внести изменения, нажать кнопку «Сохранить» (рис. 56).

Имя цели

CS git

Описание

Сохранить

Введите запрос для поиска

+ Добавить источник

Название	Путь к источнику	Тип анализа	Дата создания	Последнее состояние
GH_git		Code security	17.06.2025 17:20:56	• Доступен
GL_Test_Repo1		Code security	17.06.2025 17:22:30	• Доступен

Рисунок 55 – Список источников

× Источник

> Дополнительная информация

✓ Источник доступен.

Последнее состояние

Проверить

Тип анализа

Анализ кода

Название

Gitflic

Описание

Введите описание источника

Тип источника

GIT

Способ аутентификации

Логин и пароль

Токен доступа

SSH-ключ

Путь к источнику

Логин

Пароль

Введите пароль

Список веток

Запросить

Ветка репозитория

Сохранить

Отменить

Рисунок 56 – Редактирование источника

3.3.4.7 Удаление источника

Для удаления источника необходимо выполнить следующие действия:

- 1) Выбрать «Цель сканирования» из списка.

- 2) Нажать кнопку «Удалить источник» в контекстном меню в строке источника. Подтвердить действия.

3.4 Раздел «Настройки»

Раздел «Настройки» предназначен для ведения настроек ПК «SafeERP CS EM».

Раздел «Настройки» содержит следующие подразделы:

- «Информация»;
- «Лицензии»;
- «Пользователи»;
- «Журнал».

3.4.1 Подраздел «Информация»

В подразделе «Информация» пользователю доступна загрузка архива документации по ПК «SAFEERP CS EM» на локальную машину в формате ZIP, а также просмотр версии ПК «SAFEERP CS EM» во вкладке «Версии» (рис. 57).

Для загрузки архива с документацией необходимо нажать кнопку «Скачать» (рис. 57).

Для просмотра версии ПК «SAFEERP CS EM» необходимо выбрать вкладку «Версии» (рис. 57).

Настройки / Информация

[CS EM](#)[PS EM](#)[Версии](#)[Статический анализ](#)[SCA](#)

Статический анализатор — инструмент, предназначенный для обнаружения потенциальных проблем и уязвимостей разрабатываемого кода, который помогает улучшить безопасность и эффективность разрабатываемого программного обеспечения.

Статический анализатор предназначен для:

- обнаружения потенциальных ошибок и уязвимостей в коде на ранних этапах разработки;
- повышения качества и защищённости ПО путём соблюдения стандартов кодирования и рекомендаций по безопасности;
- сокращения затрат на исправление ошибок и поддержку кода в дальнейшем.

Статический анализатор:

- анализирует программные коды следующих языков программирования: 1C, SQLScript, JavaScript, Python, C#, Java, XSJS, XS, а также файлов: Dockerfile, XAML и XML;
- генерирует отчёты о найденных уязвимостях, включающие в себя рекомендации по их исправлению.

Основными преимуществами «Статического анализатора» являются:

- быстрая проверка больших объёмов кода;
- постоянно обновляющаяся база сценариев проверок;
- интеграция с CI/CD;
- возможность создания собственных сценариев и профилей проверок;
- возможность отложенного запуска сканирований, составления расписания запуска сканирований для каждого проекта.

Дополнительными преимуществами «Статический анализатора» при интеграции с 1C являются:

- возможность просканировать только измененный код;
- возможность просканировать только редактируемые модули (Переопределяемые модули);
- возможность выгрузки объектов 1C напрямую из БД.

[Скачать документацию модуля CS EM](#)[Скачать](#)

3.4.2 Подраздел «Лицензия»

Доступ к ПК «SafeERP CS EM» определяются свойствами действующей лицензии. Лицензия содержит одно или несколько свойств. Свойства лицензии необходимо уточнить у поставщиков услуг.

Подробное описание свойств представлено в таблице 5.

Таблица 5 – Свойства лицензии

Свойство лицензии	Назначение	Поведение при истечении срока
Количество источников для анализа в ПК «SafeERP CS EM»	Определяет лимиты максимального числа подключённых источников кода для модуля CS EM. При отсутствии свойства создание и редактирование подключений недоступно	Запрещено создание новых подключений к источникам. Редактирование существующих подключений доступно при соблюдении установленного лимита
Лицензия для сервера управления ПК «SafeERP CS EM»	Предоставляет доступ к модулю CS EM	Запрещён запуск сканирования (включая отложенный). Просмотр результатов ранее проведённых сканирований и выгрузка отчётов остаются доступными
Лицензия для сервера управления ПК «SafeERP PS EM»	Предоставляет доступ к модулю PS EM	Запрещён запуск сканирования (включая отложенный). Просмотр результатов ранее проведённых сканирований и выгрузка отчётов остаются доступными

Лицензия со свойством «Количество источников для анализа в ПК «SafeERP CS EM»

Особенности работы лицензии с свойством «Количество источников для анализа в ПК «SafeERP CS EM»:

1. Область применения. Свойство применяется только к варианту исполнения ПК «SafeERP CS EM» и не влияет на функциональность ПК «SafeERP PS EM».
2. Суммирование лимитов. При наличии нескольких активных лицензий, содержащих свойство «Количество источников для анализа в ПК «SafeERP CS EM»», их лимиты суммируются.
3. Ограничения на операции с источниками. Доступность операций создания и редактирования источников определяется соотношением текущего количества настроенных подключений и суммарного лицензионного лимита. Примечание. При достижении лимита создание подключения нового источника в ПК «SafeERP CS EM» блокируется. Доступно редактирование существующих подключений остаётся возможным. Блокировка редактирования наступает только при фактическом превышении лимита.

Влияние свойств лицензии на ПК «SafeERP EM»

В варианте исполнения ПК «SafeERP CS EM» доступны следующие свойства:

- количество источников для анализа в ПК «SafeERP CS EM»;
- лицензия для сервера управления ПК «SafeERP CS EM».

В варианте исполнения ПК «SafeERP PS EM» доступно следующее свойство:

- лицензия для сервера управления ПК «SafeERP PS EM».

3.4.2.1 Активация лицензии

Основная рабочая область подраздела «Лицензии» представлена на рис. 58.

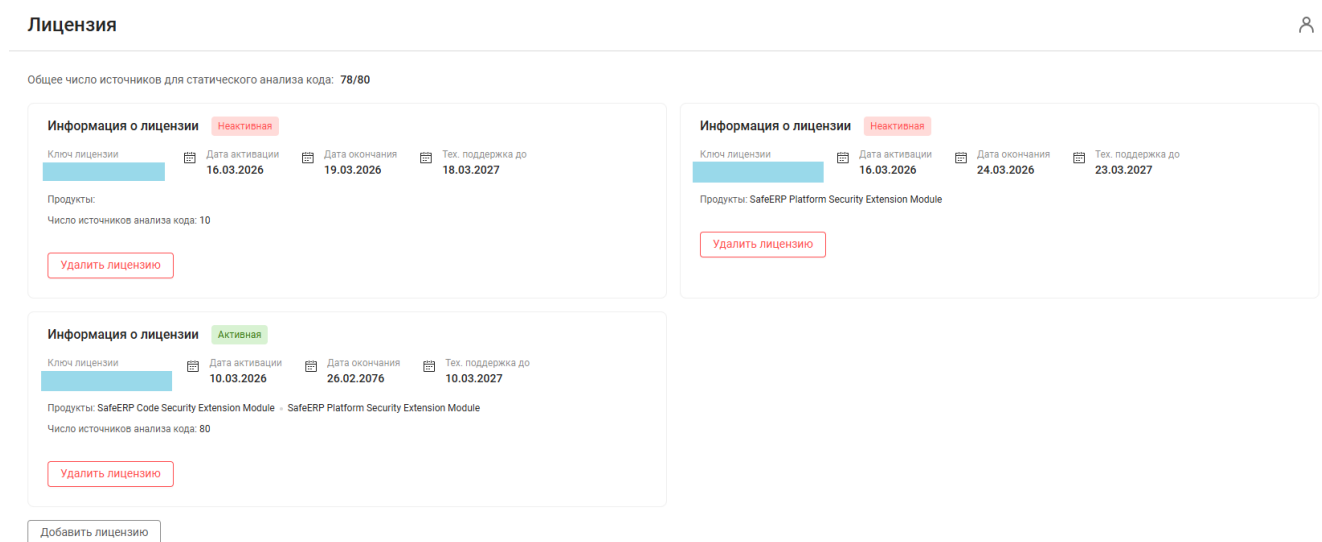


Рисунок 58 – Подраздел «Лицензии»

Для активации лицензии необходимо выполнить следующие действия:

- 1) Нажать кнопку «Добавить лицензию» (рис. 58).
- 2) Ввести ключ активации (предоставляется в комплекте поставки), адрес электронной почты. Нажать кнопку «Сгенерировать запрос» (рис. 59). Автоматически начнется процедура загрузки файла license_request формата json, который сохраняется в папку «Загрузки».

< Офлайн активация SafeERP EM

Ключ лицензии

00000-00000-00000-000



Е-mail адрес

На него будет отправлен файл лицензии

Сгенерировать запрос

- ❗ 1. Файл запроса вставить на странице активации продуктов
<https://license.gaz-is.ru/offlineActivate/>
2. Следуя инструкциям на сайте, активировать продукт
3. Загрузить лицензию, полученную на ваш электронный ящик

⬆ Загрузить лицензию

Рисунок 59 – Окно активации лицензии

- 3) Перейти по ссылке, которая указана в окне «Офлайн активация SAFEERP EM» (см. рис. 59). На сайте по активации лицензии нажать кнопку «*Выберите файл*», с помощью проводника выбрать файл, скачанный в пункте 2, нажать кнопку «*Активировать*» (рис. 60).

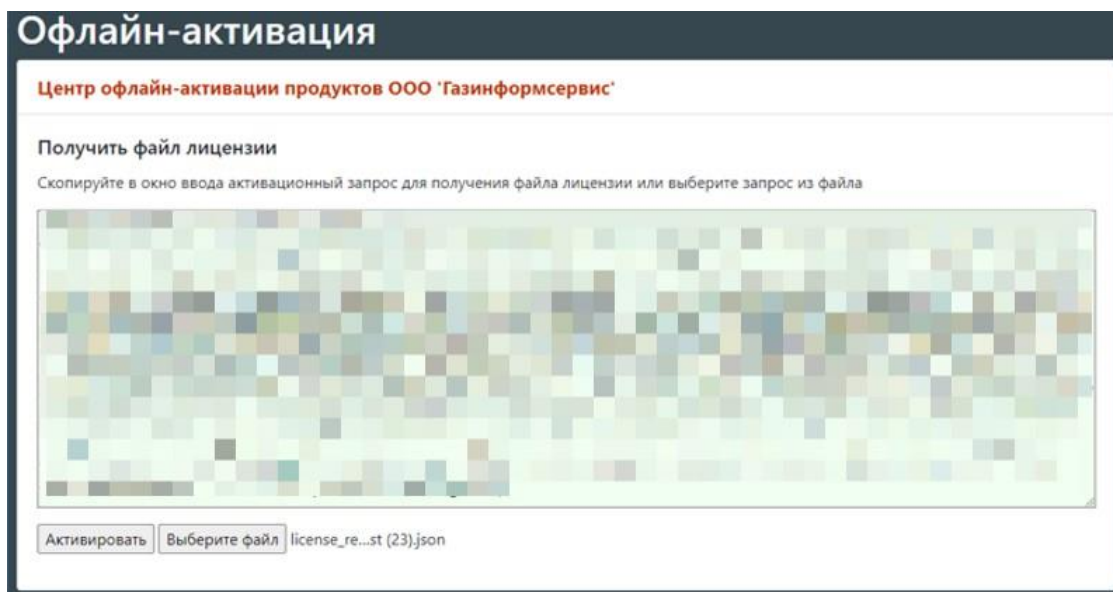


Рисунок 60 – Получение файла лицензии

- 4) Ввести ключ лицензии из почтового уведомления (рис. 61) в окно офлайн-активации (рис. 62), нажать кнопку «Активировать».



Активация успешно завершена

Вы успешно активировали вашу копию продукта
SafeERP Code Security Extension Module
с лицензионным ключом



Ваша лицензия во вложении

Благодарим за использование продуктов
компании ООО "ГАЗИНФОРМСЕРВИС"!
В случае возникновения вопросов по работе продукта
просим **обращаться в техническую поддержку.**

С уважением, коллектив
ООО "ГАЗИНФОРМСЕРВИС"
Контактная информация

Рисунок 61 – Ключ активации продукта, полученный по электронной почте

Офлайн-активация

Центр офлайн-активации продуктов ООО 'Газинформсервис'

Введите ключ активации, отправленный на ваш адрес электронной почты test-1@gaz-is.ru

Ключ активации:

Активировать

Рисунок 62 – Окно для ввода ключа лицензии

- 5) При успешной активации лицензии её можно сохранить в файл, нажав кнопку «Сохранить в файл» (рис. 63). На адрес электронной почты, указанный в пункте 2) поступит письмо, содержащее zip-архив с лицензией.

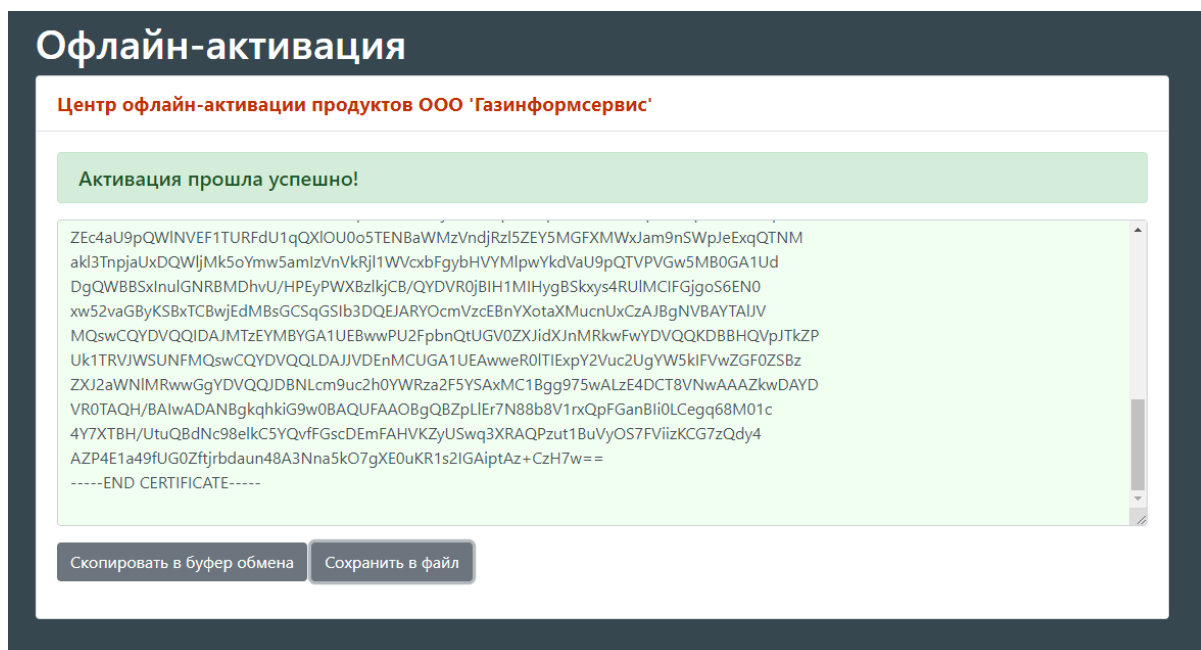


Рисунок 63 – Сообщение об успешной активации лицензии

- 6) В окне «Офлайн активация SafeERP EM» (рис. 59) нажать кнопку «Загрузить лицензию», в окне выбора файла указать лицензию, сформированную в пункте 5. Перед загрузкой лицензии необходимо извлечь bin-файл из архива.
- 7) Данные о лицензии после успешной процедуры активации представлены на рис. 64.

Лицензия



Рисунок 64 – Информации о лицензии

3.4.2.2 Обновление лицензии

Для обновления лицензии необходимо выполнить следующие действия:

- 1) Нажать кнопку «Удалить лицензию» в области лицензии (см. рис. 58).
- 2) Активировать лицензию согласно подпункту 3.4.2.1 .

3.4.3 Подраздел «Jira»

Подраздел «Jira» предназначен для настройки системы отслеживания задач в ПК «SafeERP CS EM».

Примечание. При настройке с системой отслеживания задач «Jira» необходимо настроить вебхуки согласно документу «Установка, обновление и удаление ПК SafeERP EM».

В подразделе «Jira» доступны следующие области:

- основная рабочая;
- «Соответствие статусов SafeERP в Jira» – предназначена для сопоставления статусов в ПК «SafeERP CS EM»;
- «Соответствие статусов Jira в SafeERP» – предназначена для сопоставления статусов в системе отслеживания задач «Jira».

В основную рабочую область входят следующие поля:

- «URL сервера Jira» – адрес сервера, на котором развернута система отслеживания задач «Jira»;
- «Версия API» – выбор версии API для системы отслеживания задач «Jira»;
- «Способ аутентификации» – выбор способа аутентификации пользователя. Доступна аутентификация с помощью логина и пароля и токена доступа;
- «Логин» – логин пользователя системы отслеживания задач «Jira»;
- «Пароль» – пароль пользователя системы отслеживания задач «Jira»;
- «Токен доступа» – токен доступа пользователя системы отслеживания задач «Jira»;
- «Проект» – название проекта в ПК «SafeERP CS EM»;
- «Тип задачи» – типа задачи в системе отслеживания задач «Jira».

Примечание. При выборе типа задачи в области «Соответствие статусов SafeERP в Jira» выводится информационная подсказка.

3.4.4 Подраздел «Пользователи»

В подразделе «Пользователи» администратору доступно ведение пользователей ПК «SAFEERP CS EM».

Основная рабочая область представлена на рис. 65.

Настройки / Список пользователей



Пользователи

Роли

🔍 Введите запрос для поиска

[+ Новый пользователь](#)

Фамилия и Имя	Роли	Логин	E-mail	Телефон	Технический	Смена пароля	Создание	Обновление	
	1					24.03.2026 14:52:58	24.03.2026 14:52:35	28.05.2026 11:24:40	
	1					04.03.2026 08:30:30	04.03.2026 08:30:29	28.05.2026 13:10:38	
	1					04.03.2026 08:30:56	04.03.2026 08:30:56	03.06.2026 15:05:16	
	1						28.05.2026 10:28:22	28.05.2026 10:28:22	
	1					04.03.2026 08:30:40	04.03.2026 08:30:39	28.05.2026 13:02:21	
	1					04.05.2026 15:48:17	01.04.2026 09:47:09	03.06.2026 16:24:33	
	1				☑	01.04.2026 09:47:09	01.04.2026 09:47:09	10.06.2026 15:19:58	
	1					26.05.2026 09:15:12	26.05.2026 09:14:42	26.05.2026 09:15:21	
	1					19.01.2026 10:49:21	19.01.2026 10:48:37	17.02.2026 10:40:51	
	1					03.06.2026 15:00:41	01.04.2026 09:47:09	03.06.2026 15:26:01	

Всего: 25

Рисунок 65 – Подраздел «Пользователи»

3.4.4.1 Создание учётной записи

Для создания новой учётной записи (УЗ) необходимо выполнить следующие действия:

- 1) Нажать кнопку «+Новый пользователь» (рис. 65).
- 2) В открывшемся окне (рис. 66) ввести данные создаваемого пользователя.

× Новый пользователь

Технический пользователь	☐
Роли	OPERATOR ×
Логин	operator_2
Фамилия	Operator
Имя	Operator
Отчество	Введите отчество
E-mail адрес	mail_operator@mail.ru ✓
Телефон	Введите номер телефона
Учетная запись в jira	00
Пароль	 🔍
Подтвердите пароль	 🔍 ✓

Добавить

Отменить

Рисунок 66 – Окно создания пользователя

3) После ввода необходимой информации нажать кнопку «Добавить» (рис. 66).

Примечания:

1. При создании нового пользователя доступен элемент выбора «Технический пользователь». После установки флага напротив «Технический пользователь» администратору будет доступен список технических ролей (создание технических ролей см. в подпункте 3.4.4.8).
2. Техническому пользователю после создания не требуется менять пароль при первой авторизации, а также пароль не имеет срок действия.
3. После создания технического пользователя администратору будет недоступно снятие флага напротив элемента выбора «Технический пользователь» при изменении учетной записи.

3.4.4.2 Удаление учётной записи

Для удаления УЗ необходимо выполнить следующие действия:

- 1) Выбрать вкладку «Пользователи» (см. рис. 65).
- 2) В открывшемся списке пользователей выбрать УЗ, которую необходимо удалить и нажать на неё левой кнопки мыши.
- 3) Нажать кнопку «Удалить».
- 4) Нажать кнопку  в окне подтверждения (рис.67).

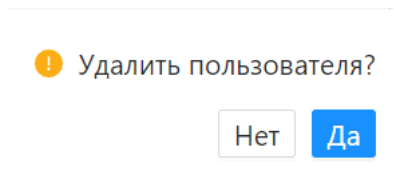


Рисунок 67 – Удаление УЗ

3.4.4.3 Изменение учётной записи

Доступные изменения в следующих полях УЗ (рис. 68):

- роли;
- имя, фамилия и отчество пользователя;
- e-mail адрес;
- телефон;
- учетная запись в Jira.

Для изменения УЗ необходимо выполнить следующие действия:

- 1) Выбрать вкладку «Пользователи» (рис. 65).
- 2) В открывшемся списке пользователей выбрать УЗ, которую необходимо изменить и нажать на неё левой кнопки мыши.
- 3) После внесения изменений в УЗ нажать кнопку «Сохранить».

3.4.4.4 Сброс пароля УЗ

Для сброса пароля УЗ необходимо выполнить следующие действия:

- 1) Выбрать вкладку «Пользователи» (см. рис. 65).
- 2) В открывшемся списке пользователей выбрать УЗ, пароль которой необходимо сбросить и нажать на неё левой кнопки мыши.
- 3) Нажать кнопку «Сбросить пароль» (рис. 68).
- 4) Ввести новый пароль и подтвердить его.

Примечание. После сброса пароля, пользователь, чей пароль был сброшен, будет должен пройти процедуру смены пароля.

✕ Пользователь: operator

Технический пользователь	☐
Роли	OPERATOR ✕
Логин	operator
Фамилия	operator
Имя	operator
Отчество	Введите отчество
Е-mail адрес	operator@mail.ru ✓
Телефон	Введите номер телефона
Учетная запись в jira	00

Сохранить

Сбросить пароль

Заблокировать

Удалить

Рисунок 68 – Окно изменения пользователя

3.4.4.5 Блокировка и разблокировка учётной записи

Для блокировки или разблокировки УЗ необходимо выполнить следующие действия:

- 1) Выбрать вкладку «Пользователи» (см. рис. 65).
- 2) Выбрать УЗ из списка пользователей, которую необходимо заблокировать или разблокировать, нажать на неё левой кнопкой мыши.
- 3) Нажать кнопку «Заблокировать» (рис. 68) или «Разблокировать», если соответствующая учётная запись была заблокирована ранее.

3.4.4.6 Полномочия и роли

Роли в ПК «SAFEERP CS EM» присваиваются при создании нового пользователя (см. рис. 66).

В ПК «SAFEERP CS EM» по умолчанию существуют следующие роли (рис. 69):

- admin;
- operator;
- pentest_agent_callback;
- security_admin.

Настройки / Роли

Пользователи Роли

Введите запрос для поиска

[+ Новая роль](#)

Название	Тип	Группа AD	III
ADMIN		SafeErpAdmins	
OPERATOR		SafeErpOperators	
PENTEST_AGENT_CALLBACK		SafeErpAdmins	
SECURITY_ADMIN		SafeErpSecurityAdmins	
		SafeErpOperators	
		SafeErpOperators	
		SafeErpOperators	
		SafeErpOperators	

Рисунок 69 – Вкладка «Роли»

Роли, предоставляемые по умолчанию, нельзя изменить или удалить. Пользователю доступна функциональность по созданию пользовательских ролей и присваивать им необходимые полномочия.

3.4.4.6.1 Роль ADMIN

Пользователи, которым присвоена роль ADMIN, имеют доступ ко всей функциональности ПК «SAFEERP CS EM», в том числе создание новых пользователей с ролью ADMIN, блокировка, разблокировка пользователей с ролью ADMIN.

3.4.4.6.2 Роль OPERATOR

Пользователи, которым присвоена роль OPERATOR, имеют ограниченный доступ к функциональности ПК «SAFEERP CS EM», а именно полномочия на:

- запуск сканирования проекта, остановку сканирования проекта, обновление данных об итерации после запуска сканирования проекта;
- просмотр списка проектов, просмотр настроек проектов (автор проекта, дата создания, дата последнего изменения, а также источник данных и профили проверок), скачивание отчётов о выявленных недостатках кода в проектах;
- просмотр списка источников данных, а также на просмотр информации об источнике данных;

- просмотр списка профилей, а также просмотр списка проверок, применённых к профилю;
- просмотр информации о лицензии.

3.4.4.6.3 Роль SECURITY_ADMIN

Пользователи, которым присвоена роль SECURITY_ADMIN, имеют такие же полномочия, как и пользователи с ролью ADMIN за исключением обновления лицензии ПК и администрирования пользователей.

3.4.4.6.4 Роль PENTEST_AGENT_CALLBACK

Роль «PENTEST_AGENT_CALLBACK» – это системная роль, предназначенная для корректной работы раздела «Pentest». Роль нужна для авторизации Pentest Agent в сервисе аутентификации ПК «SafeERP EM», поскольку Pentest Agent может находиться вне контура ПК «SafeERP EM». После авторизации Pentest Agent имеет возможность отправлять HTTP-запросы на Pentest Backend через SafeERP Gateway. Отправка этих запросов необходима для получения данных при выполнении сканирования (например, получение данных из БДУ).

3.4.4.7 Пользовательские роли

Создание ролей является процессом, позволяющим гибко настраивать необходимые полномочия.

Подробные действия с пользовательскими ролями изложены в подпунктах 3.4.4.8 – 3.4.4.12 .

3.4.4.8 Создание пользовательских ролей

Для администратора ПК «SAFEERP CS EM» в интерфейсе реализована функциональность создания пользовательских (кастомных) ролей, содержащих наборы полномочий на выполнение определённых действий в ПК «SAFEERP CS EM».

Для создания новых пользовательских ролей необходимо выполнить следующие действия:

- 1) Выбрать вкладку «Роли» (рис. 69).
- 2) Нажать кнопку «+Новая роль» (рис. 69).
- 3) Ввести название новой роли (рис. 70).

× Новая роль

Название

просмотр и запуск проектов

Техническая роль

☐

Группа в ActiveDirectory

Введите название группы

Введите запрос для поиска

Название	Полномочие
☒ Чтение полномочий	authority.read
☒ Чтение списка алгоритмов code-security	cs-algorithm.read
☒ Запуск анализа code-security	cs-analyze.start
☒ Остановка анализа code-security	cs-analyze.stop
☐ Создание проверок code-security	cs-check.create

Добавить

Отменить

Рисунок 70 – Окно «Новая роль»

- 4) Выбрать необходимые полномочия согласно подпункту 3.4.4.9
- 5) Нажать кнопку «Добавить» (рис. 70).

Примечания:

1. В названии роли используются буквы верхнего и нижнего регистра латинского алфавита, буквы верхнего и нижнего регистра русского алфавита, цифры 0 – 9, пробел, тире и нижнее подчеркивание.
2. Название роли должно состоять хотя бы из одного символа.
3. Поле «Active Directory» предназначено для сопоставления пользовательской роли и группы из Active Directory. Данное поле является необязательным для заполнения.
4. Элемент выбора «Техническая роль» предназначен для создания технических ролей.

3.4.4.9 Полномочия, назначаемые пользовательским ролям

Для создания пользовательских ролей необходимо при создании новой роли присвоить полномочия.

Полномочия распределяются по следующим подразделам:

1) Статический анализ.

Полномочия на:

- запуск анализа code-security (cs-analyze.start) – запуск сканирования проекта;
- остановка анализа code-security (cs-analyze.stop) – остановка сканирования проекта;
- чтение проектов code-security (cs-report.read) – просмотр данных проекта, а также просмотр стартовой страницы ПК «SAFEERP CS EM» ;
- чтение уязвимостей code-security (cs-flaw.read) – просмотр найденных уязвимостей в дополнительном окне;
- чтение списка алгоритмов code-security (cs-algorithm.read) – просмотр описания сработанных проверок;
- создание проектов code-security (cs-project.create) – создание проектов;
- изменение проектов code-security (cs-project.update) – редактирование проекта;
- удаление проектов code-security (cs-project.delete) – удаление проектов;
- удаление итераций code-security (cs-iteration.delete) – удаление итерации проектов;
- чтение отчета code-security (cs-report.read) – просмотр отчетов по результатам итерации в отдельном окне;
- чтение статистики code-security (cs-statistics.read) – просмотр панели мониторинга по проекту;
- чтение исключений уязвимостей code-security (cs-flaw-exclusion.read) – просмотр исключений в подразделе «Проекты»;
- создание исключений уязвимостей code-security (cs-flaw-exclusion.create) – создание исключений в подразделе «Проекты»;
- изменение исключений уязвимостей code-security (cs-flaw-exclusion.update) – изменение исключений в подразделе «Проекты»;
- удаление исключений уязвимостей code-security (cs-flaw-exclusion.delete) – удаление исключений в подразделе «Проекты»;
- чтение профилей code-security (cs-profile.read) – просмотр профилей;
- создание профилей code-security (cs-profile.create) – создание пользовательских профилей;
- изменение профилей code-security (cs-profile.update) – редактирование пользовательских профилей;
- удаление профилей code-security (cs-profile.delete) – удаление проверок в пользовательских профилях;
- чтение проверок code-security (cs-check.read) – просмотр пользовательских и стандартных проверок;
- создание проверок code-security (cs-check.create) – создание пользовательских проверок;
- изменение проверок (cs-check.update) – внесение изменений в пользовательские проверки;
- экспорт проверок code-security (cs-check.export) – экспорт проверок для

копирования профилей проверок;

- импорт проверок (cs-check.import) – импорт проверок для копирования профилей проверок;
- удаление проверок code-security (cs-check.delete) – удаление пользовательских проверок.

2) SCA.

Полномочия на:

- запуск анализа sca (sca-analyze.start) – запуск сканирования проектов;
- остановка анализа sca (sca-analyze.stop) – остановка сканирования проектов;
- чтение проектов sca (sca-project.read) – просмотр данных проектов;
- создание проектов sca (sca-project.create) – создание проектов;
- изменение проектов sca (sca-project.update) – редактирование проектов;
- удаление проектов sca (sca-project.delete) – удаление проектов;
- чтение итераций sca (sca-iteration.read) – просмотр списка итераций проектов;
- чтение уязвимостей sca (sca-flaw.read) – просмотр найденных уязвимостей в дополнительном окне.

3) Цели сканирования и источники.

Полномочия на:

- чтение цели сканирования (target.read) – просмотр цели сканирования;
- создание цели сканирования (target.create) – создание цели сканирования;
- изменение цели сканирования (target.update) – изменение цели сканирования;
- удаление цели сканирования (target.delete) – удаление цели сканирования;
- чтение источников данных code-security (cs-datasource.read) – просмотр данных источника;
- создание источников данных code-security (cs-datasource.create) – подключение источников;
- изменение источников данных code-security (cs-datasource.update) – изменение источников;
- удаление источников данных code-security (cs-datasource.delete) – удаление источников.

4) Настройки.

Полномочия на:

- чтение полномочий (authority.read) – запрос списка доступных полномочий для пользователя;
- чтение лицензии (license.read) – просмотр информации о лицензии;
- запрос лицензии (license.request) – отправка запроса на активацию лицензии;
- создание лицензии (license.create) – активация и загрузка активированной лицензии;
- удаление лицензии (license.delete) – удаление лицензии ПК «SAFEERP CS EM»;
- чтение ролей (role.read) – просмотр ролей;
- создание ролей (role.create) – создание пользовательских ролей;
- изменение ролей (role.update) – редактирование пользовательских ролей;

- удаление ролей (role.delete) – удаление созданных пользовательских ролей;
- чтение пользователя (user.read) – просмотр информации о пользователе, а также список пользователей в ПК «SAFEERP CS EM» ;
- создание пользователей (user.create) – создание новых пользователей;
- изменение пользователей (user.update) – редактирование пользователей;
- блокировка пользователя (user.lock) – блокировка пользователя;
- разблокировка пользователя (user.unlock) – разблокировка пользователя;
- сброс пароля пользователя (user.passwordReset) – сброс пароля пользователя;
- удаление пользователей (user.delete) – удаление пользователя;
- чтение лога code-security (cs-log.read) – просмотр событий, зарегистрированных в ПК «SAFEERP CS EM» , а также загрузка файла лога на локальную машину;
- чтение информации code-security (cs-info.read) – просмотр информации ПК «SAFEERP CS EM» в подразделе «Настройки»;
- чтение документов code-security (cs-doc.read) – просмотр и выгрузка архива с документацией;
- чтение версий установленных клиентов 1С (settings.read) – чтение версии агентов в подразделе «Информация».

5) Jira.

Полномочия на:

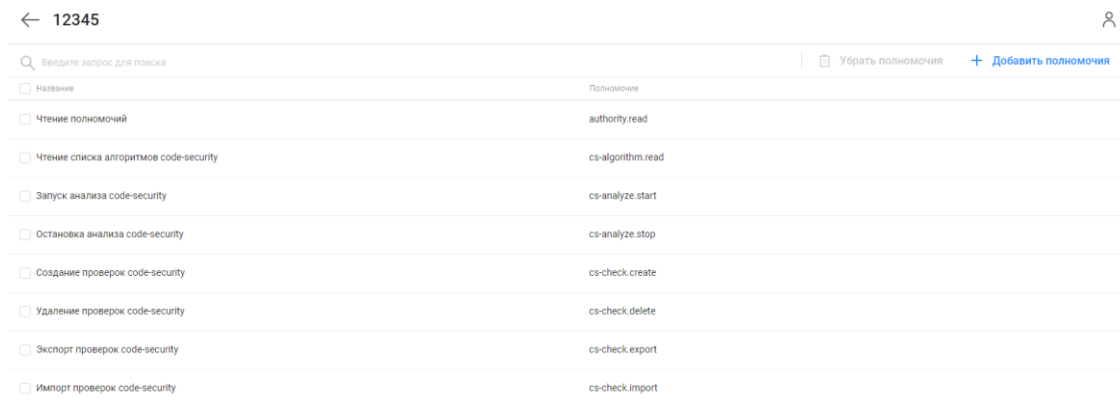
- чтение версии API Jira (jira-api-version.read) – просмотр версии API системы отслеживания задач «Jira»;
- чтение приоритетов задач Jira (jira-issue-priority.read) – просмотр приоритетов задач системы отслеживания задач «Jira» в разделе «Настройки»;
- чтение типов задач Jira (jira-issue-type.read) – просмотр типов задач системы отслеживания задач «Jira» в разделе «Настройки»;
- проверка статуса конфигурации настроек Jira (jira-settings-configured.read) – - предназначено для корректного отображения элементов управления системы отслеживания задач «Jira» в интерфейсе ПК «SafeERP CS EM», при отсутствии полных прав к настройкам в системе отслеживания «Jira». Является обязательным полномочием при работе с системой отслеживания задач «Jira»;
- чтение проектов Jira (jira-project.read) – просмотр списка проектов в разделе «Настройки»;
- чтение настроек Jira (jira-settings.read) – просмотр настроек по интеграции с системой отслеживания задач «Jira» в разделе «Настройки»;
- изменение настроек Jira (jira-settings.update) – изменение настроек по интеграции с системой отслеживания задач «Jira»;
- чтение статусов задачи Jira (jira-status.read) – просмотр статусов задач системы отслеживания задач «Jira»;
- чтение пользователей Jira (jira-user.read) – просмотр списка пользователей системы отслеживания задач «Jira».

3.4.4.10 Редактирование пользовательских ролей

В пользовательских ролях доступно добавление или удаление полномочий.

Для добавления новых полномочий в пользовательские роли необходимо выполнить следующие действия:

- 1) Выбрать вкладку «Роли» (рис. 69).
- 2) Выбрать пользовательскую роль из списка.
- 3) Нажать кнопку «+Добавить полномочия» (рис. 71).



← 12345		Убрать полномочия + Добавить полномочия	
Название	Полномочие		
☐ Чтение полномочий	authority.read		
☐ Чтение списка алгоритмов code-security	cs-algorithm.read		
☐ Запуск анализа code-security	cs-analyze.start		
☐ Остановка анализа code-security	cs-analyze.stop		
☐ Создание проверок code-security	cs-check.create		
☐ Удаление проверок code-security	cs-check.delete		
☐ Экспорт проверок code-security	cs-check.export		
☐ Импорт проверок code-security	cs-check.import		

Рисунок 71 – Окно просмотра пользовательской роли

- 4) Поставить флаг  напротив полномочий (рис. 72).

× Добавление полномочий

🔍 Введите запрос для поиска

☐ Название

Полномочие

☒ Чтение полномочий

authority.read

☒ Чтение списка алгоритмов code-security

cs-algorithm.read

☐ Запуск анализа code-security

cs-analyze.start

☐ Остановка анализа code-security

cs-analyze.stop

☐ Создание проверок code-security

cs-check.create

Всего: 110 Выбранных: 2

Применить

Отменить

Рисунок 72 – Окно «Добавление полномочий»

5) Нажать кнопку «Применить» (см. рис. 72).

Для удаления полномочий из пользовательских ролей необходимо выполнить следующие действия:

- 1) Выбрать вкладку «Роли» (рис. 69).
- 2) Выбрать пользовательскую роль из списка.
- 3) Поставить флаг ☒ напротив полномочий (рис. 71).
- 4) Нажать кнопку «Убрать полномочия» (рис. 71).

Примечание. Для обновления полномочий у пользователей необходимо повторно авторизоваться в ПК «SAFEERP CS EM».

3.4.4.11 Копирование ролей

Для копирования ролей необходимо пункт «Копировать» в контекстном меню (рис. 73), нажать кнопку «Копировать», внести необходимые данные в окне «Добавить роль» (см. рис. 70), нажать кнопку «Добавить».

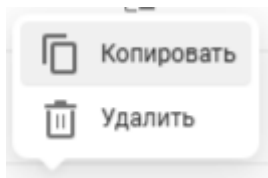


Рисунок 73 – Доступные действия с пользовательской ролью

3.4.4.12 Удаление пользовательских ролей

Для удаления пользовательских ролей необходимо выбрать пункт «Удалить» в контекстном меню (см. рис. 73), подтвердить действие.

Примечание. Удалению подлежат только пользовательские роли.

3.4.5 Подраздел «Журнал»

В ПК «SAFEERP CS EM» реализована функциональность просмотра журнала событий.

К регистрируемым событиям ПК «SAFEERP CS EM» относится следующее (рис. 74):

- системные события (ошибки, предупреждения, информационные сообщения);
- пользовательские действия (события в разделах ПК «SafeERP CS EM», аутентификация, изменения настроек в ПК «SafeERP CS EM»).

Журнал				👤
🔍 Введите запрос для поиска				☰ Фильтр Скачать журнал
Дата	Тип события	Область	Сообщение	⋮
12.01.2026 14:22:02	DEBUG	kafka-ui	Metrics updated for cluster: Default	
12.01.2026 14:22:02	DEBUG	kafka-ui	Start getting metrics for kafkaCluster: Default	
12.01.2026 14:21:32	DEBUG	kafka-ui	Metrics updated for cluster: Default	
12.01.2026 14:21:32	DEBUG	kafka-ui	Start getting metrics for kafkaCluster: Default	
12.01.2026 14:21:27	DEBUG	debezium-embedded	transaction (txId: '734654') update-event for: 'dast.iterations', for row with id: '{"id":26}'	
12.01.2026 14:21:27	DEBUG	debezium-embedded	composite first-last payload:	
12.01.2026 14:21:27		debezium-embedded	{ "before": {"id": 26, "is_launched": true, "is_canceled": false, "project_id": 11, "launch_time": "12.01...	
12.01.2026 14:21:07	DEBUG	debezium-embedded	transaction (txId: '734647') update-event for: 'dast.iterations', for row with id: '{"id":26}'	
12.01.2026 14:21:07	DEBUG	debezium-embedded	composite first-last payload:	
12.01.2026 14:21:07		debezium-embedded	{ "before": {"id": 26, "is_launched": true, "is_canceled": false, "project_id": 11, "launch_time": "12.01...	
Всего: 14514462 Доступных для просмотра: 10000				< 1 2 3 4 5 ... 100 >

Рисунок 74 – Подраздел «Журнал»

По умолчанию в журнале событий выводятся события всех типов.

Для того чтобы отфильтровать журнал по выбранным параметрам необходимо выполнить следующие действия:

- 1) Нажать кнопку «*Фильтр*».
- 2) Выбрать в окне необходимые параметры. Нажать кнопку «*Применить*».

The screenshot shows a web application interface. At the top, there are two buttons: 'Фильтр' (Filter) and 'Скачать журнал' (Download log). Below these is a modal window titled 'Фильтр'. Inside the modal, there are three sections: 'Дата' (Date) with 'Начальная дата' (Start date) and 'Конечная дата' (End date) fields, 'Тип' (Type) with a 'Тип события' (Event type) dropdown, and 'Область' (Area) with an 'Область события' (Event area) dropdown. At the bottom of the modal are two buttons: 'Применить' (Apply) and 'Сбросить' (Reset).

Рисунок 75 – Окно «Фильтр»

Доступны следующие параметры, по которым доступна фильтрация событий в журнале:

1. Типы событий (рис. 76).

Дата

Начальная дата → Конечная дата

Тип

Тип события

- ☐ ERROR
- ☐ WARN
- ☐ INFO
- ☐ DEBUG
- ☐ TRACE

Рисунок 76 – Типы событий журнала

2. По дате и времени возникновения события (рис. 77).

Дата

Начальная дата → Конечная дата

<< < янв. 2025 > >>

Пн	Вт	Ср	Чт	Пт	Сб	Вс	00	00
30	31	1	2	3	4	5	01	01
6	7	8	9	10	11	12	02	02
13	14	15	16	17	18	19	03	03
20	21	22	23	24	25	26	04	04
27	28	29	30	31	1	2	05	05
3	4	5	6	7	8	9	06	06
							07	07
							08	08

OK

Рисунок 77 – Фильтрация журнала по дате и времени

3. По области событий.

В подразделе «Журнал» доступен фильтр по следующим областям:

- authentication – регистрируются события, связанные с процессом аутентификации пользователей, созданием, редактированием и удалением пользователей и ролей, лицензиями;
- code-security – регистрируются события, связанные с разделом «Статический анализ»;
- dast – регистрируются события, связанные с подразделом «DAST»;
- frontend-react – регистрируются события, относящиеся к фронтенду веб-приложений, написанных на React.js;
- gateway – регистрируются события, связанные с шлюзом (Gateway);
- infodb-c2server – предназначен для событий обновления БДУ PS EM;
- kafka – регистрируются события, связанные с распределительной системой Apache Kafka;
- mailing – предназначен для обработки событий, предназначенных для почтовой рассылки;
- pentest_agent – регистрируются события, связанные с агентами подраздела «Pentest»;
- pentest_backend – регистрация событий раздела «Pentest»;
- platform-security – регистрируются события, связанные с разделом «Анализ платформы»;
- target-manager – регистрируются события, связанные с разделом «Цели сканирования»;
- task-orchestrator – регистрируются события, связанные с системой отслеживания задач «Jira»;
- web-security-service – регистрируются события, связанные со сканером WSC.

3.4.5.1 Просмотр журнала

Для просмотра журнала необходимо выполнить следующие действия:

- 1) Выбрать раздел «Настройки».
- 2) Выбрать подраздел «Журнал».

Примечания:

1. При просмотре журнала доступен поиск событий. Для поиска события необходимо ввести текст сообщения в поисковую строку.
2. Доступен поиск сообщений на русском и английском языках.

3.4.5.2 Выгрузка журнала

Для выгрузки журнала необходимо выполнить следующие действия:

- 1) Выбрать раздел «Настройки».
- 2) Выбрать подраздел «Журнал».
- 3) Нажать кнопку «Скачать журнал» (рис. 74).

3.5 Профиль пользователя

Для вызова профиля пользователя необходимо нажать кнопку в верхнем правом углу рабочей области ПК «SAFEERP CS EM».

В профиле пользователя доступны следующие действия:

- просмотр данных текущего пользователя;
- смена пароля;
- просмотр и настройка почтовых подписок;
- просмотр списка проектов, по которым пользователь получает почтовые рассылки;
- переход в проект;
- отмена почтовых подписок.

3.5.1 Просмотр данных текущего пользователя

Для просмотра данных текущего пользователя необходимо выбрать пункт меню «Настройки пользователя».

3.5.2 Смена пароля

Для смены пароля необходимо выбрать следующие действия:

- 1) Выбрать пункт меню «Настройки пользователя».
- 2) Нажать кнопку «Сменить пароль».
- 3) Ввести старый пароль в поле «Текущий пароль». Ввести новый пароль в поля «Новый пароль» и «Подтвердите пароль».
- 4) Нажать кнопку «Изменить».

Примечание. После смены пароля необходимо повторно авторизироваться.

3.5.3 Просмотр списка активных подписок

Для просмотра списка активных подписок необходимо обратиться к профилю пользователя, выбрать раздел «Активные подписки» (рис. 78).

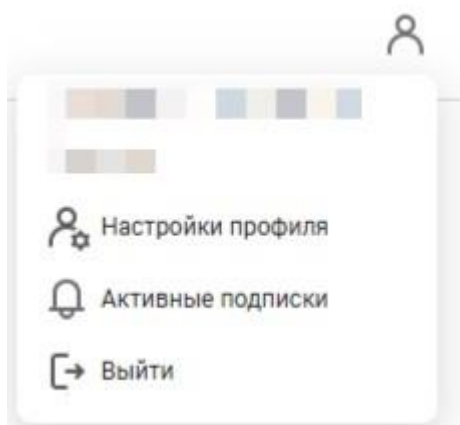


Рисунок 78 – Профиль пользователя

При нажатии на название проекта раскрывается список событий по данному проекту, на

которые подписан пользователь. Список подписок представлен на рис. 79

× Активные подписки

🔍 Введите запрос для поиска	🚫 Отменить подписки
☐ Название	Тип проекта
☒ ST1_1	Статический анализ
☐ K2	Статический анализ
☐ Test	Анализ платформы

Рисунок 79 – Список активных подписок

3.5.4 Отмена почтовых подписок

Для отмены почтовых подписок на проект по всем событиям необходимо нажать кнопку «Отменить подписку по проекту» в контекстном меню напротив имени проекта (рис. 80).

Примечание. При просмотре списка активных подписок доступно массовая отмена. Для массовой отмены подписок необходимо поставить флаг напротив проектов, нажать кнопку «Отменить подписки».

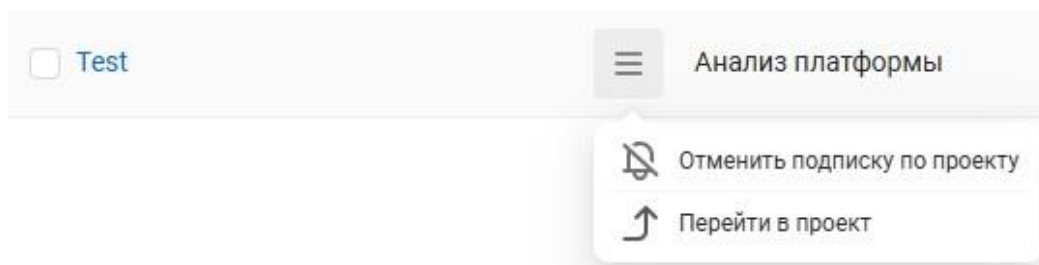


Рисунок 80 – Контекстное меню при просмотре списка активных подписок

4 Парольная политика

Для создания пароля необходимо использовать следующие символы:

- буквы латинского алфавита в верхнем регистре A-Z;
- буквы латинского алфавита в нижнем регистре a-z;
- цифры 0 - 9;
- символы (!@#\$%^&*?()[]{}|<>_+,.\\';:~"-).

Парольная политика в ПК «SAFEERP CS EM» соответствует минимальным требованиям ФСТЭК для четвёртого уровня защищённости ПДн. Согласно данной политике, устанавливаются следующие характеристики пароля в качестве средства аутентификации:

- минимальная длина пароля – 8;
- минимальное количество цифр – 2;
- минимальное количество букв – 2;
- минимальное количество символов - 2;
- минимальное количество символов в верхнем регистре – 1;
- минимальное количество букв в нижнем регистре – 1;
- максимальное число не успешных попыток ввода пароля – 7;
- время блокировки ввода пароля после превышения максимального числа неудачных попыток ввода пароля – 10 минут.

Примечания:

1. Срок действия пароля с даты его последнего обновления составляет 90 дней. Минимальный срок действия пароля – 30 дней. За 7 дней до окончания срока действия пароля пользователю будет отображено уведомление об истечении срока действия пароля и необходимости его изменения. После истечения срока действия пароля его необходимо изменить.
2. Новый пароль должен отличаться от старого минимум на 3 символа. Изменением не считаются следующие:
 - изменение регистра букв;
 - перестановка символов.
3. Для каждого пользователя в базе данных сохраняются история последних 10 паролей.

Список сокращений

АРМ	—	Автоматизированное рабочее место
БДУ	—	База данных уязвимостей
ИБ	—	Информационная безопасность
ИС	—	Информационная система
ПК	—	Программный комплекс
ПО	—	Программное обеспечение
СУБД	—	Система управления базами данных
УЗ	—	Учётная запись
АПК	—	Администратор программного комплекса
CVE	—	Common Vulnerabilities and Exposures
IDS	—	Intrusion Detection System
IPS	—	Intrusion Prevention System
PDF	—	Portable Document Format
EM	—	Extension Module
DNS	—	Domain Name System
IP	—	Internet Protocol
SCA	—	Software Composition Analysis: