

ПК «SafeERP CS EM»
Руководство оператора

Аннотация

Руководство оператора программного комплекса программного комплекса (далее – ПК) «SafeERP Code Security Extension Module» (далее – «SafeERP CS EM») является программным документом, определяющим порядок эксплуатации данного ПК. Руководство ориентирована на пользователей, осуществляющих работу с данным ПК. 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»;
- запуск веб-интерфейса оператора ПК «SafeERP CS EM»;
- описание веб-интерфейса оператора 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»	4
2	Общая схема работы ПК «SafeERP CS EM»	5
3	Запуск веб-интерфейса ПК «SafeERP CS EM»	6
4	Описание веб-интерфейса ПК «SafeERP CS EM»	7
4.1	Раздел «Статический анализ»	7
4.1.1	Подраздел «Проекты»	7
4.1.1.1	Просмотр настроек проекта	9
4.1.1.2	Запуск и остановка сканирования проектов	9
4.1.1.3	Просмотр проектов и результатов сканирования	10
4.1.1.4	Выгрузка отчетов	13
4.1.1.5	Подключение почтовых оповещений	16
4.1.2	Подраздел «Профили»	16
4.1.3	Подраздел «Проверки»	25
4.2	Раздел «SCA»	27
4.2.1	Просмотр проекта	29
4.2.2	Запуск проекта	29
4.2.3	Просмотр результатов сканирования	30
4.3	Раздел «Цели сканирования»	32
4.4	Раздел «Настройки»	32
4.4.1	Информация о ПК «SafeERP CS EM»	32
4.4.2	Лицензии	34
4.5	Профиль пользователя	35
4.5.1	Просмотр данных текущего пользователя	35
4.5.2	Смена пароля	35
4.5.3	Просмотр списка активных подписок	36
4.5.4	Отмена почтовых подписок	36
5	Парольная политика	38
	Список сокращений	39

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:

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

Функции ПК «SafeERP CS EM», реализованные для оператора ПК в веб-интерфейсе:

- запуск сканирования проектов для проведения процедур анализа кода контролируемых систем;
- просмотр результатов анализа после выполнения итерации;
- подключение почтовых уведомлений по проекту;
- загрузка отчётов по результатам анализа;
- проверка статусов доступности ранее подключенных источников данных;
- просмотр профилей проверок;
- просмотр информации о версии сервера и интерфейса ПК «SafeERP CS EM»;
- просмотр информации о лицензии ПК «SafeERP CS EM».

2 Общая схема работы ПК «SafeERP CS EM»

Общая схема работы ПК «SafeERP CS EM» в режиме работы оператора представлена на рис. 1.

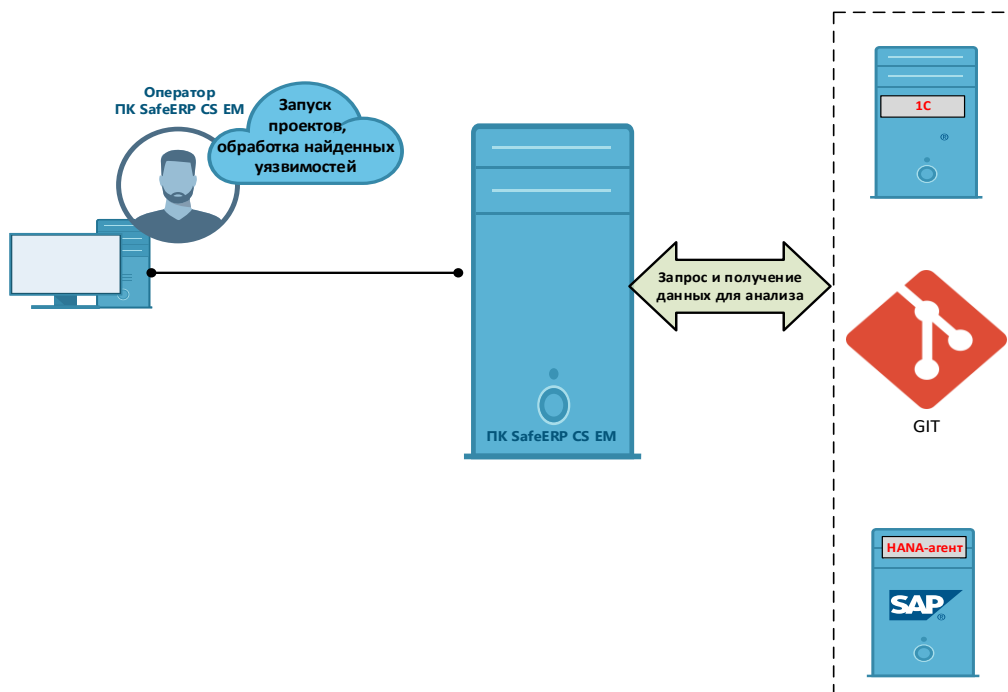
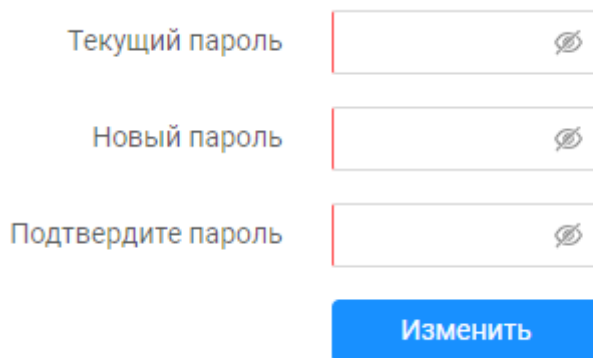


Рисунок 1 – Общая схема работы ПК «SafeERP CS EM» в режиме оператора

3 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. После перехода оператору по данному адресу откроется форма аутентификации, в которую необходимо ввести логин пользователя и пароль, предоставленные администратором ПК. После ввода верной аутентификационной информации откроется окно смены пароля (рис. 2).



Текущий пароль

Новый пароль

Подтвердите пароль

Изменить

Рисунок 2 – Окно смены пароля

После прохождения процедуры смены пароля необходимо аутентифицироваться повторно, после чего откроется стартовая страница ПК «SafeERP CS EM» (рис. 3).

CS EM

PS EM

<

Рисунок 3 – Стартовая страница оператора ПК «SafeERP CS EM»

4 Описание веб-интерфейса ПК «SafeERP CS EM»

ПК «SafeERP CS EM» содержит следующие функциональные разделы:

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

4.1 Раздел «Статический анализ»

Раздел «Статический анализ» содержит следующие функциональные подразделы:

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

4.1.1 Подраздел «Проекты»

Основная область подраздела «Проекты» представлена на рис. 4.

Проекты				👤
🔍 Введите запрос для поиска				
Название	Статус	Последний запуск	Выявленных угроз	⋮
	⚠ 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 4 – Основная рабочая область подраздела «Проекты»

Для просмотра анализа проекта необходимо нажать на название проекта. В окне показаны следующие столбцы (рис. 5):

- «Дата сканирования»;
- «Статус итерации»;

- «Тип проекта» – тип источника данных. Источники данных бывают следующих видов: архив и цели сканирования;
- «Количество строк кода»;
- «Профили» – количество профилей, которое применено к данной итерации проекта;
- «Языки»;
- «Недостатки кода»;
- «Время сканирования».

Обновить

Настройки проекта

Оповещения

Запустить сканирование

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

1

2

3

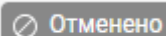
Рисунок 5 – Просмотр списка итераций проекта

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



Сканирование было отменено пользователем

Недостатки кода

В таблице 2 представлены уровни критичности для недостатков кода.

Таблица 2– Значения цветов для каждого статуса

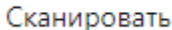
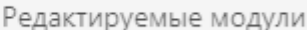
Цвет	Значение
	Высокий
	Средний
	Низкий
	Информация

4.1.1.1 Просмотр настроек проекта

Для просмотра настроек проекта, необходимо выполнить следующие действия:

- 1) Выбрать меню «Проекты».
- 2) Выбрать проект или ввести его название в поисковую строку.
- 3) Нажать кнопку «*Настройка проекта*» (рис. 5).

Примечания:

1. Если источником данных является 1С, то необходимо выбрать сканировать всю конфигурацию или только редактируемые модули    . Для выбора необходимо обратиться к администратору ПК «SAFEERP CS EM».
2. Если источником данных выбран 1С, то необходимо выбрать сканировать весь код или только код, в который были внесены изменения с момента последнего сканирования. Для выбора необходимо обратиться к администратору ПК «SAFEERP CS EM».

4.1.1.2 Запуск и остановка сканирования

Запуск сканирования осуществляется двумя способами:

- через контекстное меню;
- со страницы проекта.

Для запуска сканирования со страницы проекта необходимо выполнить следующие действия:

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

Для запуска сканирования через контекстное меню необходимо выполнить следующие действия:

- 1) Выбрать пункт меню «Проекты» (см. рис. 3).

- 2) Нажать кнопку  в строке проекта, выбрать пункт «*Запустить*» в

раскрывшемся меню.

Примечание. 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 момента её продления. Подробнее об условиях доступа см. в пункте 4.4.2

Остановка сканирования проекта

Остановка сканирования проекта осуществляется следующими способами:

- через контекстное меню;
- 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.

4.1.1.3 Просмотр проектов и результатов сканирования

Для просмотра панели мониторинга необходимо выполнить следующие действия:

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

Данные панели мониторинга представлены на рис. 6. 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. 6).

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

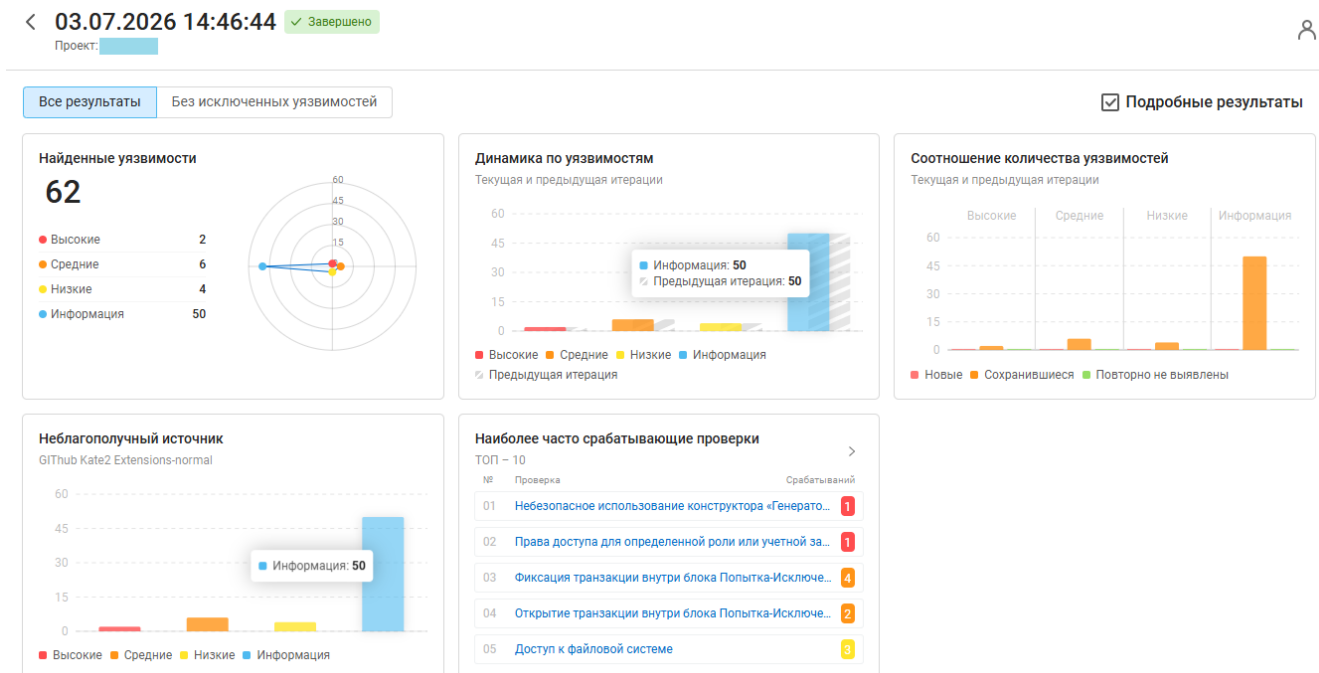


Рисунок 6 – Панель мониторинга по результатам итерации

Просмотр результатов итерации

Для просмотра результатов итерации необходимо выполнить следующие действия:

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

Просмотр найденной уязвимости

Для просмотра 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. 7).

< 28.05.2026 09:21:00 ✓ Завершено

Проект:

Найденные уязвимости 21

Исключенные уязвимости

Q Введите з...

Doc2 bd 10 2 2 7

Некорректная деактивация привилегированн... 5

Основная конфигурация/HTTPСервисы/Мо... ●

Основная конфигурация/HTTPСервисы/Мо... ●

Основная конфигурация/HTTPСервисы/Мо... ●

Основная конфигурация/HTTPСервисы/Мо... ●

Основная конфигурация/HTTPСервисы/Мо... ●

Привилегированный режим 1С 5

Основная конфигурация/HTTPСервисы/Мо... ●

Основная конфигурация/HTTPСервисы/Мо... ●

Основная конфигурация/HTTPСервисы/Мо... ●

Основная конфигурация/HTTPСервисы/Мо... ●

Основная конфигурация/HTTPСервисы/Мо... ●

Получение метаданных объекта конфигурации 2

Доступ к файловой системе 2

Отсутствие аргументов при вызове метода "З... 1

Отсутствие конструкции «Иначе» в условном ... 4

Пустой блок 1

Сравнение с булевым литералом 1

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 ПроверитьСпособности(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 ПроверитьСпособности(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 7 – Строка с найденной уязвимостью

При просмотре результатов итерации пользователю доступны следующие действия (см. рис. 7):

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

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;
- устранена;
- ложное срабатывание.

Примечания:

1. Уязвимости со статусом «В работе» или «Не устранена» отображаются на вкладке «Найденные уязвимости» (рис. 7).
2. Уязвимости со статусом «Ложное срабатывание», «Принята», «Устранена» отображаются на вкладке «Исключенные уязвимости».
3. Для выделения всех найденных уязвимостей доступна кнопка «*Выбрать все*». Кнопка доступна в дереве найденных уязвимостей (см. рис. 7).

4.1.1.4 Выгрузка отчетов

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

Выгрузка отчёта доступна со следующих страниц:

- список проектов (рис. 8);
- списка итераций (рис. 9);
- подробных результатов – вкладки «Найденные уязвимости» и «Исключенные уязвимости» (рис. 10)

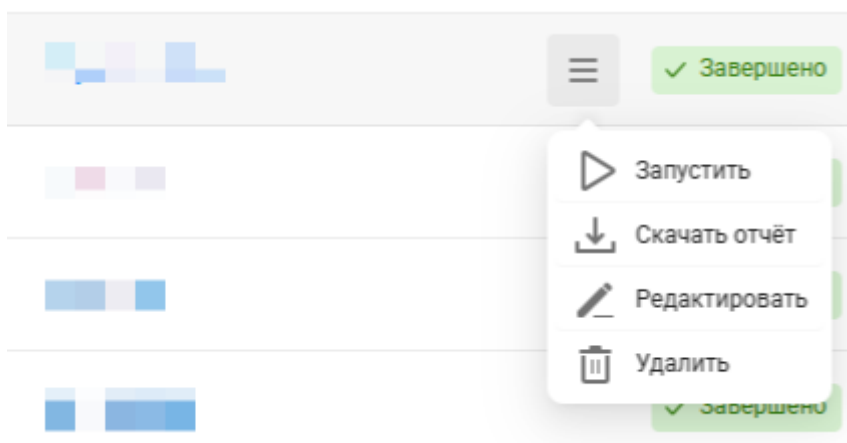


Рисунок 8 – Выгрузка отчета на странице списка проектов

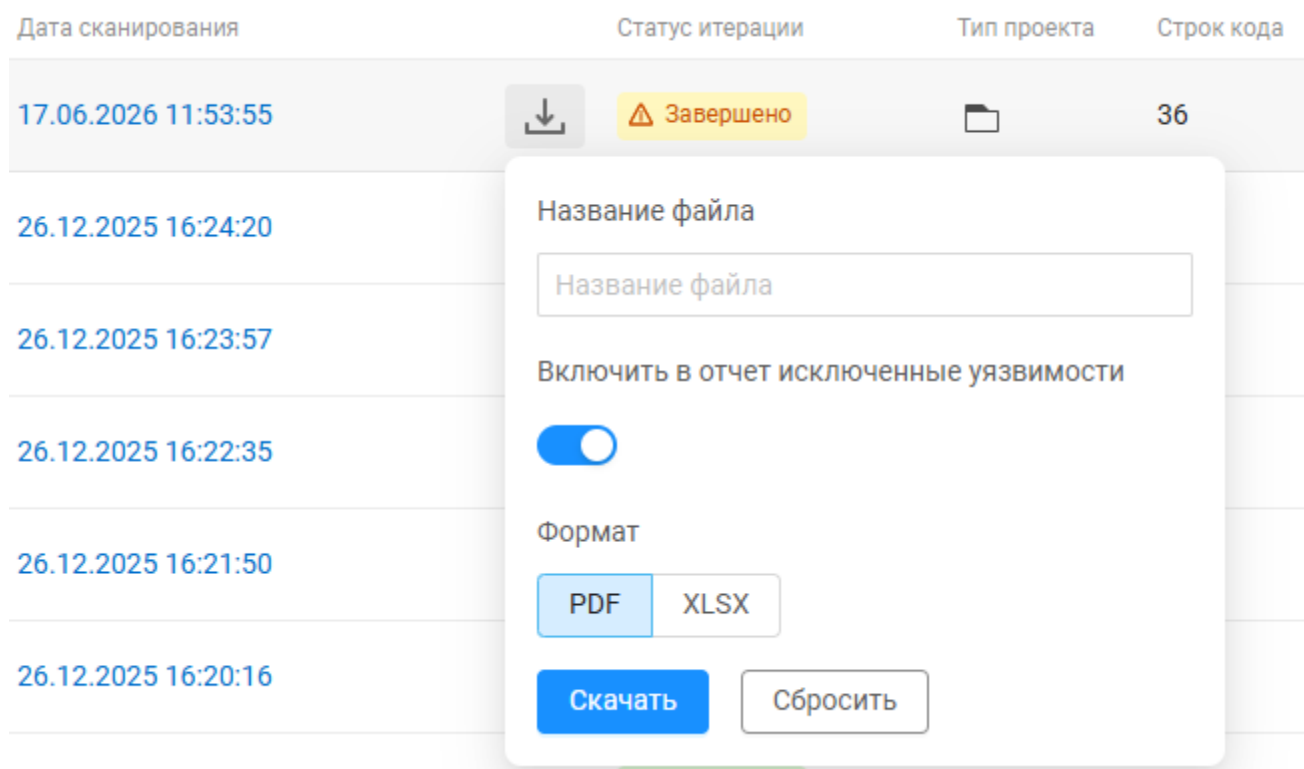


Рисунок 9 – Выгрузка отчета

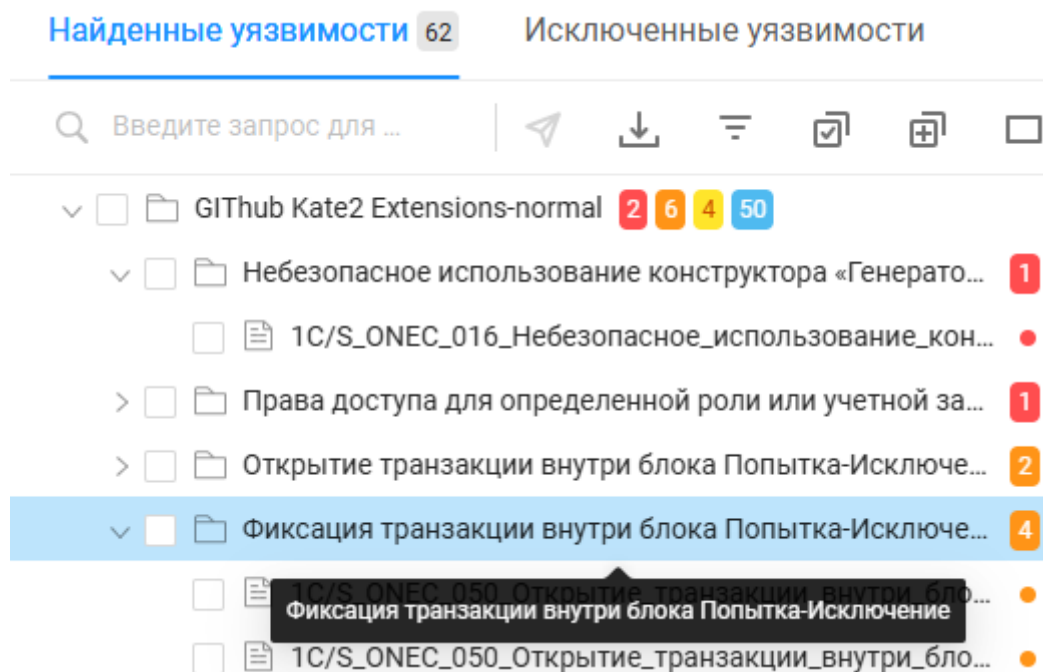


Рисунок 10 – Выгрузка отчета при просмотре дерева уязвимостей

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.

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 выгрузки отчёта;
- настраиваемый отчёт – выгружается по выбранным в дереве уязвимостям.

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

Название файла

Формат

PDF

XLSX

Скачать

Сбросить

Рисунок 11 – 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.

4.1.1.5 Подключение почтовых оповещений

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

Для подключения почтовых уведомлений необходимо выполнить следующие действия:

- 1) Выбрать проект.
- 2) Нажать кнопку «Оповещения» (рис. 12).

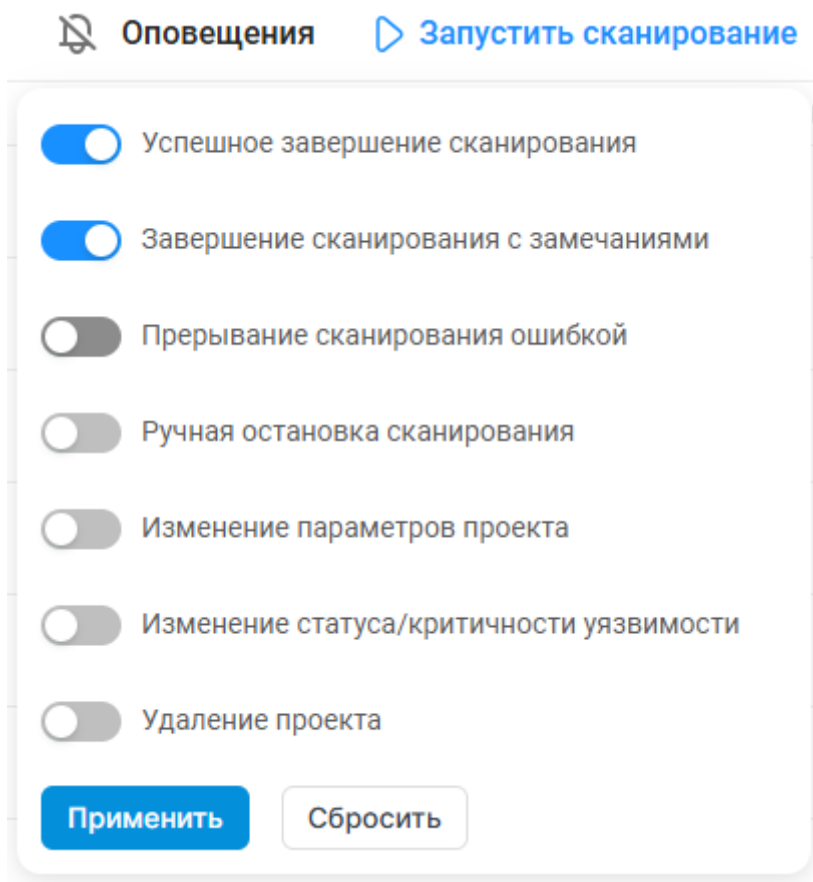


Рисунок 12 – Список событий (раздел «Статический анализ»)

3) Выбрать события в окне (см. рис. 12).

4) Нажать кнопку «Применить».

Примечание. Для корректной работы почтовых уведомлений необходимо убедиться, что в профиле пользователя указана электронная почта.

Примеры почтовых уведомлений приведены на рисунках 13, 14, 15, 16, 17, 18, 19, 20.



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 13 – 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 14 – 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

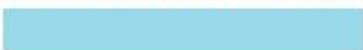
Перейти к детальной информации по итерации [17.06.2026 11:39:45](#)

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

Рисунок 15 – 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 16 – 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 17 – 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 18 – 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 19 – 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 20 – Почтовое уведомление при выборе события «Удаление проекта»

Просмотр активных подписок

Для просмотра списка активных подписок необходимо обратиться к подразделу 4.5 .

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 4.5 .

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. 12).

4.1.2 Подраздел «Профили»

Основная рабочая область подраздела «Профили» представлена на рис. 21 .

Профили проверок						⌵
🔍 Введите запрос для поиска						
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	SECSEM	28.11.2025 15:17:41	
Проверки C#	📁	10	1 ^	SECSEM	28.11.2025 15:17:41	
Проверки Dockerfile	📁	20	1 ^	SECSEM	28.11.2025 15:17:41	
Проверки Java	📁	6	1 ^	SECSEM	28.11.2025 15:17:41	
Проверки JS	📁	12	1 ^	SECSEM	28.11.2025 15:17:41	
Проверки Python	📁	10	1 ^	SECSEM	28.11.2025 15:17:41	
Всего: 27						

Рисунок 21 – 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 пользовательскими (создает администратор ПК «SafeERP CS EM»).

4.1.2.1 Просмотр профилей проверок

Для просмотра профиля проверок необходимо выполнить следующие действия:

- 1) Выбрать пункт меню «Профили» (см. рис. 3).
- 2) Выбрать профиль проверок или ввести его название в поисковую строку.
- 3) Нажать на название профиля проверок.

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. 22):

- тип;
- язык;
- критичность;
- категория;
- вектор атаки;
- теги.

Тип

Тип

Язык

Язык

Критичность

Критичность

Категория

Категория

Вектор атаки

Вектор атаки

Теги

Теги

Применить

Сбросить

Рисунок 22 – Окно «Фильтр»

4.1.3 Подраздел «Проверки»

Проверки - шаблоны для поиска уязвимостей исходного кода. Оператору ПК «SafeERP CS EM» доступен просмотр проверок.

Основная рабочая область подраздела «Проверки» представлена на рис. 23.

Проверки

Введите запрос для поиска

Фильтр

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 23 – Основная рабочая область подраздела «Проверки»

Для просмотра проверки необходимо выполнить следующие действия:

- 1) Выбрать пункт меню «Проверки».
- 2) Выбрать проверку или ввести её название в поисковую строку.
- 3) Нажать на название проверки.

Подробная информация о проверке представлено на рис. 24.

× Программное назначение роли пользователю

Критичность

Высокая

Язык

1С

Описание

Проверка «Программное назначение роли пользователю» выявляет случаи использования в программном коде системы «1С:Предприятие» программного назначения роли пользователю. Проверяется использование метода «Добавить» с объектом «РолиПользователя». Данный метод позволяет выполнить программное назначение роли пользователю.

Возможные угрозы

- Обход системы авторизации;
- Выполнение бизнес-логики с расширенными полномочиями.

Рекомендации

- Проведите «ручной» анализ результатов проверки для определения степени критичности участков кода, в которых используется метод «Добавить» с объектом «РолиПользователя».

Пример

Функция УстановитьРолиНепосредственноПриИзменении(Элемент)

Пользователь = Объект.Польз.ПолучитьОбъект();

Пользователь.РолиПользователя.Добавить(Метаданные.Роли.БазовыеПрава);

Пользователь.Записать();

КонецФункции

Ссылки

- [MITRE CWE-276](#)
- [MITRE CWE-732](#)
- [OWASP TOP-10 A01_2021](#)
- [MITRE CWE-639](#)
- [MITRE CWE-708](#)
- [CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:C/C:H/I:H/A:H/E:H/RC:C/CR:H/IR:H/AR:H = 9.9](#)
- [MITRE CWE-658](#)

Рисунок 24 – Подробное описание проверки

4.2 Раздел «SCA»

Раздел «SCA» предназначен для анализа файла спецификации с целью обнаружения встроенных опенсорсных решений, определения их актуальности, выявления уязвимостей и соответствий лицензионным требованиям.

Раздел «SCA» состоит из следующего подраздела:

— «Проекты».

Проекты



Введите запрос для поиска

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 25 – 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.

Доступны следующие статусы проектов:

- «Завершено» – сканирование завершено. Угрозы не найдены;
- «Выполняется» – идет сканирование объектов;
- «Нет сканирований» – нет объектов для сканирования. Проект был создан;
- «Предупреждение» – сканирование завершено. Обнаружены угрозы;
- «Отменено» – сканирование было отменено пользователем;
- «Ошибка» – сканирование было прервано из-за возникших ошибок.

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

4.2.1 Просмотр проекта

Для просмотра проекта необходимо выбрать проект из списка или ввести название проекта в поисковую строку.

4.2.2 Запуск 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 применять 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 4.4.2 .

Остановка сканирования

Остановка сканирования осуществляется следующими способами:

- через контекстное меню;
- со страницы проекта.

Для остановки сканирования через контекстное меню необходимо выполнить следующие действия:

- 3) Выбрать пункт меню «Проекты».

- 4) Нажать кнопку  в строке проекта, выбрать пункт «Остановить» в контекстном меню.

Для остановки сканирования со страницы проекта необходимо выполнить следующие действия:

- 4) Выбрать подраздел «Проекты».
- 5) Выбрать проект.
- 6) Нажать кнопку «Остановить сканирование».

4.2.3 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. 25).
- 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	Введите запрос для поиска	Фильтр
debug	Наименование угрозы	Статус угрозы
electron	CVE-2026-4800	Критичный
got	CVE-2021-23337	Высокий
lodash	CVE-2020-28500	Средний
minimist	CVE-2025-13465	Средний
	CVE-2026-2950	Средний
Всего: 5		

Рисунок 26 – Список компонентов

Подробное описание уязвимости представлено на рис. 27.

× 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 27 – Подробное описание уязвимости

4.3 Раздел «Цели сканирования»

В разделе «Цели сканирования» оператору доступен просмотр целей сканирования, а также источников.

Основная рабочая область представлена на рис. 28.

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

Рисунок 28 – Основная рабочая область раздела «Цели сканирования»

Для просмотра источника необходимо выполнить следующие действия:

- 1) Ввести название цели сканирования в поисковую строку или выбрать из списка.
- 2) Ввести название источника в поисковую строку или выбрать из списка

4.4 Раздел «Настройки»

В разделе «Настройки» пользователю с ролью «Оператор» доступны следующие страницы:

- информация о ПК «SafeERP CS EM»;
- лицензии.

4.4.1 Информация о ПК «SafeERP CS EM»

В подразделе «Информация» содержится актуальная информация о версиях сервера и интерфейса ПК «SafeERP CS EM».

Доступна загрузка архива с пользовательской документацией ПК «SafeERP CS EM» на локальную машину. Для загрузки архива с документацией на локальную машину необходимо нажать кнопку «Скачать» (рис. 29).

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 1С являются:

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

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

4.4.2 Лицензии

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 «Safe 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».

В подразделе «Лицензия» содержится актуальная информация о ключе лицензии, дате активации лицензии, дате окончания лицензии и статусе технической поддержки ПК «SafeERP CS EM» (рис. 30).

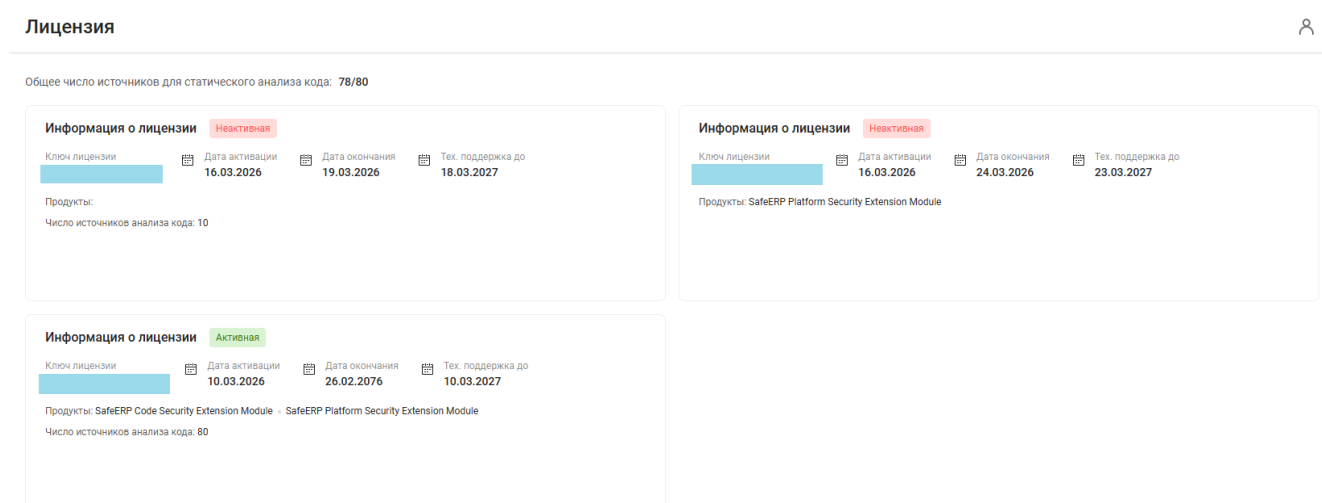


Рисунок 30 – Подраздел «Лицензии»

4.5 Профиль пользователя

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

4.5.1 Просмотр данных текущего пользователя

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

4.5.2 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.

4.5.3 Просмотр списка активных подписок

Для просмотра списка активных подписок необходимо обратиться к профилю пользователя, выбрать раздел «Активные подписки» (рис. 31).

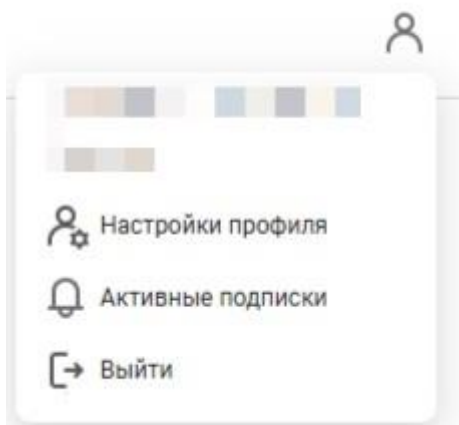


Рисунок 31 – Профиль пользователя

При нажатии на название проекта раскрывается список событий по данному проекту, на которые подписан пользователь. Список подписок представлен на рис. 32

× Активные подписки

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

Рисунок 32 – Список активных подписок

4.5.4 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. 33).

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

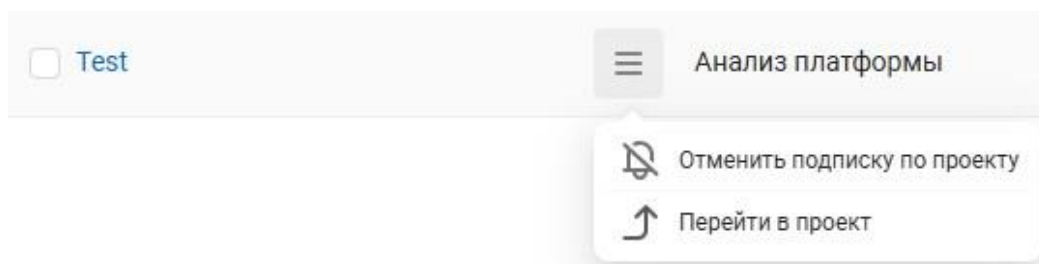


Рисунок 33 – Контекстное меню при просмотре списка активных подписок

5 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 согласно 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 90 дней. Минимальный срок действия пароля – 30 дней. За 7 дней до окончания действия пароля пользователю будет отображаться уведомление об истечении срока действия пароля и необходимости изменения. После истечения срока действия пароля необходимо изменить пароль.
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
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