ГАЗИНФОРМ СЕРВИС

ПК «SAFEERP PS EM»
Руководство администратора

Санкт-Петербург, 2026

Аннотация

Данное руководство является программным документом, определяющим порядок работы программного комплекса (далее – ПК) «SAFEERP Platform Security Extension Module» (далее – «SAFEERP PS EM»).

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

- сведения о назначении ПК «SAFEERP PS EM»;
- технические средства, обеспечивающие работу ПК «SAFEERP PS EM»;
- порядок запуска веб-интерфейса ПК «SAFEERP PS EM»;
- описание веб-интерфейса ПК «SAFEERP PS EM».

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

Содержание

1 Назначение ПК «SAFEERP PS EM» 6
2 Технические средства, обеспечивающие работу ПК «SAFEERP PS EM» 7
3 Запуск интерфейса ПК «SAFEERP PS EM» 8
3.1. Запуск веб-интерфейса 8
3.2. Вход 8
3.3. Интеграция раздела «DAST» с CI/CD 8
3.3.1 Настройка параметров запуска скрипта 9
3.3.2 Настройка пайплайна 9
4 Описание веб-интерфейса ПК «SAFEERP PS EM» 11
4.1 Раздел «DAST» 11
4.1.1 Добавление проекта 12
4.1.2 Изменение настроек проекта 15
4.1.3 Запуск и остановка сканирования 16
4.1.4 Просмотр результатов сканирования 17
4.1.4.1 Просмотр панели мониторинга по результатам итерации 17
4.1.4.2 Просмотр подробного результата сканирования выбранной уязвимости 18
4.1.5 Подключение почтовых уведомлений 20
4.1.6 Удаление проекта 26
4.2 Раздел «Анализ платформы» 26
4.2.1 Подраздел «Проекты» 28
4.2.1.1 Добавление проекта 29
4.2.1.2 Изменение настроек проекта 31
4.2.1.3 Запуск и остановка сканирования 32
4.2.1.4 Просмотр результатов сканирования 33
4.2.1.5 Управление уязвимостями 39
4.2.1.6 Подключение почтовых уведомлений 44
4.2.1.7 Удаление проекта 50
4.2.2 Подраздел «Профили» 50
4.2.2.1 Создание профилей 50
4.2.2.2 Редактирование пользовательских профилей 52
4.2.2.3 Копирование профилей 52
4.2.2.4 Удаление пользовательского профиля 53
4.2.3 Подраздел «Проверки» 53
4.2.3.1 Просмотр проверок 54

4.2.3.2 Добавление пользовательской проверки 54
4.2.3.3 Редактирование пользовательской проверки 54
4.2.3.4 Удаление пользовательской проверки 54
4.3 Раздел «Pentest» 55
4.3.1 Подраздел «Проекты» 55
4.3.1.1 Добавление проекта 56
4.3.1.2 Изменение настроек проекта 59
4.3.1.3 Запуск и остановка сканирования проекта 59
4.3.1.4 Результаты сканирования 61
4.3.1.5 Просмотр логов проекта 61
4.3.1.6 Удаление проекта 62
4.3.2 Подраздел «Агенты» 62
4.3.2.1 Добавление агентов 63
4.3.2.2 Редактирование агента 63
4.3.2.3 Просмотр лога агента 65
4.3.2.4 Скачивание лога агента 66
4.3.2.5 Удаление агента 66
4.4 Раздел «Цели сканирования» 66
4.4.1 Добавление цели сканирования 66
4.4.2 Редактирование цели сканирования 67
4.4.3 Удаление целей сканирований 67
4.4.4 Источники 67
4.4.4.1 Источники для раздела «DAST» 67
4.4.4.2 Источники для раздела «Анализ платформы» 71
4.4.4.3 Источники для раздела «Pentest» 76
4.5 Раздел «Настройки» 79
4.5.1 Подраздел «Информация» 79
4.5.2 Подраздел «Лицензия» 80
4.5.2.1 Активация лицензии 81
4.5.2.2 Обновление лицензии 84
4.5.3 Подраздел «Пользователи» 84
4.5.3.1 Создание учётной записи 85
4.5.3.2 Изменение учётной записи 86
4.5.3.3 Сброс пароля учётной записи 87
4.5.3.4 Блокировка и разблокировка учётной записи 87
4.5.3.5 Удаление учётной записи 88
4.5.3.6 Роли 88
4.5.3.7 Создание пользовательских ролей 91

4.5.3.8 Полномочия, назначаемые пользовательским ролям 92
4.5.3.9 Редактирование пользовательских ролей 95
4.5.3.10 Копирование ролей 97
4.5.3.11 Удаление пользовательских ролей 97
4.5.4 Подраздел «Журнал» 97
4.5.4.1 Просмотр журнала 101
4.5.4.2 Выгрузка журнала 101
4.5.5 Подраздел «БДУ» 101
4.6 Профиль пользователя 102
4.6.1 Просмотр данных текущего пользователя 102
4.6.2 Смена пароля 102
4.6.3 Просмотр списка активных подписок 102
4.6.4 Отмена почтовых подписок 103
5 Парольная политика 104
Приложения 105
Приложение 1 105
Список сокращений 108

1 Назначение ПК «SAFEERP PS EM»

ПК «SAFEERP PS EM» предназначен для:

- динамического анализа безопасности веб-ресурса и его компонентов
- для анализа платформы 1С на наличие изменений в профилях безопасности 1С, а также на наличие небезопасных настроек;
- сканирования хостов (целевых систем) на наличие уязвимостей с возможностью их эксплуатации.

ПК «SAFEERP PS EM» реализует следующие функциональные возможности:

- создание, редактирование и удаление проектов;
- подключение источников для сканирования,
- выбор модулей для сканирования при запуске проекта;
- просмотр отчета в дополнительном окне, которое содержит перечисленную выше информацию.

2 Технические средства, обеспечивающие работу ПК «SAFEERP PS EM»

Технические характеристики компьютеров, на базе которых созданы автоматизированные рабочие места оператора и администратора ПК «SAFEERP Platform Security Extension Module» (далее – «SAFEERP PS EM»), должны иметь характеристики не ниже:

- процессор – 16 виртуальных или физических ядер;
- ОЗУ – 32 Гбайт;
- HDD/SSD 500 Гбайт.

3 Запуск интерфейса ПК «SAFEERP PS EM»

3.1. Запуск веб-интерфейса

Доступ к веб-интерфейсу ПК «SAFEERP PS EM» осуществляется через веб-браузер по адресу, заданному при установке или настройке комплекса в явном виде https://<IP-адрес>:443.

Примечание. После установки ПК «SAFEERP PS EM» первичная авторизация осуществляется с помощью пользователя system с заданным паролем System__12. После авторизации необходимо сменить пароль пользователю system согласно разделу 5 данного руководства.

3.2. Вход

Для первичного входа в ПК «SAFEERP PS EM» используются учётные данные, задаваемые при установке ПК «SAFEERP PS EM», указанные в подразделе 2.2 документа «Установка, обновление и удаление ПК SAFEERP EM» (рис. 1).

После успешного входа появится форма смены пароля – необходимо изменить пароль по умолчанию. До смены пароля другие действия на сервере управления **будут недоступны**.

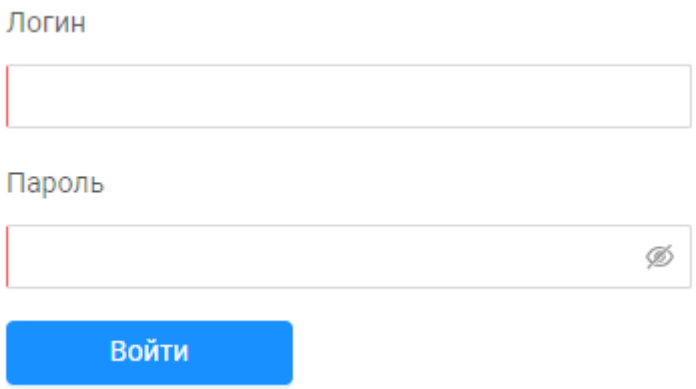


Рисунок 1 – Форма авторизации ПК «SAFEERP PS EM»

3.3. Интеграция раздела «DAST» с CI/CD

ПК «SafeERP PS 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 со сканируемым источником.

3.3.1 Настройка параметров запуска скрипта

В настройках Gitlab во вкладке «variables» необходимо ввести следующие параметры:

- DAST_DOMAIN – адрес сервера, на котором развернут ПК «SafeERP PS EM»;
- DAST_PROJECT_NAME – название созданного проекта в ПК «SafeERP PS EM»;
- SE_LOGIN – логин пользователя ПК «SafeERP PS EM» для доступа к веб-интерфейсу;
- SE_PASS – пароль пользователя ПК «SafeERP PS EM» для доступа к веб-интерфейсу.

3.3.2 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 PS EM» данный файл выглядит следующим образом:

```
stages:
  - dast

dast:
  stage: dast
  image:
    name: nexus.da.lan/da/safeerp/ems/base/sast:latest
    entrypoint: [""]
  tags:
    - docker
    - test
  variables:
    DAST_WAIT: "1"              # ждать завершения внутри скрипта
    DAST_POLL_INTERVAL: "20"    # сек
    DAST_POLL_TIMEOUT: "21600"  # 6 часов
    SAVE_JSON: "1"
    DAST_FLAT_COPY: "dast-report.json"   # плоская копия (создаёт сам
ci/dast.py)
  timeout: "6h"
  script:
    - |
      set -e
      test -f ci/dast.py || { echo "ci/dast.py не найден"; exit 1; }
      echo -n "SE_LOGIN length: "; echo -n "${SE_LOGIN:-}" | wc -c
      echo -n "SE_PASS  length: "; echo -n "${SE_PASS:-}" | wc -c
      test -n "${DAST_DOMAIN:-}"       || { echo "DAST_DOMAIN пуст"; exit
1; }
      test -n "${SE_LOGIN:-}"          || { echo "SE_LOGIN пуст"; exit 1; }
      test -n "${SE_PASS:-}"           || { echo "SE_PASS пуст"; exit 1; }
      echo "CI_PROJECT_DIR=${CI_PROJECT_DIR}"
      ls "${CI_PROJECT_DIR}"
      test -n "${DAST_PROJECT_NAME:-}" || { echo "DAST_PROJECT_NAME пуст";
exit 1; }
      python -W ignore ci/dast.py -d "${DAST_DOMAIN}" -u "${SE_LOGIN}" -p
"${SE_PASS}" -n "${DAST_PROJECT_NAME}"
```

```
      # диагностика наличия файлов
      ls -la "${CI_PROJECT_DIR}/results" || true
      [ -z "${DAST_FLAT_COPY:-}" ] || ls -la
"${CI_PROJECT_DIR}/${DAST_FLAT_COPY}" || true
  artifacts:
    when: always
    paths:
      - results/AnalysisResult_${DAST_PROJECT_NAME}.json
      - dast-report.json
    expire_in: 1 week
```

4 Описание веб-интерфейса ПК «SAFEERP PS EM»

ПК «SAFEERP PS EM» содержит следующие функциональные разделы:

- «DAST»;
- «Анализ платформы»;
- «Pentest»;
- «Цели сканирования»;
- «Настройки».

4.1 Раздел «DAST»

Раздел «DAST» предназначен для динамического анализа безопасности веб-ресурса и его компонентов. Раздел «DAST» является одним из компонентов ПК «SAFEERP PS EM».

Раздел состоит из следующего подраздела:

- «Проекты».

В основную область подраздела «Проекты» входят следующие столбцы (рис. 2):

- название проекта;
- статус – статус последней итерации проекта;
- ресурсы – количество сканируемых ресурсов;
- последний запуск – дата и время запуска последнего сканирования;
- критичных угроз – количество угроз со степенью «Критичные»;
- высоких угроз – количество угроз со степенью «Высокие»;
- средних угроз – количество угроз со степенью «Средние»;
- низких угроз – количество угроз со степенью «Низкие»;
- потенциальных угроз – количество угроз со степенью «Потенциально».

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	Сканирование проекта запущено
Завершено	Сканирование завершено. Ошибки не обнаружены
Ошибка	Сканирование было прервано из-за возникших ошибок
Отменено	Сканирование было отменено пользователем

Доступные статусы найденных угроз представлены в таблице 2.

Таблица 2 – Статус найденных угроз (раздел «DAST»)

Индикация	Статус угрозы
	Критичный
	Высокий
	Средний
	Низкий
	Потенциальный

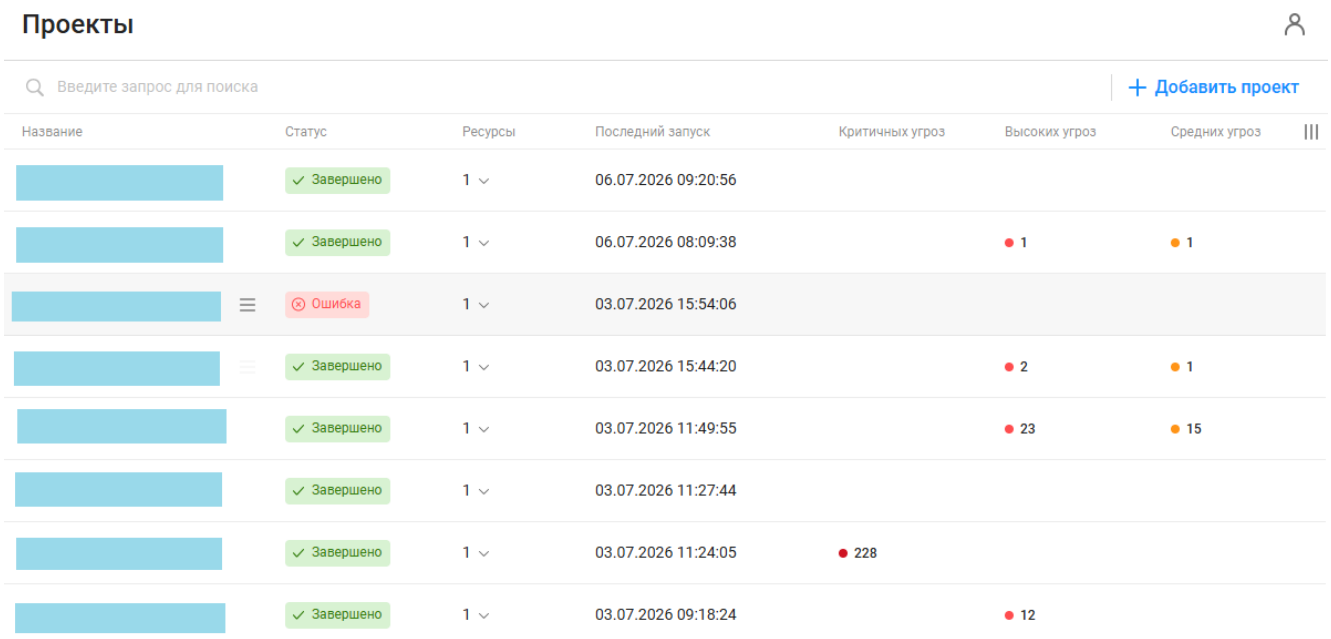


Рисунок 2 – Список проектов

4.1.1 Добавление проекта

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

1) Добавить цель сканирования. Подробное описание представлено в пункте 4.4.1.
2) Добавить источник в цель сканирования. Подробное описание представлено в подпункте 4.4.4.1.

Для добавления проекта необходимо выполнить следующие действия:

1) Нажать кнопку *«+Добавить проект»* в основной рабочей области (рис. 2).
2) Заполнить поле «Название проекта», выбрать цель сканирования из выпадающего списка (рис. 3).
3) Нажать кнопку *«+Добавить источник»*, выбрать источник и модули сканирования. Нажать кнопку *«Добавить»* (рис.4).
4) Нажать кнопку *«Добавить»* (см. рис. 3).

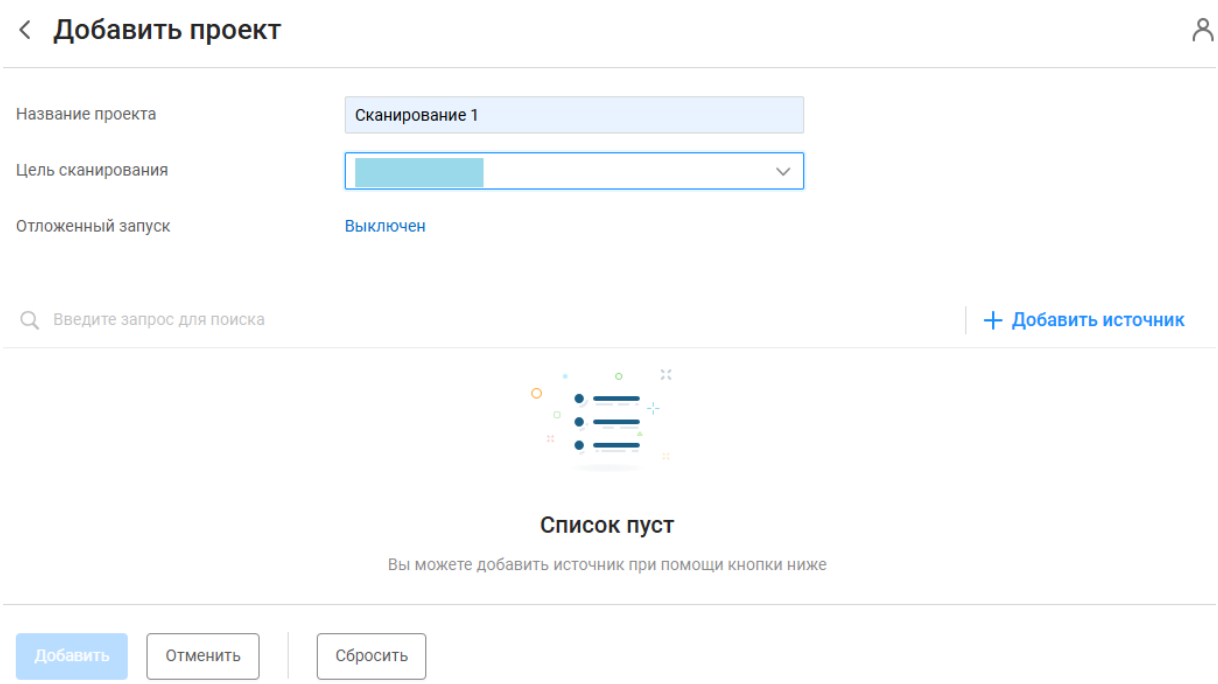


Рисунок 3 – Добавление проекта

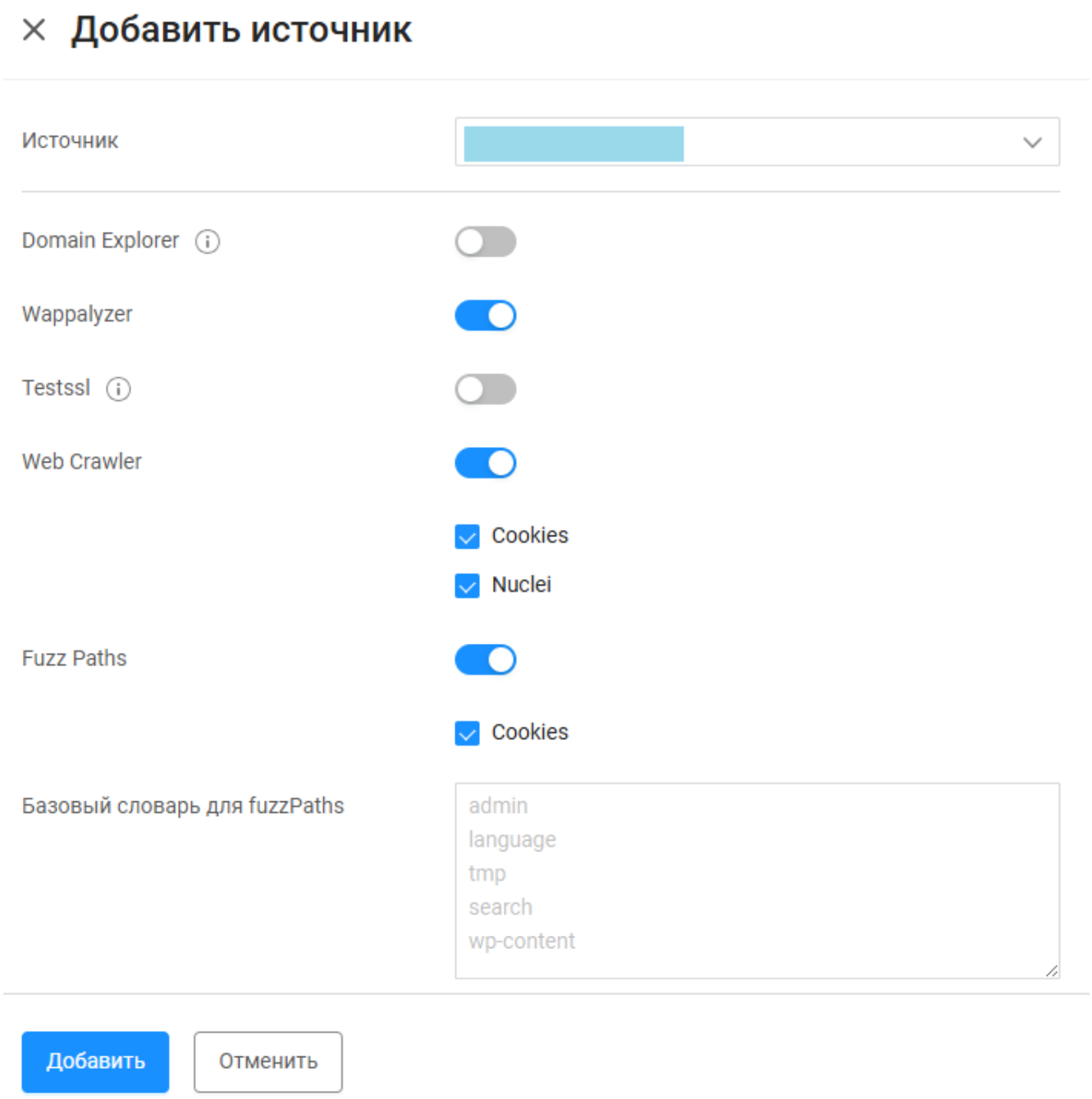


Рисунок 4 – Добавление источника и выбор модуля

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. Доступен выбор следующих модулей:
   - Domain Explorer – предназначен для поиска поддоменов различными методами (brute force, multibf, ct);
   - Wappalyzer – предназначен для обнаружения популярных веб-технологий (приложений, фреймворков, сервисов, CMS);
   - Testssl – предназначен для проверок TLS/SSL настроек;
   - Web Crawler – предназначен для поиска ссылок на целевом хосте. Доступен выбор следующего:
     А) Cookies – предназначен для поиска http cookies, не соответствующих критериям безопасности;
     Б) Nuclei – предназначен для поиска эндпоинтов, которые были найдены другими сканерами и переданы для проверки.
   - Fuzz paths – предназначен для анализа веб-ресурса методом «фаззинга». Доступен выбор следующего:
     А) Cookies – предназначен для поиска http cookies, не соответствующих критериям безопасности;
3. Поле «Базовый словарь для fuzzpaths» – базовые токены словаря для формирования перебиваемых URL. По умолчанию используются встроенные токены. Необходим для корректной работы модуля «Fuzz paths».

4.1.2 Изменение настроек проекта

Переход к странице редактирования проекта осуществляется следующими способами:

- через контекстное меню в списке проектов. Нажать кнопку *«Редактировать»* в контекстном меню;
- через кнопку *«Настройки проекта»* при просмотре проекта.

Для изменения настроек проекта через контекстное меню необходимо выполнить следующие действия:

1) Навести курсор на название проекта.
2) Нажать кнопку *«Редактировать»* в контекстном меню.
3) Внести изменения (в область «Название проекта», добавление или удаление источников, изменение).
4) Нажать кнопку *«Сохранить»*.

Для изменения настроек проекта через кнопку *«Настройки проекта»* необходимо выполнить следующие действия:

1) Открыть проект.
2) Нажать кнопку *«Настройки проекта»* в контекстном меню.

3) Внести изменения (в область «Название проекта», добавление, изменение или удаление источников, изменение).
4) Нажать кнопку *«Сохранить»*.

4.1.3 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 подраздел «Проекты».
2) Выбрать проект.
3) Нажать кнопку *«Запустить сканирование»*.

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.

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»* (рис. 5).

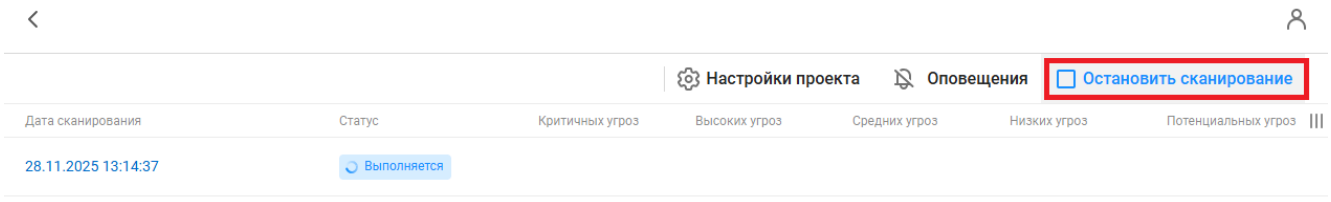


Рисунок 5 – Кнопка «Остановить сканирование»

Примечание. 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 4.5.2.

4.1.4 Просмотр результатов сканирования

После завершения сканирования доступен просмотр следующего:

- просмотр панели мониторинга по результатам итерации;
- просмотр результата сканирования по выбранной уязвимости.

4.1.4.1 Просмотр панели мониторинга по результатам итерации

Для просмотра панели мониторинга по результатам итерации проекта необходимо выполнить следующие действия:

1) Открыть проект.
2) Выбрать итерацию проекта (рис. 6).

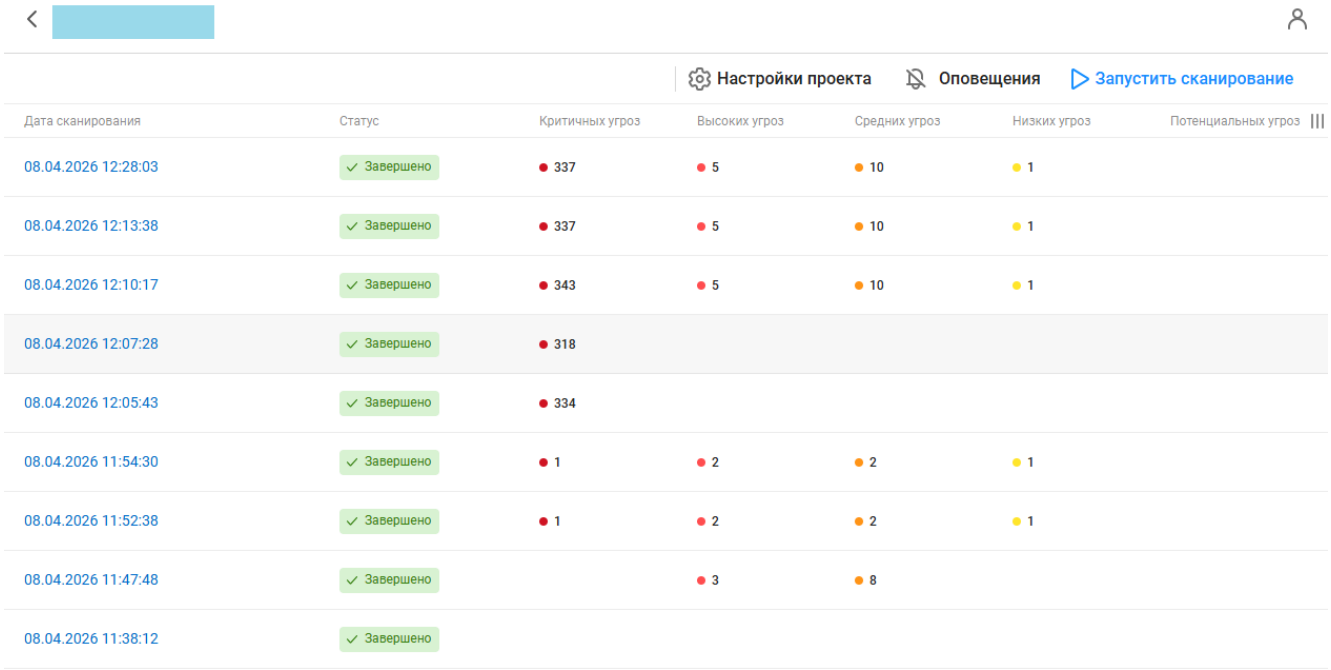


Рисунок 6 – Список итераций проекта

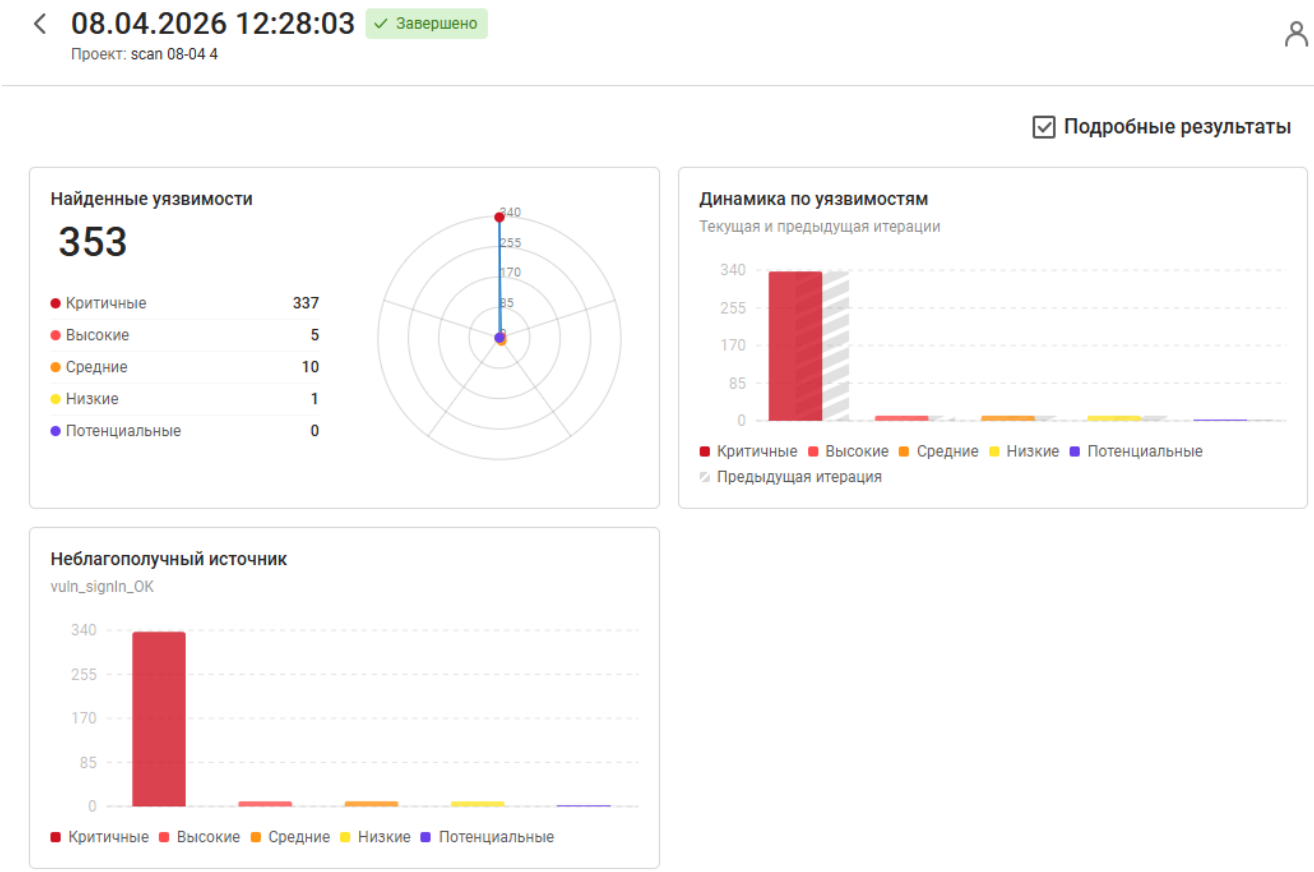


Рисунок 7 – Панель мониторинга по выбранной итерации анализа (раздел «DAST»)

После выбора итерации проекта доступен просмотр панели мониторинга (рис. 7). Доступен просмотр следующих областей:

- «Найденные уязвимости» – выводится количество и степень критичности найденных уязвимостей;
- «Динамика по уязвимостям» – выводится сравнение количества найденных уязвимостей;
- «Неблагополучный источник» – в виджете отображается источник с наибольшим количеством найденных уязвимостей и их критичность.

4.1.4.2 Просмотр подробного результата сканирования выбранной уязвимости

Для просмотра результата сканирования по выбранной уязвимости необходимо выполнить следующие действия:

1) Открыть проект.
2) Выбрать итерацию (см. рис. 6), нажать кнопку *«Подробные результаты»* (см. рис. 7).
3) Выбрать уязвимость в дереве уязвимостей (рис. 8).

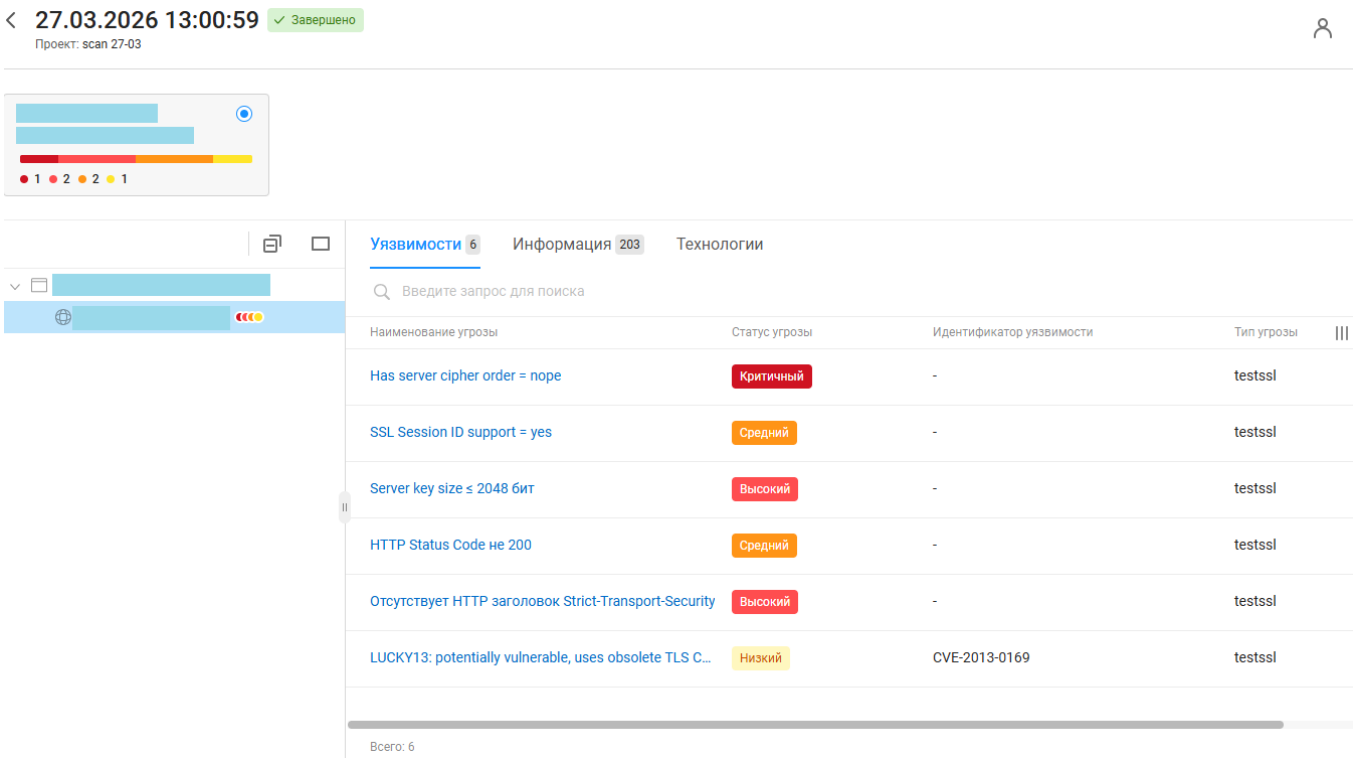


Рисунок 8 – Список найденных уязвимостей

Подробное описание найденной уязвимости представлено на рис. 9.

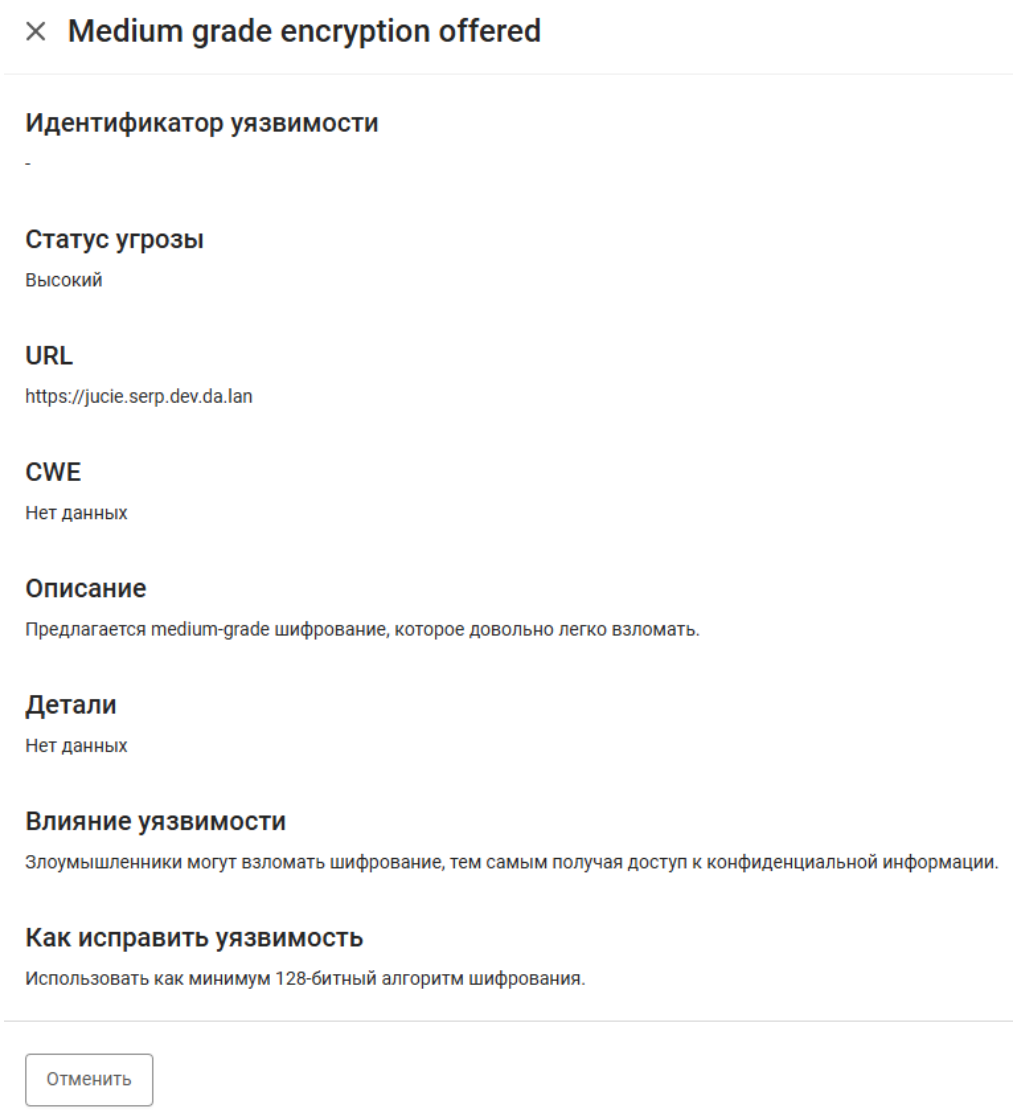


Рисунок 9 – Подробное описание найденной уязвимости

При просмотре результатов сканирования доступны следующие вкладки:

- «Уязвимости» – список найденных уязвимостей;
- «Информация» – информация, обнаруженная при сканировании;
- «Технологии» – список веб-технологий, которые были обнаружены при сканировании.

4.1.5 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 по выбранному проекту необходимо выполнить следующие действия:

1) Открыть проект.

2) Нажать кнопку *«Оповещения»* (рис. 10).

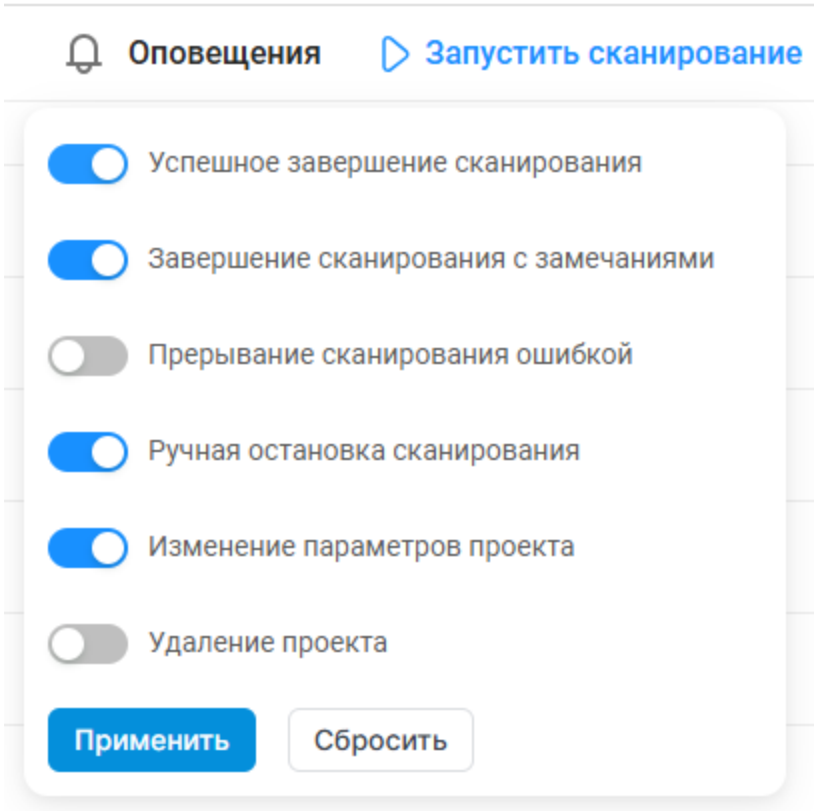


Рисунок 10 – Список событий (раздел «DAST»)

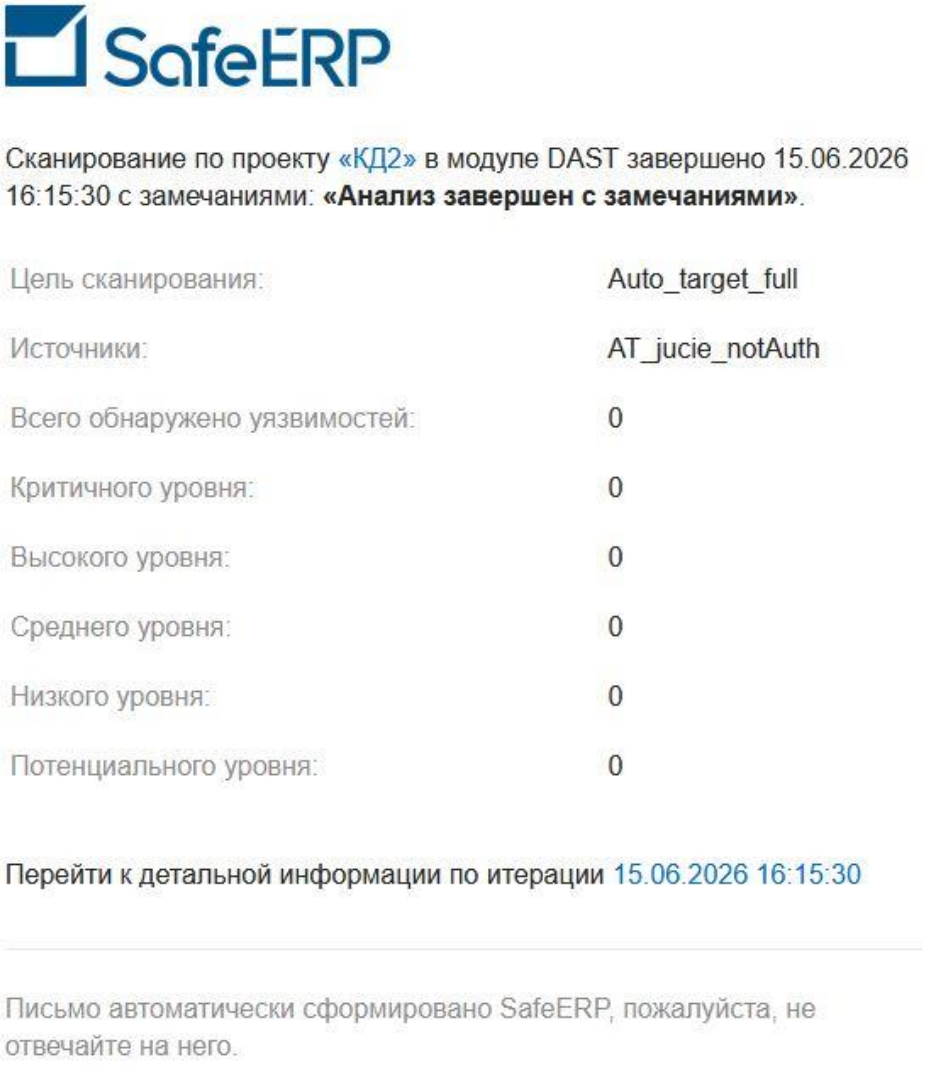
3) Выбрать события рассылки, после которых будут поступать почтовые уведомления.
4) Нажать кнопку *«Применить»*.

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

Примеры почтовых уведомлений приведены на рисунках 11, 12, 13, 14, 15, 16.



Рисунок 11 – Почтовое уведомление при выборе события «Успешное завершение сканирования»



SafeERP

Сканирование по проекту «КД2» в модуле DAST завершено 15.06.2026 16:15:30 с замечаниями: **«Анализ завершен с замечаниями»**.

Цель сканирования:	Auto_target_full
Источники:	AT_jucie_notAuth
Всего обнаружено уязвимостей:	0
Критичного уровня:	0
Высокого уровня:	0
Среднего уровня:	0
Низкого уровня:	0
Потенциального уровня:	0

Перейти к детальной информации по итерации 15.06.2026 16:15:30

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

Рисунок 12 – Почтовое уведомление при выборе события «Завершение сканирования с замечаниями»



Рисунок 13 – Почтовое уведомление при выборе события «Изменение параметров проекта»



Рисунок 14 – Почтовое уведомление при выборе события «Прерывание сканирования ошибкой»

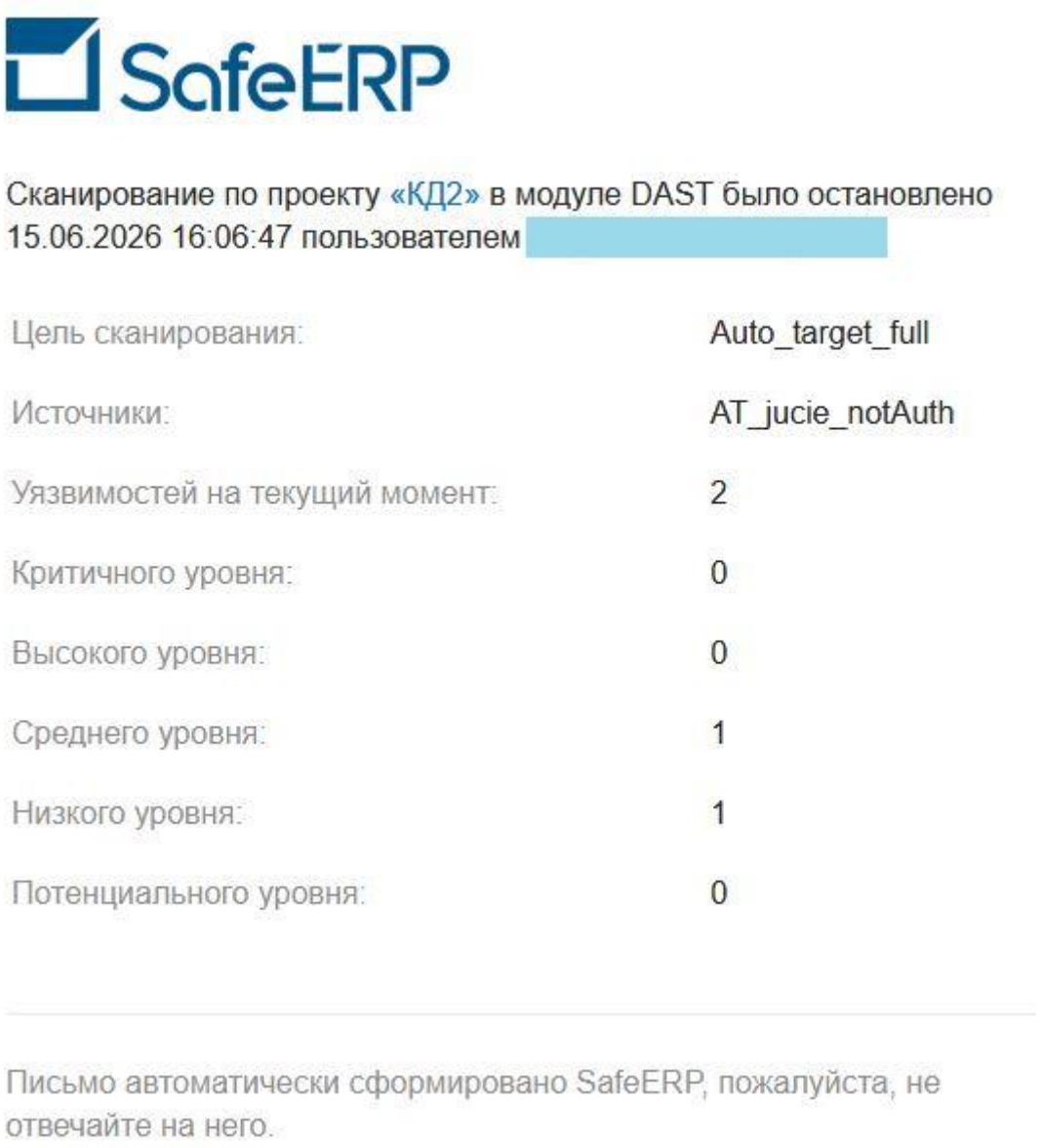


Рисунок 15 – Почтовое уведомление при выборе события «Ручная остановка сканирования»



Рисунок 16 – Почтовое уведомление при выборе события «Удаление проекта»

Просмотр активных подписок

Для просмотра списка активных подписок необходимо обратиться к подразделу 4.6.

Отмена подписок

Отмена подписок осуществляется следующими способами:

- с помощью кнопки *«Оповещения»* при просмотре проекта;
- с помощью кнопки *«Отменить подписку по проекту»* в профиле пользователя. Подробное описание представлено в подразделе 4.6.

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. 10).

4.1.6 Удаление проекта

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

4.2 Раздел «Анализ платформы»

Раздел «Анализ платформы» предназначен для анализа платформы 1С.

Раздел «Анализ платформы» состоит из следующих подразделов:

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

Основная рабочая область раздела «Анализ платформы» представлена на рис. 17.

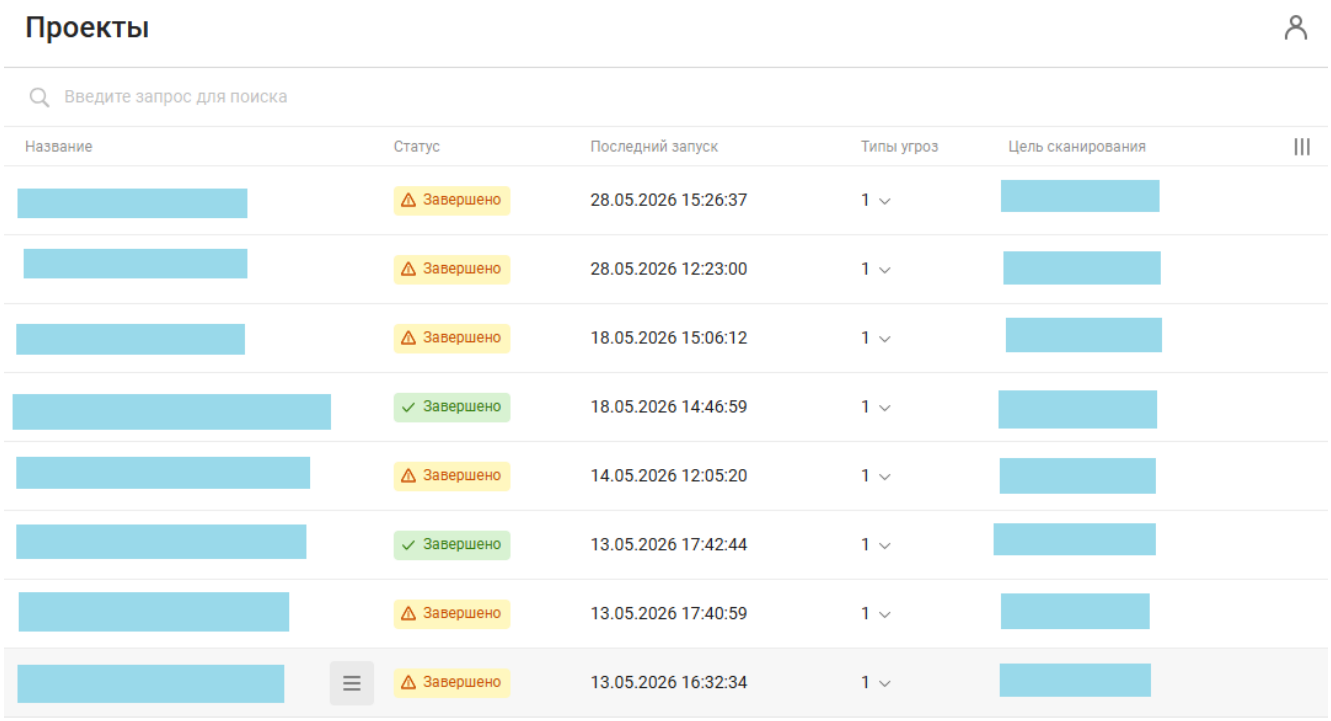


Рисунок 17 – Основная рабочая область раздела «Анализ платформы» (подраздел «Проекты»)

Запуск проекта осуществляется следующими способами:

- через кнопку *«Запустить»* в контекстном меню;
- через кнопку *«Запустить сканирование»* при просмотре проекта (рис. 18).

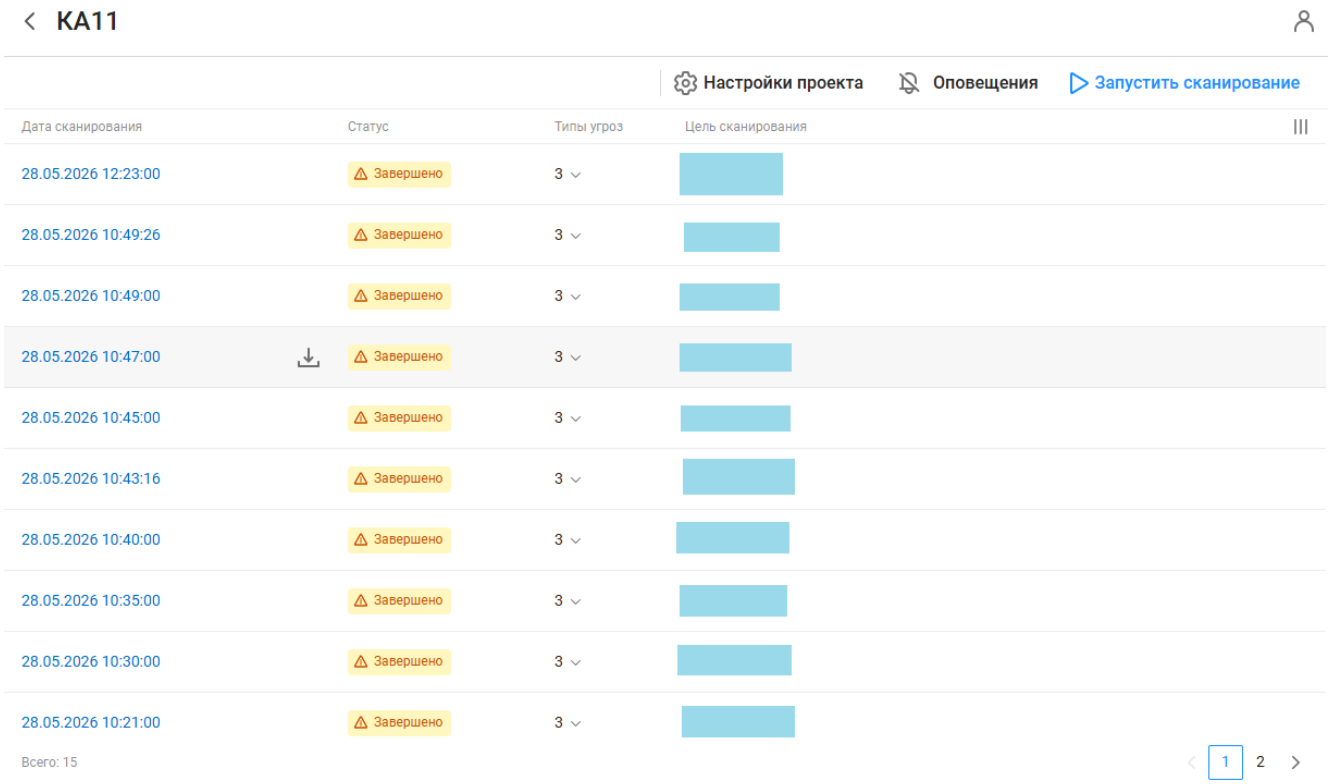


Рисунок 18 – Список итераций проекта

4.2.1 Подраздел «Проекты»

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	Сканирование проекта запущено
Завершено	Сканирование завершено. Ошибки не обнаружены
Завершено	Сканирование завершено. Обнаружены ошибки
Ошибка	Сканирование было прервано из-за возникших ошибок
Отменено	Сканирование было отменено пользователем

Доступные уровни опасности найденных уязвимостей представлены в таблице 4.

Таблица 4 – Уровни опасности найденных уязвимостей (раздел «Анализ платформы»)

Индикация	Уровень опасности
	Критичный
	Высокий

	Средний
	Низкий
	Потенциальные
	Информация

4.2.1.1 Добавление проекта

При добавлении проекта пользователю доступен анализ следующего:

- контроль профилей безопасности 1С – проверяет только источники с типом «Кластер» или «Инфобаза»;
- контроль настроек (КН) – проверяет только источники с типом «Агент».

Для добавления проекта с целью проверки «Контроль профилей безопасности 1С» необходимо выполнить следующие действия:

1) Нажать кнопку *«+Добавить проект»* (рис. 17).
2) Заполнить поле «Название проекта», выбрать цель сканирования из выпадающего списка в поле «Цель сканирования» (рис. 19).
3) Нажать кнопку *«+Добавить источник»* (рис. 19).

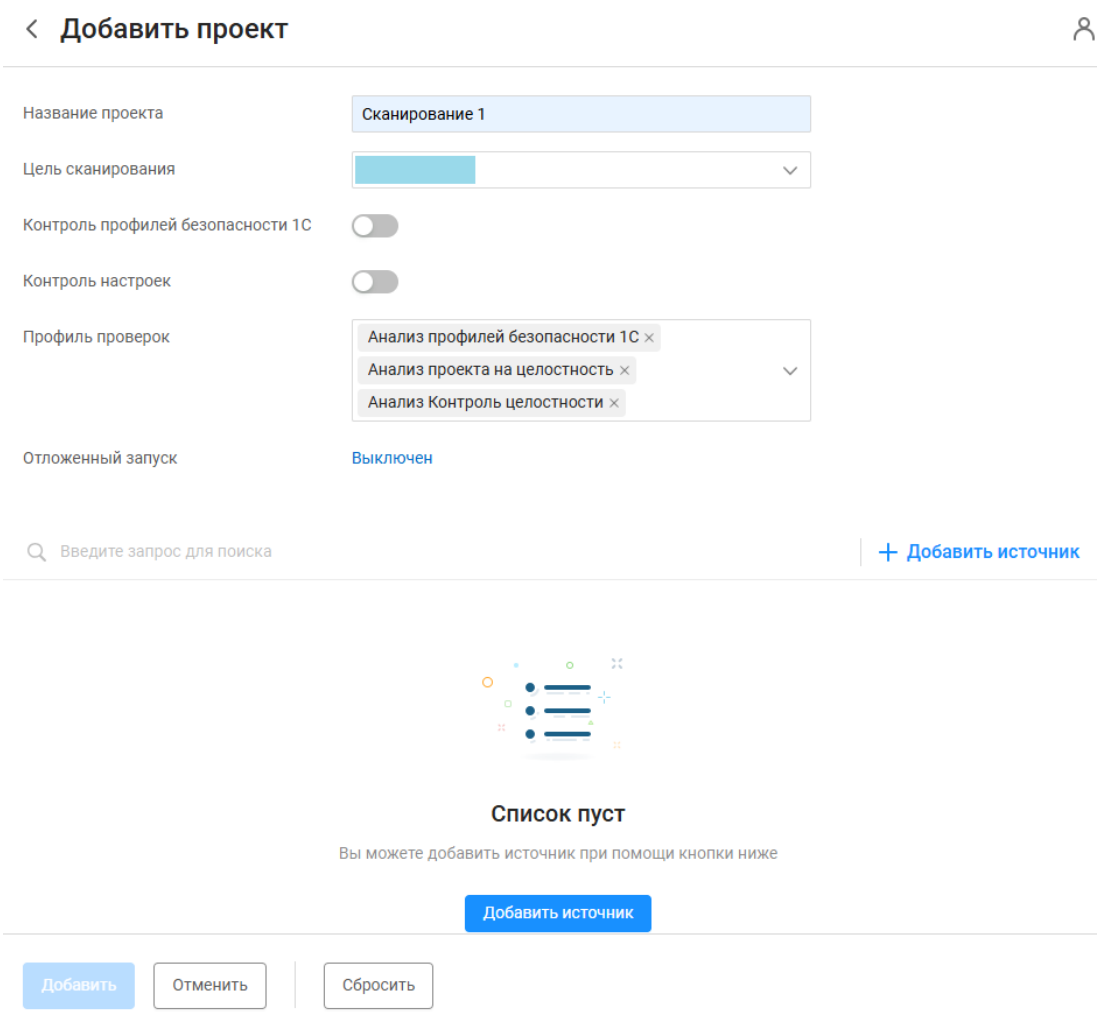


Рисунок 19 – Создание проекта (раздел «Анализ платформы»)

4) Выбрать цель проверки «Контроль профилей безопасности 1С», цель проверки и профили постановки на контроль (рис. 20). Нажать кнопку *«Добавить».*

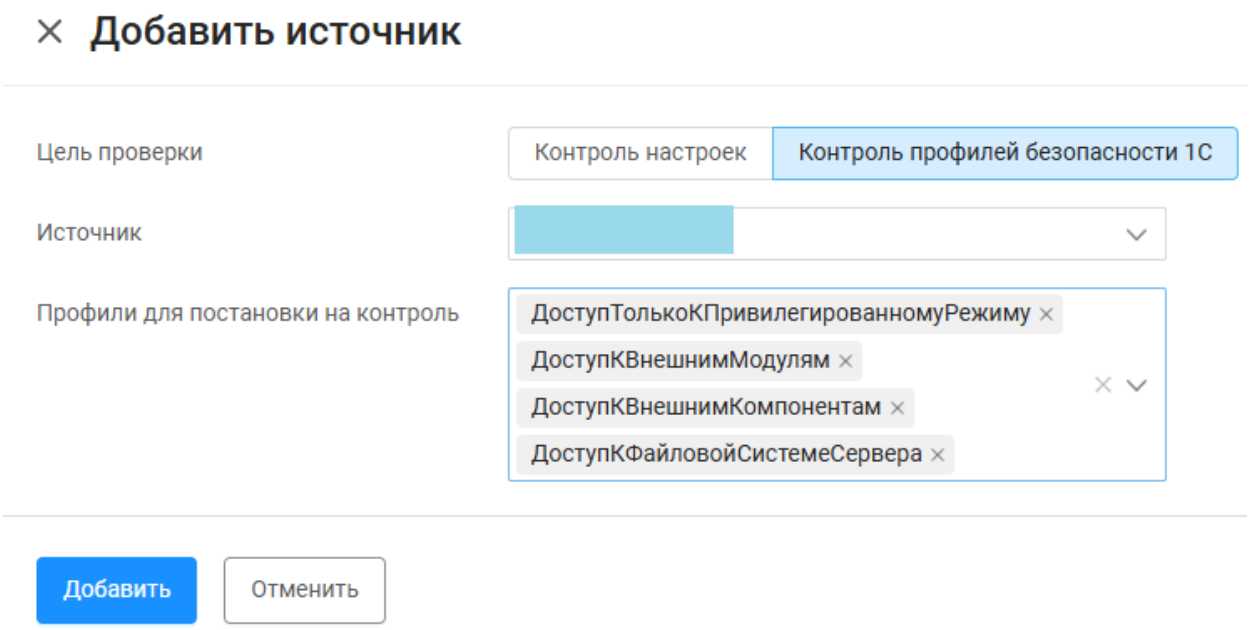


Рисунок 20 – Выбор источника для проекта с целью проверки «Контроль профилей безопасности 1С»

5) Нажать кнопку *«Добавить»* (см. рис. 19).

Для добавления проекта с целью проверки «Контроль настроек» необходимо выполнить следующие действия:

1) Нажать кнопку *«+Добавить проект»* (рис. 17).
2) Заполнить поле «Название проекта», выбрать цель сканирования из выпадающего списка в поле «Цель сканирования» (рис. 19).
3) Нажать кнопку *«+Добавить источник»* (рис. 19).
4) Выбрать цель проверки «Контроль настроек», источник (рис. 21).

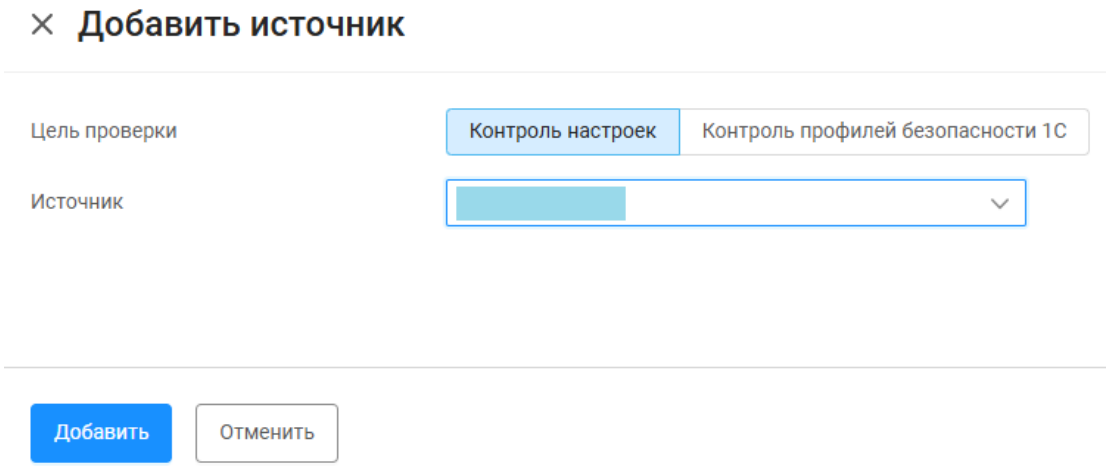


Рисунок 21 – Выбор источника для проекта с целью сканирования «Контроль настроек»

5) Нажать кнопку *«Добавить»* (см. рис. 19).

Примечание. 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).

4.2.1.2 Изменение настроек проекта

Настройка проекта осуществляется следующими способами:

— через кнопку *«Редактировать»* в контекстном меню;
— через кнопку *«Настройки проекта»* при просмотре проекта.

Для настройки с помощью кнопки *«Редактировать»* необходимо выполнить следующие действия:

1) Выбрать кнопку *«Редактировать»* в контекстном меню.
2) Внести изменения (название, профиль сканирования, добавить, изменить или удалить источник, включить или выключить сканирование «Контроль настроек» или «Контроль профилей безопасности 1С»).
3) Нажать кнопку *«Сохранить».*

Для настройки с помощью кнопки *«Настройки проекта»* необходимо выполнить следующие действия:

1) Выбрать проект из списка.
2) Нажать кнопку *«Настройки проекта».*
3) Внести изменения (название, профиль сканирования, добавить или удалить источник).
4) Нажать кнопку *«Сохранить»* (рис. 22).

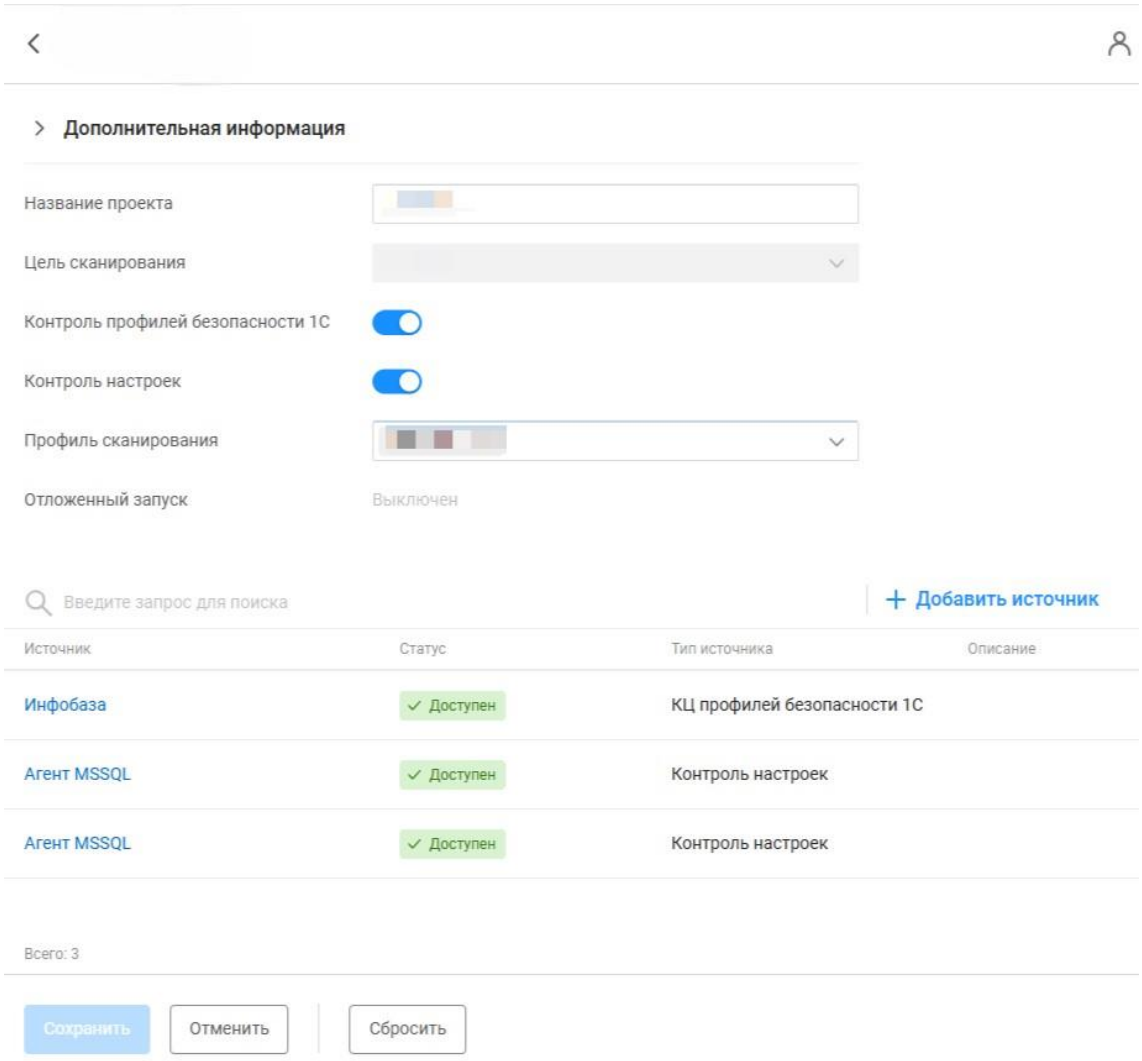


Рисунок 22 – Редактирование проекта

Примечание. При настройке проекта доступно изменение списка сканируемых профилей безопасности для проектов с целью сканирования «Контроль профилей безопасности 1С». Изменение источника данных или цели проверки для добавленного источника недоступно. Для обновления данных необходимо добавить новый источник в проект.

4.2.1.3 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 подраздел «Проекты».
2) Выбрать проект.
3) Нажать кнопку *«Запустить сканирование»*.

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.

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»*.

Примечание. 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 4.5.2.

4.2.1.4 Просмотр результатов сканирования

После завершения сканирования доступен просмотр следующего:

— просмотр результата сканирования «Контроль настроек»;
— просмотр результата сканирования «Контроль профилей безопасности 1С».

Просмотр результатов сканирования «Контроль настроек»

После завершения сканирования доступны следующее:

— просмотр панели мониторинга;
— просмотр результата сканирования;
— просмотр подробного описания найденной уязвимости.

Для просмотра панели мониторинга необходимо выполнить следующие действия:

1) Выбрать проект из списка (см. рис. 17).
2) Выбрать итерацию проекта (см. рис. 18).
3) Выбрать вкладку «Контроль настроек».

В панели мониторинга доступны следующие области (рис. 23):

— «Найденные уязвимости» – представлена информация о количестве и критичности найденных уязвимостей;
— «Соотношение количества уязвимостей» – представлена информация о

количестве и критичности найденных уязвимостей по сравнению с предыдущей итерацией;

— «Динамика уязвимостей» – представлена информация в виде гистограмм по количеству найденных уязвимостей;

— «Самая неблагополучная конфигурация» – источник, в котором обнаружено наибольшее количество уязвимостей;

— «Наиболее часто срабатывающие проверки» – топ-10 проверок с наибольшим количеством найденных уязвимостей.

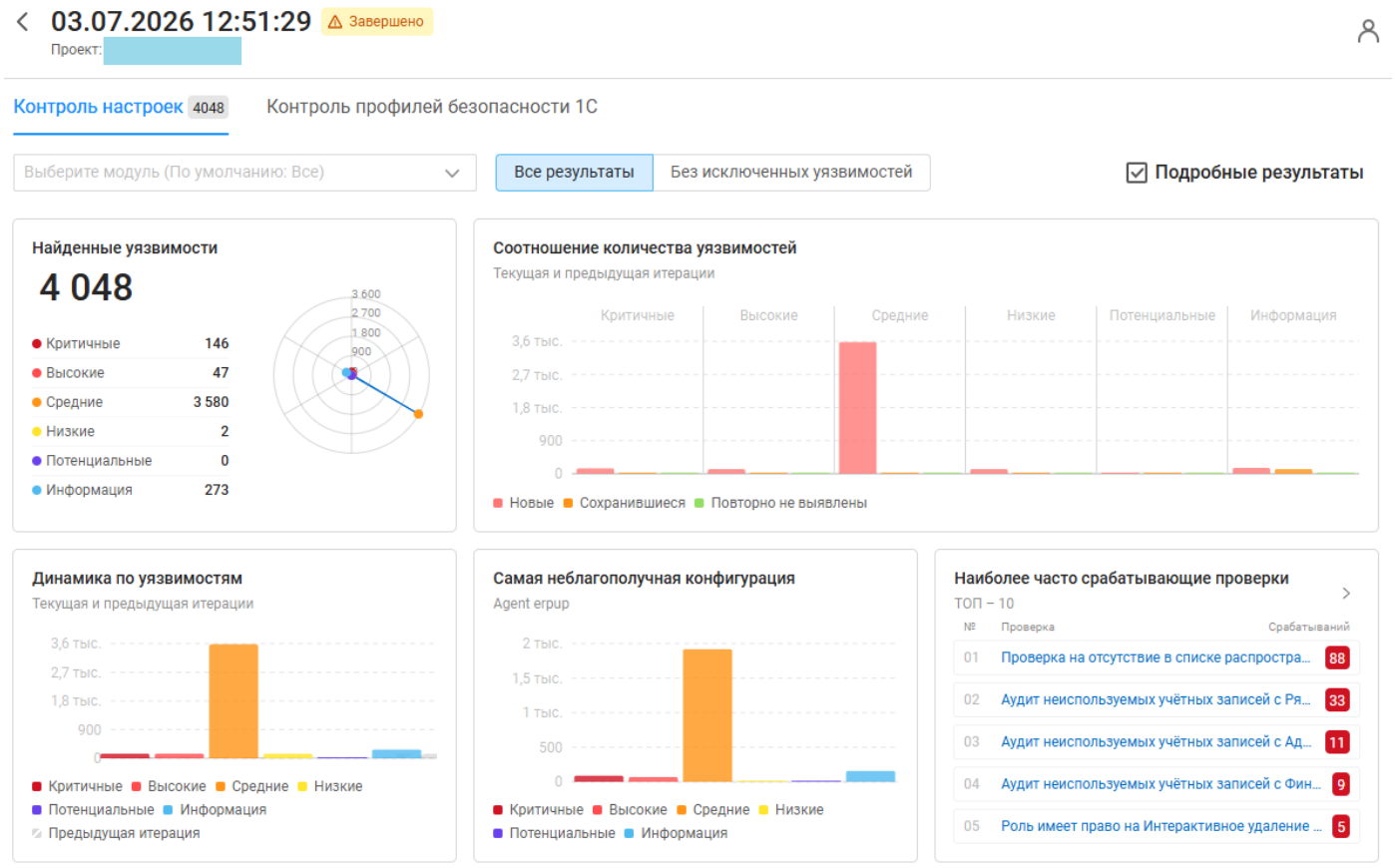


Рисунок 23 – Вкладка панели мониторинга проекта с целью сканирования «Контроля настроек»

Для просмотра результатов сканирования необходимо выполнить следующие действия:

1) Выбрать проект из списка (см. рис. 17).
2) Выбрать итерацию проекта (см. рис. 18).
3) Выбрать вкладку «Контроль настроек», нажать кнопку *«Подробные результаты»*.

Подробные данные результата по «Контролю настроек» представлены на рис. 24.

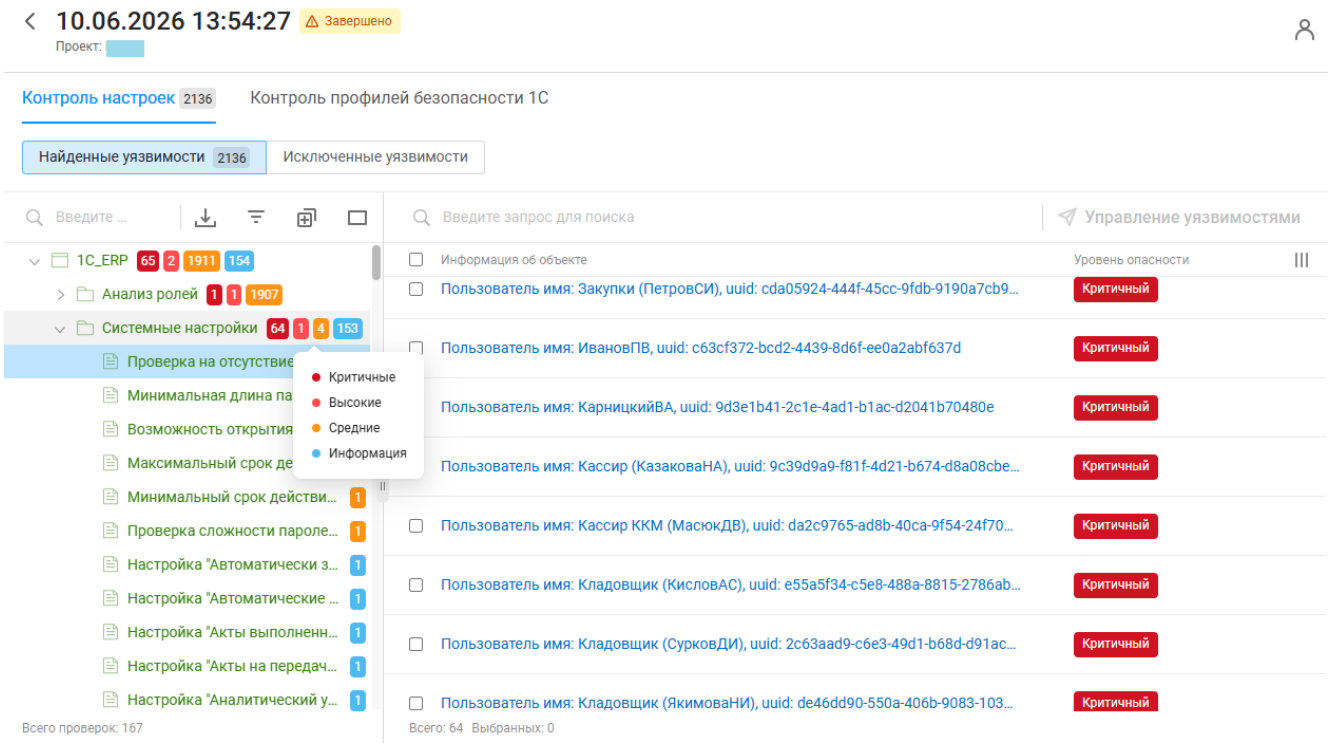


Рисунок 24 – Подробные результаты сканирования проекта с целью сканирования «Контроль настроек»

Примечание. При просмотре подробных результатов доступна фильтрация уязвимостей по следующими параметрам:

- состояние уязвимости;
- уровень опасности;
- подраздел;
- имя проверки;
- источник.

Просмотр результатов сканирования «Контроль профилей безопасности 1С»

После завершения сканирования доступны следующее:

- просмотр панели мониторинга;
- просмотр результата сканирования;
- просмотр подробного описания найденной уязвимости.

Для просмотра панели мониторинга необходимо выполнить следующие действия:

1) Выбрать проект из списка.
2) Выбрать итерацию проекта.
3) Выбрать вкладку «Контроль профилей безопасности 1С».

В панели мониторинга доступна следующая область (рис. 25):

- «Результаты контроля профилей безопасности» – выводится топ-5 профилей безопасности с наибольшим количеством изменений.

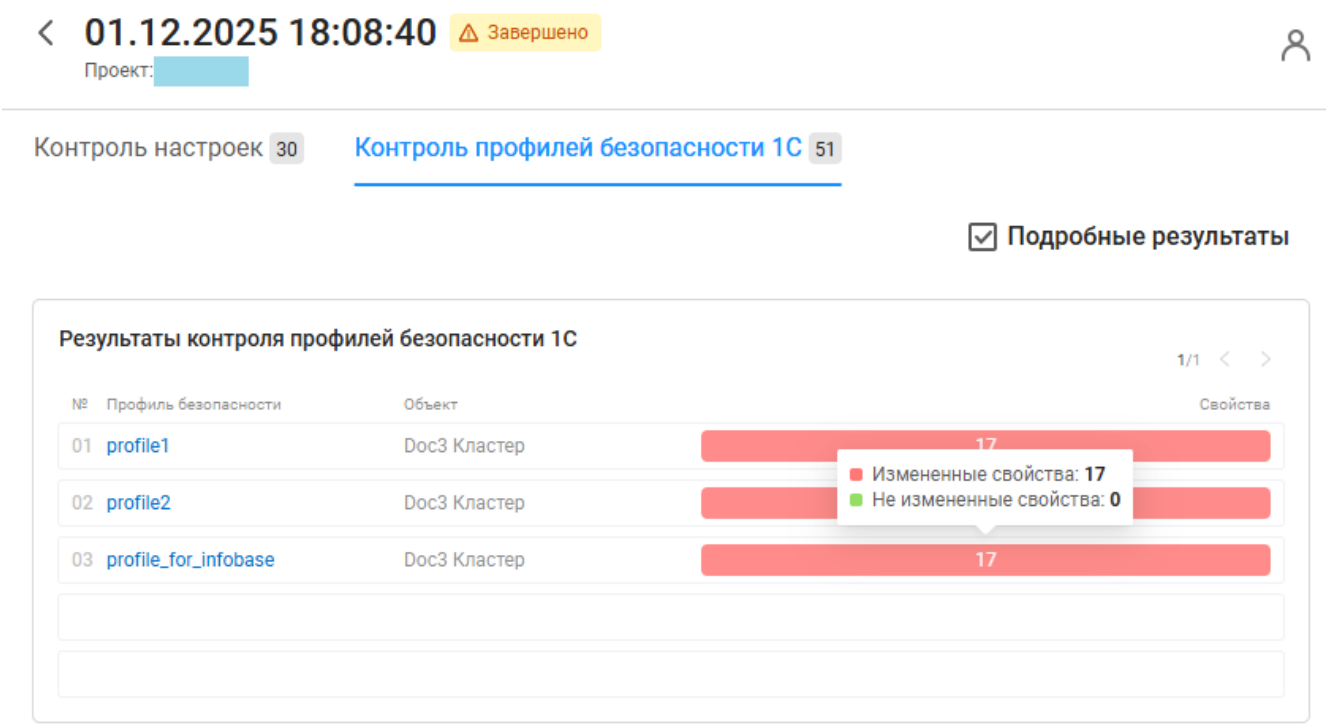


Рисунок 25 – Вкладка панели мониторинга проекта с целью сканирования «Контроль профилей безопасности 1С»

Для просмотра результатов сканирования необходимо выполнить следующие действия:

1) Выбрать проект из списка (см. рис. 17).
2) Выбрать итерацию проекта (см. рис. 18).
3) Выбрать вкладку «Контроль профилей безопасности 1С», нажать кнопку *«Подробные результаты».*

Подробные данные результата по «Контроль профилей безопасности 1С» представлены на рис. 26.

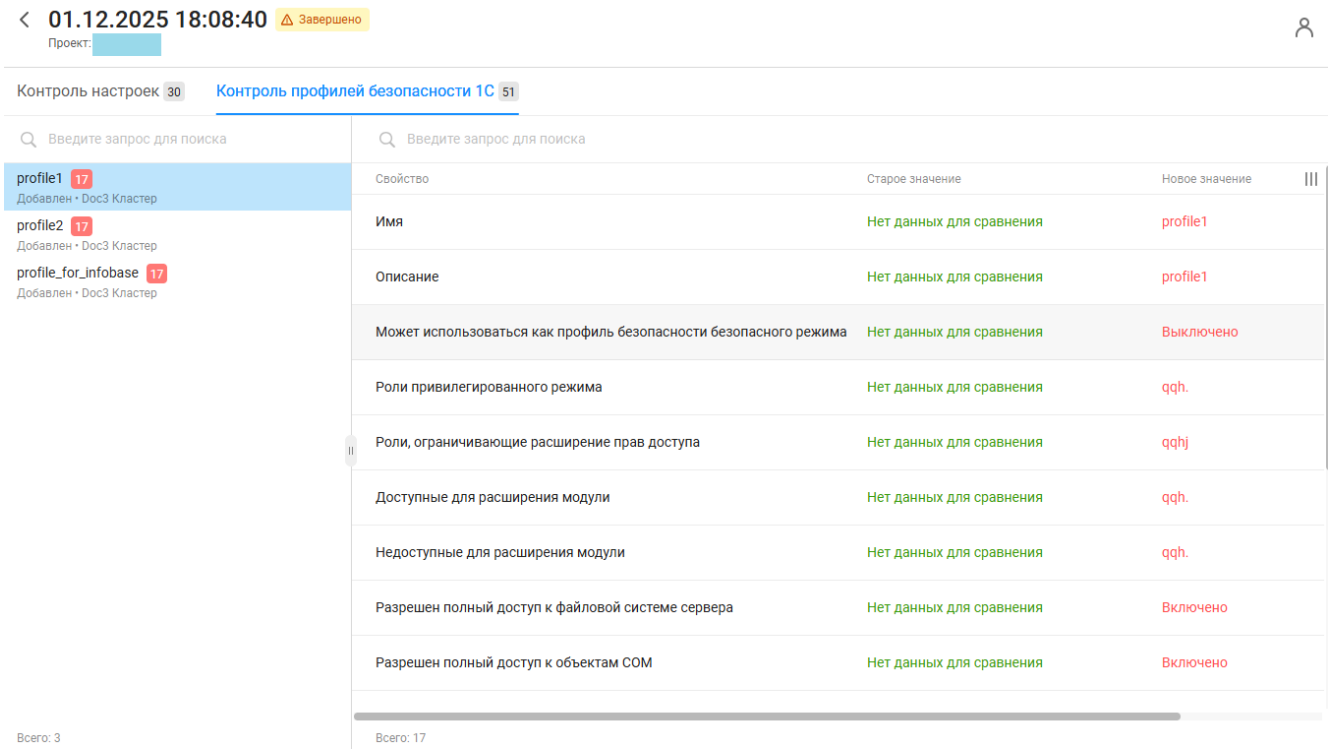


Рисунок 26 – Подробные результаты сканирования проекта с целью сканирования «Контроль профилей безопасности 1С»

При просмотре результатов сканирования «Контроль профилей безопасности 1С» доступны следующие области:

- список профилей безопасности 1С;
- список свойств профиля и их значений.

В область «Список профилей безопасности 1С» входят следующие столбцы:

- «Свойство» – свойство профиля;
- «Старое значение» – значение параметра в предыдущей итерации;
- «Новое значение» – значение параметра в текущей итерации.

Подробные данные по «Контролю настроек» представлены на рис. 27.

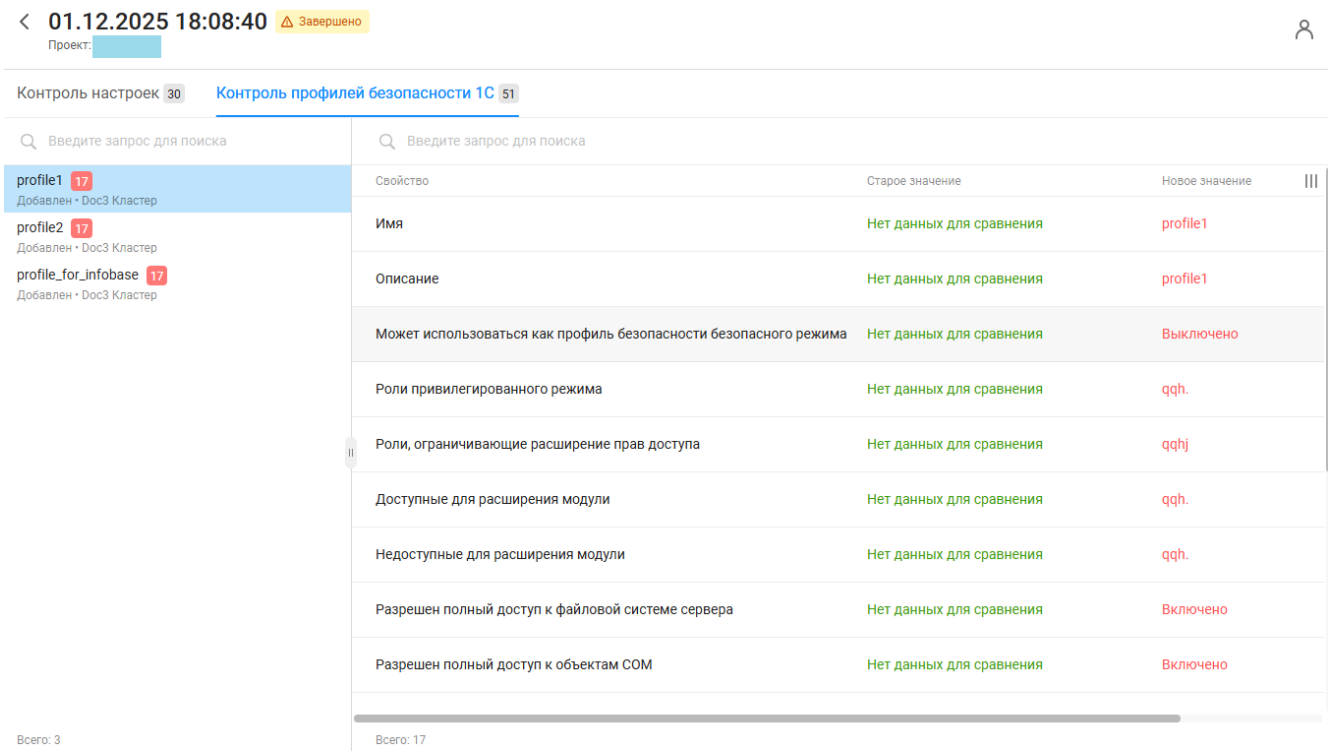


Рисунок 27 – Подробные результаты сканирования проекта с целью сканирования «Контроль настроек»

При просмотре подробных результатов сканирования «Контроль настроек» доступны следующие области:

- список подразделов – перечислены подразделы проверок, в которых обнаружены уязвимости, а также критичность и их количество;
- подробное описание найденных уязвимостей.

В область «Список подразделов» входят следующие столбцы:

- «Наименование угрозы» – список обнаруженных угроз;
- «Информация об объекте» – подробности об объекте, где сработали проверки;
- «Уровень опасности» – уровень опасности обнаруженной угрозы.

Примечание. В поле «Информация об объекте» выводится следующая информация:

- настройки кластера – название профиля безопасности, где сработала проверка.
- системные настройки – текущее значение проверяемого параметра;
- анализ ролей – название роли и название объектов;
- настройки журналирования – доступна следующая информация:
  а) проверки журнала регистрации событий (ЖРС) и журнала замера производительности (ЖЗП) – текущее значение проверяемого параметра.
  б) проверки журнала версионирования объектов (ЖВО) – название настройки и название объектов.

В подразделе «Проекты» доступен подробный просмотр уязвимости.

Для подробного просмотра уязвимости необходимо выполнить следующие действия:

1) Выбрать проект.
2) Выбрать итерацию
3) Выбрать вкладку «Контроль настроек», нажать кнопку *«Подробные результаты»*.
4) Выбрать уязвимости в дереве уязвимостей.
5) Выбрать уязвимость.

Подробное описание уязвимости представлено на рис. 28.

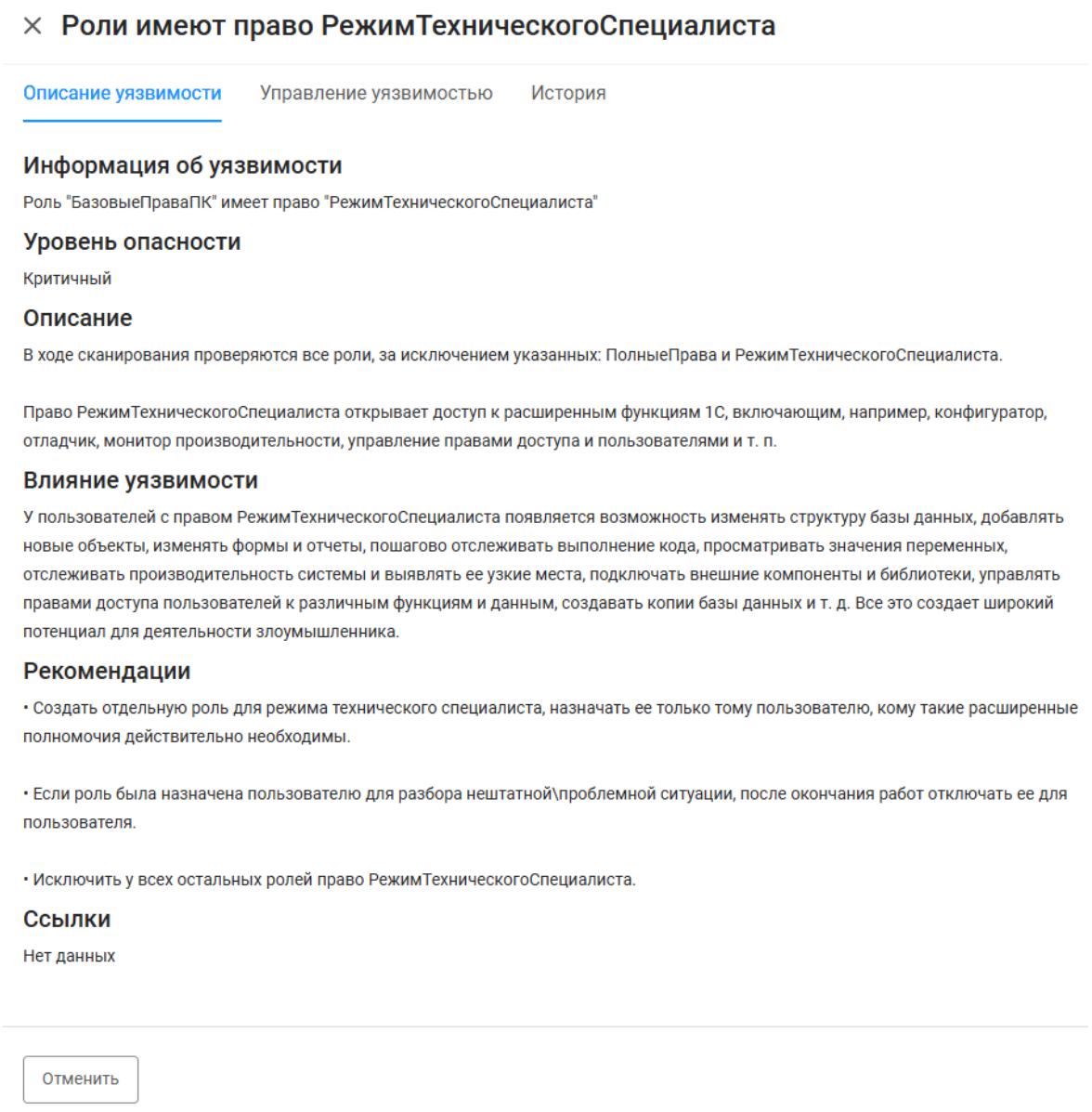


Рисунок 28 – Подробное описание уязвимости (раздел «Анализ платформы»)

4.2.1.5 Выгрузка отчетов

В подразделе «Проекты» доступна выгрузка отчетов по результатам сканирования. Выгрузка отчетов доступна для проектов и итераций со статусом «Завершено». Выгрузка отчёта доступна со следующих страниц:

— списка проектов (рис. 29);
— списка итераций (рис. 30);
— подробных результатов – вкладки «Найденные уязвимости» и «Исключенные уязвимости» (рис. 31).

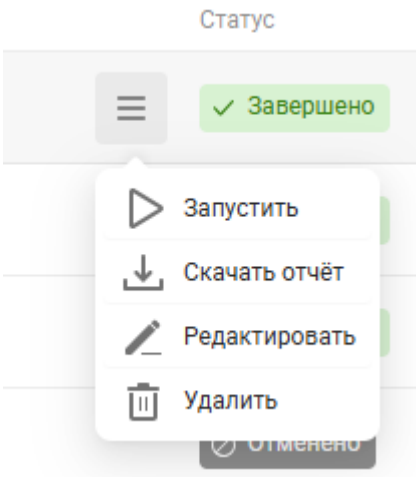


Рисунок 29 – Выгрузка отчета на странице списка проектов

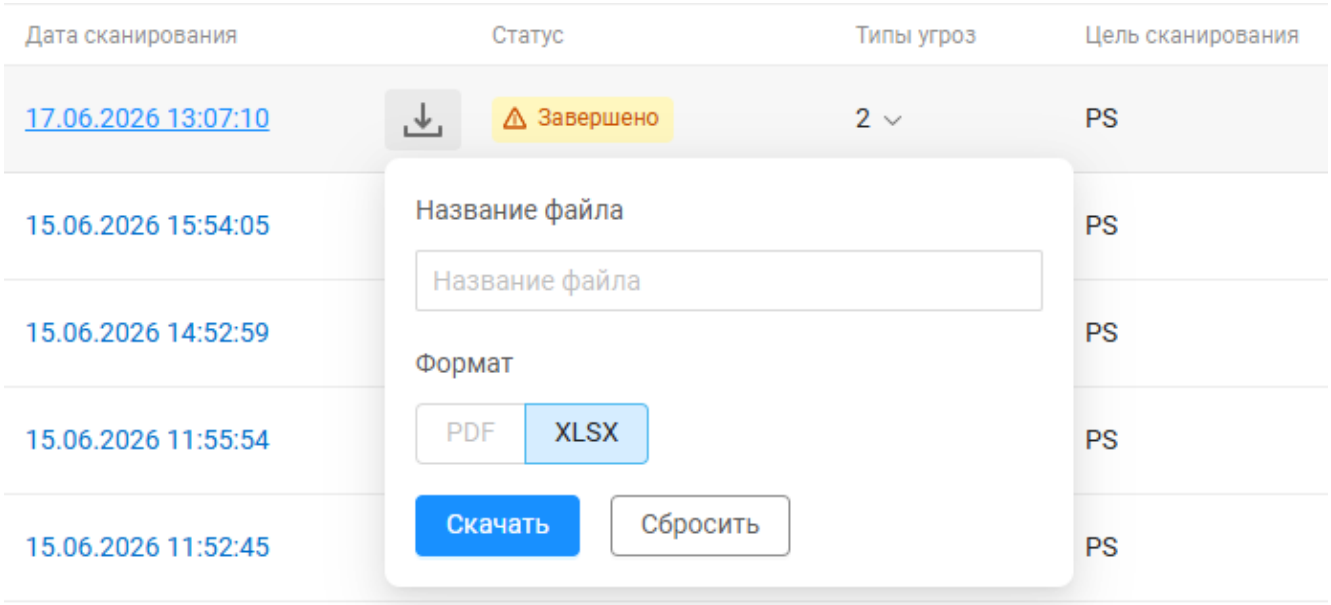


Рисунок 30 – Выгрузка отчета

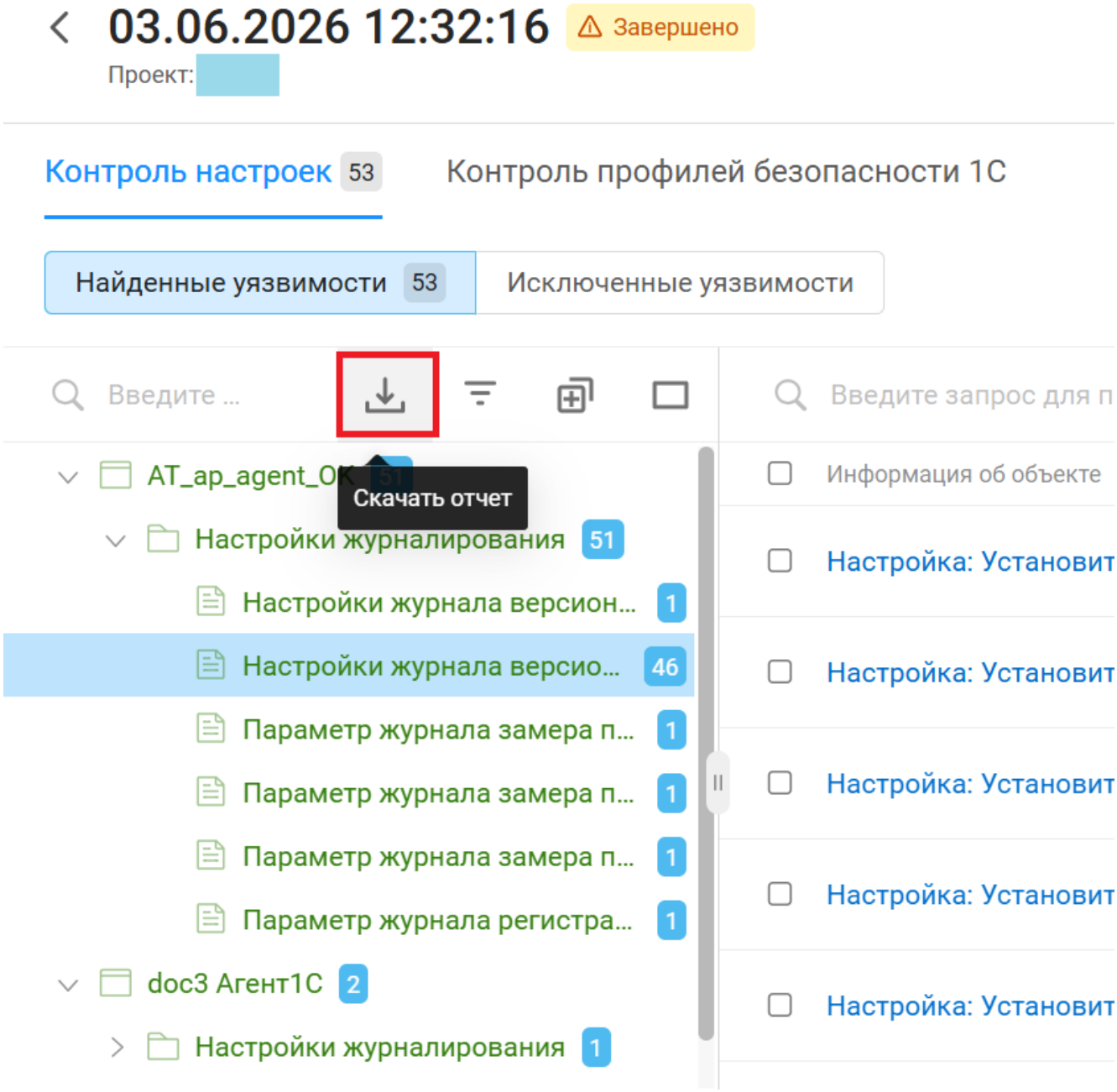


Рисунок 31 – Выгрузка отчета при просмотре дерева уязвимостей

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 формате XLSX.

Выгрузка отчета со страницы списка проектов

На странице списка проектов доступна выгрузка отчета по результатам итераций.

Выгрузка отчета со страницы списка итераций

На странице списка итераций доступна выгрузка отчета по результатам итераций.

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 следующем варианте:

— отчёт по умолчанию – выгружаются все уязвимости. Содержит информацию по всем уязвимостям вне зависимости от места выгрузки отчёта.

4.2.1.6 Управление уязвимостями

В подразделе «Проекты» пользователю доступно управление найденными уязвимостями.

Управление уязвимостями осуществляется в текущей итерации проекта.

Доступны следующие способы управления уязвимостями:

— массовое управление уязвимостями – при просмотре списка найденных уязвимостей;

— управление одной уязвимостью – при подробном просмотре найденной уязвимости.

Окно «Управление уязвимостями» состоит из следующих полей (рис. 32):

— «Уровень опасности»;

— «Статус уязвимости»;

— «Комментарий».

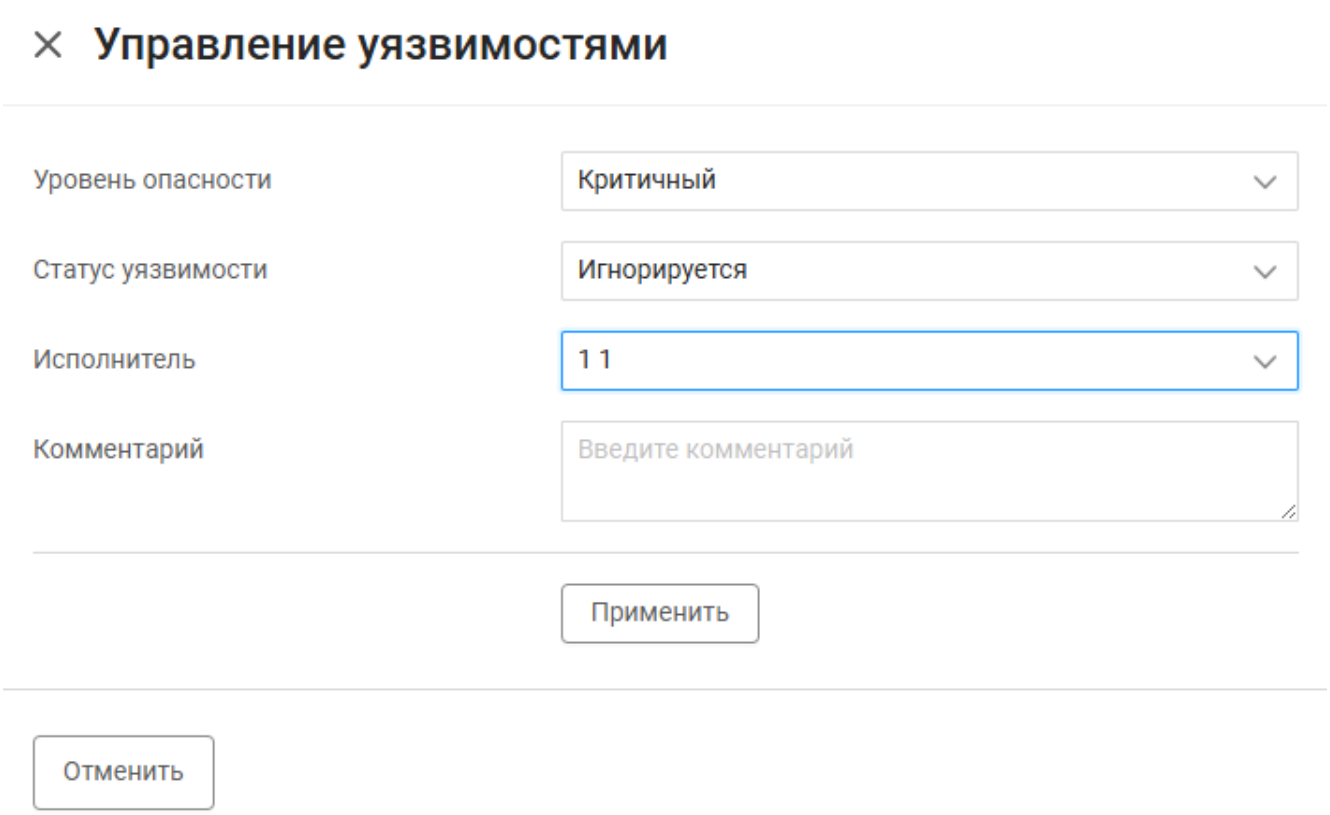


Рисунок 32 – Окно «Управление уязвимостью»

В поле «Статусы уязвимости» доступны следующие статусы:

- «Не устранена» – уязвимость не устранена;
- «Устранена» – уязвимость устранена. Статус переводит уязвимость в исключенные;
- «Игнорируется» – уязвимость игнорируется. Статус переводит уязвимость в исключенные.

В поле «Уровень опасности» доступны следующие варианты:

- критичный;
- высокий;
- средний;
- низкий;
- потенциальный;
- информация.

При изменении уровня опасности необходимо учитывать следующее:

1) При изменении уровня опасности проверки, связанной с уязвимостью, на странице раздела «Проверки», в текущей и последующих итерациях изменения к результатам сканирования не применяются.
2) При изменении уровня опасности проверки в подразделе «Профиль», связанном с уязвимостью, изменения применяются только для будущих сканирований. Результаты прошлых итераций остаются без изменений.
3) При смене уровня опасности вручную для конкретной уязвимости в итерации изменения применяются в текущей и будущих итерациях. Изменение базового уровня опасности в подразделах «Проверки» или «Профили» не применяются.

Для массового управления уязвимостями необходимо выполнить следующие действия:

1) Выбрать уязвимости в дереве уязвимостей.
2) Нажать кнопку *«Управление уязвимостями»*.
3) Заполнить поля во вкладке «Управление уязвимостями». Нажать кнопку *«Применить»*.

Для управления одной уязвимостью необходимо выполнить следующие действия:

1) Выбрать уязвимость из списка.
2) Выбрать вкладку «Управление уязвимостью».
3) Заполнить необходимые данные. Нажать кнопку *«Применить»*.

Примечания:

1. При массовом управлении уязвимостями во вкладке «Найденные уязвимости» доступен статус «Игнорируется».
2. При массовом управлении уязвимостями во вкладке «Исключенные уязвимости» доступен статус «Не устранена». После присвоения данного статуса уязвимости переходят во вкладку «Найденные уязвимости».
3. При подробном просмотре описания уязвимости доступен просмотр истории. Для просмотра истории необходимо выбрать вкладку «История» (см. рис. 32).
4. При управлении одной уязвимостью пользователю доступно добавление комментария во вкладке «История». Для добавления комментария необходимо

выбрать вкладку «История», внести комментарий в поле «Введите комментарий», нажать кнопку *«Добавить комментарий»*.

4.2.1.7 Подключение почтовых уведомлений

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

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

Для подключения почтовых уведомлений необходимо выполнить следующие действия:

1) Выбрать проект из списка или ввести название проекта в поисковую строку.
2) Нажать кнопку *«Оповещения»*. Выбрать события в окне (рис. 33).

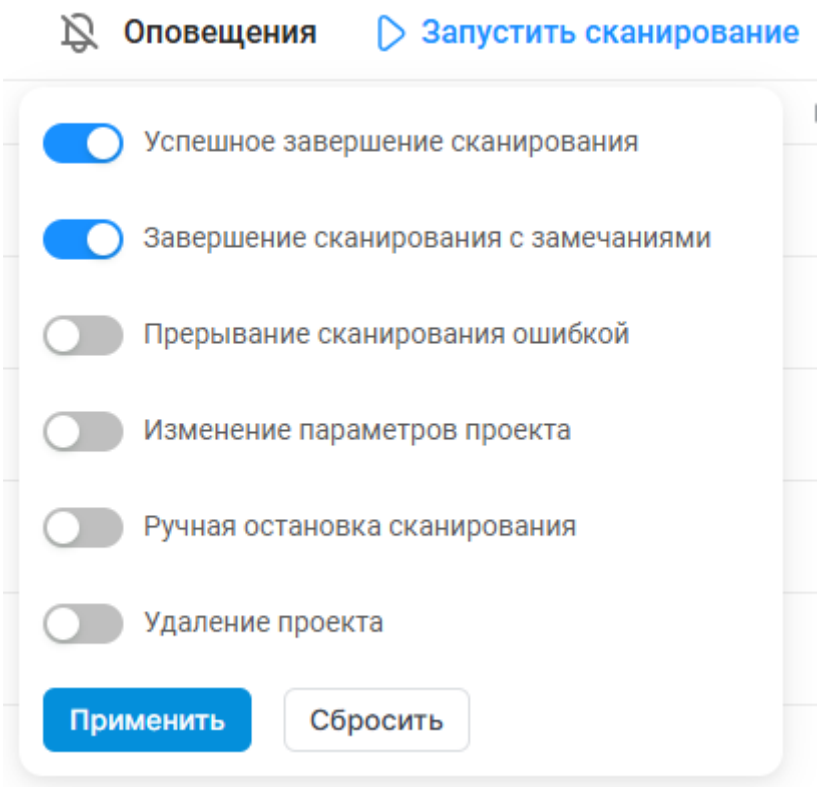


Рисунок 33 – Список событий (раздел «Анализ платформы»)

3) Нажать кнопку *«Применить»*.

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

Примеры почтовых уведомлений приведены на рисунках 34, 35, 36, 37, 38, 39.

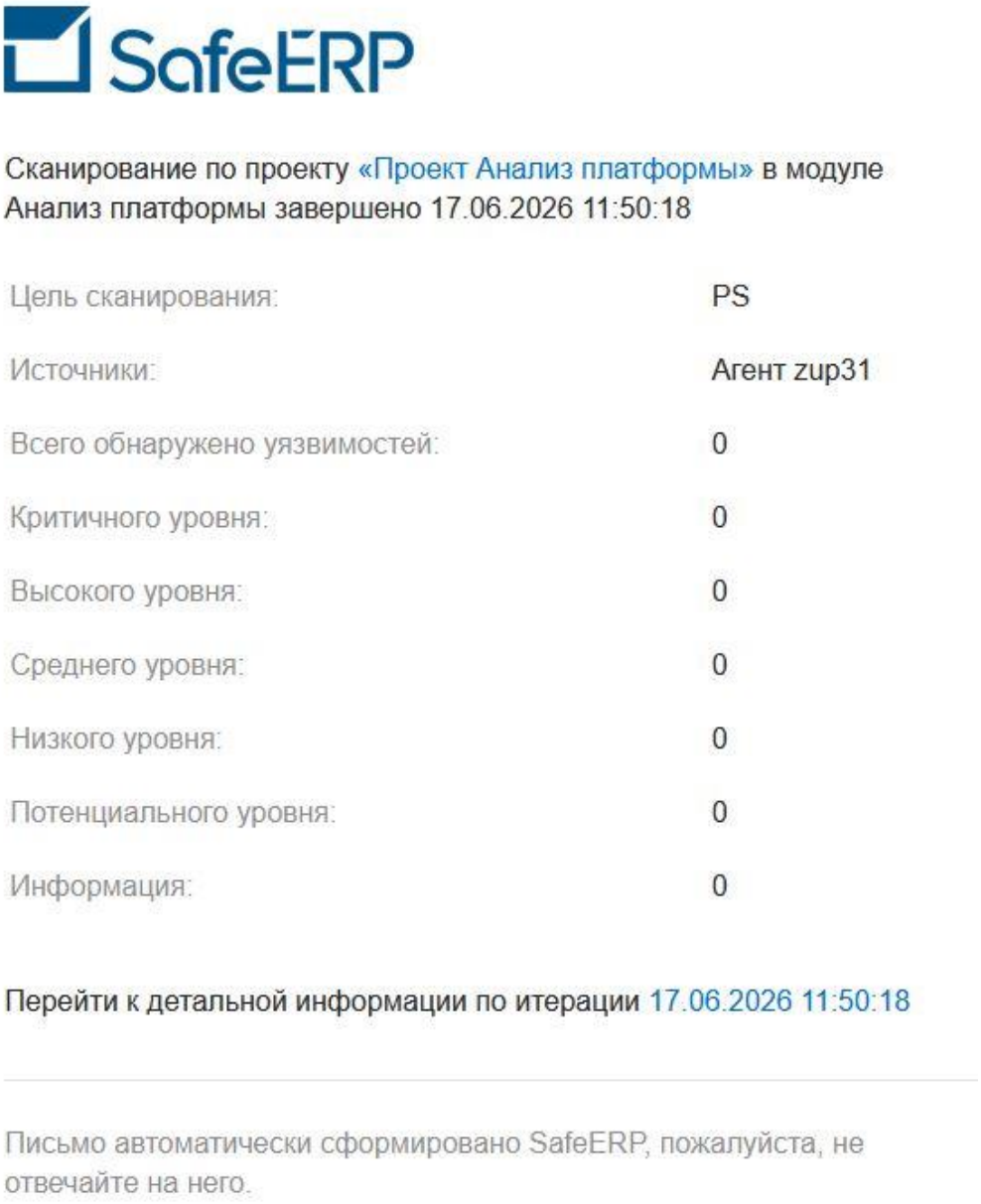


Рисунок 34 – Почтовое уведомление при активации события «Успешное завершение сканирования»



Рисунок 35 – Почтовое уведомление при активации события «Завершение сканирования с замечаниями»

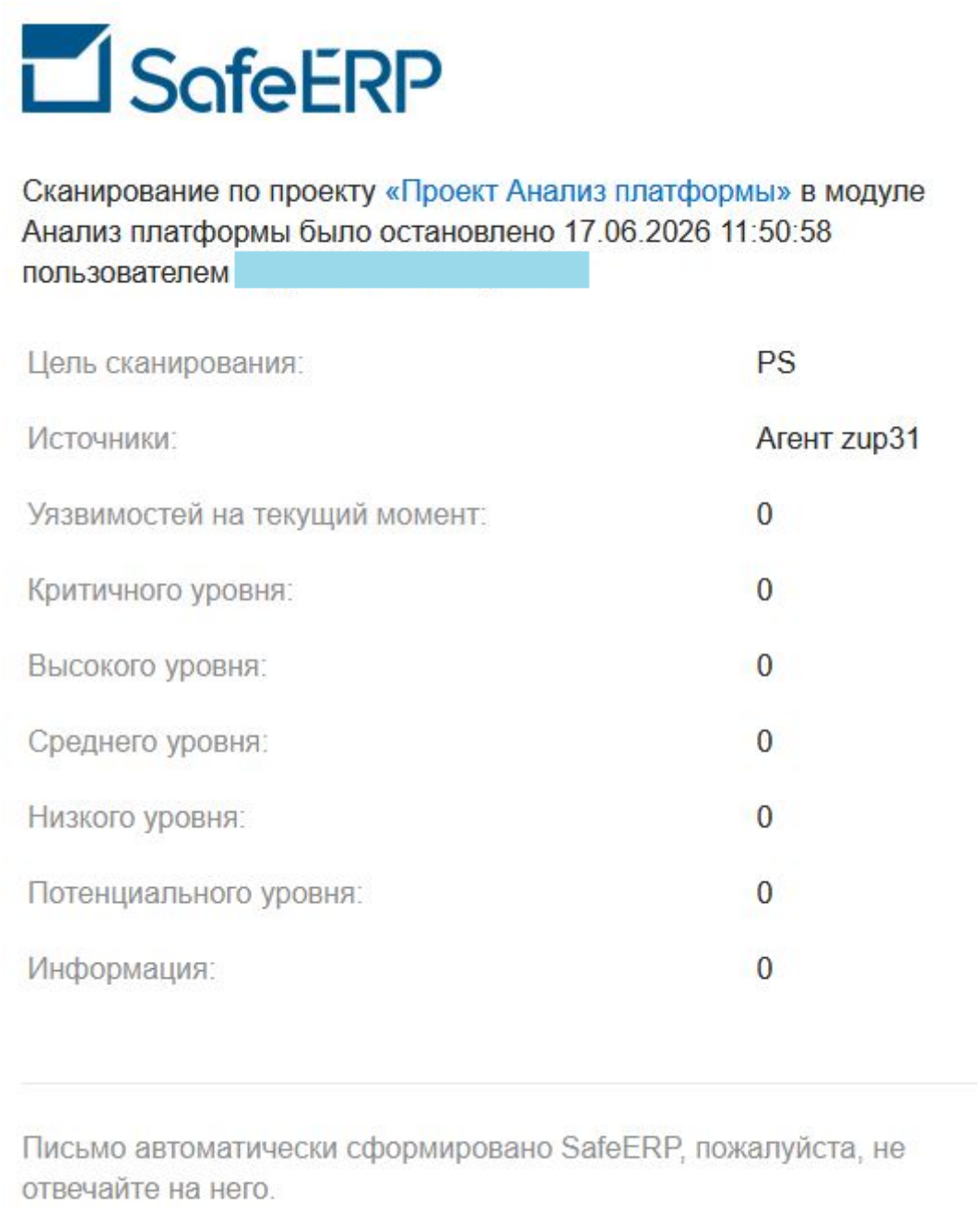


Рисунок 36 – Почтовое уведомление при активации события «Ручная остановка сканирования»



Рисунок 37 – Почтовое уведомление при активации события «Прерывание сканирования с ошибкой»



Рисунок 38 – Почтовое уведомление при активации события «Изменения параметров проекта»



Рисунок 39 – Почтовое уведомление при активации события «Удаление проекта»

Просмотр активных подписок

Для просмотра списка активных подписок необходимо обратиться к подразделу 4.6.

Отмена подписок

Отмена подписок осуществляется следующими способами:

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

Подробное описание представлено в подразделе 4.6.

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. 33).

4.2.1.8 Удаление проекта

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

4.2.2 Подраздел «Профили»

Подраздел «Профили» предназначен для ведения профилей проверок. Пользователю доступно создание, редактирование, копирование и удаление пользовательских профилей.

Основная рабочая область подраздела «Профили сканирования» представлена на рис. 40.

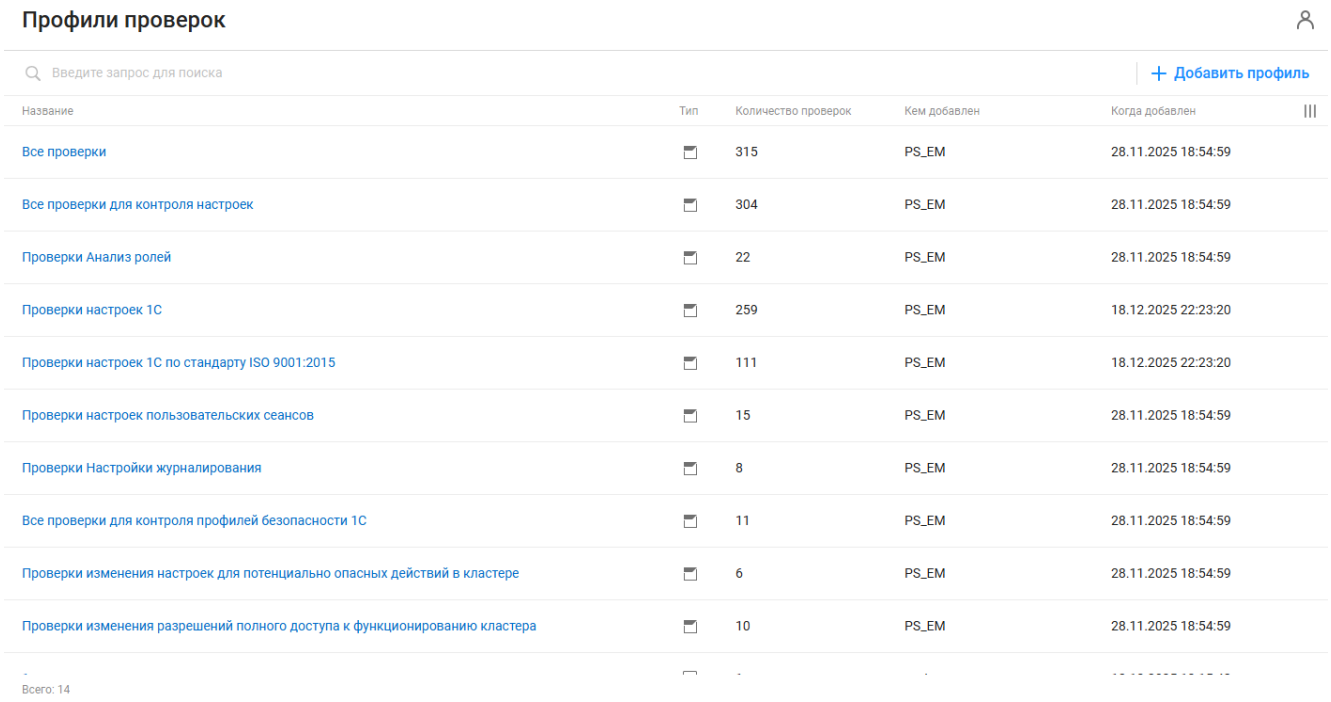


Рисунок 40 – Подраздел «Профили сканирования»

4.2.2.1 Создание профилей

Для создания профилей необходимо выполнить следующие действия:

1) Нажать кнопку *«+Добавить профиль».*
2) Ввести название профиля, нажать кнопку *«Создать»* в открывшемся окне (рис. 41).

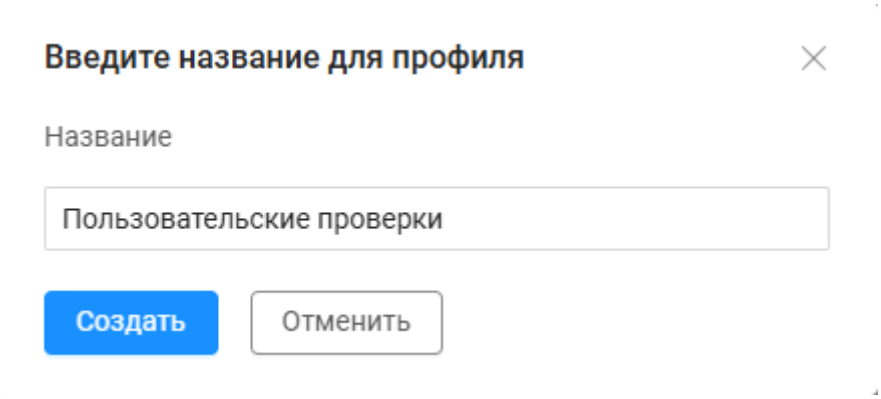


Рисунок 41 – Окно создания пользовательского профиля

3) Нажать кнопку *«+Добавить проверки»* (рис. 42).

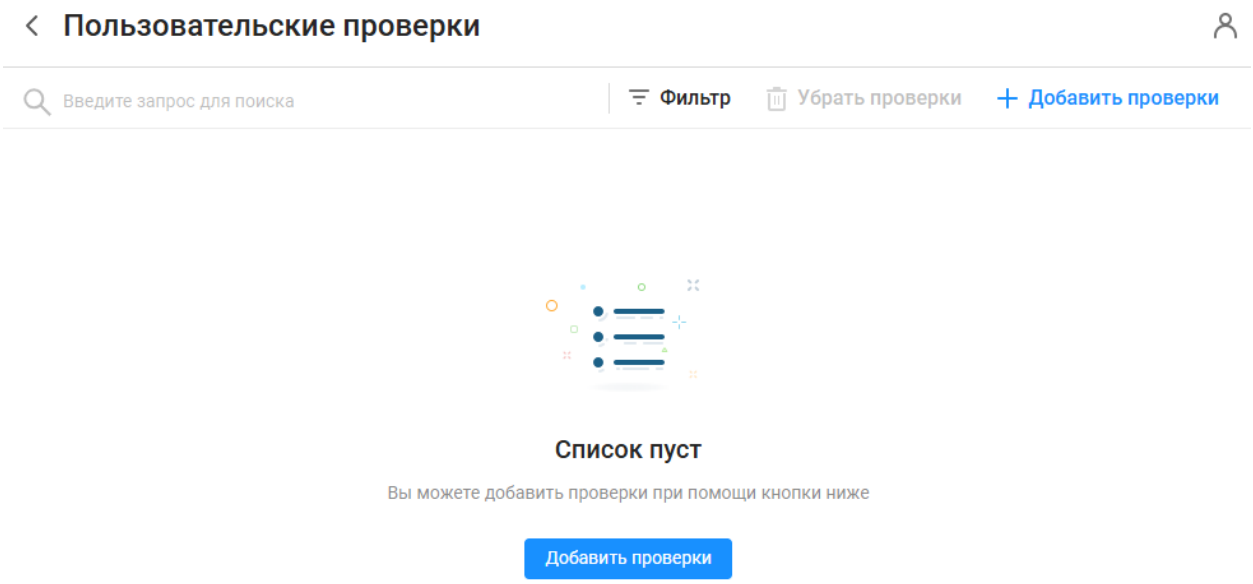


Рисунок 42 – Пользовательский профиль

4) Поставить флаги напротив проверок. Нажать кнопку *«Добавить»* (рис. 43).

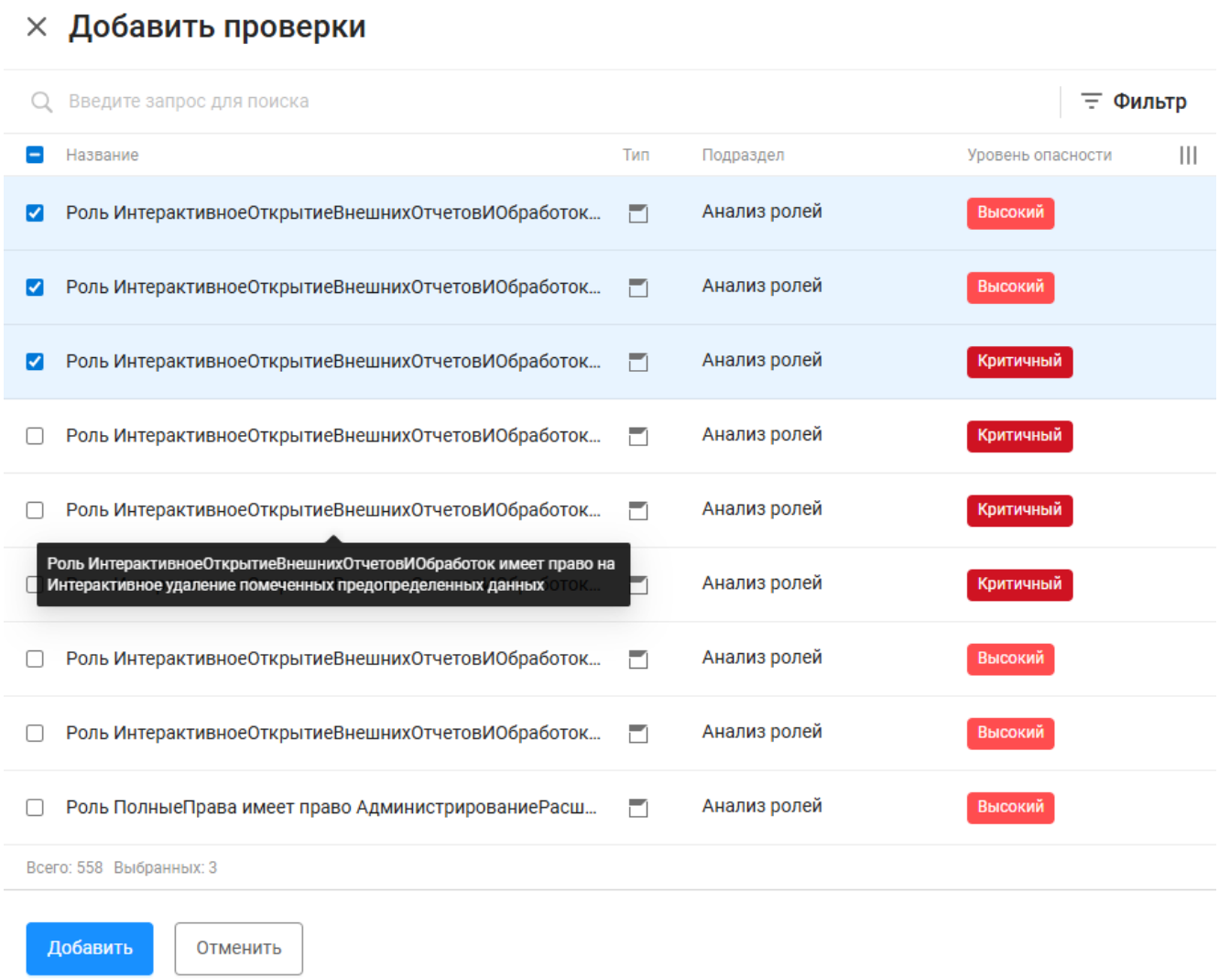


Рисунок 43 – Добавление проверок в пользовательский профиль

4.2.2.2 Редактирование пользовательских профилей

Для редактирования профилей необходимо выполнить следующие действия:

1) Выбрать профиль из списка.
2) Внести изменения (добавить или убрать проверки, изменить уровень опасности проверки).

Примечания:

1. При редактировании пользовательского профиля доступно изменение параметров стандартных и пользовательских проверок. Для изменения проверок необходимо выбрать проверку из списка, внести изменения, нажать кнопку *«Сохранить»*. Внесённые изменения будут применены только для данного профиля сканирования.
2. Для проверок из подразделов «Системные настройки» и «Настройки кластера» доступно изменение релевантного значения.

4.2.2.3 Копирование профилей

Для копирования профилей необходимо выполнить следующие действия:

1) Нажать кнопку *«Копировать профиль»* в контекстном меню.

2) Ввести название профиля в окне (рис. 44). Нажать кнопку *«Создать копию»*.

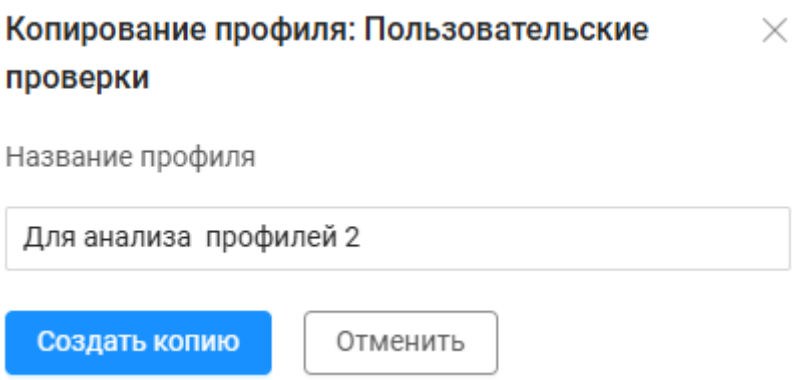


Рисунок 44 – Копирование профиля

Примечание. При копировании профилей скопируется набор проверок родительского профиля, а также настройки проверок, произведённые в копируемом профиле (уровень опасности и релевантное значение проверки).

4.2.2.4 Удаление пользовательского профиля

Для удаления пользовательского профиля необходимо нажать кнопку *«Удалить профиль»* в контекстном меню.

4.2.3 Подраздел «Проверки»

В подразделе «Проверки» доступно ведение проверок. Основная рабочая область подраздела «Проверки» представлена на рис. 45.

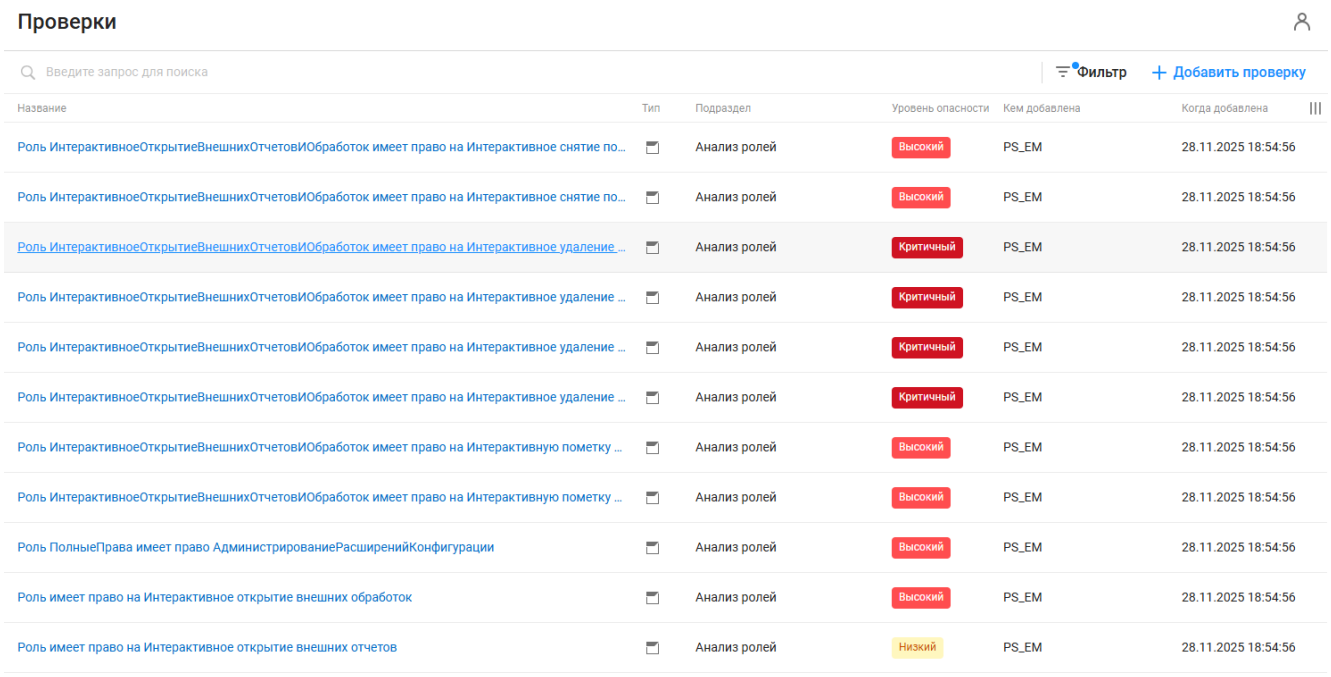


Рисунок 45 – Подраздел «Проверки»

В ПК «SAFEERP PS EM» доступны следующие действия:

— просмотр проверок;
— создание проверок;
— редактирование проверок;
— удаление проверок.

Для сканирования проверок вне стандартных профилей необходимо выполнить следующие действия:

1) Добавить пользовательскую проверку в пользовательский профиль сканирования (см. в подпункте 4.2.2.2).
2) Выбрать пользовательский профиль сканирования в настройках проекта (см. подпункте 4.2.1.2).

4.2.3.1 Просмотр проверок

Для просмотра проверок необходимо выбрать проверку из списка или ввести название проверки в поисковую строку и открыть её.

4.2.3.2 Добавление пользовательской проверки

Для добавления пользовательской проверки необходимо выполнить следующие действия:

1) Нажать кнопку *«+ Добавить проверку».*
2) Заполнить необходимые поля.
3) Нажать кнопку *«Добавить»*.

Примечания:

1. Подробное описание параметров для создания пользовательских проверок приведено в приложении 1.
2. После заполнения полей «Подраздел» и «Шаблон проверки», то после поля «Имя параметры» появляются дополнительные поля согласно выбранному шаблону. Доступно для проверок из подраздела «Системные настройки» и для шаблона «Проверка значений параметров настроек 1С».
3. Поле «Описание» заполняется автоматически после выбора значений в поле «Имя параметра».
4. При смене значений в полях «Подраздел» или «Шаблон» очищаются все поля, кроме полей «Название» и «Шаблон».

4.2.3.3 Редактирование пользовательской проверки

Для редактирования пользовательской проверки необходимо выполнить следующие действия:

1) Выбрать проверку из списка или ввести название проверки в поисковую строку и открыть её.
2) Нажать кнопку *«Редактировать»* в открывшемся окне.
3) Внести изменения. Нажать кнопку *«Сохранить»*.

4.2.3.4 Удаление пользовательской проверки

Для удаления пользовательской проверки необходимо выполнить следующие действия:

1) Выбрать проверку из списка или ввести название проверки в поисковую строку и открыть её.

2) Нажать кнопку *«Удалить»* в контекстном меню.
3) Подтвердить действия.

4.3 Раздел «Pentest»

Раздел «Pentest» предназначен сканирования хостов (целевых систем) на наличие уязвимостей с возможностью их эксплуатации.
Раздел «Pentest» состоит из следующих подразделов:

— «Проекты»;
— «Агенты».

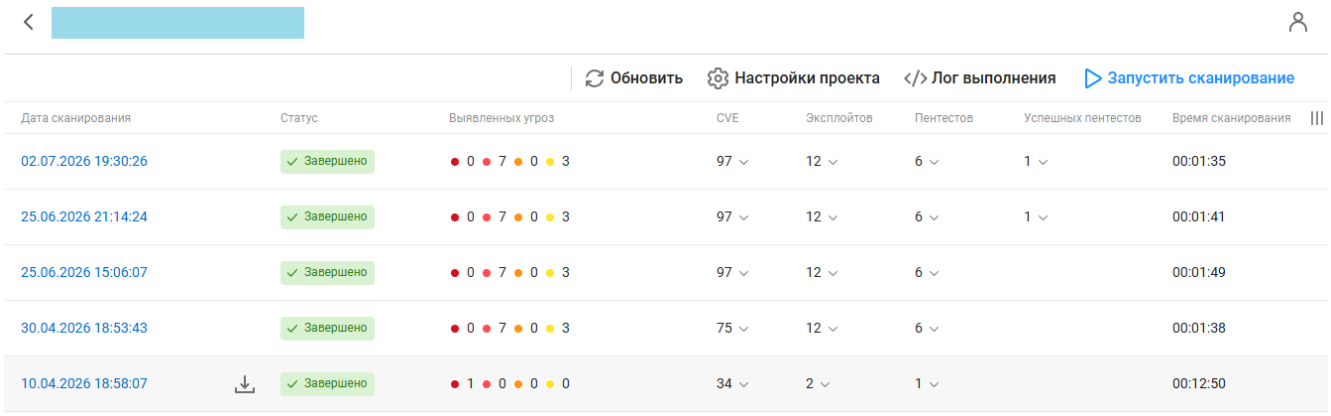


Рисунок 46 – Список итераций проекта

4.3.1 Подраздел «Проекты»

Основная рабочая область подраздела «Проекты» представлено на рис. 47.

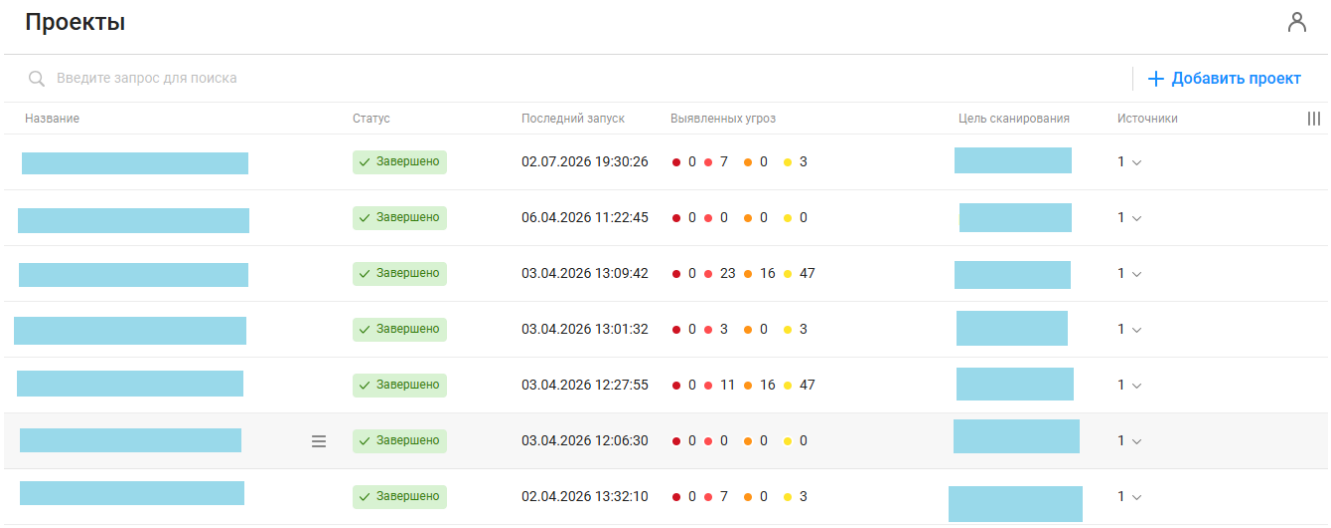


Рисунок 47 – Подраздел «Проекты»

В основную область подраздела «Проекты» входят следующие столбцы (рис. 47):

— «Название проекта»;

— «Статус» – статус последней итерации проекта;
— «Последний запуск» – дата и время последнего запуска сканирования;
— «Выявленных угроз» – количество и критичность найденных угроз;
— «Цели сканирования» – количество целей сканирование в проекте;
— «Источники» – количество источников в проекте.

Доступные статусы итераций и проектов представлены в таблице 5.
Таблица 5 – Статусы итераций и проектов

Статус	Значение
Новый	Проект создан. Сканирование не было запущено. Доступно для проектов
Выполняется	Сканирование проекта запущено
Остановка	Сканирование проекта остановлено
Завершено	Сканирование завершено. Ошибки не обнаружены
Ошибка	Сканирование было прервано из-за возникших ошибок
Отменено	Сканирование было отменено пользователем

Доступные статусы найденных угроз представлены в таблице 6.
Таблица 6 – Статус найденных угроз (раздел «Pentest»)

Индикация	Статус угрозы
	Критичный
	Высокий
	Средний
	Низкий

4.3.1.1 Добавление проекта

Для добавления проекта необходимо выполнить следующие действия:

1) Нажать кнопку *«+Добавить проект»* (см. рис. 47).
2) Заполнить необходимые поля (рис. 48).

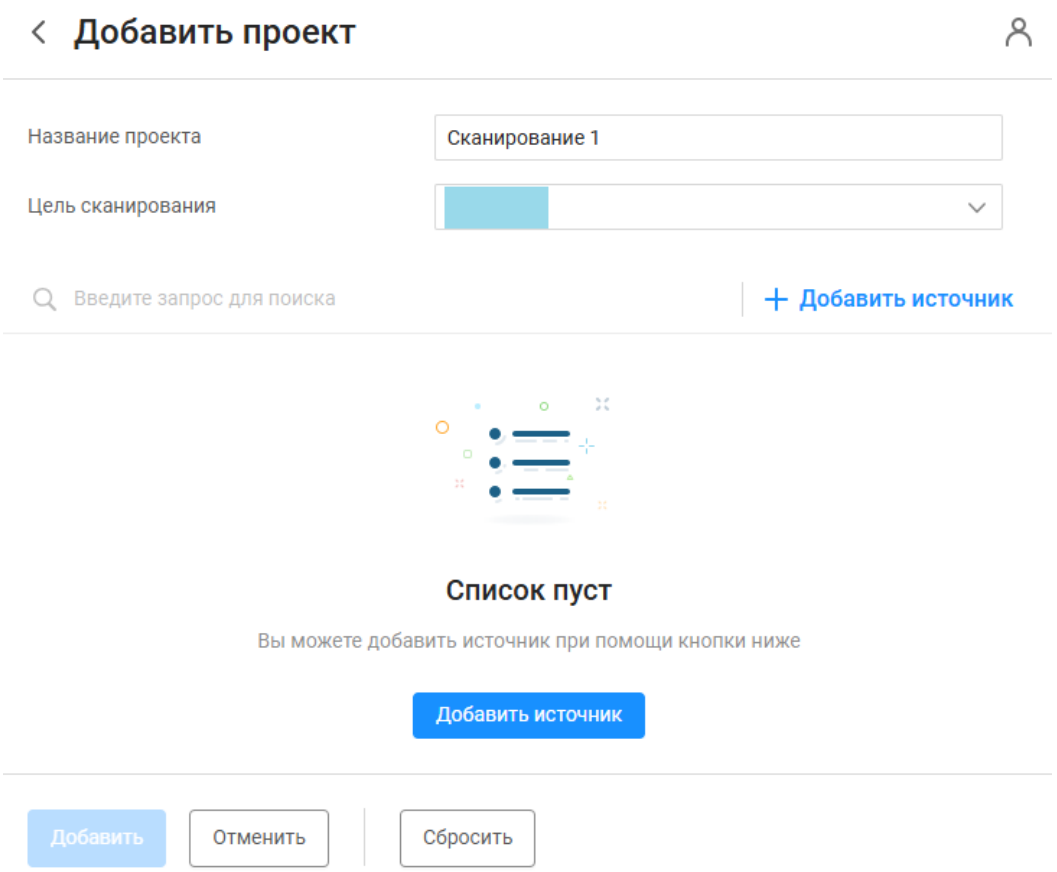


Рисунок 48 – Добавление проекта

3) Нажать кнопку *«Добавить источник».*
4) Выбрать источник и режим сканирования в окне «Добавить источник». Нажать кнопку *«Добавить источник»* (рис. 49).

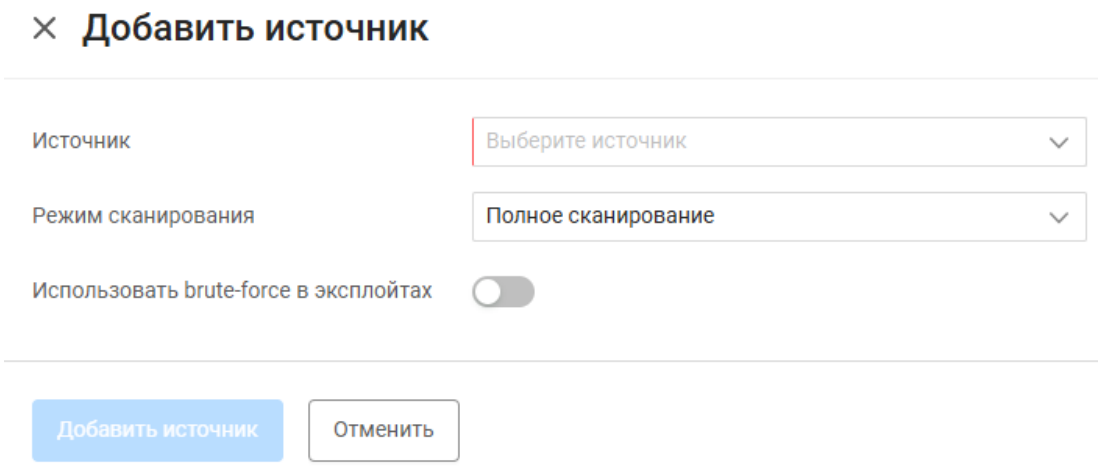


Рисунок 49 – Добавление источника

5) Нажать кнопку *«Добавить»* (см. рис. 48).

Режимы сканирования

При создании или редактировании проекта доступно следующее:

1. Режим «Сканирование хостов» предназначен для проверки доступных хостов с помощью ICMP запросов, проверки TCP и UDP соединений, а также DHCP-проверок.
2. Режим «Сканирование портов на хостах» предназначен для:

— проверки переданных хостов с помощью ICMP запросов, проверки TCP и UDP соединений, а также DHCP-проверок;
— проверки переданных открытых TCP и UDP портов на указанных хостах.

3. Режим «Сканирование служб на портах» предназначен для:

— проверки доступных хостов с помощью ICMP запросов, проверки TCP и UDP соединений, а также DHCP-проверок;
— проверки открытых TCP и UDP портов на указанных хостах;
— поиска служб на переданных TCP и UDP портах.

4. Режим «Применение пентестов» предназначен для:

— проверки доступных хостов с помощью ICMP запросов, проверки TCP и UDP соединений, а также DHCP-проверок;
— проверки открытых TCP и UDP портов на указанных хостах;
— поиска служб на переданных TCP и UDP портах;
— применения пентестов к найденным службам.

5. Режим «Поиск уязвимостей» предназначен для:

— проверки доступных хостов с помощью ICMP запросов, проверки TCP и UDP соединений, а также DHCP-проверок;
— проверки открытых TCP и UDP портов на указанных хостах;
— поиска служб на переданных TCP и UDP портах;
— поиска CVE на каждом порту хоста.

6. Режим «Поиск эксплойтов» предназначен для:

— проверки доступных хостов с помощью ICMP запросов, проверки TCP и UDP соединений, а также DHCP-проверок
— проверки открытых TCP и UDP портов на указанных хостах;
— поиска служб на переданных TCP и UDP портах
— поиска CVE на каждом порту хоста;
— поиска известных эксплойтов найденных ранее уязвимостей.

7. Режим «Поиск уязвимостей и применение пентестов» предназначен для:

— проверки доступных хостов с помощью ICMP запросов, проверки TCP и UDP соединений, а также DHCP-проверок;
— проверки переданных открытых TCP и UDP портов на указанных хостах;
— поиска служб на переданных TCP и UDP портах;
— поиска CVE на каждом порту хоста;
— применения пентестов к найденным службам.

8. Полное сканирование.

4.3.1.2 Изменение настроек проекта

Настройка проекта осуществляется следующими способами:

— через кнопку *«Настройки проекта»* при просмотре проекта.

Для настройки проектов необходимо выполнить следующие действия:

1) Открыть проект.
2) Нажать кнопку *«Настройки проекта».*
3) Внести изменения (название проекта, описание проекта, добавление или удаление источника, активация или деактивация brute-force в эксплойтах, режим сканирования).
4) Нажать кнопку *«Сохранить»* (рис. 50).

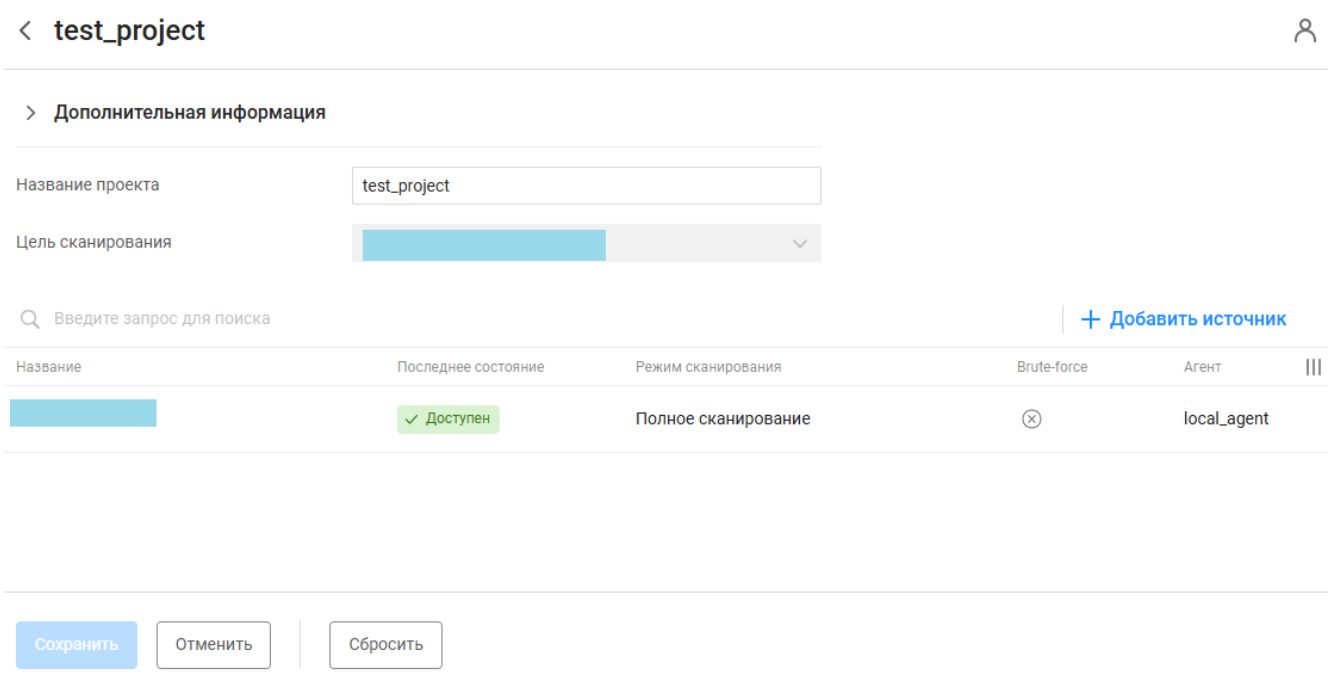


Рисунок 50 – Редактирование проекта

4.3.1.3 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 подраздел «Проекты».
2) Выбрать проект.
3) Нажать кнопку *«Запустить сканирование»*.

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.

Остановка сканирования проекта

Остановка сканирования проекта осуществляется следующими способами:

— через контекстное меню в строке проекта;

— со страницы проекта.

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

1) Выбрать пункт меню «Проекты».
2) Выбрать проект или ввести его название в поисковую строку.
3) Нажать левой кнопкой мыши на выбранный проект.
4) Нажать кнопку *«Остановить сканирование»*.

Для остановки сканирования проекта из пункта меню «Проекты» необходимо выполнить следующие действия:

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

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»*.

Примечание. 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 4.5.2.

4.3.1.4 Результаты сканирования

После завершения сканирования доступно следующее:

— выгрузка отчета по результатам итерации в формате pdf;
— просмотр результата сканирования.

Выгрузка отчета

Выгрузка отчета по результатам итерации осуществляется следующими способами:

— при просмотре списка итераций;
— при просмотре списка хостов по результатам сканирования.

Для выгрузки отчета при просмотре списка итераций необходимо выполнить следующие действия:

1) Выбрать проект.
2) Навести курсор на выбранную итерацию. Нажать кнопку *«Скачать отчёт»*.
3) Ввести название отчета. Нажать кнопку *«Скачать»* (рис. 51).

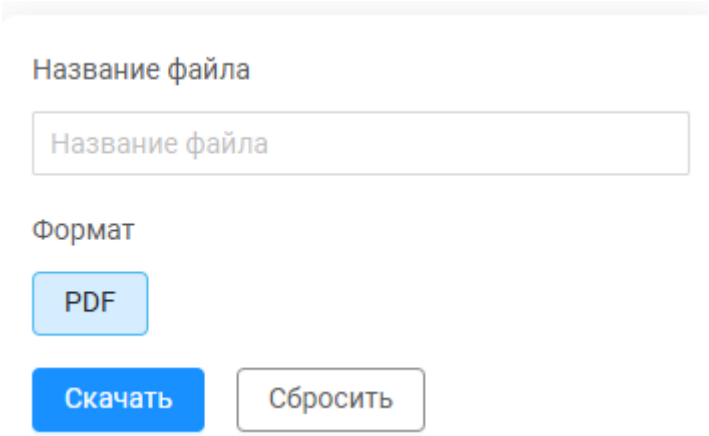


Рисунок 51 – Выгрузка отчета (раздел «Pentest»)

Для выгрузки отчета при просмотре списка хостов необходимо выполнить следующие действия:

1) Выбрать проект.
2) Выбрать итерацию проекта.
3) Нажать кнопку *«Скачать отчет»*.
4) Ввести название отчета. Нажать кнопку *«Скачать»* (см. рис. 51).

Просмотр результата сканирования по выбранной уязвимости

Для просмотра результата сканирования по выбранной уязвимости необходимо выполнить следующие действия:

1) Выбрать проект.
2) Выбрать итерацию проекта.
3) Выбрать просканированный хост.
4) Выбрать просканированный порт.

4.3.1.5 Просмотр логов проекта

Для просмотра логов проекта необходимо выполнить следующие действия:

1) Выбрать проект.
2) Нажать кнопку *«Лог выполнения»* (см. рис. 46).

Лог выполнения представлен на рис. 52.



Рисунок 52 – Подробный лог выполнения проекта

4.3.1.6 Удаление проекта

Для удаления проекта необходимо нажать кнопку *«Удалить»* в контекстном меню в строке проекта, подтвердить действие.

4.3.2 Подраздел «Агенты»

Подраздел предназначен для ведения агентов.

Основная рабочая область подраздела «Агенты» представлена на рис. 53.

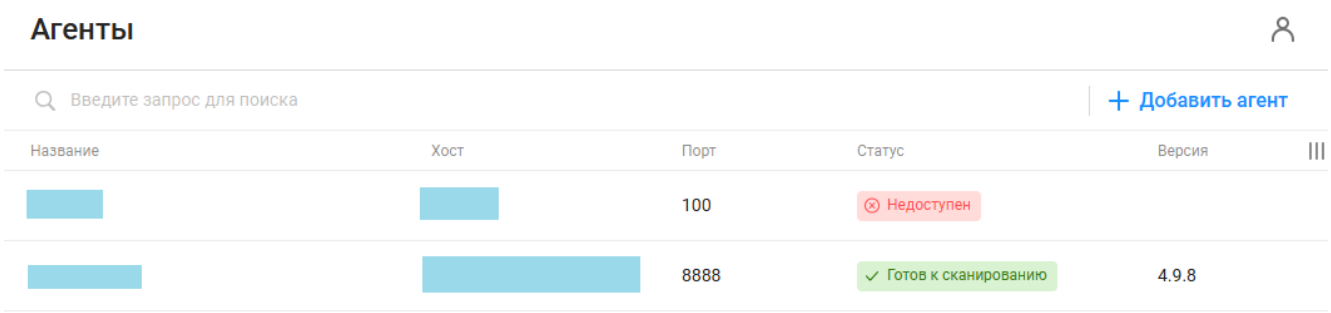


Рисунок 53 – Подраздел «Агенты»

4.3.2.1 Добавление агентов

Для корректной работы агентов необходимо произвести настройку аутентификации согласно документу «Установка, обновление, удаление ПК SAFEERP EM»

Для добавления агентов необходимо выполнить следующие действия:

1) Нажать кнопку *«+Добавить агент»* (см. рис. 53).
2) Заполнить необходимые поля (рис. 54).
3) Нажать кнопку *«Добавить»* (см. рис. 54).

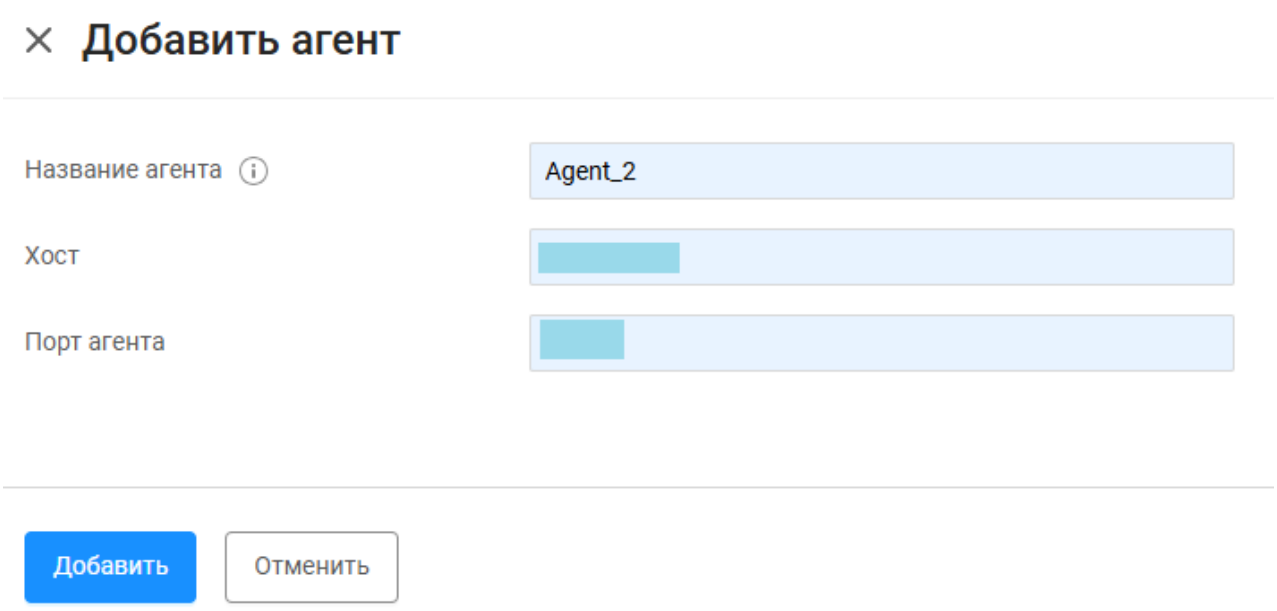


Рисунок 54 – Добавление агента

4.3.2.2 Редактирование агента

Для редактирования агента необходимо выполнить следующие действия:

1) Выбрать агент из списка (см. рис. 53).
2) Нажать кнопку *«Редактировать»* (рис. 55). Внести изменения (название, хост, порт агента).

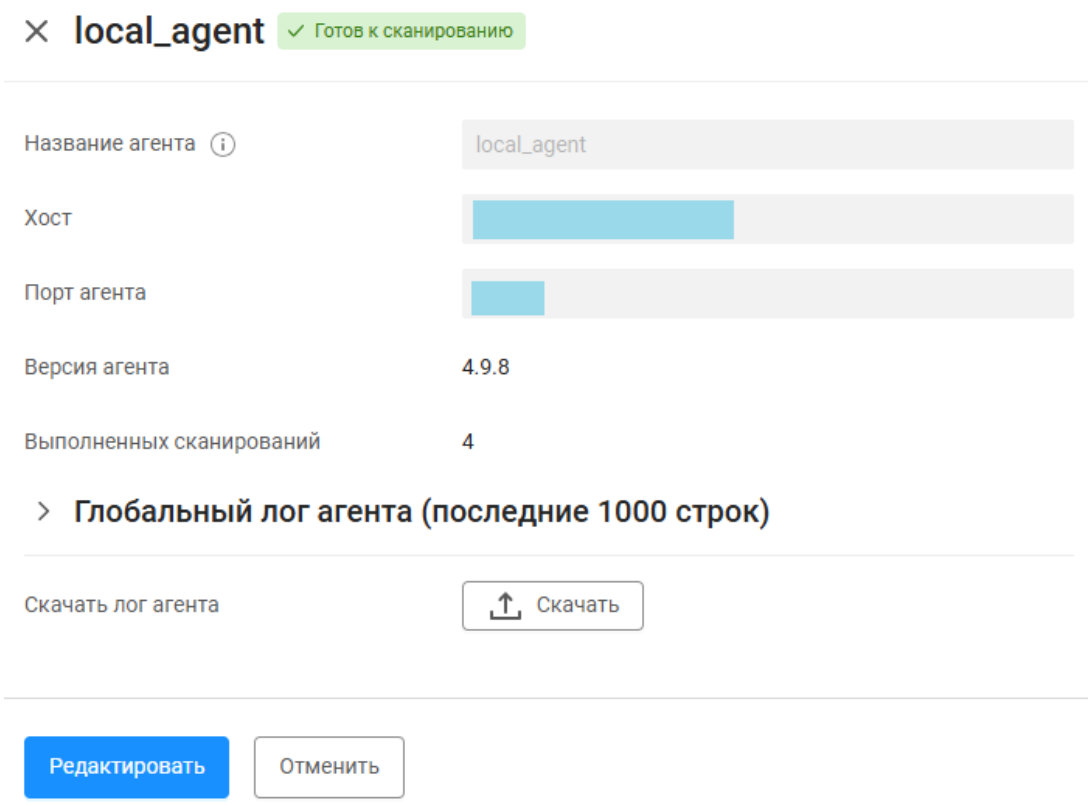


Рисунок 55 – Просмотр данных агента

3) Нажать кнопку *«Сохранить»* (рис. 56).

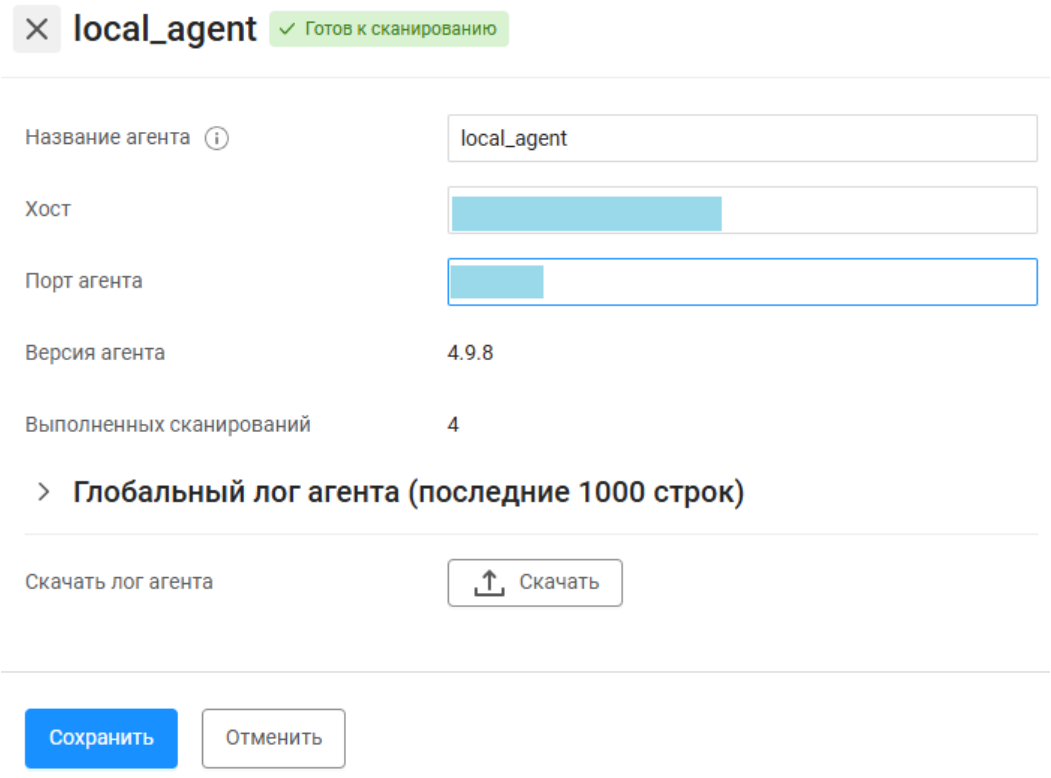


Рисунок 56 – Редактирование агента

4.3.2.3 Просмотр лога агента

Для просмотра лога агента необходимо выполнить следующие действия:

1) Выбрать агент.
2) Развернуть вкладку «Глобальный лог агента (последние 1000 строк)» (см. рис. 56).

Подробное описание лога агента представлено на рис. 57.

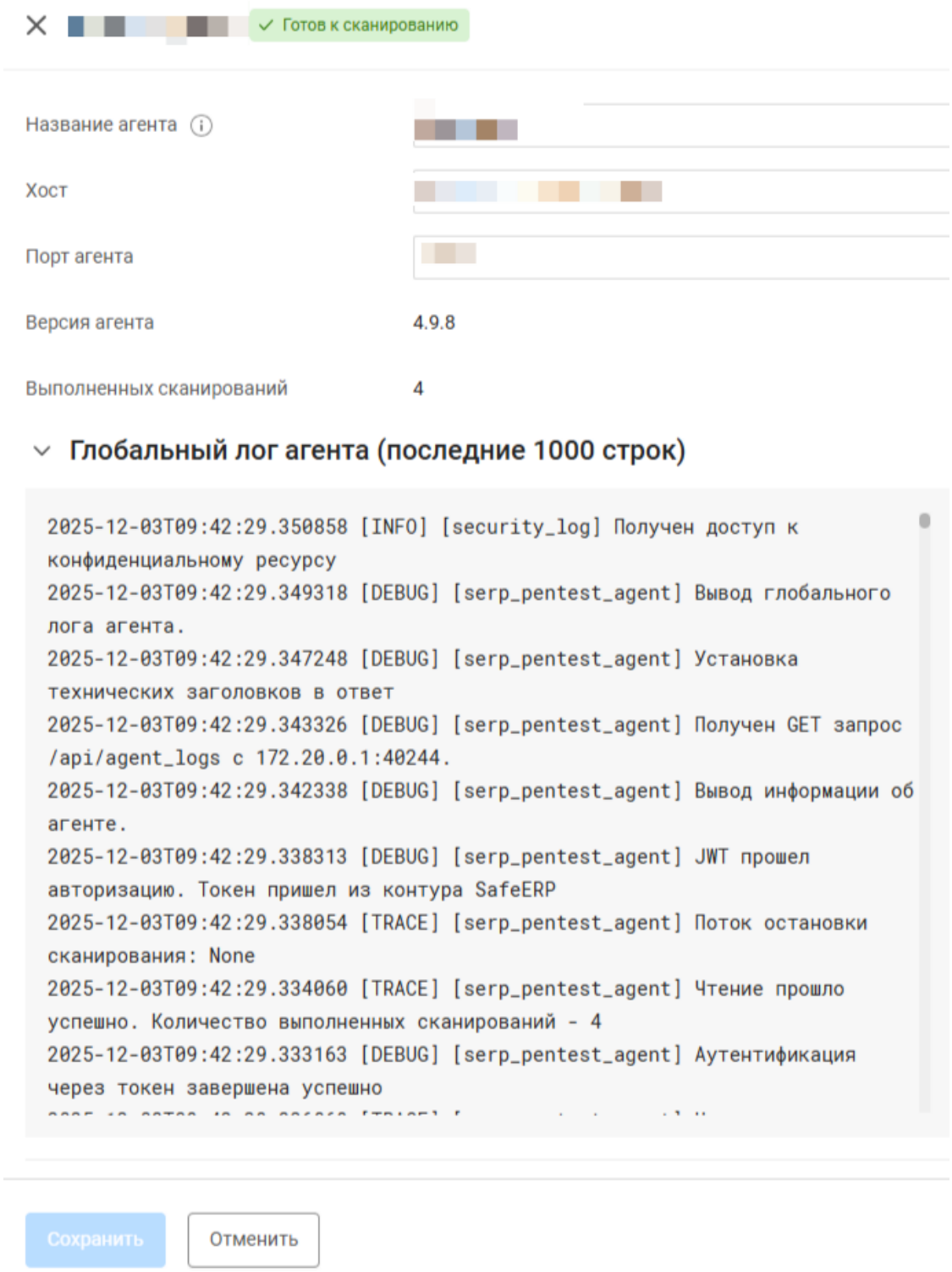


Рисунок 57 – Подробный лог агента

4.3.2.4 Скачивание лога агента

Для скачивания лога агента необходимо выполнить следующие действия:

1) Выбрать агент.
2) Нажать кнопку *«Скачать»* в окне просмотра данных агента (см. рис. 56).

4.3.2.5 Удаление агента

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

4.4 Раздел «Цели сканирования»

Раздел «Цели сканирования» предназначен для ведения целей сканирования, а также для ведения источников.
Основная рабочая область представлена на рис. 58.

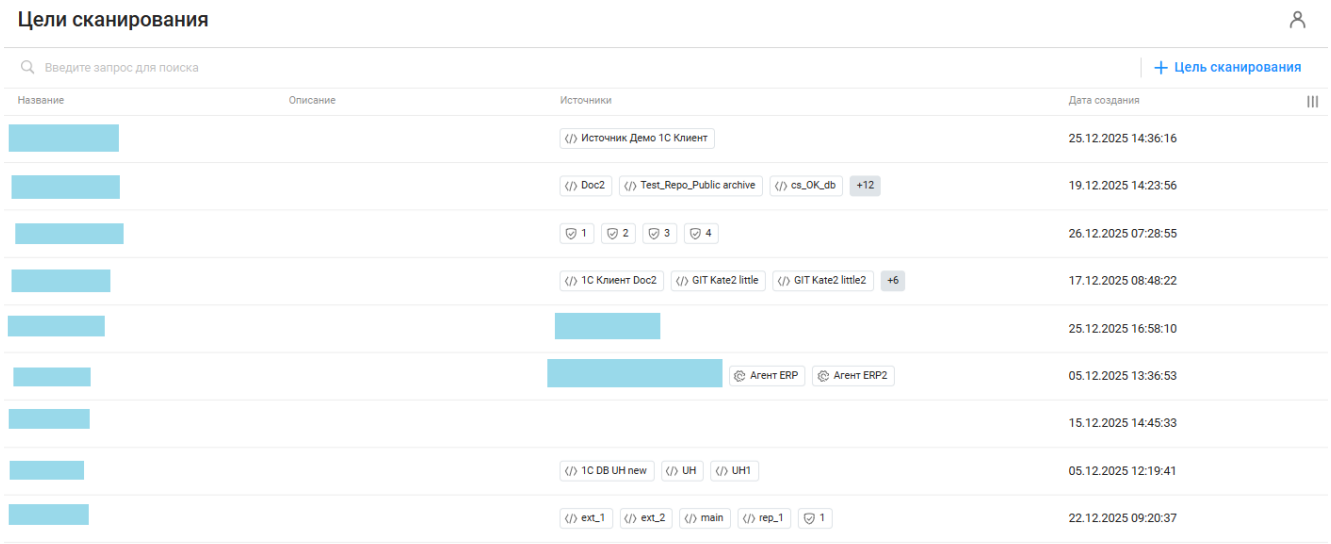


Рисунок 58 – Основная рабочая область раздела «Цели сканирования»

4.4.1 Добавление цели сканирования

Для добавления цели сканирования необходимо выполнить следующие действия:

1) Нажать кнопку *«+Цель сканирования»* (рис. 58).
2) Заполнить поля «Название», «Описание» (рис. 59).

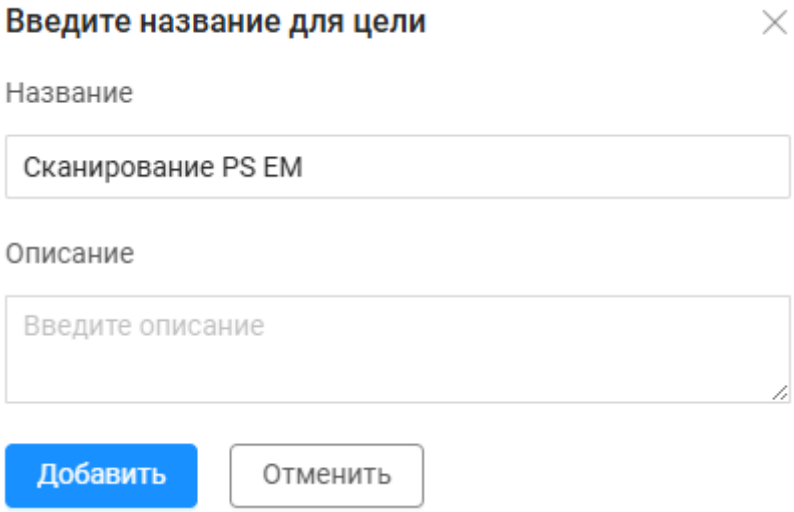


Рисунок 59 – Добавление цели сканирования

3) Нажать кнопку *«Добавить»* (рис. 59).

4.4.2 Редактирование цели сканирования

Для редактирования цели сканирования необходимо выполнить следующие действия:

1) Выбрать цель из списка (рис. 58).
2) Внести изменения (название, описание).
3) Нажать кнопку *«Сохранить»* (рис. 58).

4.4.3 Удаление целей сканирований

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

4.4.4 Источники

4.4.4.1 Источники для раздела «DAST»

Добавление источника

Для добавления источника необходимо выполнить следующие действия:

1) Создать цель сканирования согласно пункту 4.4.1 или выбрать из списка.
2) Нажать кнопку *«+Добавить источник»*.
3) Выбрать тип анализа «DAST анализ».
4) Заполнить необходимые поля (рис. 60). Выбрать способ аутентификации, заполнить необходимые поля (рис. 60, 61, 62)
5) Нажать кнопку *«Добавить»* (см. рис. 60, 61, 62).

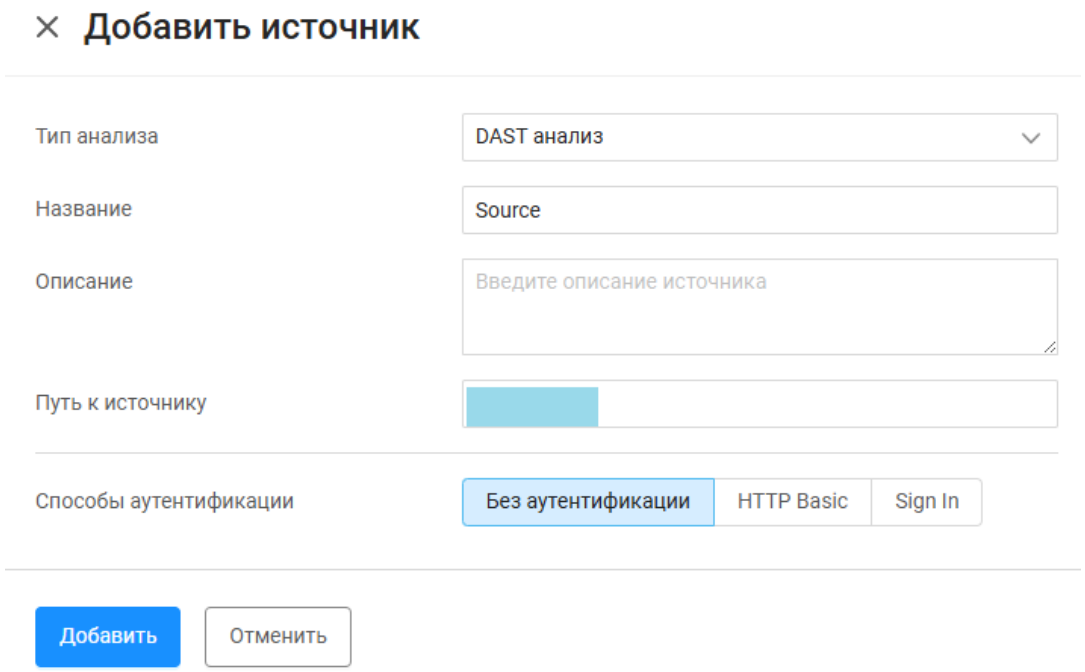


Рисунок 60 – Добавление источника для раздела «DAST» без аутентификации

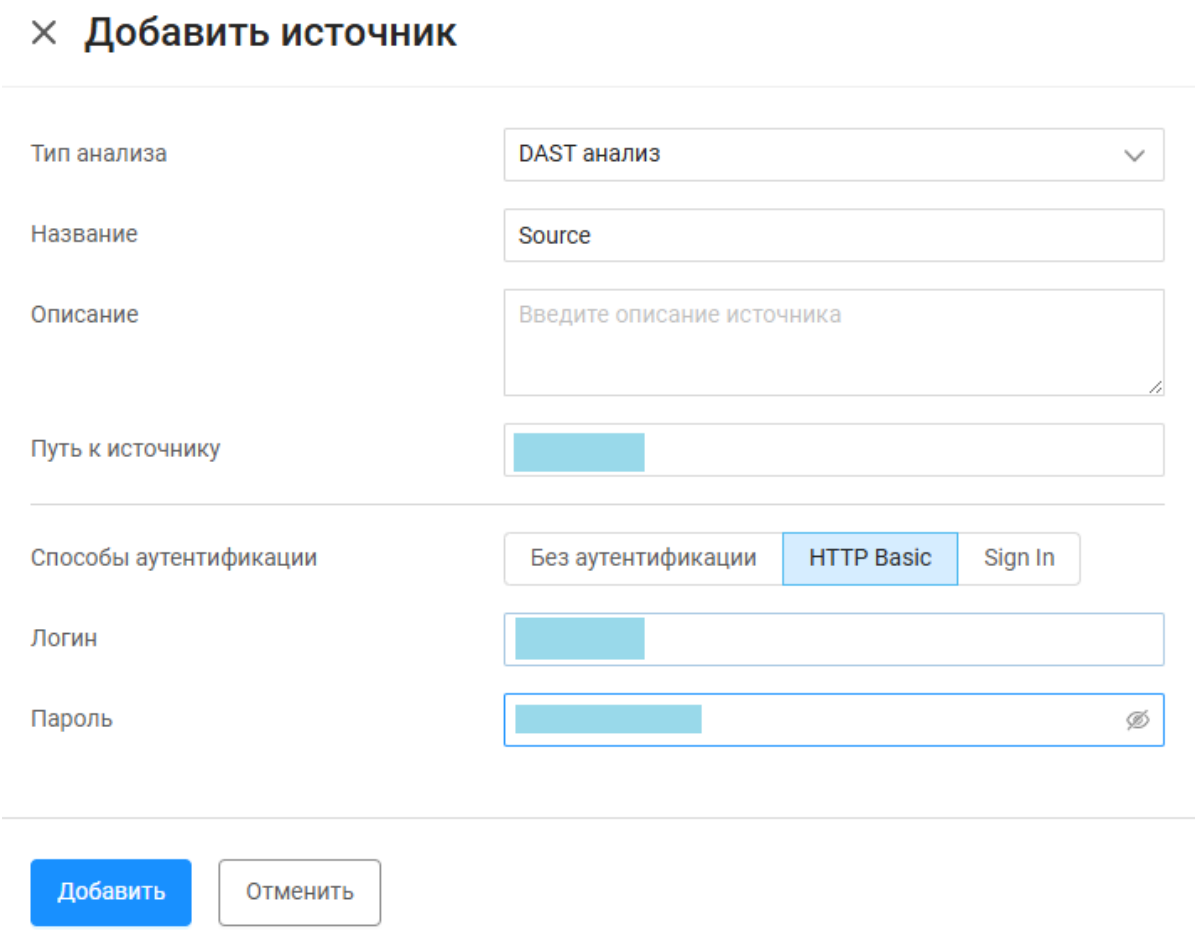


Рисунок 61 – Добавление источника для раздела «DAST» с аутентификацией типа http basic

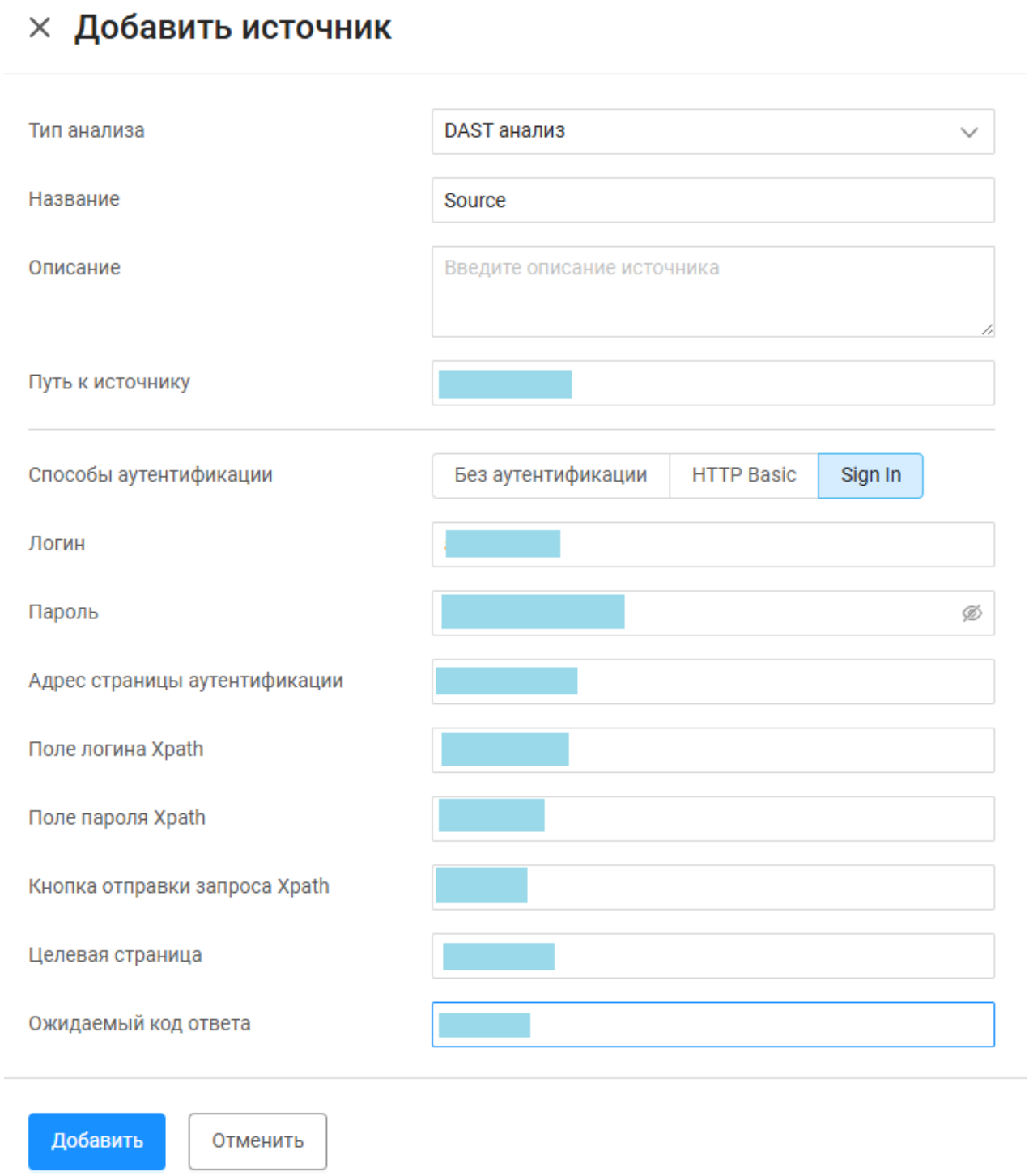


Рисунок 62 – Добавление источника для раздела «DAST» с аутентификацией типа sign in

Примечание. Для источников с аутентификацией типа sign in необходимо заполнить следующие поля:

- «Логин» – указывается логин, под которым выполняется процесс аутентификации;
- поле «Пароль» – указывается пароль, под которым выполняется процесс аутентификации;
- «Адрес страницы аутентификации» – указывается URL путь до веб-страницы, где

выполняется аутентификация;
- «Поле логина Xpath» – указывается Xpath поля, где выполняется ввод логина;
- «Поле пароля Xpath» – указывается Xpath поля, где выполняется ввод пароля;
- «Поле кнопка отправки запроса Xpath» – указывается Xpath кнопки, которая выполняет отправку запроса при нажатии;
- «Целевая страница» – указывается URL путь до веб-страницы, куда идет перенаправления после аутентификации. Поле является необязательным для заполнения.
- «Ожидаемый код ответа» – указывается HTTP код ответа, ожидаемый при успешной аутентификации. Поле является необязательным для заполнения.

Редактирование источника

Примечание. Если у источника есть поле «Пароль», то оно обязательно для заполнения при редактировании. Без указания пароля кнопка *«Редактировать»* будет внедоступна. Для редактирования источника необходимо выполнить следующие действия:

1) Выбрать цели сканирования из списка (рис. 58).
2) Выбрать источник типа анализа «DAST» из списка (рис. 63).

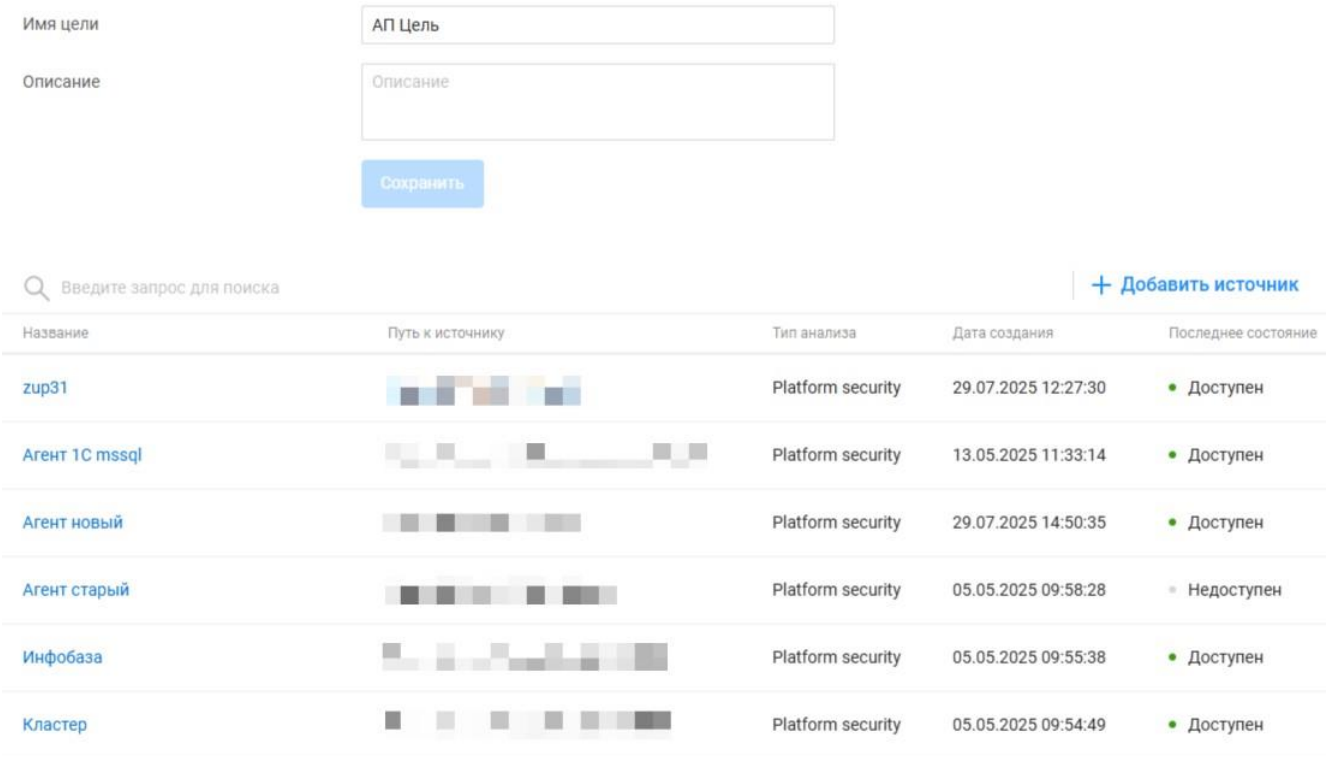


Рисунок 63 – Список источников

3) Внести изменения в источник (название, описание, путь к источнику, логин, пароль). Нажать кнопку *«Сохранить»* (рис. 64).

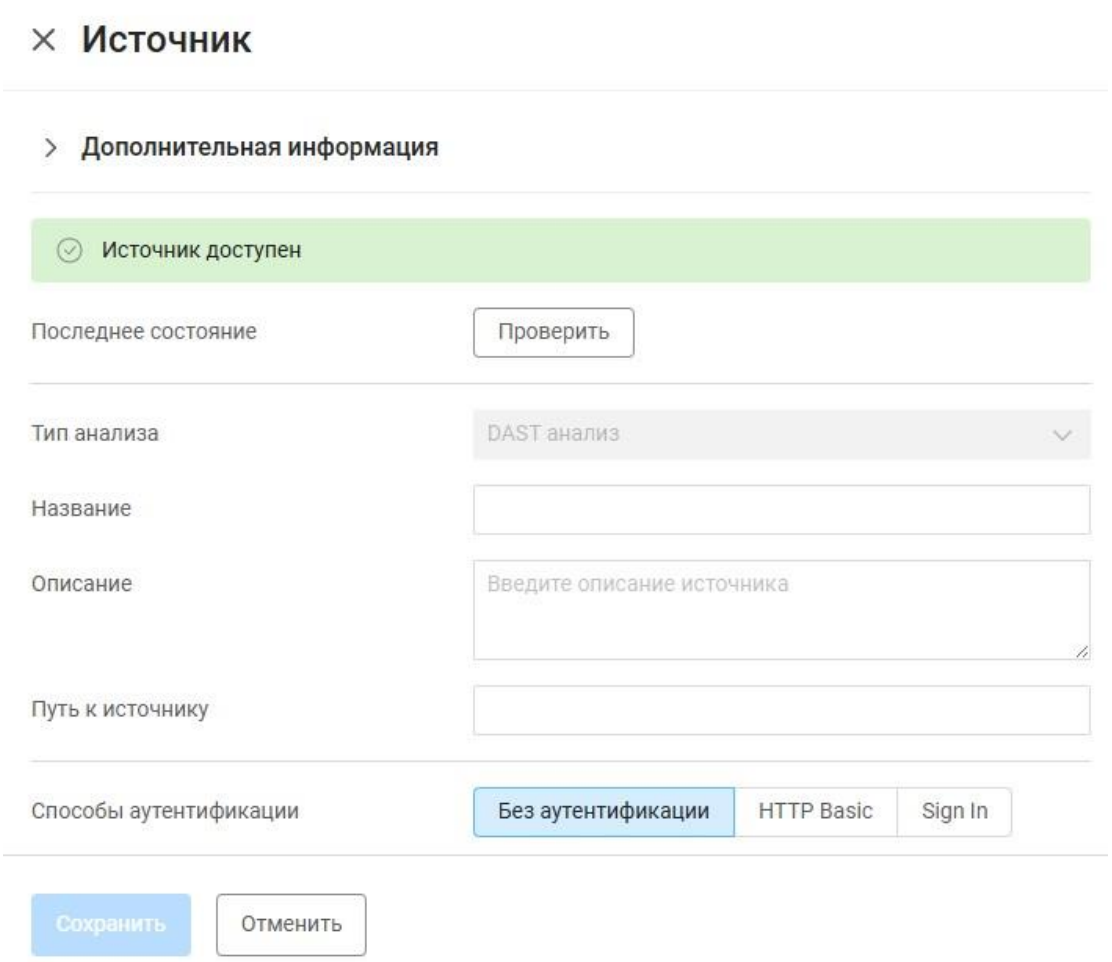


Рисунок 64 – Редактирование источника для раздела «DAST»

Удаление источника

Для удаления источника необходимо выполнить следующие действия:

1) Выбрать «Цель сканирования» из списка (рис. 58).
2) Нажать кнопку *«Удалить источник»* в контекстном меню в строке источника. Подтвердить действия.

4.4.4.2 Источники для раздела «Анализ платформы»

Добавление источника

В разделе «Анализ платформы» используются следующие типы источников:

- кластер;
- инфобаза;
- агент.

Для добавления источника с типом «Кластер» необходимо выполнить следующие действия:

1) Выбрать цель сканирования из списка.
2) Нажать кнопку *«+Добавить источник»*, выбрать тип анализа «Анализ

платформы», заполнить поля «Название», «Описание».

3) Выбрать тип источника «Кластер». Заполнить поля «Адрес центрального сервера» и «Порт» (рис. 65).

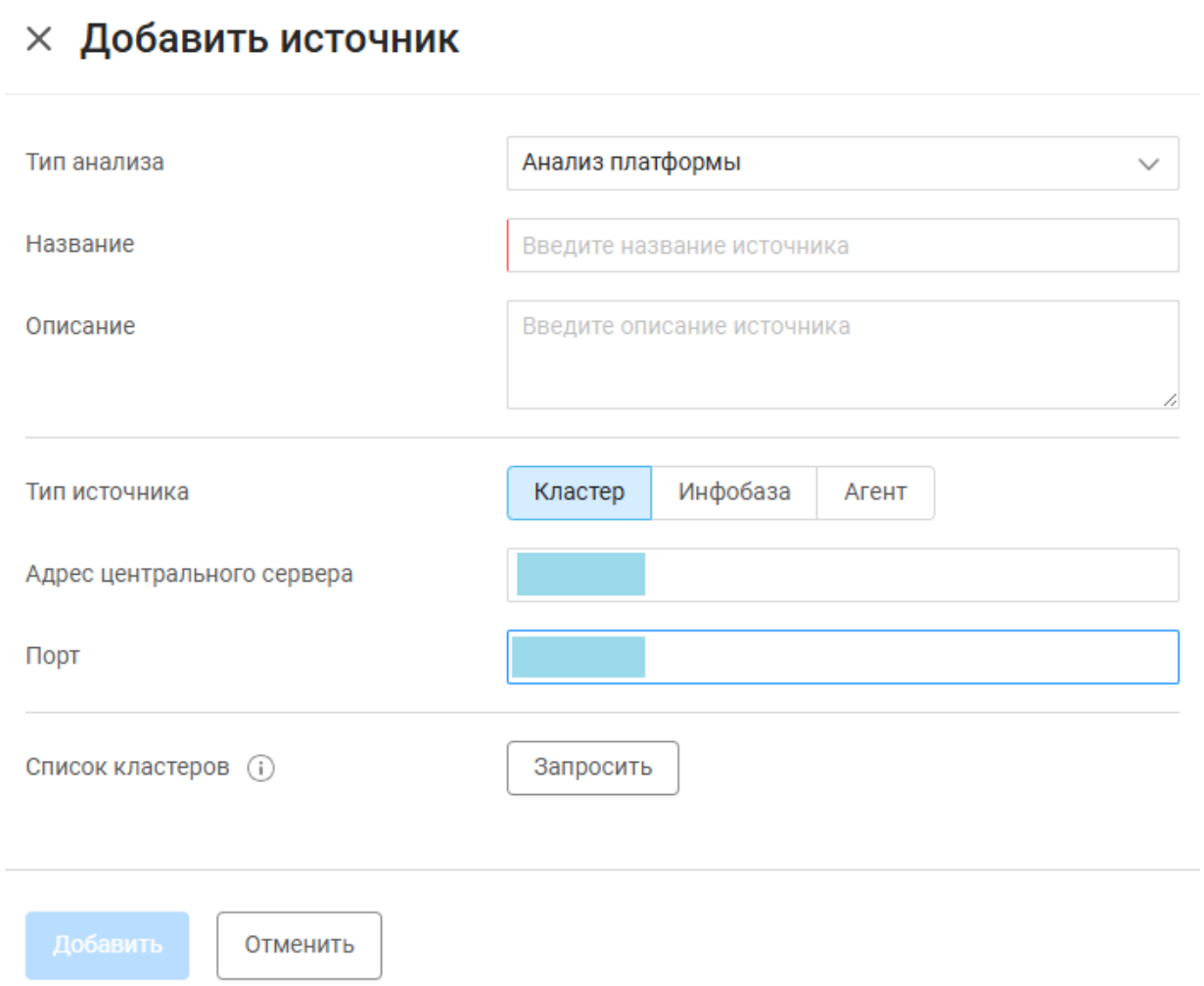


Рисунок 65 – Добавление источника типа «Кластер»

4) Нажать кнопку *«Запросить»*, выбрать кластер и указать данные пользователя, имеющего доступ к кластеру.
5) Нажать кнопку *«Добавить».*

Примечания:

1. В поле «Адрес центрального сервера» необходимо ввести IP-адрес кластера.
2. В поле «Порт» необходимо ввести номер порта в диапазоне с 1 по 65535.

Для добавления источника с типом «Инфобаза» необходимо выполнить следующие действия:

1) Выбрать цель сканирования из списка.
2) Нажать кнопку *«+Добавить источник»*, выбрать тип анализа «Анализ платформы», заполнить поля «Название», «Описание».
3) Выбрать тип источника «Инфобаза». Заполнить поля «Адрес центрального сервера» и «Порт» (рис. 65, 66).

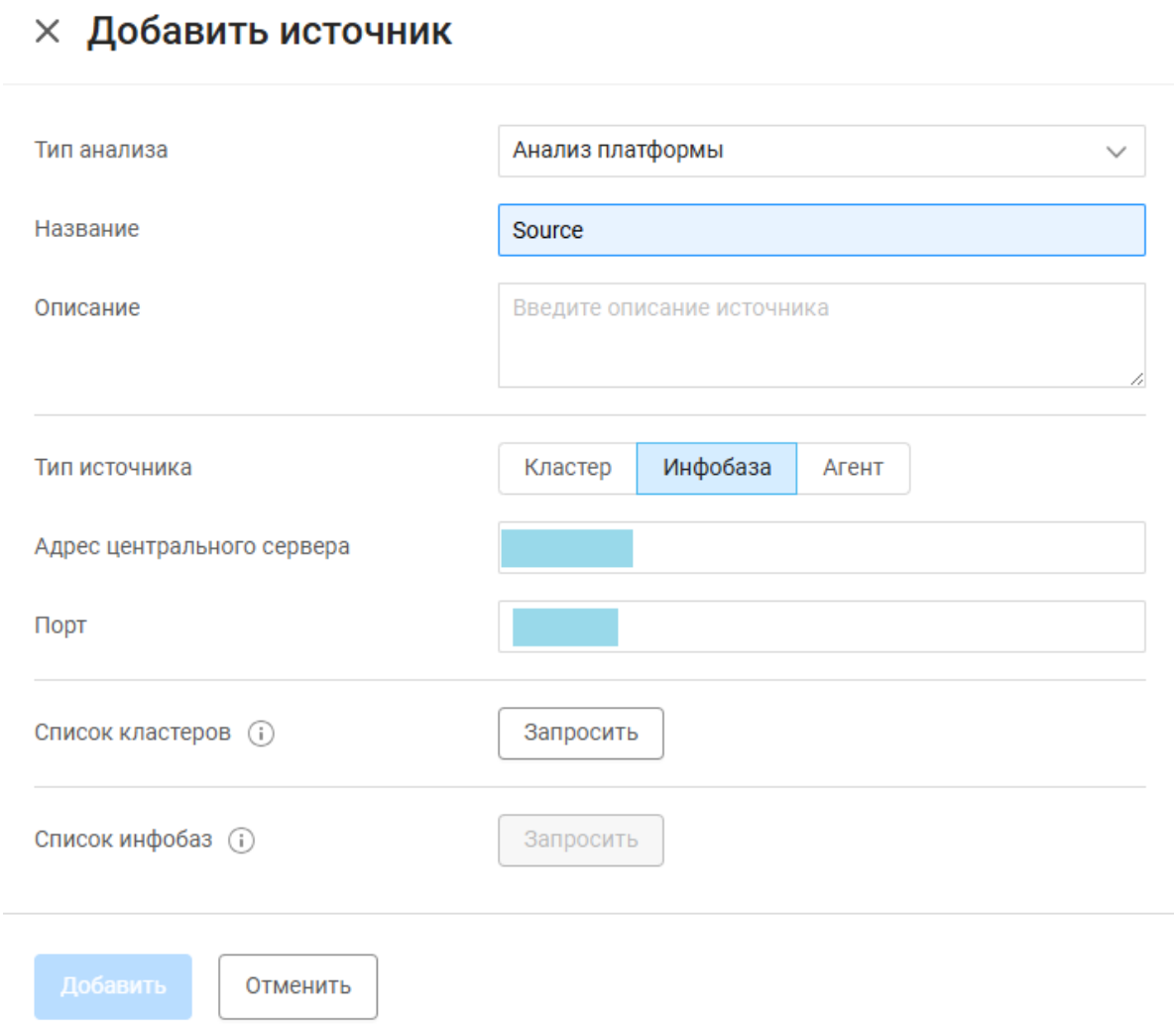


Рисунок 66 – Добавление источника типа «Инфобаза»

4) Нажать кнопку *«Запросить»* в разделе списка кластеров, выбрать кластер и указать данные пользователя, имеющего доступ к кластеру.
5) Нажать кнопку *«Запросить»* в разделе списка инфобаз, выбрать инфобазу и указать данные пользователя, имеющего доступ к инфобазе.
6) Нажать кнопку *«Добавить».*

Примечания:

1. В поле «Адрес центрального сервера» необходимо ввести IP-адрес кластера.
2. В поле «Порт» необходимо ввести номер порта в диапазоне с 1 по 65535.

Для добавления источника с типом «Агент» необходимо выполнить следующие действия:

1) Выбрать цель сканирования из списка.
2) Нажать кнопку *«+Добавить источник»*, выбрать тип анализа «Анализ платформы», заполнить поля «Название», «Описание».
3) Выбрать тип источника «Агент». Заполнить поля «Путь публикации конфигурации», «Имя пользователя инфобазы», «Пароль пользователя

инфобазы» (рис. 67).

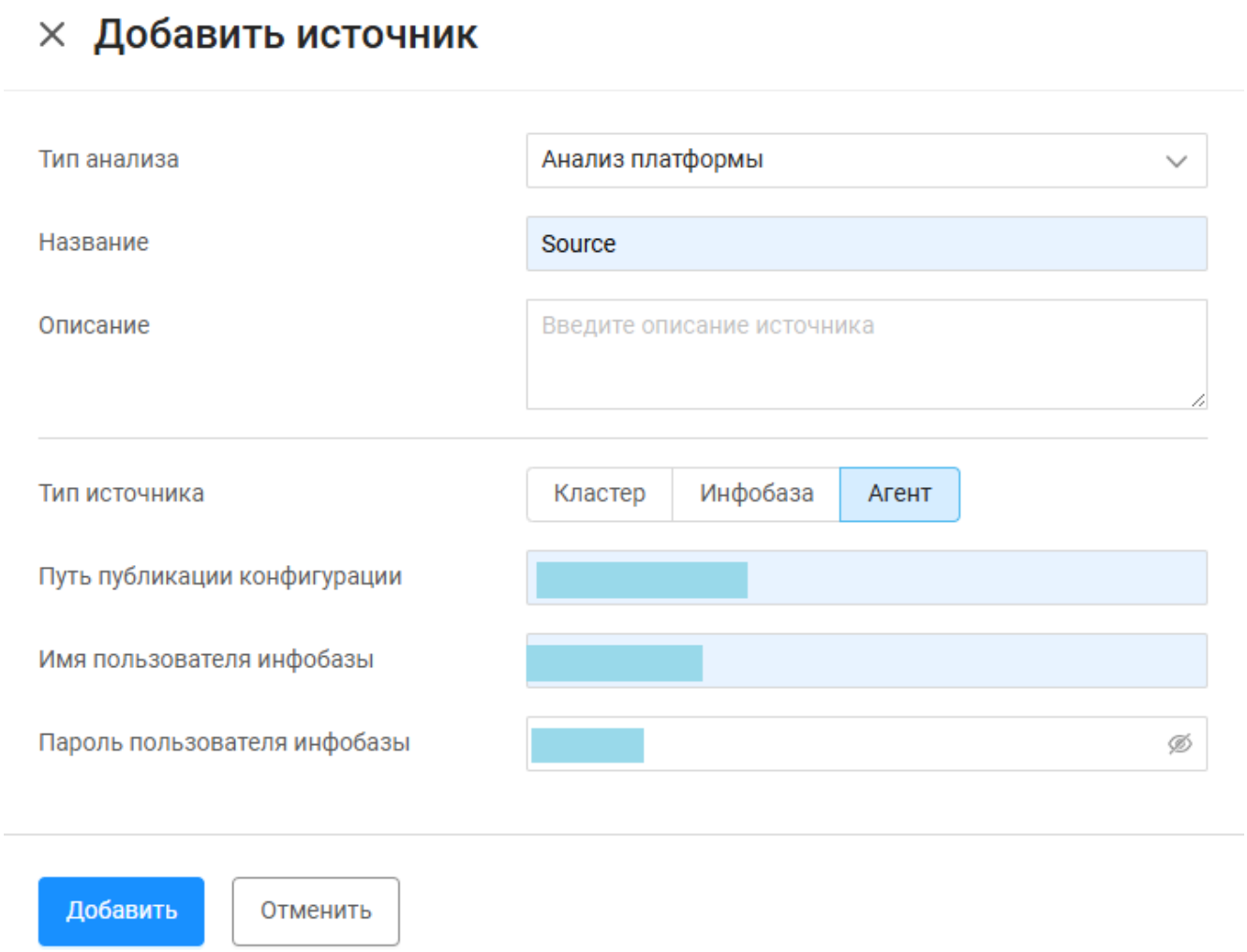


Рисунок 67 – Добавление источника типа «Агент»

4) В поле «Путь публикации конфигурации» необходимо указать путь к конфигурации. Путь выглядит следующим образом:
<protocol>://<host _name>/<project_name>/ и состоит из:
   - protocol – вид протокола. Принимает значения https или http;
   - host_name – имя сервера;
   - project_name – адрес репозитория.
5) В поле «Имя пользователя инфобазы» необходимо указать логин пользователя инфобазы.
6) В поле «Пароль пользователя инфобазы» необходимо указать пароль пользователя, проверяемой инфобазы.

Примечание. Если публикация работает по протоколу https, перед подключением необходимо добавить публичный ssl-сертификат в каталог $HOST_HOMEDIR/target_certs на сервере, где развернут ПК «SAFEERP EM», и перезапустить контейнеры командой docker-compose down && docker-compose up -d

Редактирование источника

Для редактирования источника необходимо выполнить следующие действия:

1) Выбрать цель сканирования из списка (рис. 58)
2) Выбрать источник из списка (рис. 63).
3) Внести изменения (название, описание, данные источника) (рис. 68).

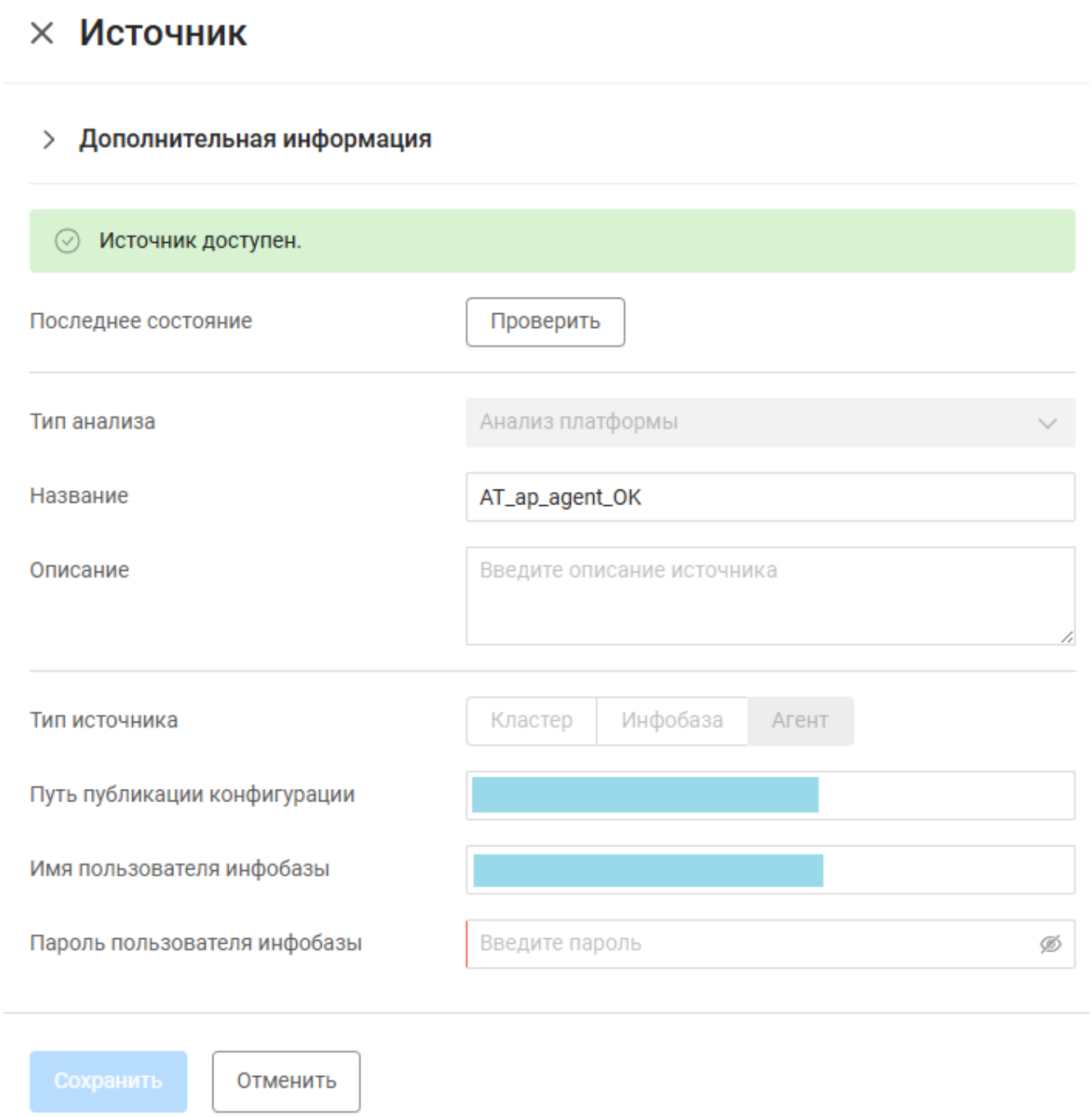


Рисунок 68 – Редактирование источника для раздела «Анализ платформы»

4) Нажать кнопку *«Сохранить»* (см. рис. 68).

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.

4.4.4.3 Источники для раздела «Pentest»

Добавление источника

Для добавления источника необходимо выполнить следующие действия:

1) Выбрать цель сканирования из списка или создать новую.
2) Нажать кнопку *«+Добавить источник»*. Выбрать тип анализа «Pentest» из выпадающего списка.
3) Заполнить необходимые поля (рис. 69).

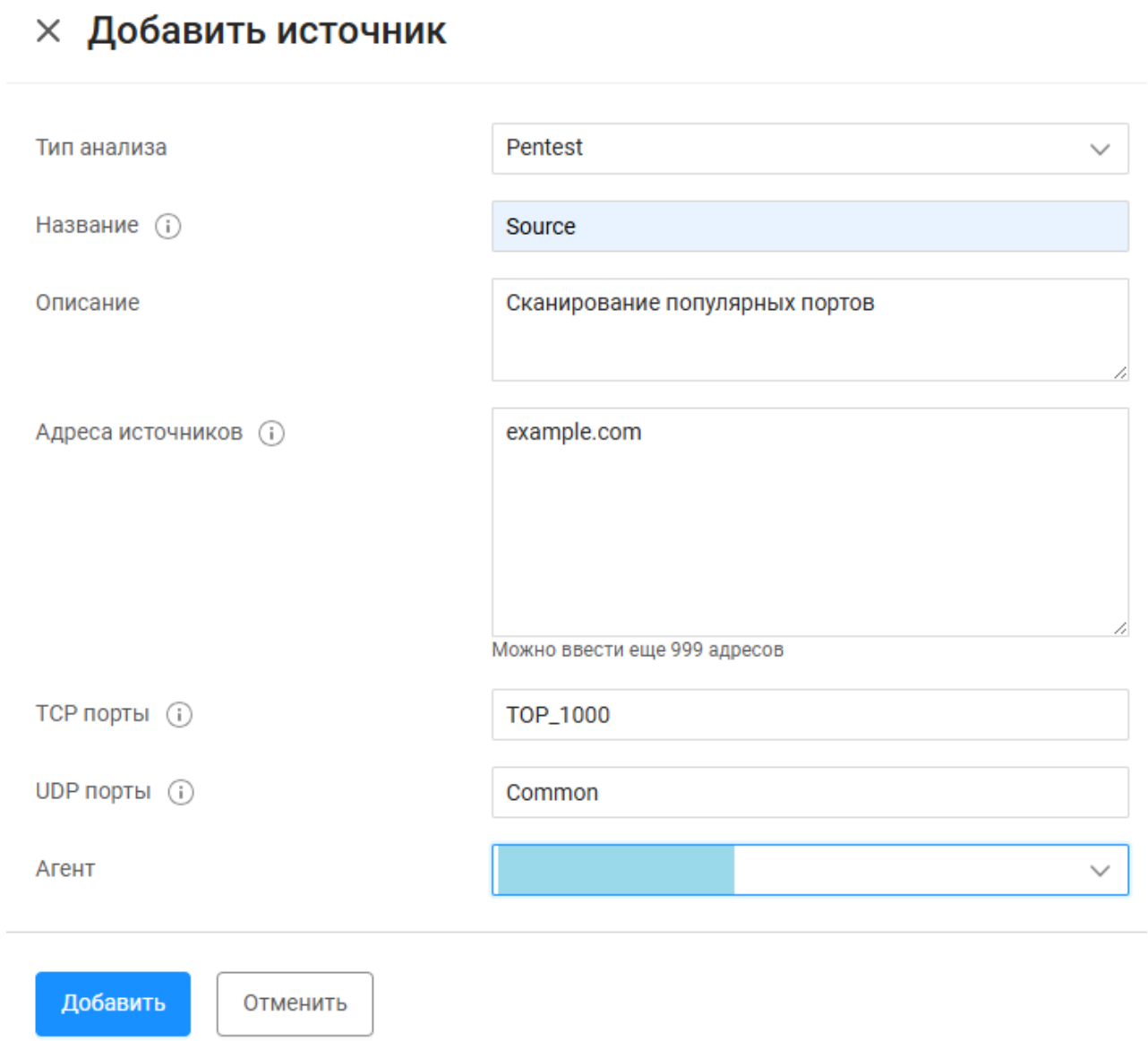


Рисунок 69 – Добавление источника типа «Pentest»

4) Нажать кнопку *«Добавить».*

Примечания:

1. В поле «TCP порты» должны быть указаны через запятую без пробелов. Можно указывать порты числами (1337) и диапазонами (1-4000). Также можно использовать ключевые слова: «ALL» (1-65535), «COMMON» (несколько самых популярных TCP-портов), «TOP_1000» (1 000 самых популярных TCP-портов), «SAP» (характерные для SAP TCP-порты). Только уникальные и валидные порты будут просканированы. Например: «1,80,234-344,COMMON,SAP».
2. В поле «UDP порты» Должны быть указаны через запятую без пробелов. Можно указывать порты числами (1337) и диапазонами (1-4000). Также можно использовать ключевые слова: «ALL» (1-65535), «COMMON» (несколько самых популярных UDP-портов), «TOP_1000» (1 000 самых популярных UDP-портов), «SAP» (характерные для SAP UDP-порты). Только уникальные и валидные порты будут просканированы. Например: «100,234-344,TOP_1000».
3. В поле «Адреса источников» должны быть указаны через запятую без пробелов. Можно указывать IP-адреса с использованием интервалов (1-244) и «*» (означает 0-255), а также доменное имя. Должна быть указана как минимум одна цель, максимум - 1000. Только уникальные и валидные цели будут просканированы. Например: «44.22.45.112,192.168.2-33.*, example.com».

Редактирование источника

Для редактирования источника необходимо выполнить следующие действия:

1) Выбрать источник из списка.
2) Внести изменения (название, описание, TCP порты, UDP порты, агент).

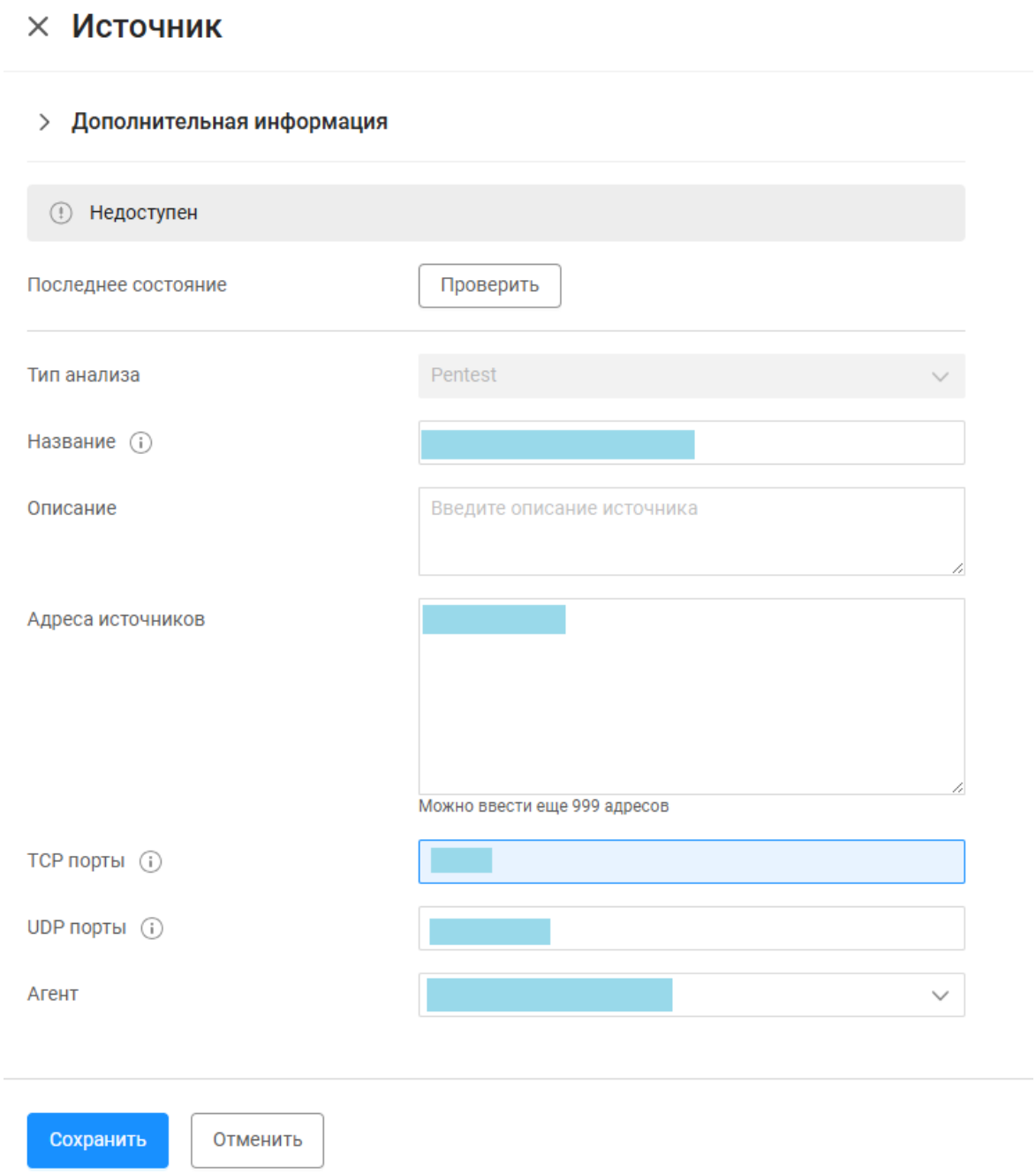


Рисунок 70 – Редактирование источника типа «Pentest»

3) Нажать кнопку *«Сохранить»* (рис. 70).

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.

4.5 Раздел «Настройки»

В разделе «Настройки» доступны следующие разделы:

- «Информация»;
- «Лицензия»;
- «Пользователи»;
- «БДУ»;
- «Журнал».

4.5.1 Подраздел «Информация»

В подразделе Информация пользователю доступен просмотр информации о ПК «SAFEERP PS EM», а также выгрузка архива с документацией.

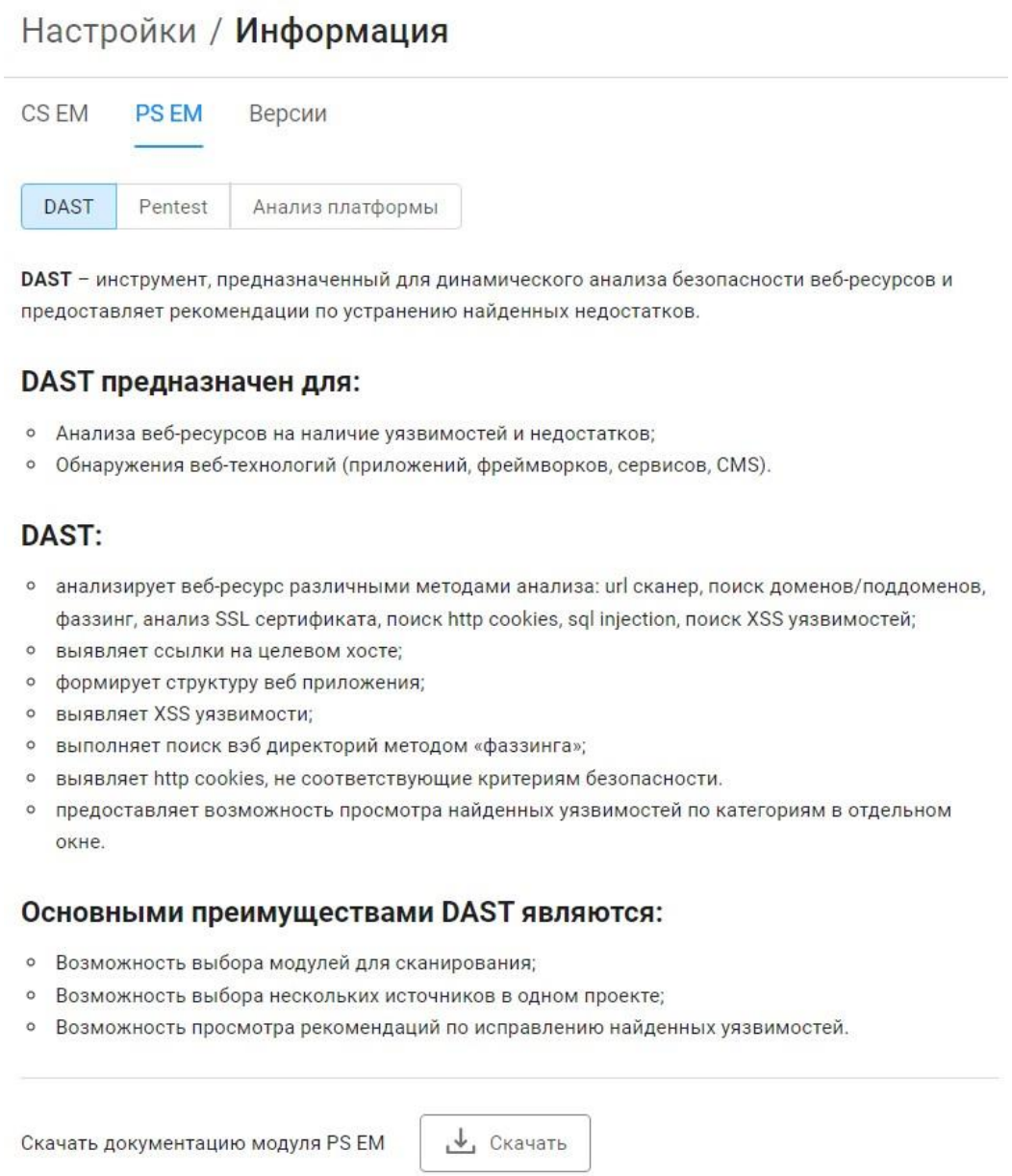


Рисунок 71 – Подраздел «Информация»

Для загрузки архива с документацией на локальную машину необходимо нажать кнопку *«Скачать»* (рис. 71).

4.5.2 Подраздел «Лицензия»

Доступ к ПК «SafeERP PS EM» определяются свойствами действующей лицензии. Лицензия содержит одно или несколько свойств. Свойства лицензии необходимо уточнить у поставщиков услуг.
Подробное описание свойств представлено в таблице 7.

Таблица 7 – 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 PS EM»

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

1. Область применения. Свойство применяется только к варианту исполнения ПК «SafeERP PS 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 PS 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 PS 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 PS EM» доступны следующие свойства:

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

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

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

4.5.2.1 Активация лицензии

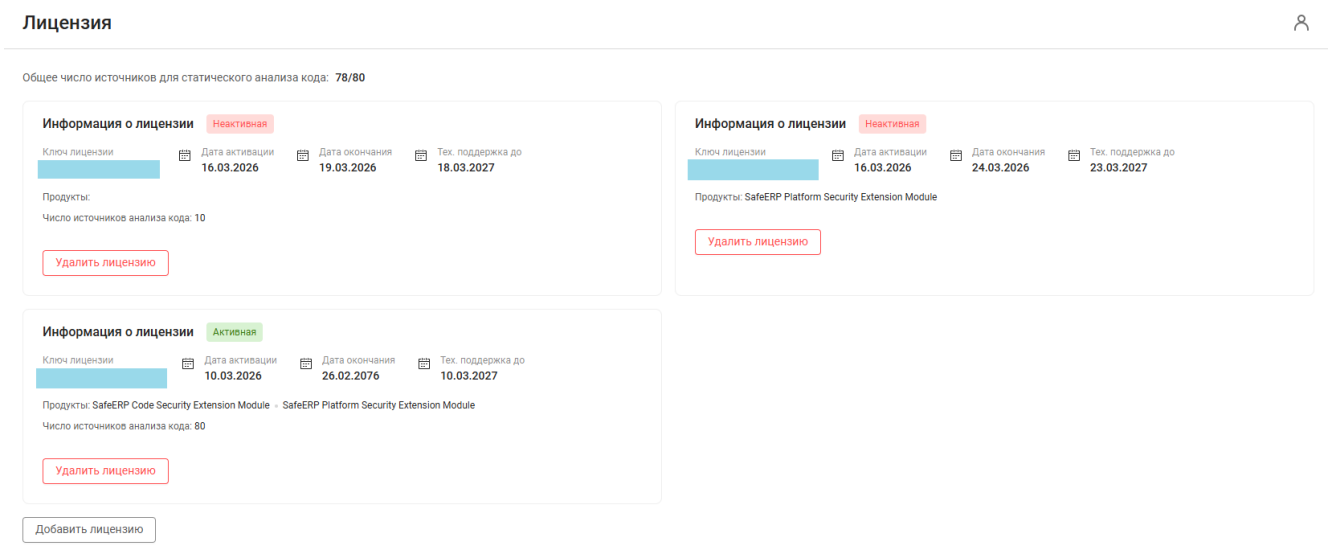


Рисунок 72 – Подраздел «Лицензии»

Для активации лицензии необходимо выполнить следующие действия:

1) Нажать кнопку *«Добавить лицензию»* (рис. 72).
2) Ввести ключ активации (предоставляется в комплекте поставки), адрес электронной почты. Нажать кнопку *«Сгенерировать запрос»* (рис. 73). Автоматически начнется процедура загрузки файла license_request формата json, который сохраняется в папку «Загрузки».

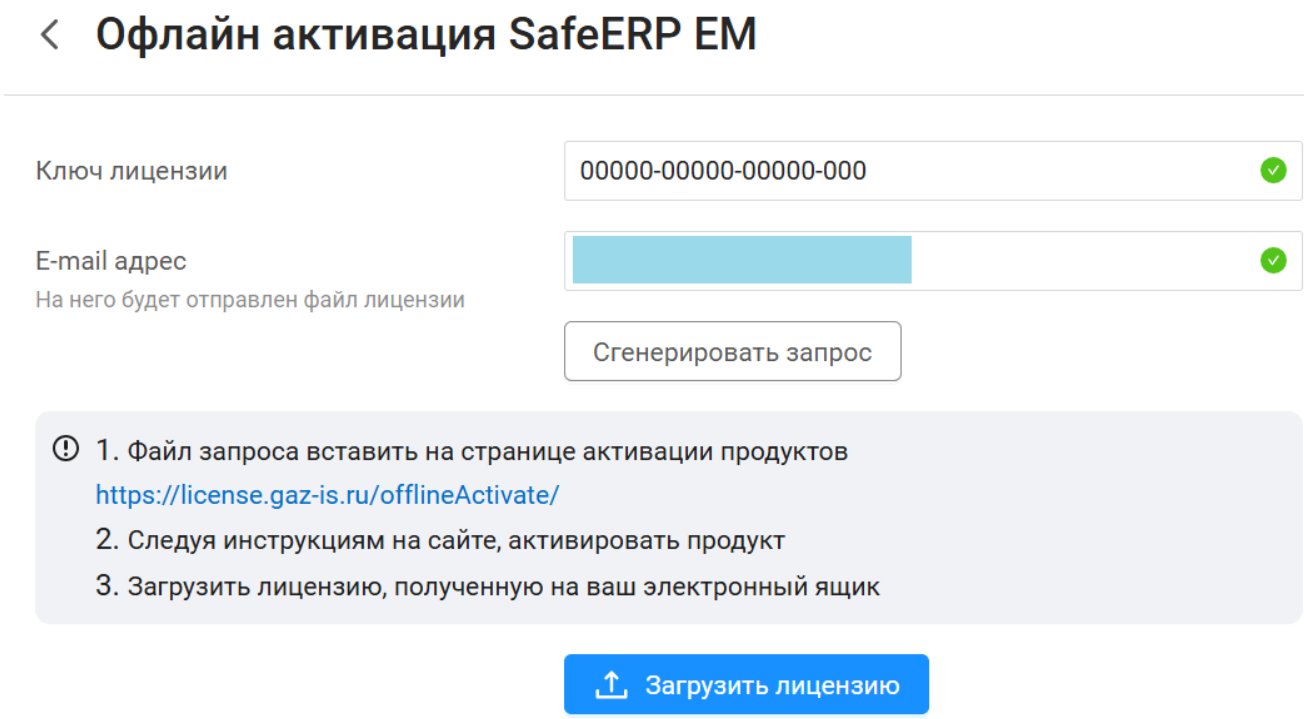


Рисунок 73 – Окно активации лицензии

3) Перейти по ссылке, которая указана в окне «Офлайн активация SAFEERP EM» (см. рис. 73). На сайте активации лицензии нажать кнопку *«Выберите файл»*, с помощью проводника выбрать файл, скачанный в пункте 2 (рис. 74).



Рисунок 74 – Получение файла лицензии

4) Ввести ключ лицензии из почтового уведомления (рис. 75) в окно офлайн-активации (рис. 76) и нажать кнопку *«Активировать»*.



Рисунок 75 – Ключ активации продукта, полученный по электронной почте

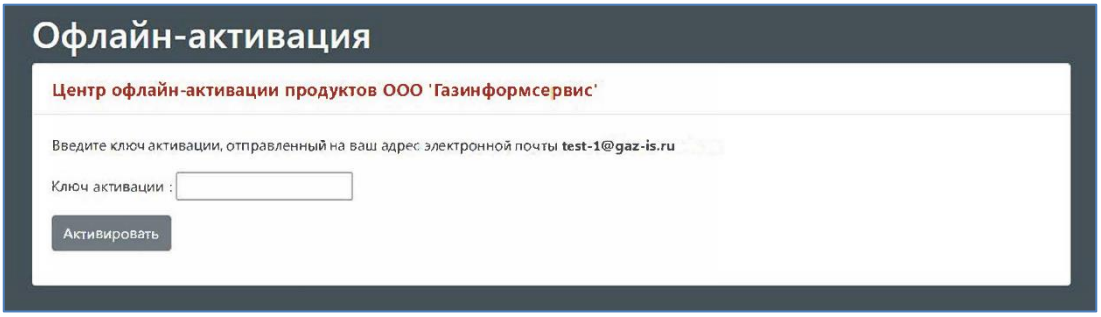


Рисунок 76 – Окно для ввода ключа лицензии

5) При успешной активации лицензии её можно сохранить в файл, нажав кнопку *«Сохранить в файл»* (рис. 77). На адрес электронной почты, указанный в пункте 2 поступит письмо, содержащее zip-архив с лицензией, идентичной данной (рис. 75).

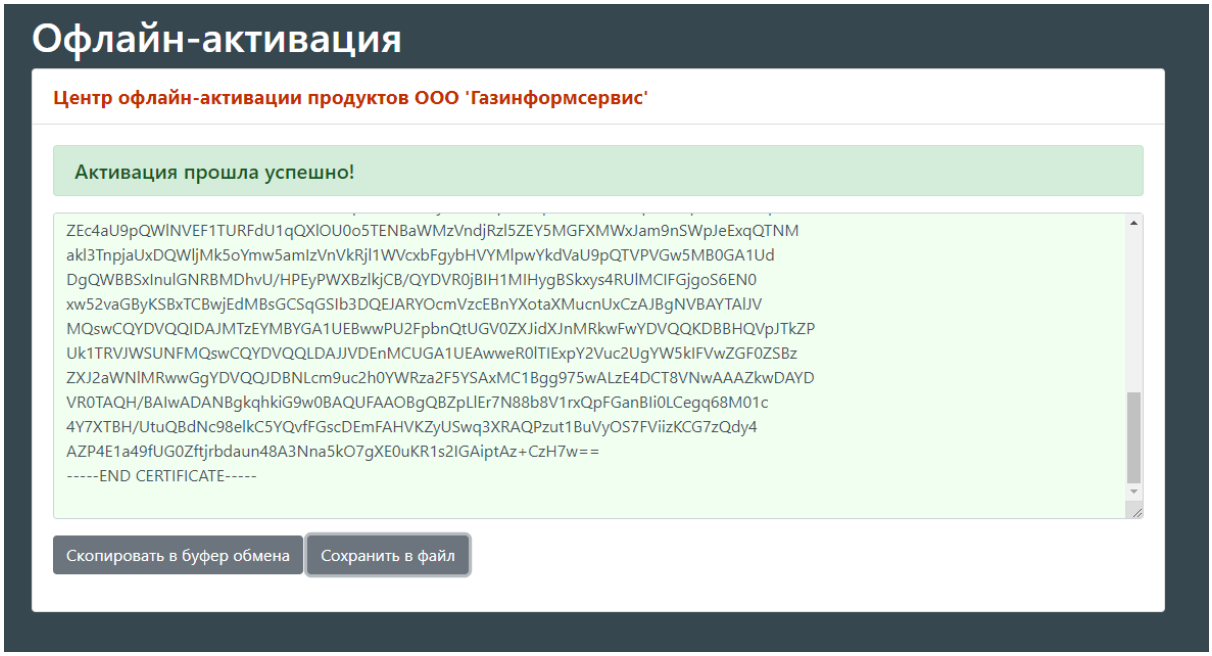


Рисунок 77 – Сообщение об успешной активации лицензии
с лицензией после успешной активации

6) В окне «Офлайн активация SAFEERP EM» (рис. 73) 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. 78.

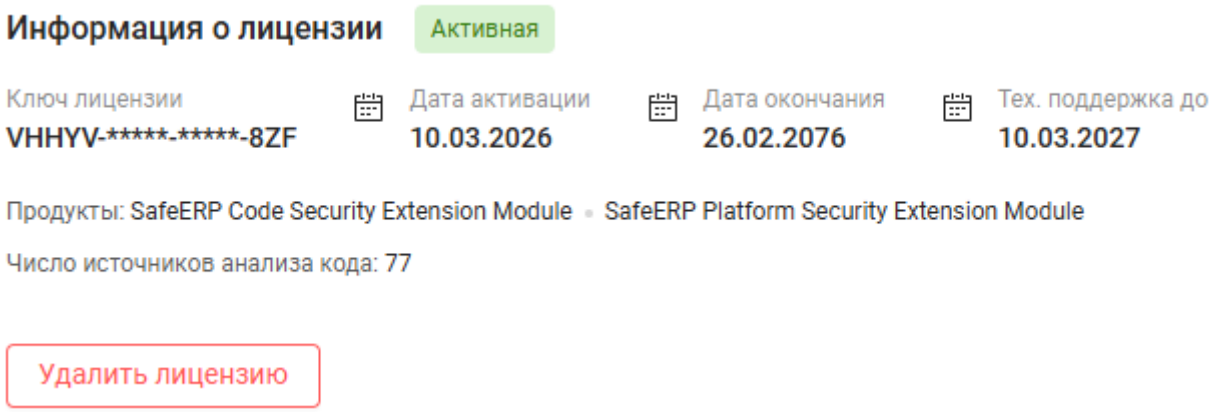


Рисунок 78 – Информации о лицензии

4.5.2.2 Обновление лицензии

Для обновления лицензии необходимо выполнить следующие действия:

1) Нажать кнопку *«Удалить лицензию»* в области лицензии (см. рис. 78).
2) Активировать новую лицензию согласно подпункту 4.5.2.1.

4.5.3 Подраздел «Пользователи»

В подразделе «Пользователи» администратору ПК «SAFEERP PS EM» предоставляется

возможность ведения пользователей ПК «SAFEERP PS EM».
Основная рабочая область представлена на рис. 79.

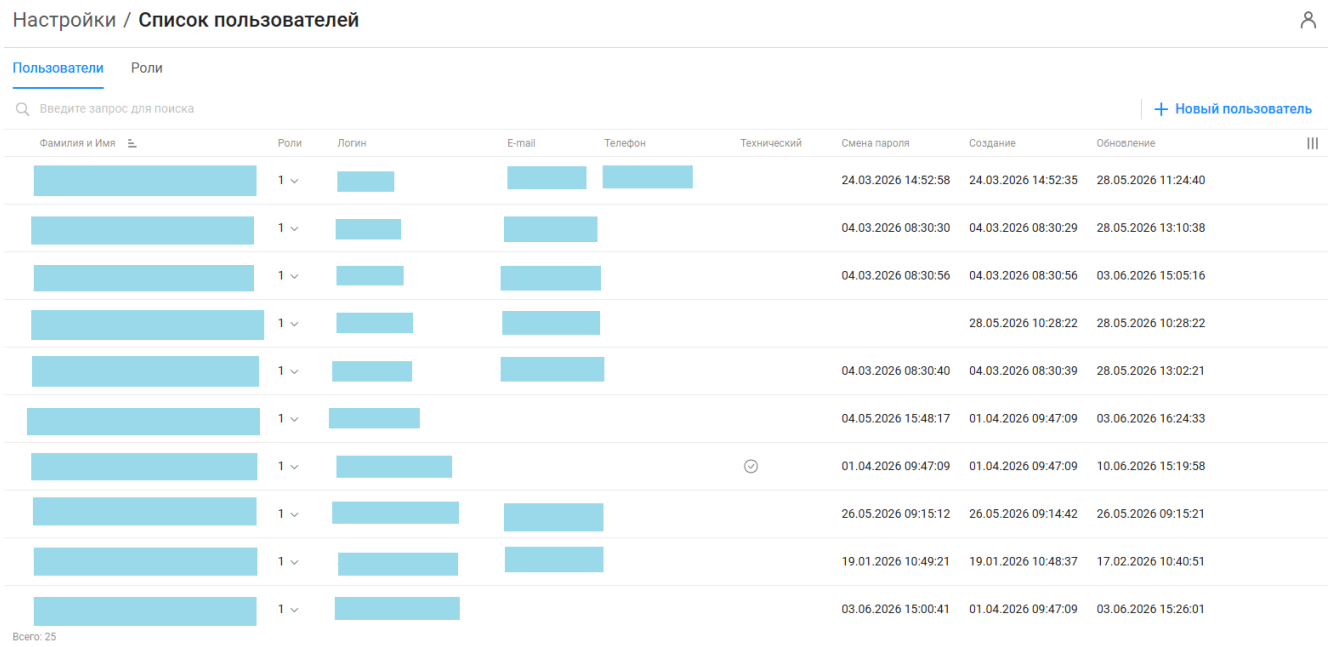


Рисунок 79 – Подраздел «Пользователи»

4.5.3.1 Создание учётной записи

В ПК «SAFEERP PS EM» доступно создание пользователей со следующими ролями:

- admin;
- security_admin.

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

1) Нажать кнопку *«+Новый пользователь»* (см. рис. 79).
2) Выбрать роль нового пользователя, заполнить необходимые поля.

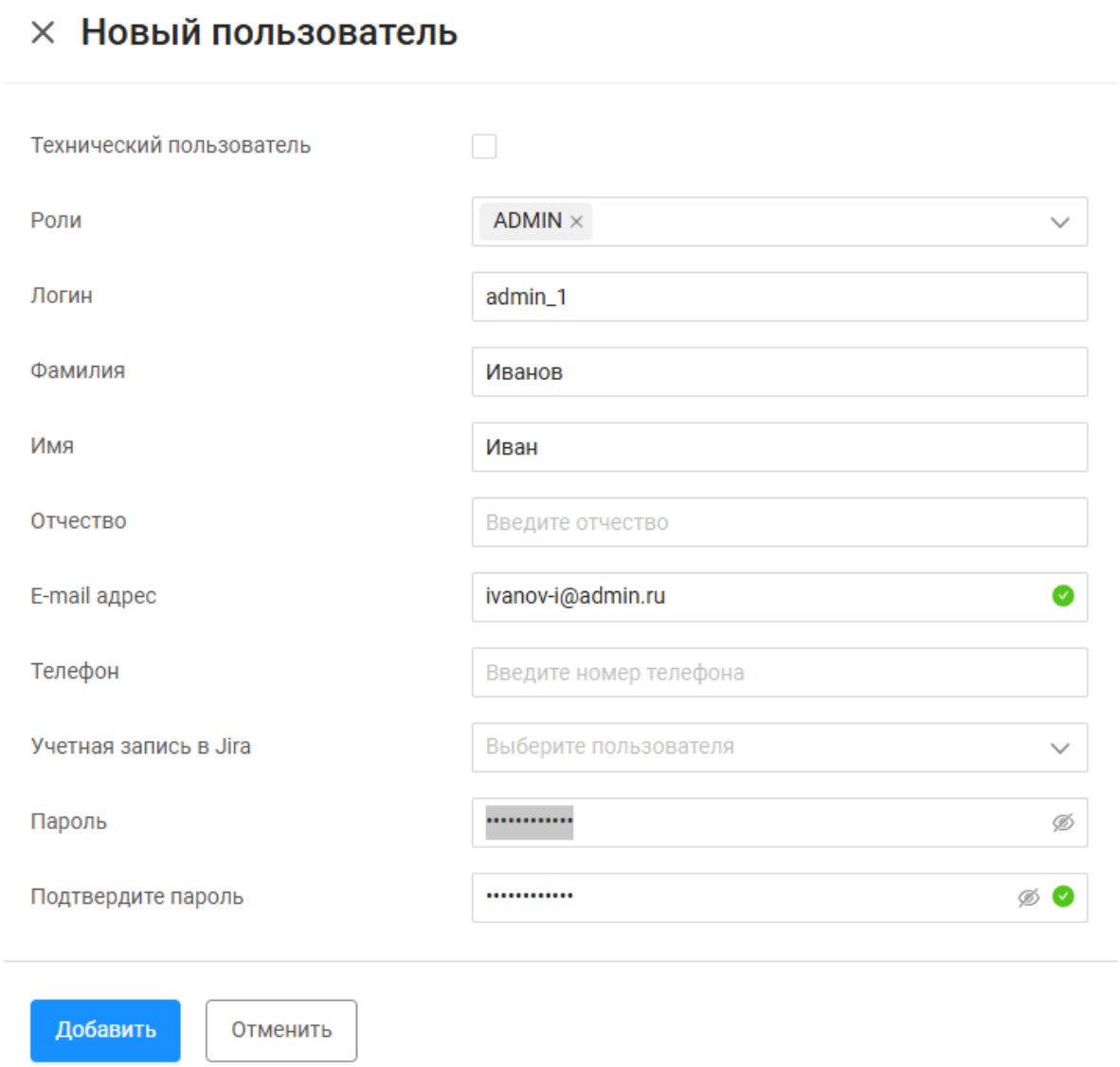


Рисунок 80 – Окно создания пользователя

3) Нажать кнопку *«Добавить»* (рис. 80).

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 4.5.3.7).
2. Техническому пользователю после создания не требуется менять пароль при первой авторизации, а также пароль не имеет срок действия.
3. После создания технического пользователь администратору будет недоступно снятие флага напротив элемента «Технический пользователь» при изменении учетной записи.

4.5.3.2 Изменение учётной записи

Доступно изменение следующих полей учётной записи (рис. 81):

— роли;
— имя, фамилия и отчество пользователя;
— e-mail адрес;
— телефон.

Для изменения УЗ необходимо выполнить следующие действия:

1) Выбрать вкладку «Пользователи» (см. рис. 79).
2) В открывшемся списке пользователей выбрать УЗ, которую необходимо изменить и нажать на неё левой кнопки мыши.
3) Нажать кнопку *«Сохранить»*.

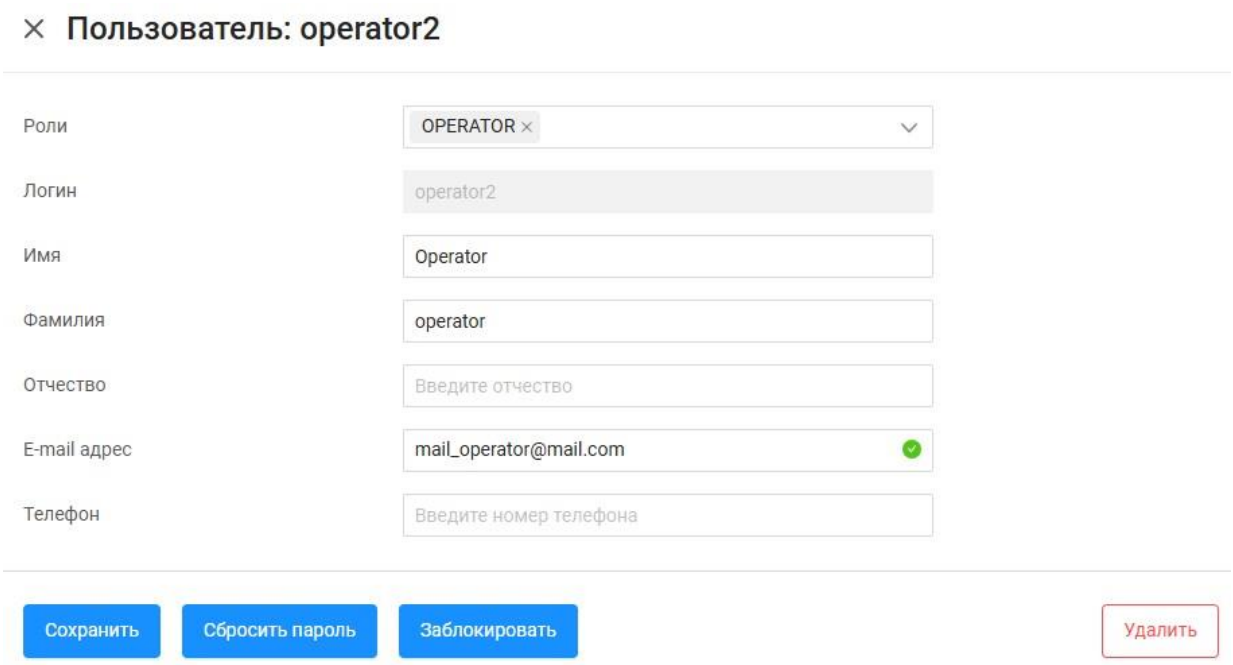


Рисунок 81 – Редактирование УЗ

4.5.3.3 Сброс пароля учётной записи

Для сброса пароля УЗ необходимо выполнить следующие действия:

1) Выбрать вкладку «Пользователи» (см. рис. 79).
2) В открывшемся списке пользователей выбрать УЗ, пароль которой необходимо сбросить, и нажать на неё левой кнопки мыши.
3) Нажать кнопку *«Сбросить пароль»* (см.рис. 81).
4) Ввести новый пароль и подтвердить его.

Примечание. После сброса пароля произойдёт выход из системы для соответствующего пользователя. Пользователь должен пройти процедуру смены пароля и авторизоваться с новым паролем.

4.5.3.4 Блокировка и разблокировка учётной записи

Для блокировки или разблокировки УЗ необходимо выполнить следующие действия:

1) Выбрать вкладку «Пользователи» (см. рис. 79).
2) Выбрать УЗ из списка пользователей УЗ, которую необходимо заблокировать или разблокировать, нажать на неё левой кнопки мыши.

3) Нажать кнопку *«Заблокировать»* (рис. 81) или *«Разблокировать»*, если соответствующая учётная запись была заблокирована ранее.

4.5.3.5 Удаление учётной записи

Для удаления УЗ необходимо выполнить следующие действия:

1) Выбрать вкладку «Пользователи» (см. рис. 79).
2) В открывшемся списке пользователей выбрать УЗ, которую необходимо удалить, и нажать на неё левой кнопки мыши.
3) Нажать кнопку *«Удалить»* (см. рис. 81).
4) Нажать кнопку Да в окне подтверждения (рис.82).

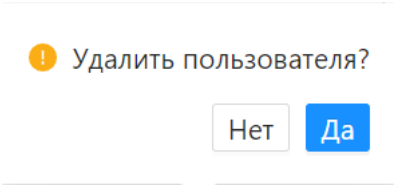


Рисунок 82 – Удаление УЗ

4.5.3.6 Роли

Роли в ПК «SAFEERP PS EM» присваиваются при создании нового пользователя (см. рис. 80)

В ПК «SAFEERP PS EM» по умолчанию существуют следующие роли (рис. 83):

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

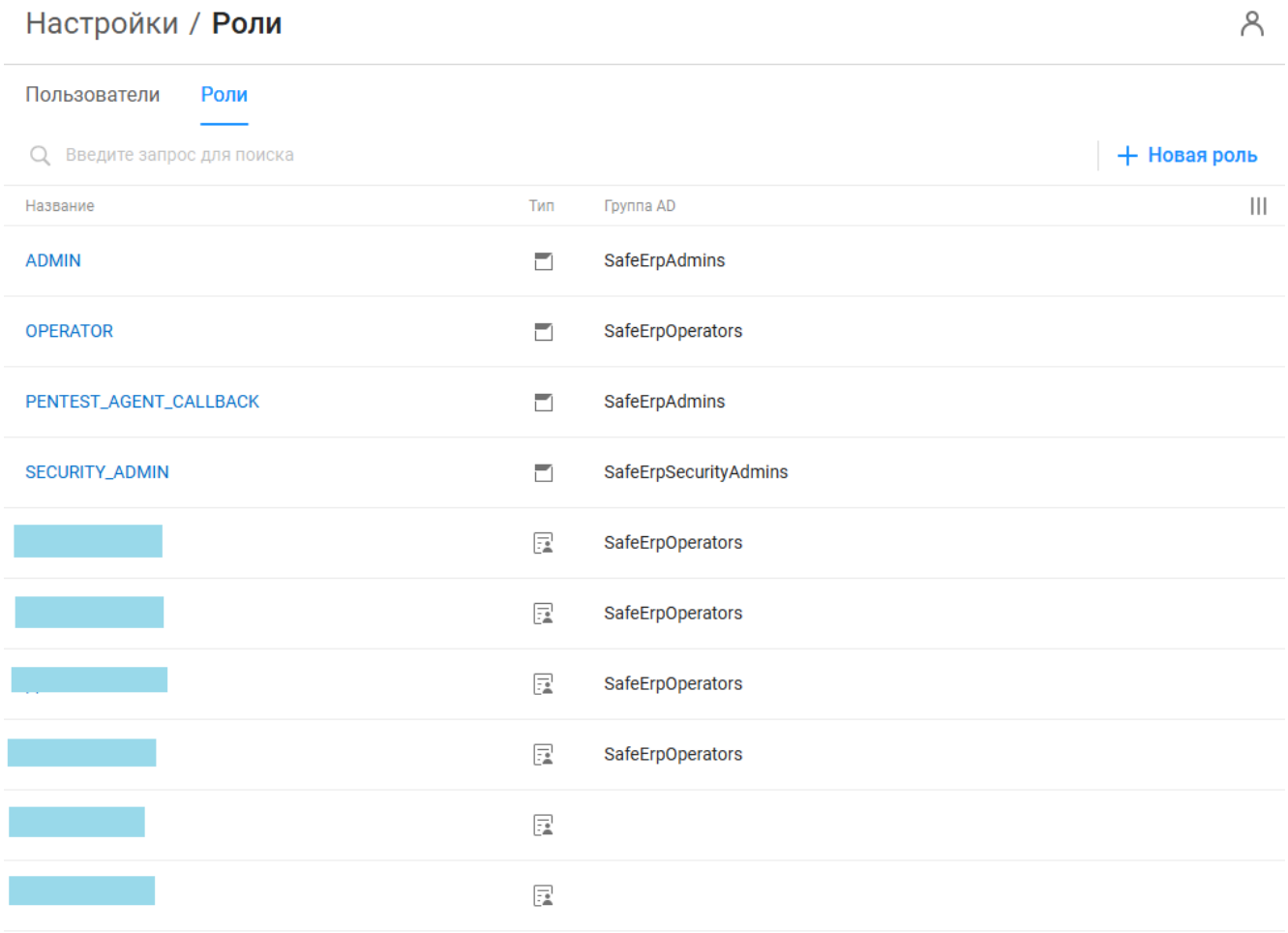


Рисунок 83 – Вкладка «Роли»

Роль ADMIN

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

Роль OPERATOR

Пользователи, которым присвоена роль OPERATOR, имеют ограниченный доступ к функциональности ПК «SAFEERP PS 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.

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).

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.

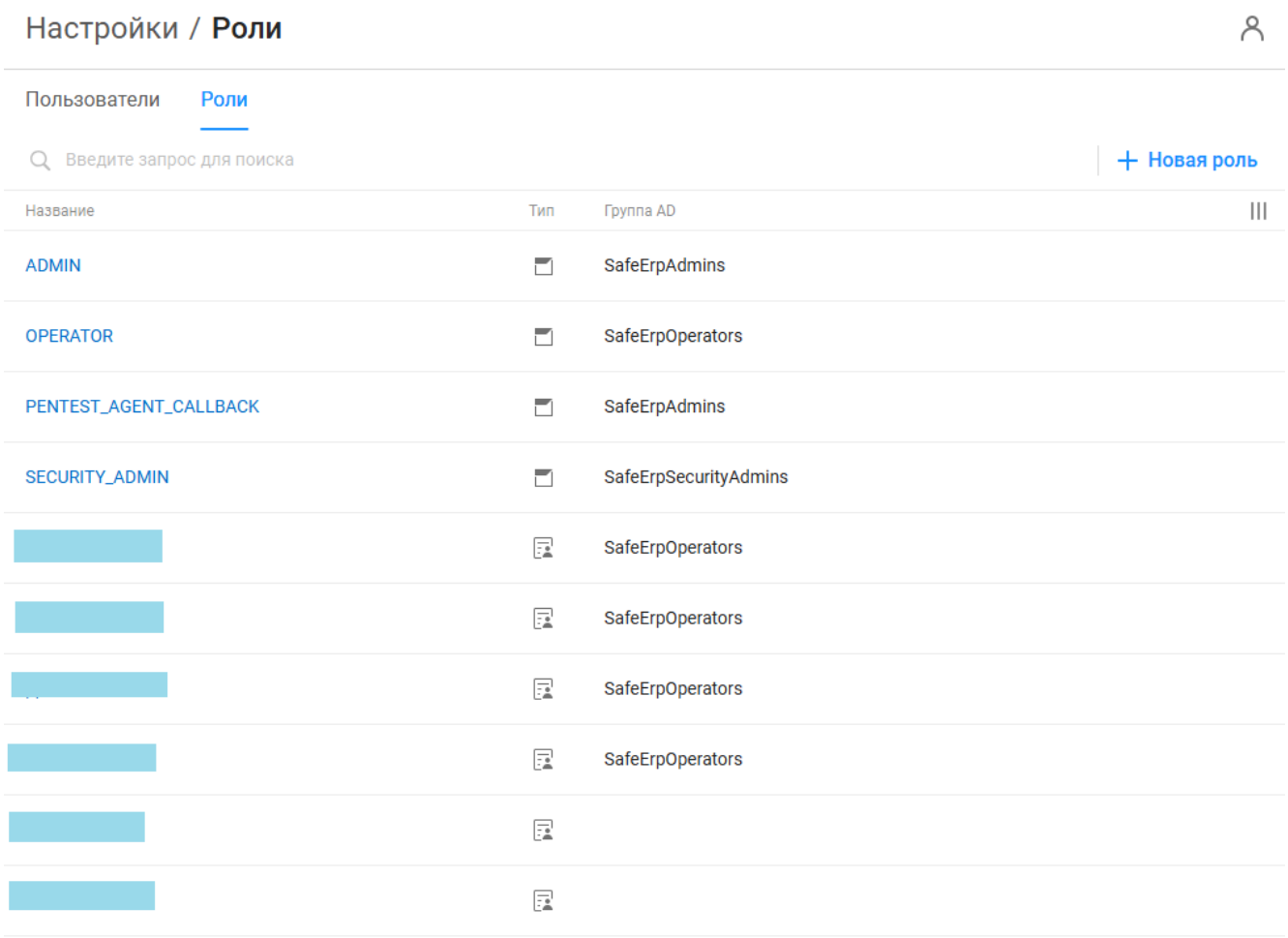


Рисунок 84 – Список ролей

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.

4.5.3.7 Создание пользовательских ролей

Для создания пользовательских ролей необходимо выполнить следующие действия:

1) Выбрать вкладку «Роли».
2) Нажать кнопку *«+ Новая роль»* (рис. 84).
3) Ввести название новой роли.
4) Выбрать необходимые полномочия (рис. 85) согласно подпункту 4.5.3.8.

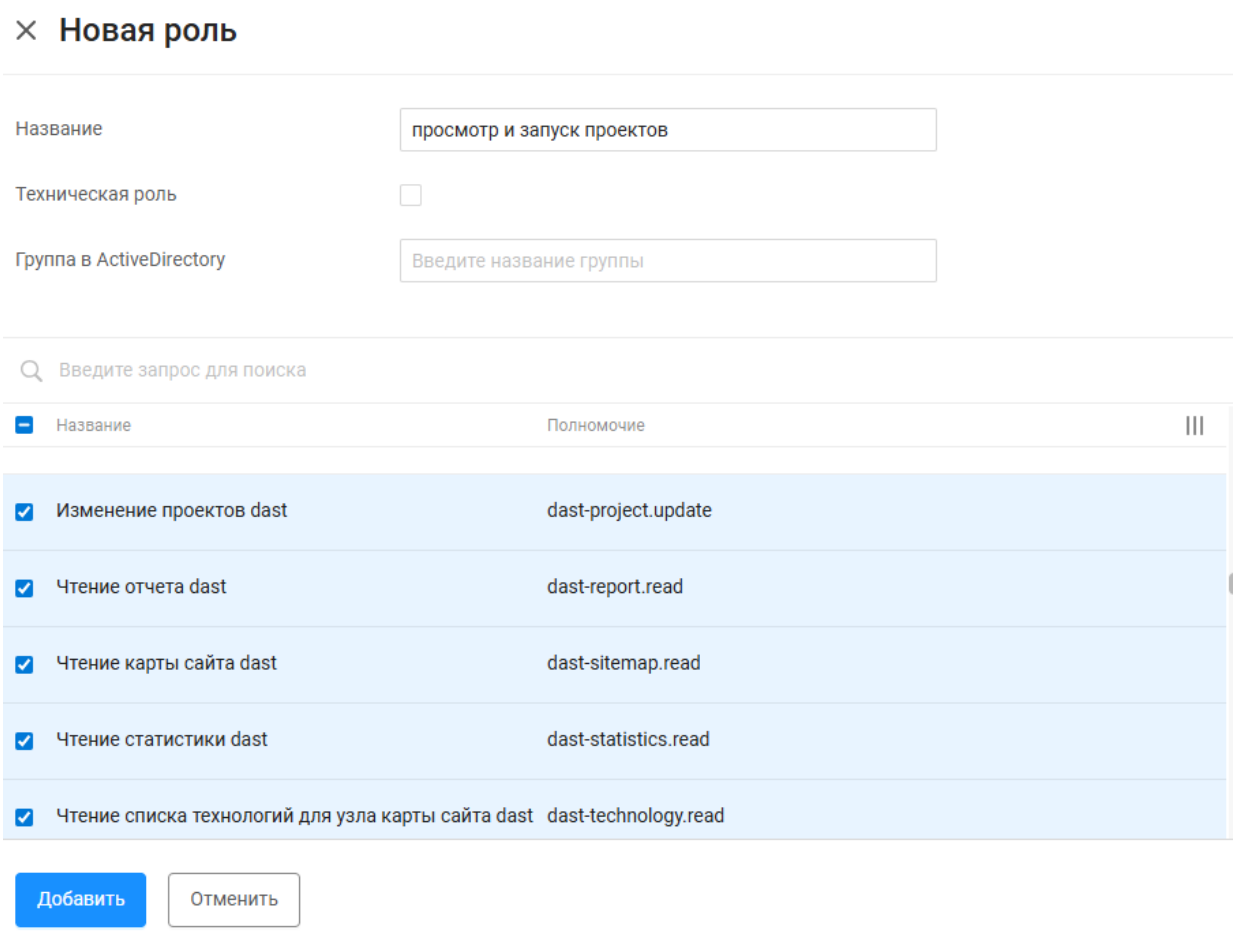


Рисунок 85 – Окно «Новая роль»

5) Нажать кнопку *«Добавить»* (см. рис. 85).

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.

4.5.3.8 Полномочия, назначаемые пользовательским ролям

Полномочия распределяются по следующим подразделам:

1) Аутентификация.
   Данный подраздел предназначен для аутентификации в ПК «SAFEERP PS EM».
   Полномочие на:

— чтение полномочий (authority.read) – запрос списка доступных полномочий для пользователя.

2) Раздел «DAST».
   Полномочия на:

— запуск анализа dast (dast-analyze.start) – запуск сканирования проекта;
— остановка анализа dast (dast-analyze.stop) – остановка сканирования проекта;
— чтение проектов dast (dast-project.read) – просмотр данных проекта, а также просмотр стартовой страницы ПК SAFEERP PS EM;
— чтение уязвимостей dast (dast-flaw.read) – просмотр результатов сканирования;
— чтение итераций dast (dast-iteration.read) – просмотр итерации проектов;
— чтение карты сайта dast (dast-sitemap.read) – просмотр данных результатов итерации;
— чтение списка технологий для узла карты сайта dast (dast-technology.read) – чтение данных во вкладке «Технологии» при просмотре результатов сканирования;
— создание проектов dast (dast-project.create) – создание проектов;
— изменение проектов dast (dast-project.update) – редактирование проекта;
— удаление проектов dast (dast-project.delete) – удаление проектов;
— чтение списка технологий для узла карты сайта dast (dast-technology.read) – просмотр описания сработанных проверок для проекта «Контроль настроек»;
— чтение карты сайта dast (dast-sitemap.read) – предназначено для просмотра карты сканируемого ресурса (сайта);
— чтение статистики dast (dast-statistics.read) – просмотр панели мониторинга по итерации проекта;
— чтение отчета dast (dast-report.read) – просмотр результатов сканирования в дереве уязвимостей;

3) Раздел «Pentest».
   Полномочия на:

— запуск анализа pentest (pentest-analyze.start) – запуск сканирования проекта;
— остановка анализа pentest (pentest -analyze.stop) – остановка сканирования проекта;
— чтение проектов pentest (pentest-project.read) – просмотр данных проекта, а также просмотр стартовой страницы ПК «SAFEERP PS EM»;
— чтение итераций pentest (pentest-iteration.read) – чтение итерации проектов;

— создание проектов pentest (pentest-project.create) – создание проектов;
— изменение проектов pentest (pentest-project.update) – редактирование проекта;
— чтение расширенной информации CVE pentest (pentest-cve-extrainfo.read) – просмотр данных CVE для раздела «Pentest»;
— чтение CPE pentest (pentest-cpe.read) – просмотр данных CPE для раздела «Pentest»;
— чтение расширенной информации CVE pentest (pentest-cve-extra-info.read) – просмотр эксплойтов;
— чтение отчета pentest (pentest-report.read) – просмотр результатов сканирования в разделе «Pentest»;
— сохранение отчета pentest (pentest-report.save) – сохранение отчета в разделе «Pentest»;
— чтение лога агента pentest (pentest-log.read) – чтение лога подраздела pentest в разделе «Журнал»;
— удаление проектов pentest (pentest-project.delete) – удаление проектов;
— чтение агентов pentest (pentest-agent.read) – чтение агента в разделе «Pentest»;
— подключение агентов pentest (pentest-agent.create) – подключение агента в разделе «Pentest»;
— изменение агентов pentest (pentest-agent.update) – изменение агентов в разделе «Pentest»;
— удаление агентов pentest (pentest-agent.delete) – удаление агентов в разделе «Pentest».

4) Раздел «Анализ платформы».
Полномочия на:

— запуск анализа platform-security (ps-analyze.start) – запуск сканирования проекта;
— остановка анализа platform-security (ps-analyze.stop) – остановка сканирования проекта;
— чтение проектов platform-security (ps-project.read) – просмотр данных проекта, а также просмотр стартовой страницы ПК «SAFEERP PS EM»;
— создание проектов platform-security (ps-project.create) – создание проектов;
— изменение проектов platform-security (ps-project.update) – редактирование проекта;
— удаление проектов platform-security (ps-project.delete) – удаление проектов;
— чтение итераций platform-security (ps-iteration.read) – чтение итерации проектов;
— удаление итераций platform-security (ps-iteration.delete) – удаление итерации проектов;
— чтение профилей безопасности 1С platform-security (ps-security-profile.read) – чтение профилей безопасности 1С в подразделе «Анализ платформы»;
— массовое изменение исключений уязвимостей platform-security (ps-flaw-exclusion.massUpdate) – массовое управление исключением уязвимостями;
— чтение исключений уязвимостей platform-security (ps-flaw-exclusion.read) – просмотр исключенных уязвимостей;
— изменение исключений уязвимостей platform-security (ps-flaw-exclusion.update) –

управление исключениями уязвимостями;

- чтение уязвимостей platform-security (ps-flaw.read) – просмотр результатов сканирования;
- чтение статистики platform-security (ps-statistics.read) – просмотр панели мониторинга по итерации проекта;
- создание профилей platform-security (ps-profile.create) – просмотр профилей;
- чтение профилей platform-security (ps-profile.read) – создание пользовательских профилей;
- изменение профилей platform-security (ps-profile.update) – редактирование пользовательских профилей;
- удаление профилей platform-security (ps-profile.delete) – удаление проверок в пользовательских профилях;
- чтение проверок platform-security (ps-check.read) – просмотр пользовательских и стандартных проверок;
- создание проверок platform-security (ps-check.create) – создание пользовательских проверок;
- изменение проверок platform-security (ps-check.update) – внесение изменений в пользовательские проверки;
- удаление проверок platform-security (ps-check.delete) – удаление пользовательских проверок.

5) Раздел «Цели сканирования».

Полномочия на:

- чтение цели сканирования (target.read) – чтение цели сканирования в ПК «SAFEERP PS EM»;
- создание цели сканирования (target.create) – создание цели сканирования в ПК «SAFEERP PS EM»;
- изменение цели сканирования (target.update) – изменение цели сканирования в ПК «SAFEERP PS EM»;
- удаление цели сканирования (target.delete) – удаление цели сканирования в ПК «SAFEERP PS EM»;
- чтение источников данных dast (dast-datasource.read) – просмотр данных источника;
- создание источников данных dast (dast-datasource.create) – подключение источников;
- изменение источников данных dast (dast-datasource.update) – изменение источников;
- удаление источников данных dast (dast-datasource.delete) – удаление источников;
- чтение источников данных pentest (pentest-datasource.read) – просмотр данных источника;
- создание источников данных pentest (pentest-datasource.create) – подключение источников;
- изменение источников данных pentest (pentest-datasource.update) – изменение

источников;
- удаление источников данных pentest (pentest-datasource.delete) – удаление источников;
- чтение источников данных platform-security (ps-datasource.read) – просмотр данных источника;
- создание источников данных platform-security (ps-datasource.create) – подключение источников;
- изменение источников данных platform-security (ps-datasource.update) – изменение источников;
- удаление источников данных platform-security (ps-datasource.delete) – удаление источников..

6) Раздел «Настройки».
Полномочия на:
- 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 PS 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 PS 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 данных из БД уязвимостей (info-db-database.read) – чтение статуса подраздела «БДУ»;
- обновление данных в БД уязвимостей (info-db-database.update) – обновление данных подраздела «БДУ»;
- чтение информации о БД уязвимостей (info-db-info.read) – просмотр информации по выбранной уязвимости.

4.5.3.9 Редактирование пользовательских ролей

Для редактирования пользовательских ролей необходимо выполнить следующие действия:

1) Выбрать вкладку «Роли».

2) Выбрать пользовательскую роль из списка.
3) Нажать кнопку *«+Добавить полномочия»* (рис. 86).

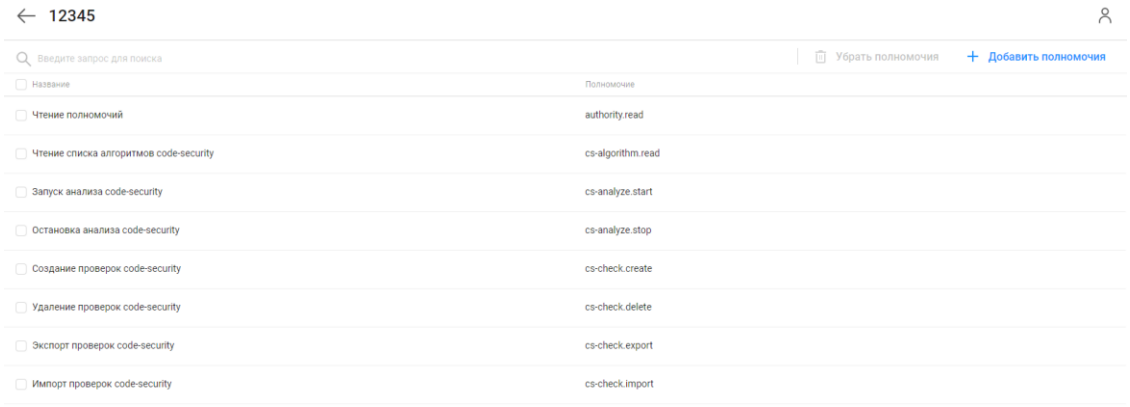


Рисунок 86 – Окно просмотра пользовательской роли

4) Поставить флаг напротив полномочий (рис. 87).

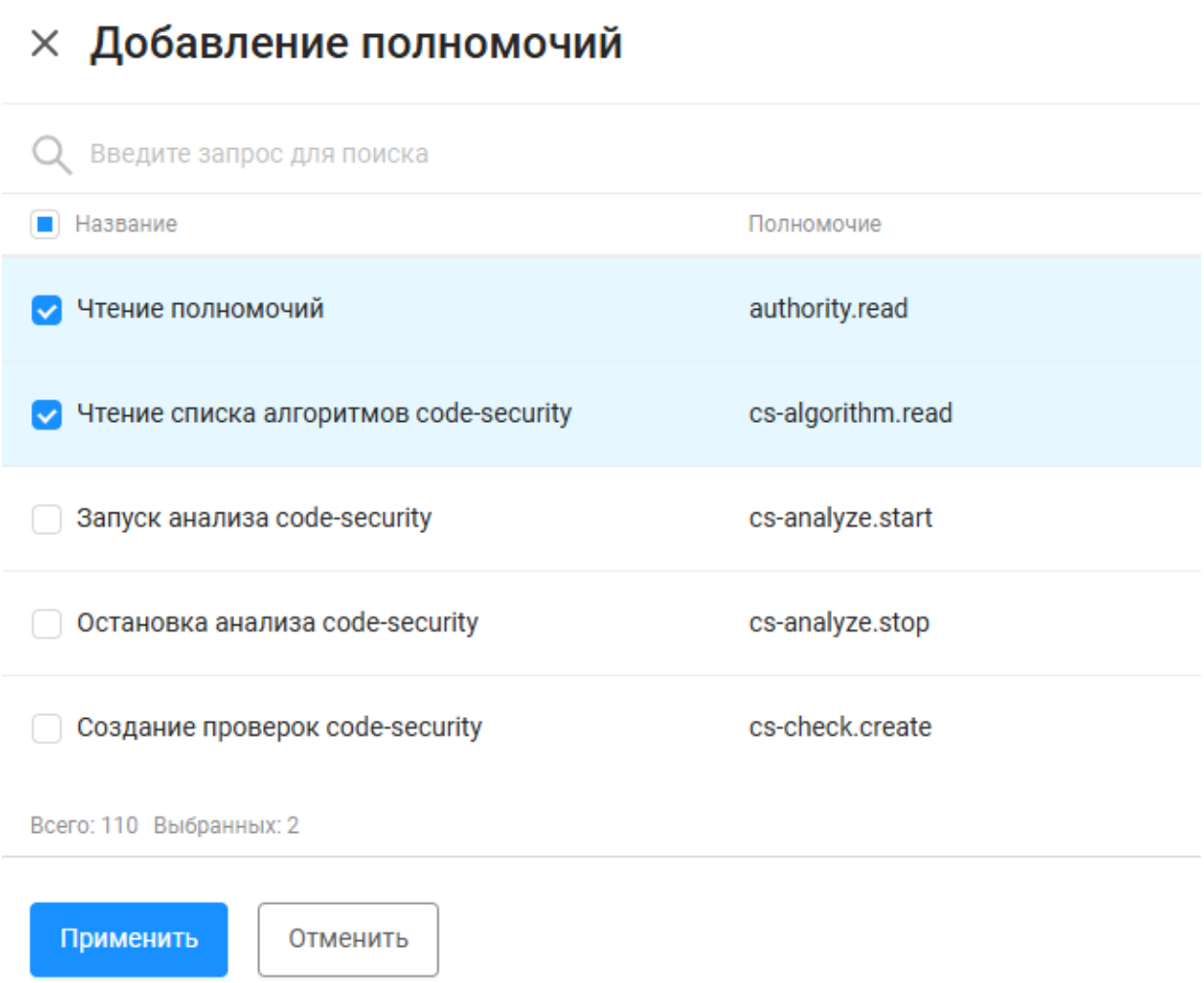


Рисунок 87 – Окно «Добавление полномочий»

5) Нажать кнопку *«Применить»* (см. рис. 87).

Для удаления полномочий из пользовательских ролей необходимо выполнить следующие действия:

1) Выбрать пользовательскую роль из списка или ввести название роли в поисковую строку.
2) Поставить флаг  напротив полномочий (рис. 86).
3) Нажать кнопку *«Убрать полномочия»* (рис. 86).

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

4.5.3.10 Копирование ролей

Для копирования ролей необходимо выбрать пункт «Копировать» в контекстном меню (рис. 88), нажать кнопку *«Копировать»*, внести необходимые данные в окне «Добавить роль» (см. рис. 85) , нажать кнопку «Добавить».

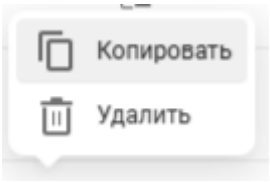


Рисунок 88 – Доступные действия с пользовательской ролью

4.5.3.11 Удаление пользовательских ролей

Для удаления пользовательских ролей необходимо выбрать пункт «Удалить» в контекстном меню (см. рис. 88), подтвердить действия.

Примечание. Удалению подлежат только пользовательские роли.

4.5.4 Подраздел «Журнал»

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

Подраздел «Журнал» предназначен для регистрации событий, возникающих в процессе эксплуатации ПК «SafeERP PS EM».

В ПК «SafeERP PS EM» регистрируются следующие события:

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

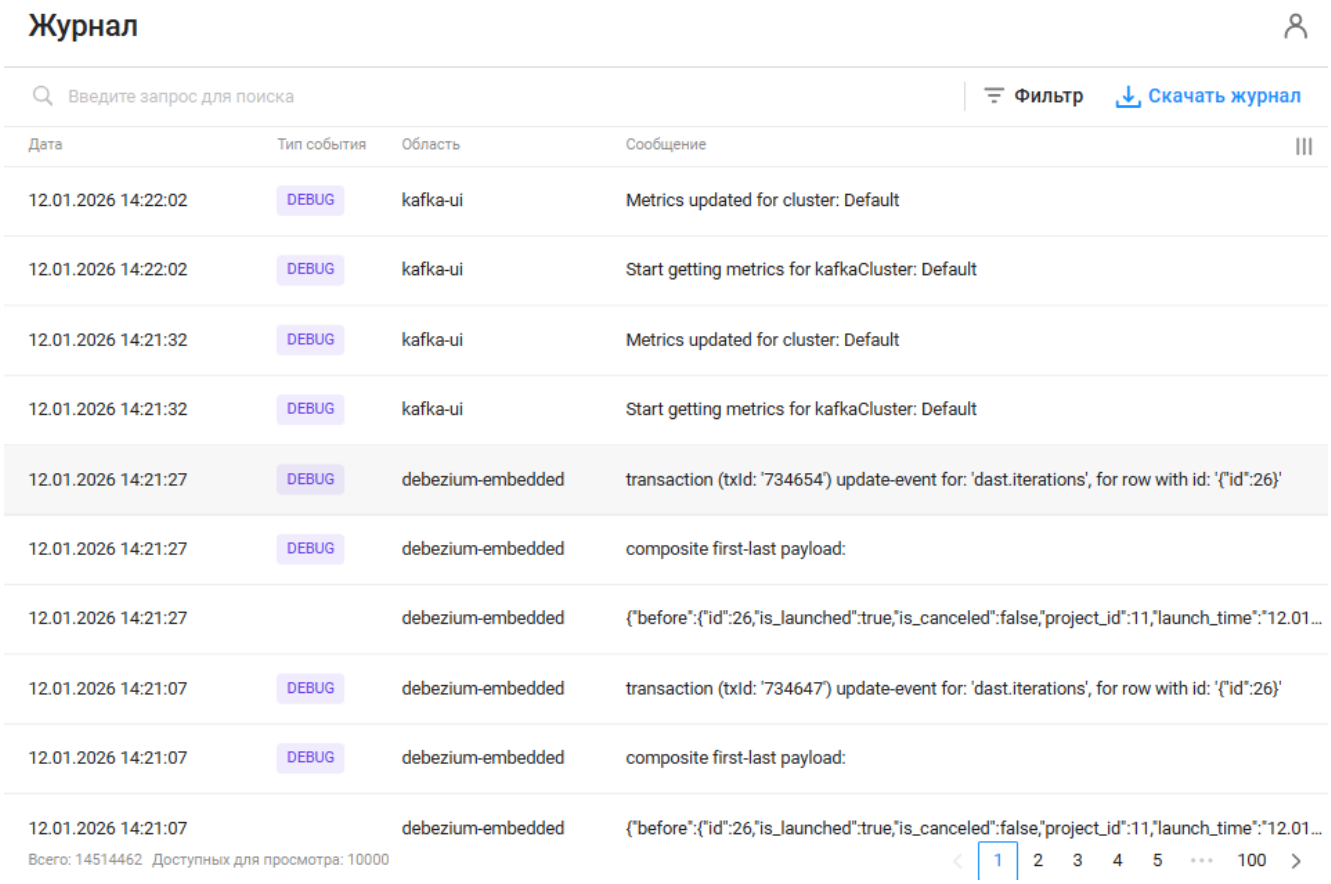


Рисунок 89 – Подраздел «Журнал»

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»*.

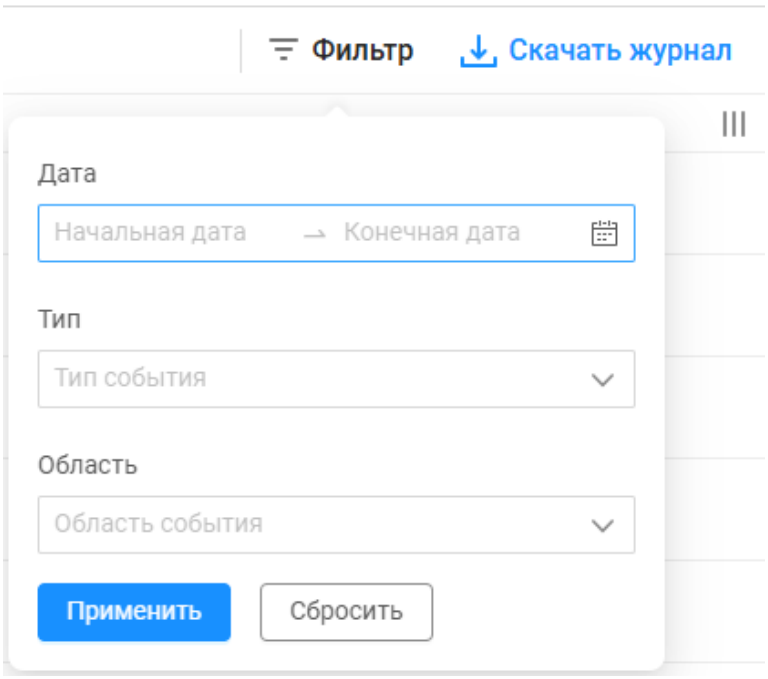


Рисунок 90 – Окно «Фильтр»

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

1. Типы событий (рис. 91).

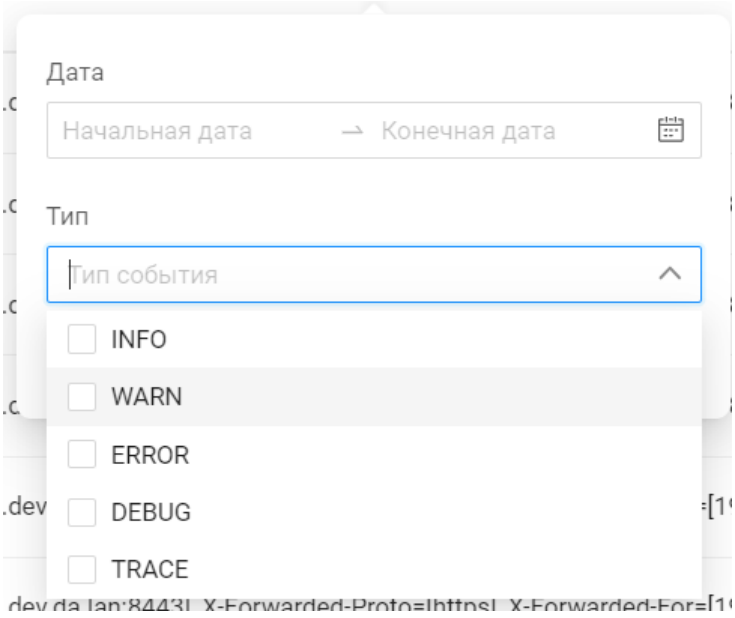


Рисунок 91 – Типы событий журнала

2. По дате и времени возникновения события (рис. 92).

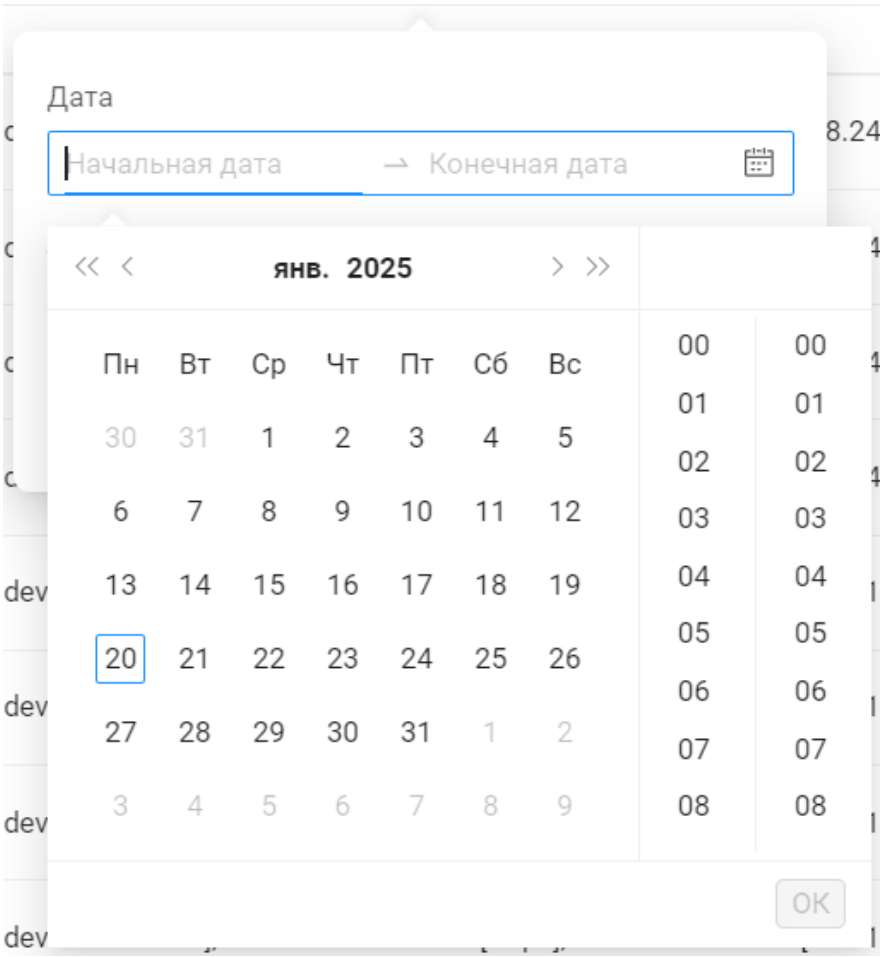


Рисунок 92 – Фильтрация журнала по дате и времени

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.

4.5.4.1 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.

4.5.4.2 Выгрузка журнала

Для выгрузки журнала необходимо выполнить следующие действия:

1) Выбрать раздел «Настройки».
2) Выбрать подраздел «Журнал».
3) Нажать кнопку *«Скачать журнал»* (рис. 89).

4.5.5 Подраздел «БДУ»

Подраздел «БДУ» предназначен для обновления базы данных уязвимостей (БДУ). Основная рабочая область представлена на рис. 93.

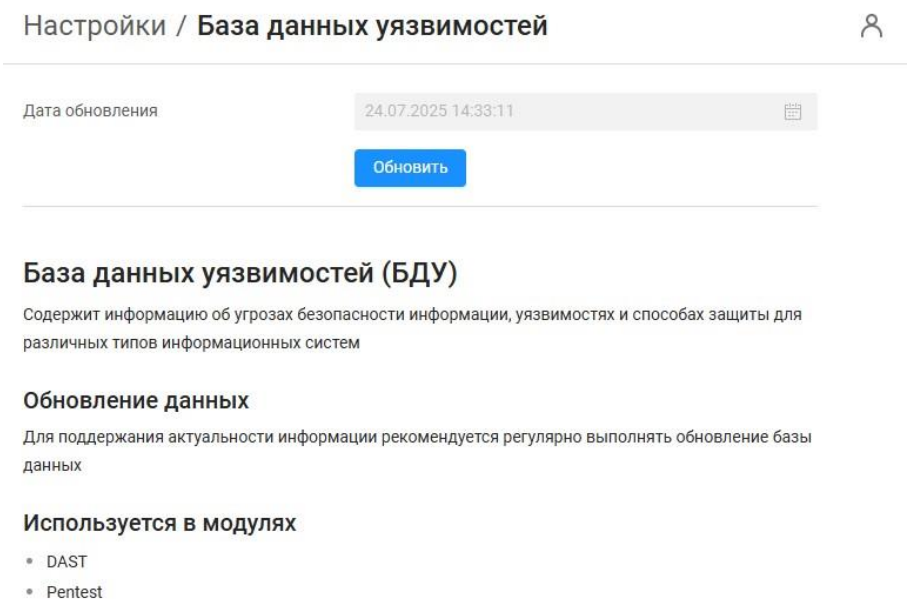


Рисунок 93 – Подраздел «БДУ»

В подразделе «БДУ» пользователю доступно обновление БД.
Для обновления БД необходимо нажать кнопку *«Обновить»* в основной рабочей области.

4.6 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;
- сброс пароля.

4.6.1 Просмотр данных текущего пользователя

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

4.6.2 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.

4.6.3 Просмотр списка активных подписок

Для просмотра списка активных подписок необходимо обратиться к профилю пользователя, выбрать раздел «Активные подписки» (рис. 94).

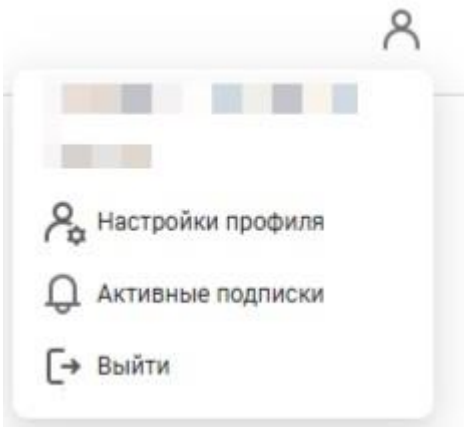


Рисунок 94 – Профиль пользователя

При нажатии на название проекта раскрывается список событий по данному проекту, на которые подписан пользователь. Список подписок представлен на рис. 95.

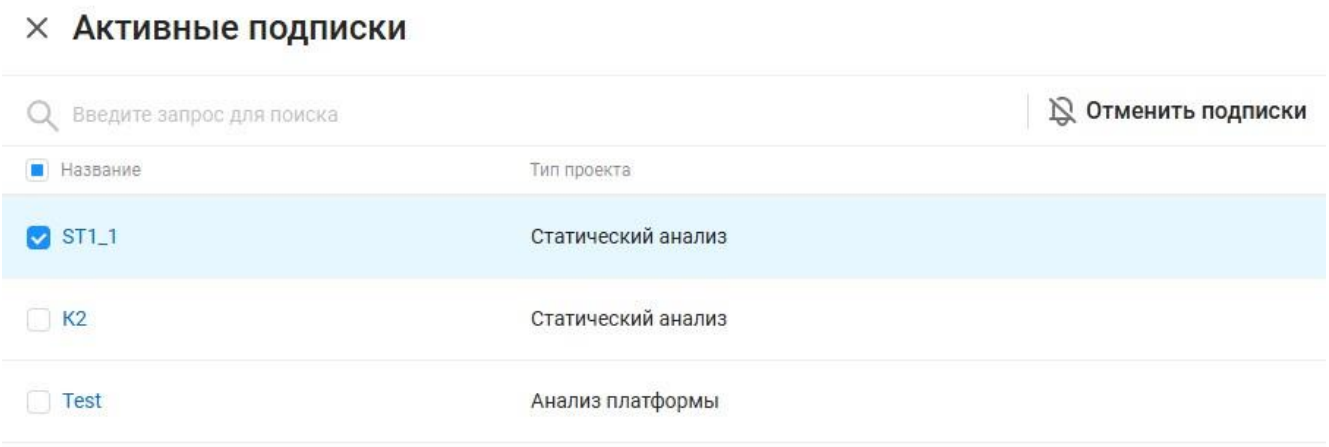


Рисунок 95 – Список активных подписок

4.6.4 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. 96).

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

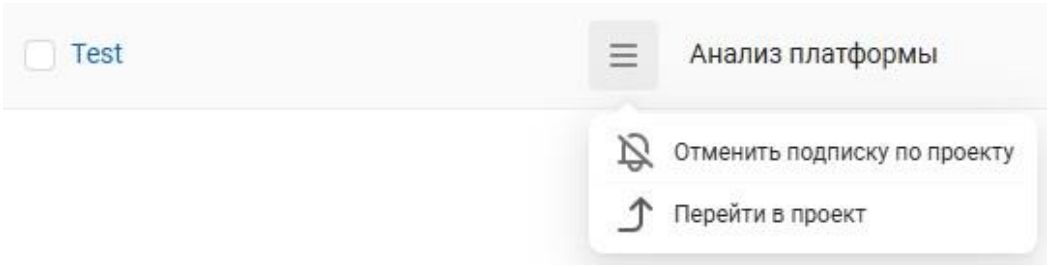


Рисунок 96 – Контекстное меню при просмотре списка активных подписок

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 PS 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.

Приложения

Приложение 1

Для подраздела «Проверки» (раздел «Анализ платформы») доступно создание пользовательских проверок.

Доступно создание пользовательских проверок с в следующих подразделах:

- «Анализ ролей»;
- «Настройки журналирования»;
- «Настройки кластера»;
- «Системные настройки».

Для каждого подраздела существуют стандартные проверки, а также возможность создать пользовательские проверки.

Проверки подраздела «Анализ ролей» определяют наличие небезопасных полномочий у ролей 1С.

Стандартные проверки включают в себя проверки по конкретным ролям (например, «Роль АдминистраторСистемы имеет право на Интерактивное открытие внешних отчетов») и общие проверки, в названии которых роль не указана. Общие проверки сканируют все роли, кроме исключений (например, «Роль имеет право на Интерактивное открытие внешних отчетов»). Исключаемые из этих проверок роли проверяются в отдельных проверках по конкретным ролям, описанных выше, и указаны в описании к каждой общей проверке.

При создании пользовательских проверок подраздела «Анализ ролей» необходимо заполнить следующее:

- поле «Название» – название пользовательской проверки;
- подраздел = «Анализ ролей»;
- поле «Шаблон проверки» – выбор проверяемого полномочия;
- поле «Проверяемые роли» – указать сканируемые роли по шаблону во всплывающем описанию к полю. Если поле «Проверяемые роли» заполнено, то данная проверка просканирует только роли из указанного списка. При этом значение в поле «Непроверяемые роли» будет проигнорировано. Если поле «Проверяемые роли» остается незаполненным, то сканируются все роли, кроме тех, которые будут указаны в поле «Непроверяемые роли»;
- поле «Непроверяемые роли» – указать игнорируемые роли по шаблону во всплывающем описании к полю. Значение учитывается только при пустом поле «Проверяемые роли».
  Если поля «Проверяемые роли» и «Непроверяемые роли» остаются незаполненными, то проверка просканирует все доступные роли;
- поле «Уровень опасности» – уровень опасности пользовательской проверки.
- поле «Описание» – описание пользовательской проверки;
- поле «Влияние уязвимости» – влияние уязвимости на безопасность системы 1С;
- поле «Рекомендации» – рекомендации по устранению уязвимости;
- поле «Ссылки» – ссылки на ресурсы.

Примечания:

1. Для шаблона проверки "Проверка прав" также доступны параметры:

— «Недопустимые права» – проверяются объектные права доступа и права доступа к механизмам платформы. Уязвимость обнаружена, если у роли имеется любое из перечисленных в данном поле прав;

— «Допустимые права доступа к механизмам платформы» – проверяются только права доступа к механизмам платформы. Уязвимость обнаружена, если у роли имеется любое право доступа к механизмам платформы, кроме перечисленных в параметре. При этом наличие перечисленных прав у роли не проверяется;

— «Недопустимые права доступа к механизмам платформы, назначенные одной роли» – проверяются только права доступа к механизмам платформы. Уязвимость обнаружена, если у роли одновременно имеются все перечисленные в параметре права.

2. Для сканирования проверок из подраздела «Анализ ролей» в проекте необходимо активировать переключатель «Контроль настроек» в настройках проекта.

Назначение пользовательских проверок подраздела «Анализ ролей» представлено в таблице 8.

Таблица 8 – Пользовательские проверки подраздела «Анализ ролей»

Название проверки	Краткое описание
Проверка прав	Проверка на наличие или отсутствие соответствующего права
Роль имеет право РежимТехническогоСпециалиста	Проверка роли на наличие соответствующего права
Роль имеет право на объекты нескольких подсистем	Проверка роли на наличие соответствующего права
Роль имеет право на Интерактивное снятие пометки удаления данных	Проверка роли на наличие соответствующего права
Роль имеет право на Интерактивное удаление помеченных предопределенных данных	Проверка роли на соответствующего права
Роль имеет право на Интерактивное удаление объекта	Проверка роли на наличие соответствующего права
Роль имеет право на Интерактивное удаление помеченных данных	Проверка роли на наличие соответствующего права
Роль имеет право на Интерактивное удаление помеченных предопределенных данных	Проверка роли на наличие соответствующего права
Роль имеет право на Интерактивное удаление предопределенных данных	Проверка роли на наличие соответствующего права
Роль имеет право на Интерактивную пометку удаления данных	Проверка роли на наличие соответствующего права

Роль имеет право на Интерактивную пометку удаления предопределенных данных	Проверка роли на наличие соответствующего права
У роли установлены права, относящиеся к роли ПолныеПрава + права, относящиеся к роли АдминистраторСистемы	Проверка роли на наличие соответствующего права

Назначение пользовательских проверок подраздела «Настройки журналирования» представлено в таблице 9.

Таблица 9 – Пользовательские проверки подраздела «Настройки журналирования»

Название проверки	Краткое описание
Проверка настроек версионирования объектов 1С	Проверка значений параметров настроек версионирования объектов 1С на соответствие рекомендуемому значению
Проверка журнала замера производительности 1С	Проверка значений параметров настроек журнала замера производительности 1С на соответствие рекомендуемым значениям
Проверка настроек журнала регистрации событий	Проверка заданного значения на соответствие рекомендуемому значению

Назначение пользовательских проверок «Настройки кластера» представлено в таблице 10.

Таблица 10 – Пользовательские проверки подраздела «Настройки кластера»

Название проверки	Краткое описание
Проверка значений профилей безопасности 1С	Проверка заданного значения на соответствие рекомендуемому значению

Назначение пользовательских проверок «Системные настройки» представлено в таблице 11.

Таблица 11 – Пользовательские проверки подраздела «Системные настройки»

Название проверки	Краткое описание
Проверка значений параметров	Проверка заданного значения на соответствие рекомендуемому значению

Список сокращений

ПК	–	программный комплекс
ПО	–	программное обеспечение
PDF	–	Portable Document Format
PS EM	–	Platform Security Extension Module