ГАЗИНФОРМ СЕРВИС

ПК «SafeERP Security Suite»
Руководство администратора

Санкт-Петербург, 2026

Аннотация

Руководство администратора программного комплекса (далее – ПК) «SafeERP Security Suite» является программным документом, определяющим порядок эксплуатации данного ПК. Руководство ориентировано на пользователей, осуществляющих работу с данным ПК.

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

- сведения о назначении ПК «SafeERP Security Suite»;
- общая схема работы ПК «SafeERP Security Suite»;
- запуск интерфейса настройки ПК «SafeERP Security Suite» в SAP GUI;
- описание интерфейса настройки ПК «SafeERP Security Suite» в SAP GUI (ведение настроек ПК и профилей сканирования модуля SafeERP Platform Security);
- запуск веб-интерфейса администратора ПК «SafeERP Security Suite»;
- описание веб-интерфейса администратора ПК «SafeERP Security Suite» (ведение проектов ПК, ведение настройки профилей сканирования модуля SafeERP Code Security).

Все примеры в данном документе приведены для ПК «SafeERP Security Suite» версии 4.9.11.

Содержание

1 Назначение ПК «SAFEERP Security Suite» ... 6
2 Общая схема работы ПК «SafeERP Security Suite» ... 7
2.1 Компоненты ПК «SafeERP Security Suite» ... 7
2.2 Технические средства, обеспечивающие работу ПК «SafeERP Security Suite» ... 7
2.3 Программные средства, обеспечивающие работу ПК «SafeERP Security Suite» ... 8
3 Запуск интерфейса настройки ПК «SafeERP Security Suite» в SAP GUI ... 9
4 Описание интерфейса настройки ПК «SAFEERP Security Suite» в SAP GUI ... 10
4.1 Настройка (подключение) агентов ПК «SafeERP Security Suite» ... 10
4.1.1 Панель инструментов ... 10
4.1.2 Компания/группа/система ... 11
4.1.3 Параметры систем ... 20
4.2 Настройка параметров ПК «SafeERP Security Suite» ... 21
4.2.1 Настройки для активации и загрузки лицензий ... 22
4.2.2 Определение пользователя для сервисного задания ... 27
4.2.3 Настройка параметров модуля SafeERP Code Security ... 28
4.2.4 Настройка параметров модуля SafeERP Platform Security ... 31
4.2.5 Активация ландшафта ... 33
4.2.6 Анализ данных ... 35
4.2.7 Анализ пользователей с помощью Ankey IDM ... 36
4.3 Загрузка SAP-нот ... 37
4.4 Запуск ПК SafeERP Platform Security Suite ... 40
4.5 Запуск ПК SafeERP Code Security Suite ... 42
4.6 Настройка почтовых уведомлений ... 46
4.7 Мониторинг фоновых заданий ... 51
4.8 Сравнение двух итераций проекта типа АК ... 52
4.9 Экспорт профилей ... 54
4.9.1 Экспорт профилей с помощью транзакции /N/GAZIS/SEGA ... 54
4.9.2 Экспорт профилей с помощью транзакции /n/gazis/export_seps ... 55
4.9.3 Экспорт профилей с помощью транзакции /n/gazis/export_secs ... 56
4.10 Импорт профилей ... 56
4.10.1 Импорт профилей с помощью транзакции /N/GAZIS/SEGA ... 56
4.10.2 Импорт профилей с помощью транзакции /n/gazis/import_seps ... 57
4.10.3 Импорт профилей с помощью транзакции /n/gazis/import_secs ... 58
4.11 Проверка системы ... 58

4.12 Настройка порядка отображений проверок статуса доступности агента в модуле «Панель мониторинга» ... 59
4.13 Поиск псевдокомментариев ... 60
4.14 Настройка количества функциональных модулей в функциональной группе ... 61
4.15 Настройка вложенности кода при сканировании ... 63
4.16 Проверка работы веб-серверов SAP FIORI ... 63
4.17 Проверка RFC соединений агентов ... 65
4.18 Сравнение двух ролей ... 67
4.19 Инструмент фиксации результатов ... 68
4.20 Выгрузка и загрузка данных освобождений ... 71
4.21 Подключение к системе отслеживания задач ... 75
4.22 Управление найденными уязвимостями ... 79
4.23 История полномочий ... 79
4.24 Проверка наименований объектов ... 81
4.24.1 Необходимые настройки ... 81
4.24.2 Запуск транзакции ... 82
4.25 Иерархия полномочий ... 84
4.26 Поиск объектов полномочий ... 84
5 Инструменты освобождения ... 86
5.1 Полномочия ... 86
5.2 Необходимые настройки ... 86
5.2.1 Настройка серверной части ... 86
5.2.2 Настройка агентской части ... 87
5.2.3 Почтовые уведомления ... 88
5.3 Статусы освобождений ... 89
5.4 Утверждение освобождения ... 89
5.4.1 Создания освобождения ... 89
6 Запуск веб-интерфейса администратора ПК «SafeERP Security Suite» ... 93
7 Описание веб-интерфейса администратора ПК «SafeERP Security Suite» ... 96
7.1. Функциональные модули «SafeERP Security Suite» ... 96
7.1.1 Модуль «Панель мониторинга» ... 104
7.1.2 Модуль «Проекты» ... 111
7.1.3 Модуль «Агенты» ... 197
7.1.4 Модуль «Ландшафт» ... 204
7.1.5 Модуль «Контроль RFC» ... 212
7.1.6 Модуль «Профили» ... 215
7.1.7 Модуль «Авторизации» ... 242
7.1.8 Модуль «Контроль качества» ... 254

7.1.9 Модуль «Администрирование» 258
7.1.10 Модуль «Аудит» 280
7.1.11 Модуль «Уведомления» 285
Приложение 1 294
Приложение 2 296
Приложение 3 297

1 Назначение ПК «SAFEERP Security Suite»

ПК «SafeERP Security Suite» состоит из двух функциональных модулей: SafeERP Code Security и SafeERP Platform Security. Модуль SafeERP Code Security отвечает за поиск и выявление небезопасного программного кода ABAP. Модуль SafeERP Platform Security отвечает за поиск и выявление изменений контрольных сумм программных объектов, фиксацию событий по объектам информации ограниченного доступа и определение небезопасного состояния настроек ПО и средств защиты.

Функции ПК «SafeERP Security Suite», реализованные для администратора ПК в интерфейсе SAP GUI:

- настройка (подключение) агентов ПК «SafeERP Security Suite»;
- настройка параметров ПК «SafeERP Security Suite»;
- настройка профилей модуля SafeERP Platform Security;
- настройка почтовых уведомлений;
- загрузка SAP-нот.

Функции ПК «SafeERP Security Suite», реализованные для администратора ПК в веб-интерфейсе:

- мониторинг результатов анализа и статусов доступности систем;
- ведение проектов для проведения процедур анализа;
- запуск проектов для проведения процедур анализа кода и настроек ПО контролируемых систем;
- просмотр отчетов по итерациям проекта;
- просмотр уведомлений по статусам работы процедур анализа и результатам анализа;
- просмотр ландшафта системы;
- просмотр и утверждение RFC-соединений;
- просмотр изменений объектов авторизаций в пользовательских ролях (просмотр истории полномочий, иерархии полномочий, сравнение ролей);
- ведение шаблонов для проверки проекта на соответствие заданных характеристик;
- настройка лицензий;
- настройка агентов;
- настройка ПК «SafeERP Security Suite».

2 Общая схема работы ПК «SafeERP Security Suite»

2.1 Компоненты ПК «SafeERP Security Suite»

Общая схема работы ПК «SafeERP Security Suite» в режиме работы администратора представлена на рис. 1.

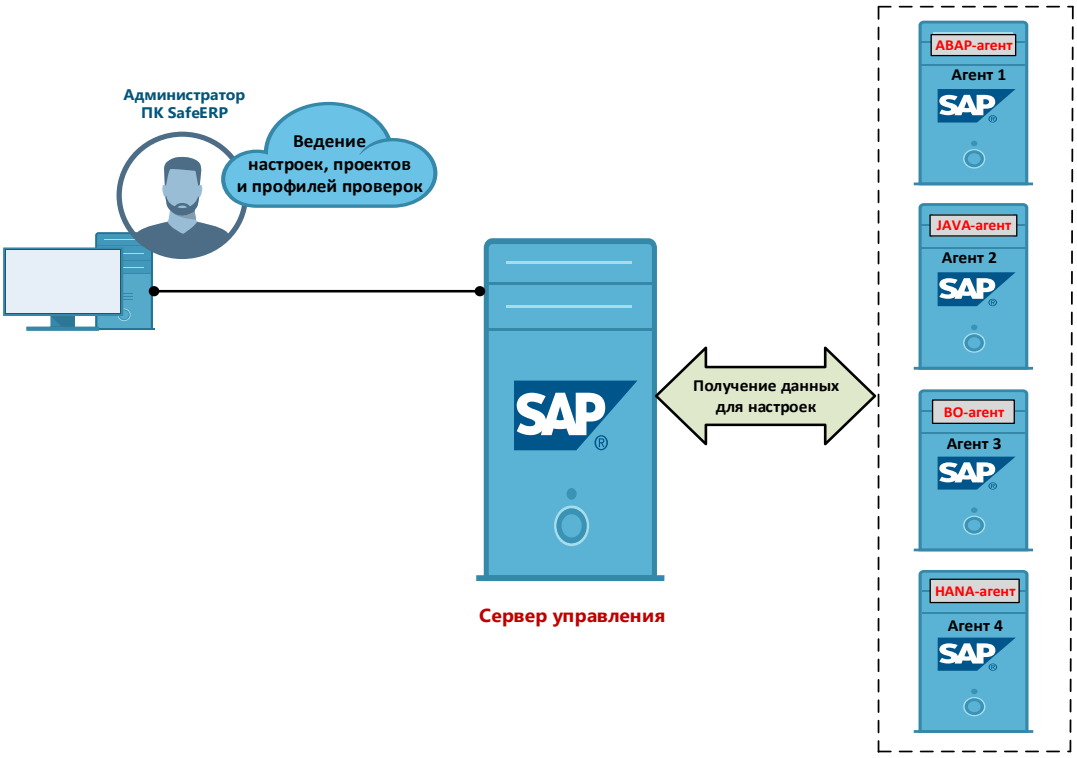


Рисунок 1 – Общая схема работы ПК в режиме администратора ПК SafeERP Security Suite

Компоненты ПК «SafeERP Security Suite»:

- сервер управления;
- ABAP-агент (агент для систем SAP NetWeaver на ABAP-стеке);
- Java-агент (агент для систем SAP NetWeaver на Java-стеке);
- BO-агент (агент для систем SAP Business Objects);
- HANA-агент (агент для систем SAP).

2.2 Технические средства, обеспечивающие работу ПК «SafeERP Security Suite»

К техническим средствам, обеспечивающим работу ПК «SafeERP Security Suite», относятся: сервер управления, автоматизированные рабочие места оператора и администратора ПК «SafeERP Security Suite». Дополнительных требований к техническим средствам при установке ПК не предъявляется. ПК «SafeERP Security Suite» может быть установлен на любом техническом средстве заказчика, где уже

установлена система SAP и составляющие ее компоненты.

2.3 Программные средства, обеспечивающие работу ПК «SafeERP Security Suite»

ПО ПК «SafeERP Security Suite» состоит из серверной части и агентской части. Серверная часть устанавливается на SAP-систему, где будет работать оператор ПК «SafeERP Security Suite». Серверная часть содержит функциональность для анализа объектов SAP-системы на безопасность. Для получения данных о проверяемом объекте серверная часть отправляет запрос агентской части. Агентская часть устанавливается на SAP-систему, объекты которой необходимо анализировать. Агентская часть содержит набор функций, которые по запросу собирают данные о проверяемом объекте и передают их на серверную часть для анализа. ПО ПК позволяет осуществлять прямое обращение к коду системы SAP без выгрузки кода.

Для работы сервера управления необходима платформа SAP NetWeaver AS ABAP не ниже версии 7.53 SP2 с установленным компонентом SAP FIORI FRONT-END SERVER не ниже версии 5.0 SP1.

Для работы сервера управления необходимо следующее:

- платформа SAP NetWeaver AS ABAP не ниже версии 7.52 с установленным компонентом SAP FIORI FRONT-END SERVER не ниже версии 6.0 и компонентом SAP_UI 7.54.

Примечание. Допускается некорректная работа ПК «SafeERP Security Suite» в интерфейсе SAP FIORI на версиях SAP_UI ниже 7.54 SP05, а также на SAP_UI 7.54 с более ранними пакетами поддержки, в том числе SP04 и ниже.

Для работы агентов необходимы платформы:

- для ABAP-агента – SAP NetWeaver AS ABAP не ниже версии 7.0;
- для JAVA-агента – SAP NetWeaver AS Java не ниже версии 7.31;
- для BO-агента – SAP BusinessObject BI не ниже версии 4.1;
- для HANA-агента – SAP HANA не ниже версии 1.0.

Для корректной работы ПК «SafeERP Security Suite» в интерфейсе SAP Fiori необходимы следующие браузеры:

- Mozilla Firefox – последняя стабильная версия и ESR;
- Yandex Browser – последняя версия.

На автоматизированные рабочие места оператора и администратора ПК «SafeERP Security Suite» должны быть установлены: SAP GUI for Windows не ниже версии 7.50 и Microsoft Office – для формирования и просмотра отчетов.

3 Запуск интерфейса настройки ПК «SafeERP Security Suite» в SAP GUI

Запуск интерфейса настройки ПК «SafeERP Security Suite» осуществляется через меню пользователя в SAP-системе. Пункт меню для активации интерфейса настроек ПК «SafeERP Security Suite» приведен на рис. 2.

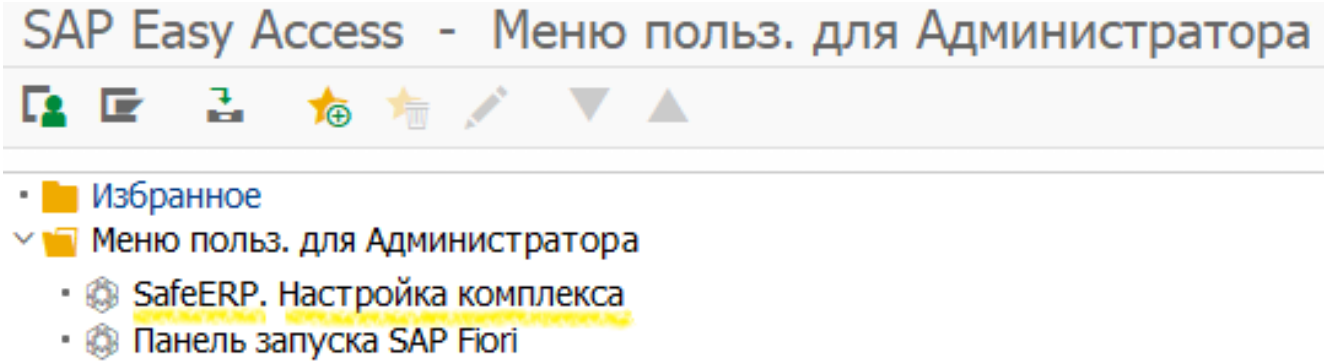


Рисунок 2 – Пункт меню для активации интерфейса настроек ПК «SafeERP Security Suite»

Для проведения необходимых настроек необходимо нажать на данный пункт меню левой кнопкой мыши.

Примечание. Предполагается, что ПК «SafeERP Security Suite» уже установлен на рабочем месте администратора ПК «SafeERP Security Suite» и соответствующие полномочия ему предоставлены.

4 Описание интерфейса настройки ПК «SAFEERP Security Suite» в SAP GUI

Интерфейс окна настроек ПК «SafeERP Security Suite» представлен на рис. 3.

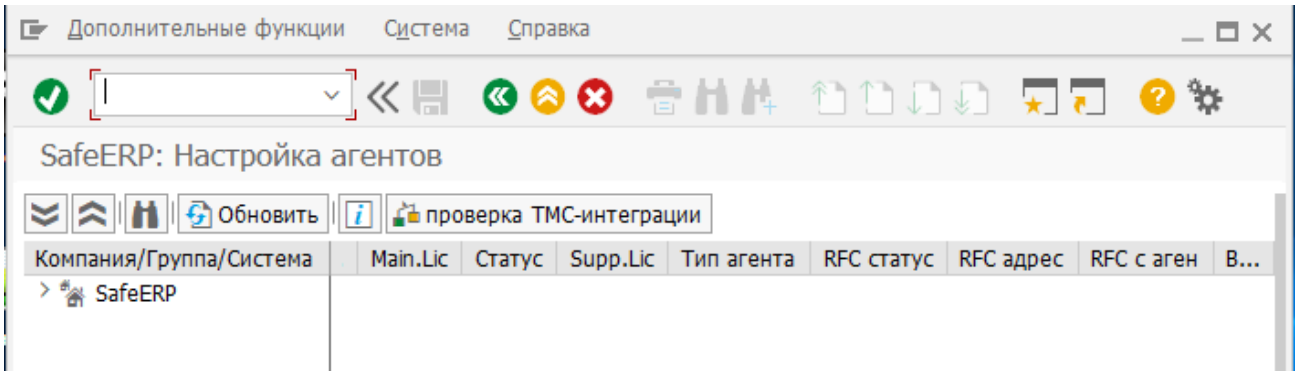


Рисунок 3 – Интерфейс окна настроек ПК «SafeERP Security Suite»

В окне настроек ПК «SafeERP Security Suite» осуществляется переход к следующим действиям:

- настройка (подключение) агентов ПК «SafeERP Security Suite»;
- настройка параметров ПК «SafeERP Security Suite»;
- настройка профилей модуля SafeERP Platform Security;
- загрузка SAP-нот.

4.1 Настройка (подключение) агентов ПК «SafeERP Security Suite»

Функциональность по настройке (подключению) агентов ПК «SafeERP Security Suite» предназначена для ведения и контроля списка проверяемых агент-систем и содержит три области (см. рис. 3):

1) Панель инструментов.
2) Компания/группа/система.
3) Параметры систем.

4.1.1 Панель инструментов

Область «Панель инструментов» содержит следующие функциональные кнопки:

- «Развернуть/свернуть ветвь» – развернуть/свернуть списки систем в области «Компания/группа/система»;
- «Поиск» – поиск по списку систем с заданным параметром в области «Компания/группа/система»;
- Обновить «Обновление данных об агентах» – обновление данных в областях «Компания/группа/система» и «Параметры систем»;
- «Справка» – справочная информация по функциональности;
- проверка TMS-интеграции «Проверка TMS-интеграции» – обновление статуса результата установки проверки транспортных запросов (см. пункт 4.1.3).

4.1.2 Компания/группа/система

Область «Компания/группа/система» содержит функциональность для настройки списка (дерева) подключаемых агентов (систем). Контекстное меню для настройки списка представлено на рис. 4. Активация контекстного меню осуществляется одним нажатием правой кнопкой мыши на наименование компании.

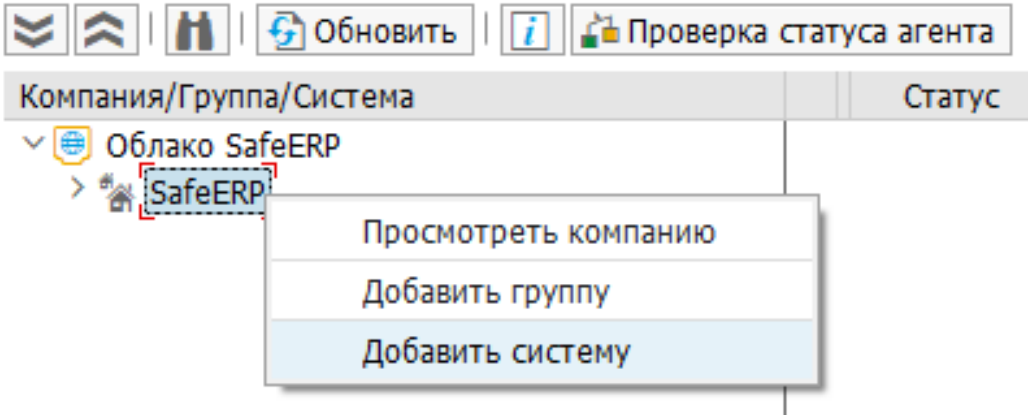


Рисунок 4 – Добавление системы

4.1.2.1. Просмотреть компанию

Чтобы просмотреть полное описание компании, необходимо активировать пункт «Просмотреть компанию» в контекстном меню (см. рис. 4). Откроется окно просмотра компании (рис. 5).

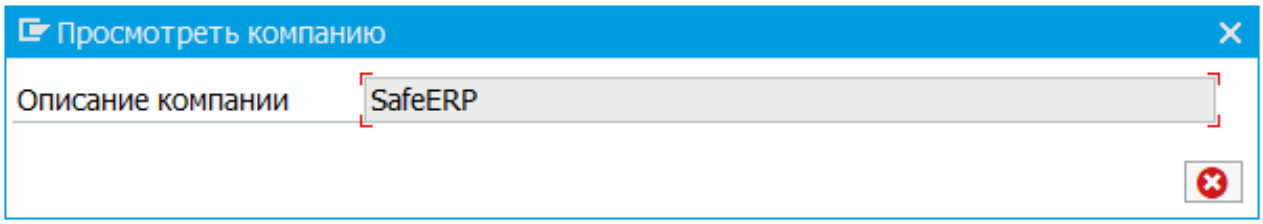


Рисунок 5 – Окно просмотра компании

4.1.2.2. Добавить группу

Для просмотра мониторинга событий с систем-агентов системы можно объединить в группы. Чтобы добавить группу, необходимо выбрать пункт «Добавить группу» в контекстном меню (см. рис. 4). Откроется окно добавления группы (рис. 6).

В поле описания группы необходимо указать новое название. Для сохранения измененных данных необходимо нажать кнопку «Создать группу».

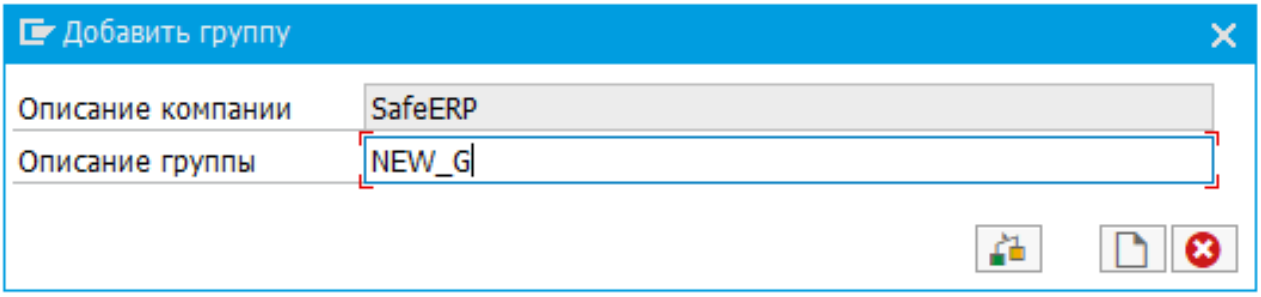


Рисунок 6 – Добавление группы

Группа появится в списке под названием «Все системы» (рис. 7).

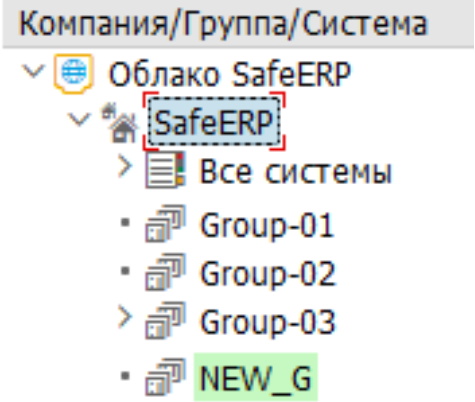


Рисунок 7 – Список групп

Список операций для работы с группой находится в контекстном меню, которое разворачивается одним нажатием правой кнопки мыши на наименование группы (рис. 8):

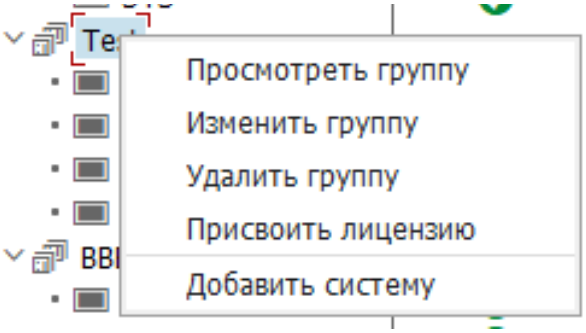


Рисунок 8 – Контекстное меню для работы с группой

Для работы с группой доступны следующие операции:

1) Просмотреть группу.

Чтобы просмотреть группу, необходимо выбрать пункт «Просмотреть группу» в контекстном меню (см. рис. 8). Откроется окно просмотра группы с информацией о ее параметрах (рис. 9).

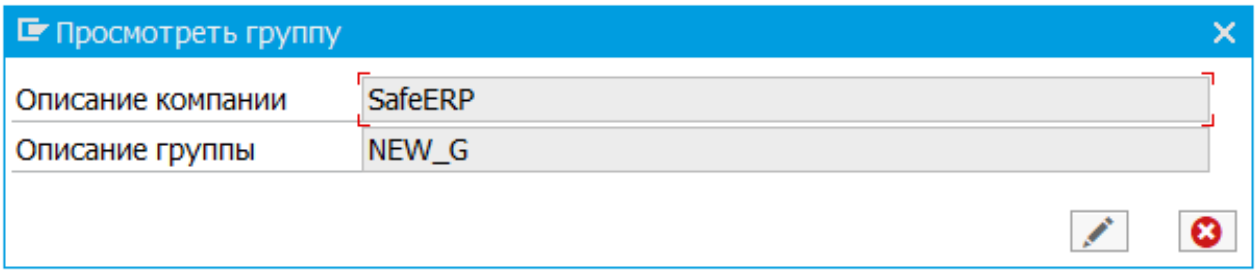


Рисунок 9 – Окно просмотра группы

В окне просмотра группы доступна операция изменения описания группы с помощью кнопки (рис. 10).

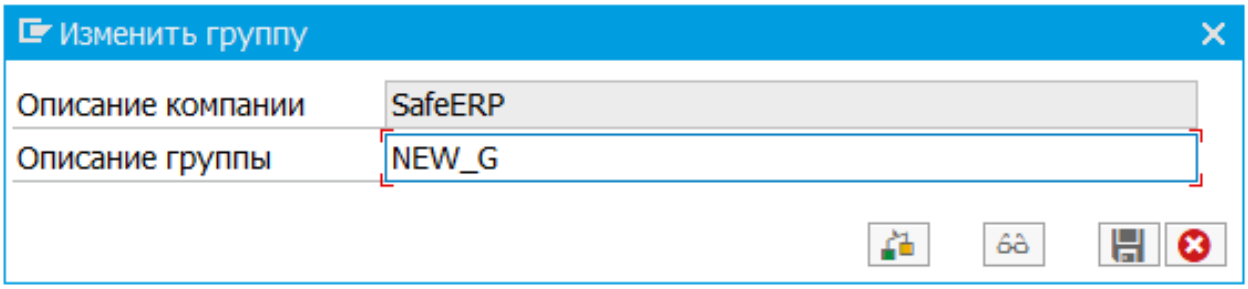


Рисунок 10 – Окно изменения группы

2) Изменить группу.

Чтобы изменить группу, необходимо выбрать пункт «Изменить группу» в контекстном меню (см. рис. 8). Откроется окно изменения группы с информацией о ее параметрах и возможностью редактировать поле «Описание группы» (см. рис. 10).

3) Удалить группу.

Чтобы удалить группу, необходимо выбрать пункт «Удалить группу» в контекстном меню (см. рис. 8). Откроется окно удаления группы с информацией о ее параметрах и доступом к кнопке удаления (рис. 11).

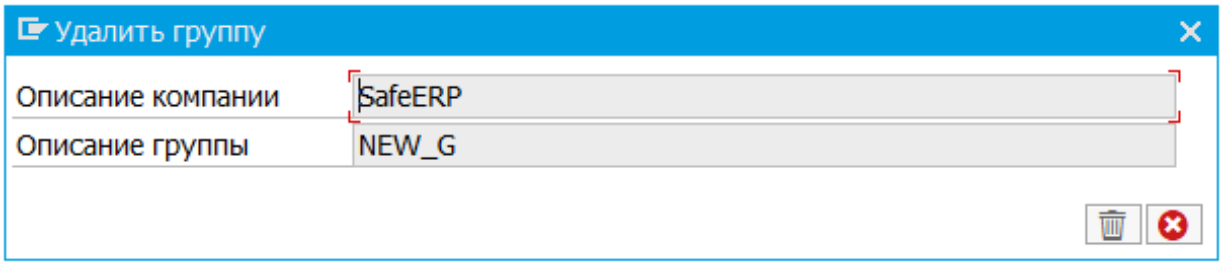


Рисунок 11 – Окно удаления группы

4) Присвоить лицензию.

Чтобы присвоить лицензии сразу всем системам, включенным в данную группу, необходимо выбрать пункт «Присвоить лицензию» в контекстном меню (см. рис. 8). Откроется окно присвоения лицензий системам (рис. 12).

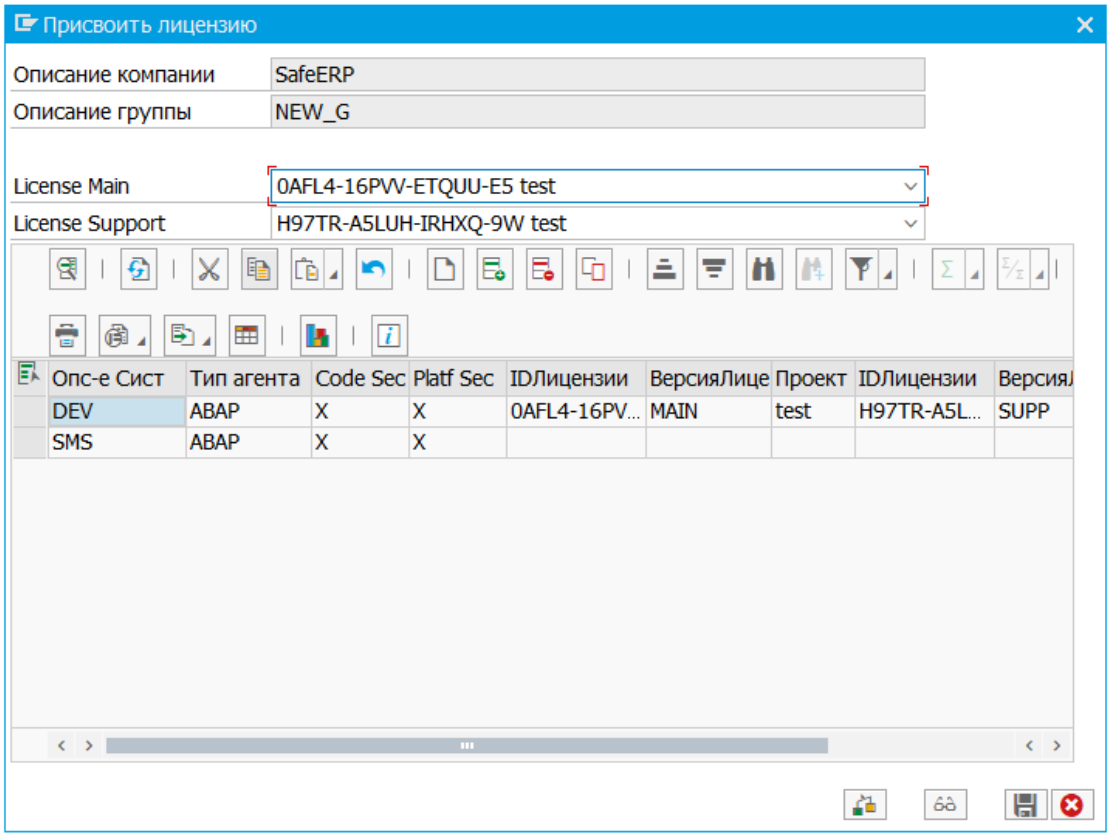


Рисунок 12 – Окно присвоения лицензий системам группы

В окне «Присвоить лицензию» для выбора лицензий доступны два поля «License Main» и «License Support»:

- MAIN – основная лицензия на подключение агентов (данный тип лицензии имеет срок действия);
- SUPPORT – лицензия на техническую поддержку выбранного программного продукта (как правило, со сроком действия один год).

Для распределения лицензий необходимо в таблице со списком систем группы выделить системы, зажав кнопку ctrl, которым необходимо присвоить лицензию, и нажать кнопку «Сохранить». Для систем, которым лицензии не были назначены, произойдет присвоение лицензий, указанных в полях «License Main» и «License Support». Для систем, которым лицензии были назначены, произойдет перезапись лицензий, указанных в полях «License Main» и «License Support».

В случае если при присвоении лицензий количество свободных лицензий будет превышать количество систем в группе, будет выведено информационное сообщение (рис. 13).

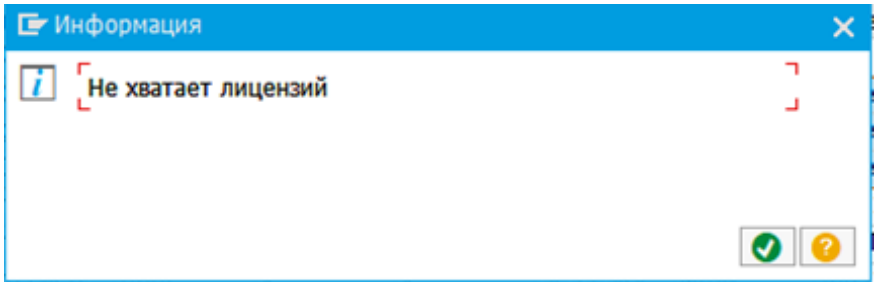


Рисунок 13 – Информационное сообщение о нехватке лицензий

После успешного присвоения лицензий группе систем в области «Параметры системы» (см. пункт 4.1.3) в соответствующих полях «Main.Lic» и «Supp.Lic» напротив систем появится статус , определяющая наличие лицензии (рис. 14).

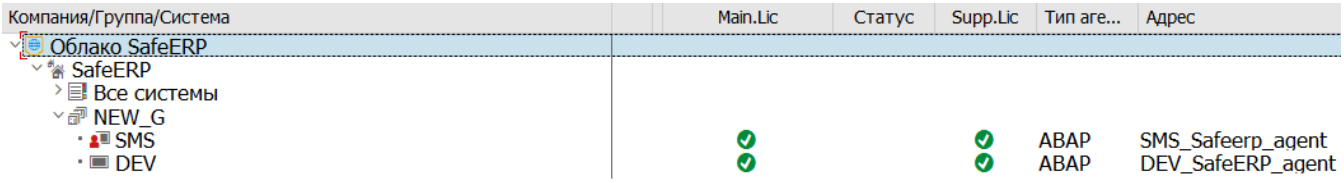


Рисунок 14 – Пиктограмма наличия лицензии у системы

5) Добавить систему.

Чтобы добавить систему в группу, необходимо выбрать пункт «Добавить систему» в контекстном меню (см. рис. 8). Откроется окно добавления системы с информацией о ее параметрах. Действия по работе с системой представлены в подпункте 4.1.2.3.

4.1.2.3. Добавить систему

Чтобы добавить систему, необходимо выбрать пункт «Добавить систему» в контекстном меню (см. рис. 4). Откроется окно для установки параметров добавляемой системы (рис. 15).

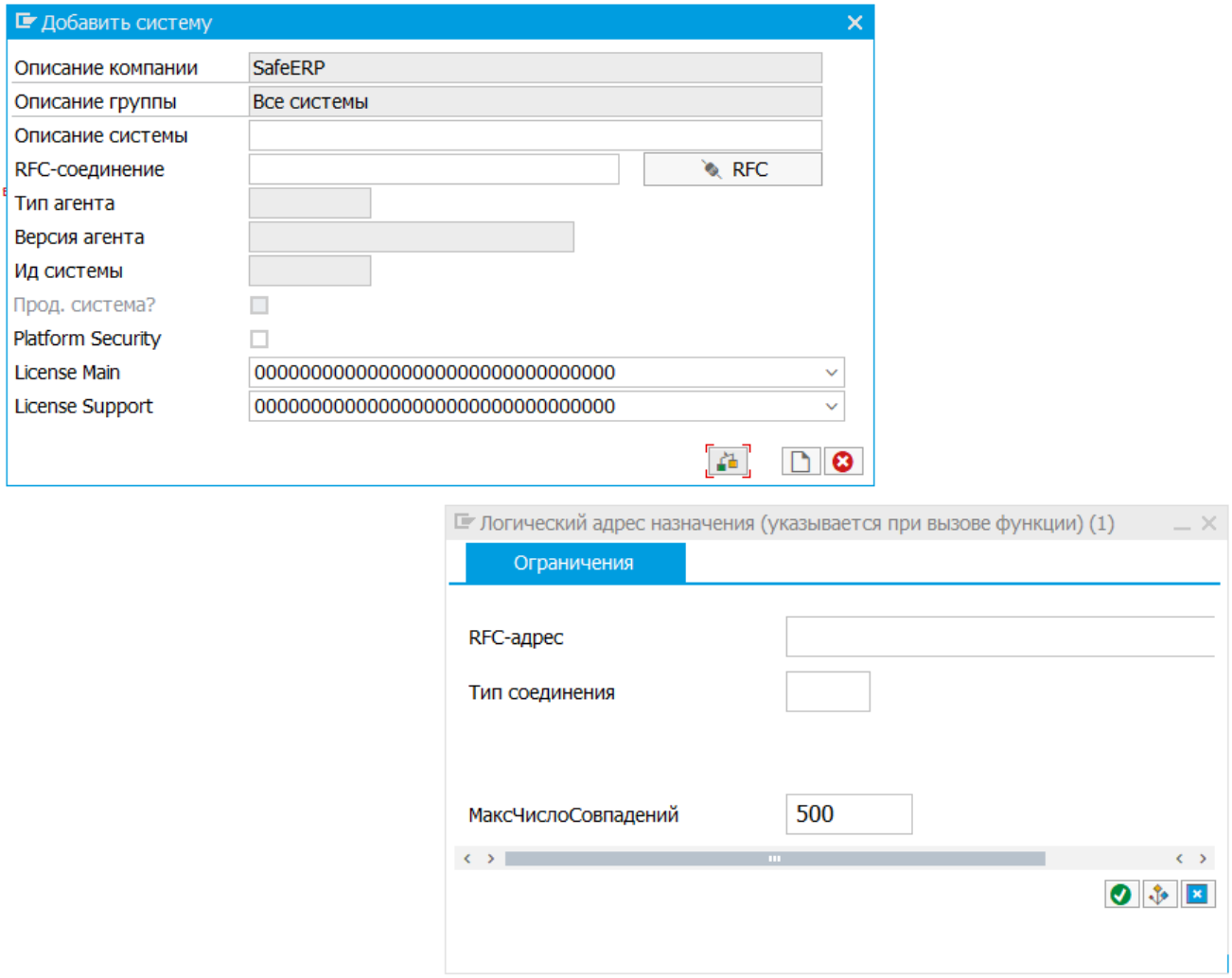


Рисунок 15 – Данные необходимые для заполнения системы

Поля, выделенные серым цветом, будут заполнены автоматически при выборе RFC-соединения.

В окне для установки параметров добавляемой продуктивной системы (агента) предусмотрено обязательное для заполнения поле, в котором необходимо указать одну из лицензий, в рамках которой приобретён добавляемый агент (рис. 16).

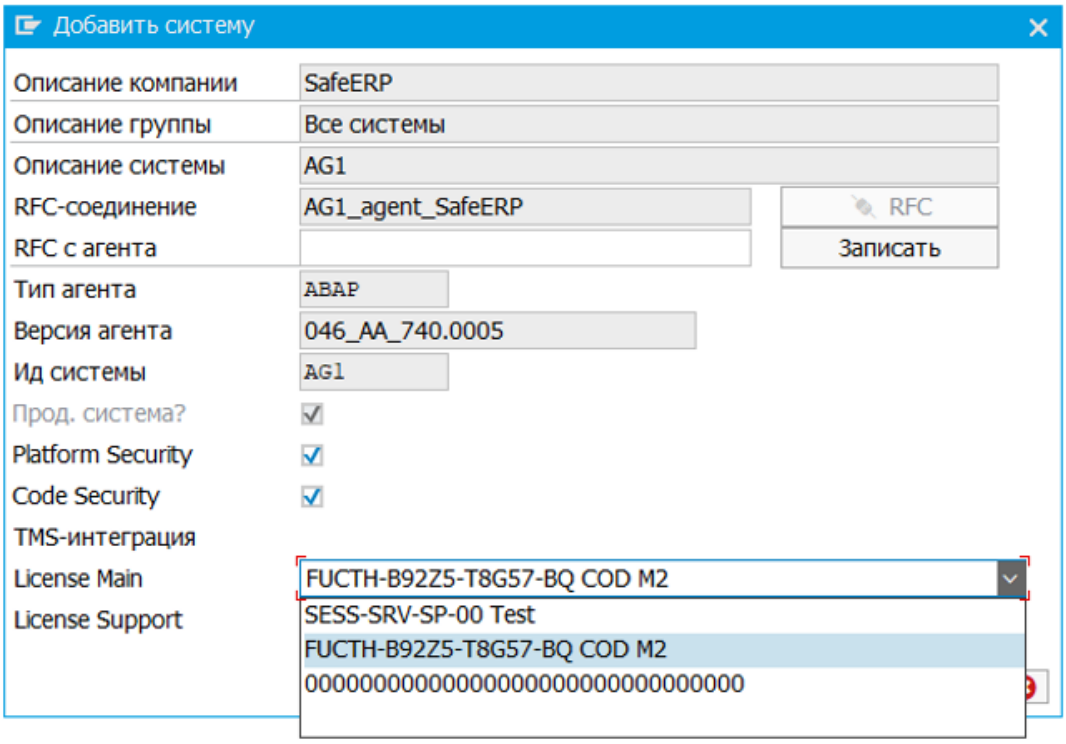


Рисунок 16 – Поле выбора лицензии при добавлении системы

Для выбора доступно два типа лицензий:

- MAIN – основная лицензия на подключение агентов (может быть двух типов: бессрочная и со сроком действия (временная));
- SUPPORT – лицензия на техническую поддержку выбранного программного продукта (как правило, со сроком действия один год).

Процедура загрузки файла лицензий определена в пункте 4.2.1.***лицензий***

После установки требуемых значений необходимо нажать кнопку «Создать систему» (см. рис. 15). Система появится в списке агентов под наименованием компании (рис. 17).

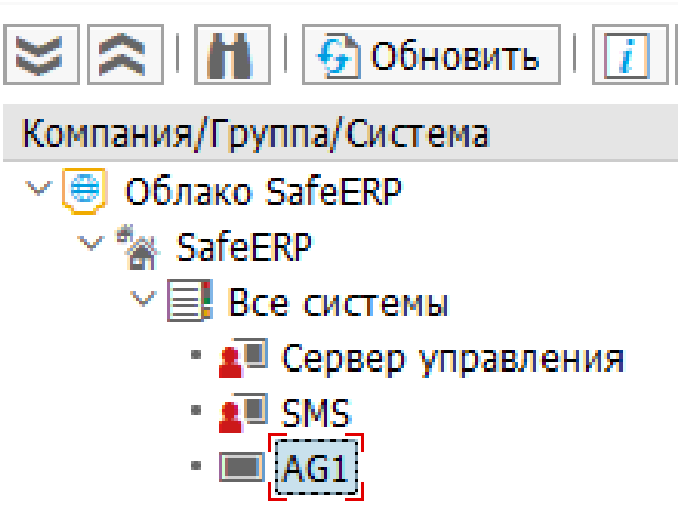


Рисунок 17 – Список агентов

Список операций для работы с системой находится в контекстном меню, которое откроется одним нажатием правой кнопкой мыши на наименование системы (рис. 18).

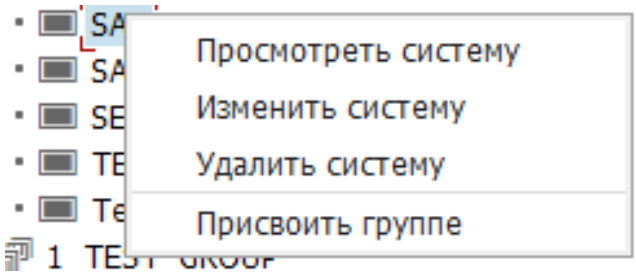


Рисунок 18 – Контекстное меню для работы с системой

Для работы с системой доступны следующие операции:

1) Просмотреть систему.

Чтобы просмотреть систему, необходимо выбрать пункт «Просмотреть систему» в контекстном меню (см. рис. 18). Откроется окно просмотра системы с информацией о ее параметрах, аналогичное окну добавления системы, но поля не будут доступны для редактирования (рис. 19).

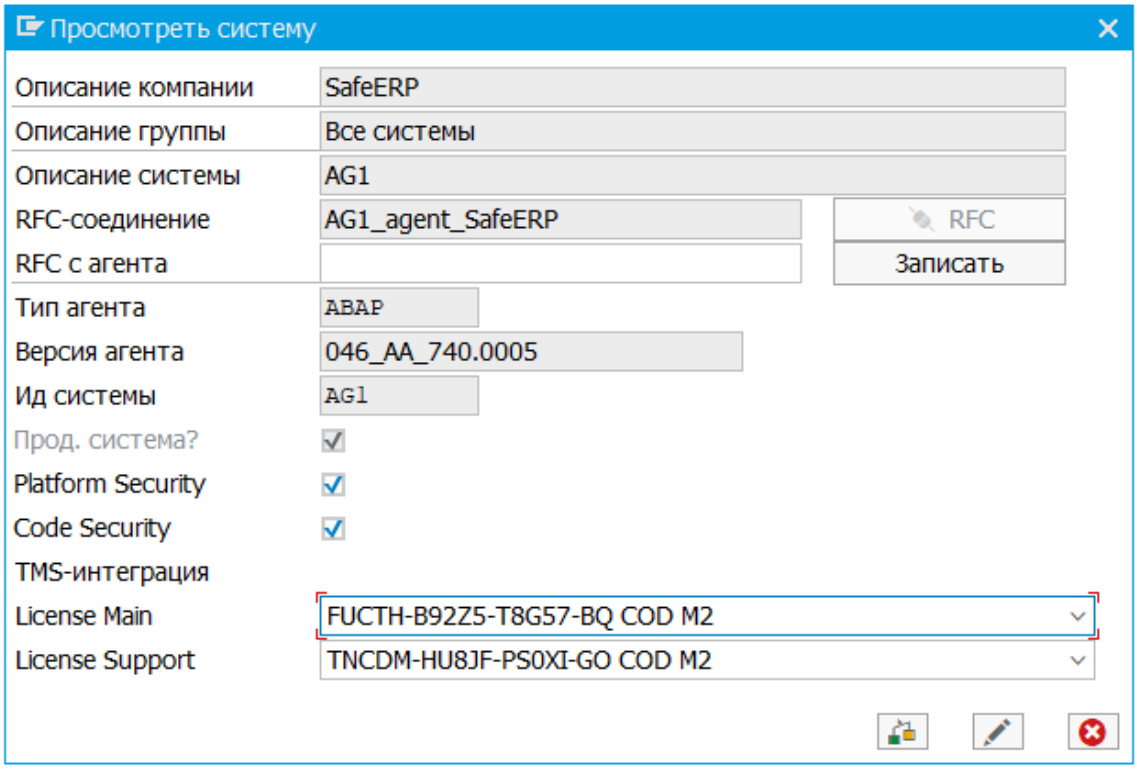


Рисунок 19 – Просмотр системы

2) Изменить систему.

Чтобы изменить систему, необходимо выбрать пункт «Изменить систему» в контекстном меню (см. рис. 18). Откроется окно изменения системы с информацией о ее параметрах, аналогичное окну добавления системы. Поля «Описание системы», «RFC-соединение» и активации инструментов анализа (поля выбора Platform Security и Code Security) будут доступны для редактирования (рис. 20). Для сохранения

измененных данных необходимо нажать кнопку «Сохранить».

Примечание. В режиме «Редактирование» доступна активации метки «Учет прагм в коде». Активировать настройку необходимо в следующих случаях:

— корректной работы проверок по поиску прагм;
— версия netweaver агента содержит прагмы.

Для активации метки «Учет прагм в коде» необходимо нажать кнопку в окне редактирования агента, после проверки необходимо поставить флаг напротив «Учет прагм в коде», нажать кнопку .

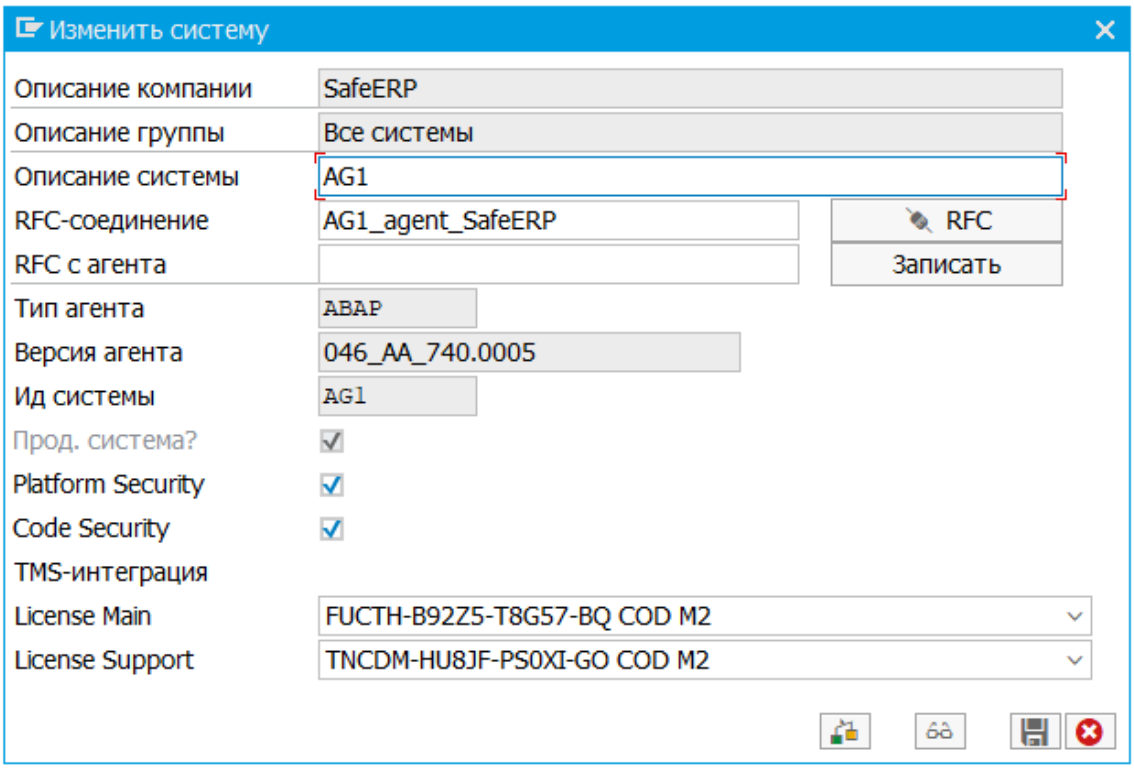


Рисунок 20 – Изменение системы

3) Удалить систему.

Чтобы удалить систему, необходимо выбрать пункт «Удалить систему» в контекстном меню (см. рис. 18). Откроется окно удаления системы с информацией о ее параметрах, аналогичное окну добавления системы (см. рис. 15), но поля не будут доступны для редактирования. Для удаления данных необходимо нажать кнопку *«Удалить».*

4) Присвоить группе.

Чтобы присвоить систему группе, необходимо выбрать пункт «Присвоить группе» в контекстном меню (см. рис. 18). Откроется окно для выбора названия группы (рис. 21). Добавление системы в группу будет доступно, если ранее хотя бы одна группа была создана (название группы выбирается из списка). Для сохранения данных необходимо после выбора названия группы для системы нажать кнопку

«Создать».

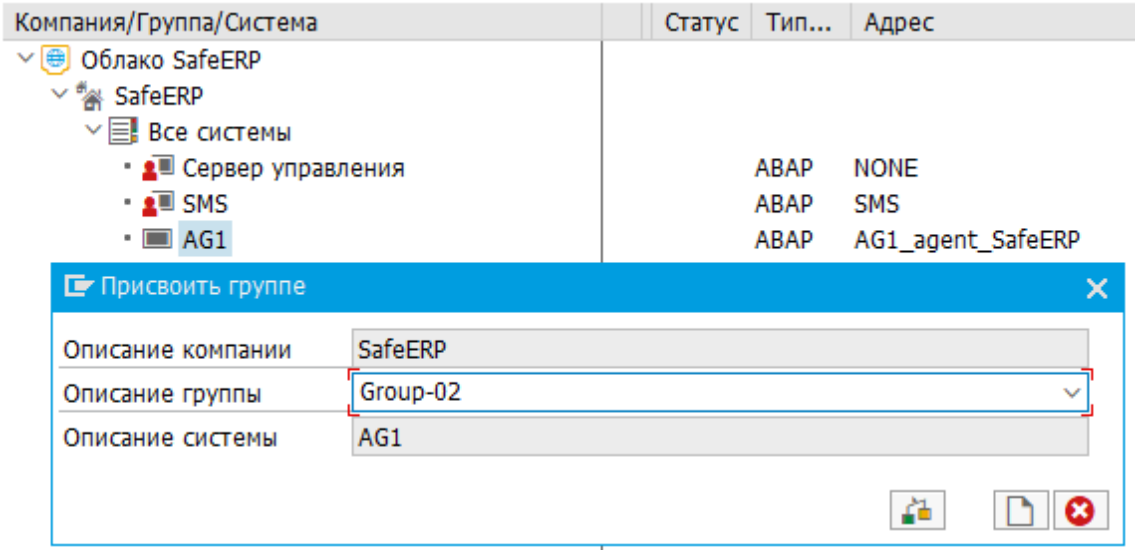


Рисунок 21 – Присвоение системы группе

4.1.3 Параметры систем

Область «Параметры систем» содержит подробную информацию о параметрах настроенных агент-систем. Для активации данной области необходимо развернуть список систем любой выбранной группы с помощью кнопки › (рис. 22).

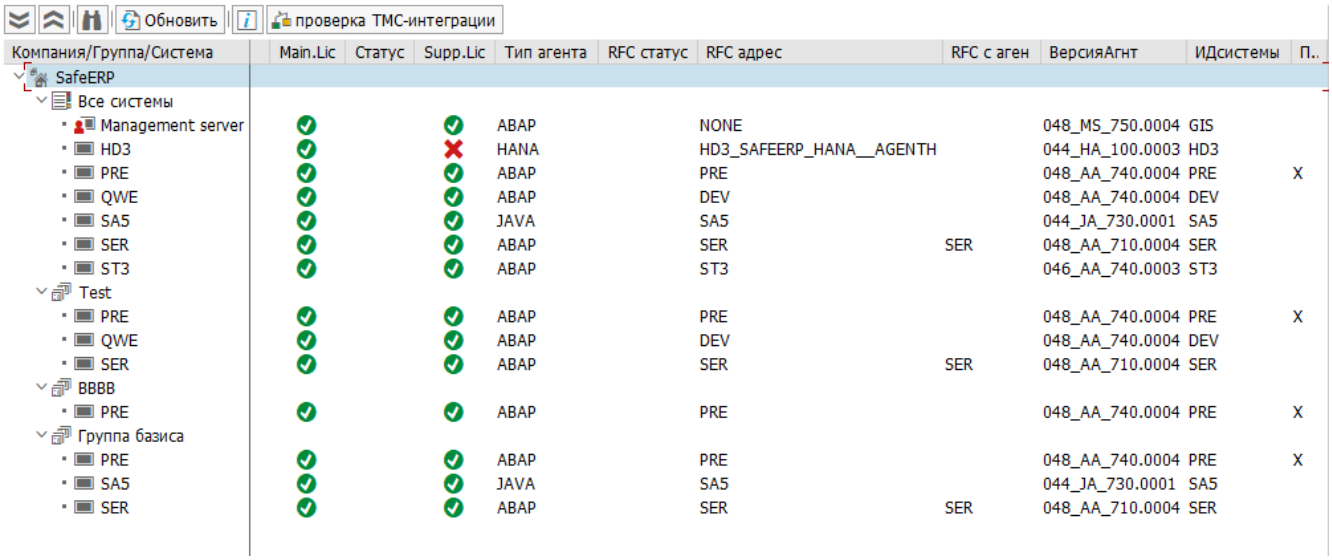


Рисунок 22 – Область просмотра параметров агент-систем

Статусы систем-агентов в области «Параметры систем» обновляются при нажатии кнопки проверка ТМС-интеграции. При обнаружении ошибок в установке транспортных запросов в столбце «Статус» таблицы параметров агент-систем появится индикатор ✖. Для просмотра статуса необходимо левой кнопкой мыши нажать кнопку ✖ в столбце «Статус» (рис. 23).

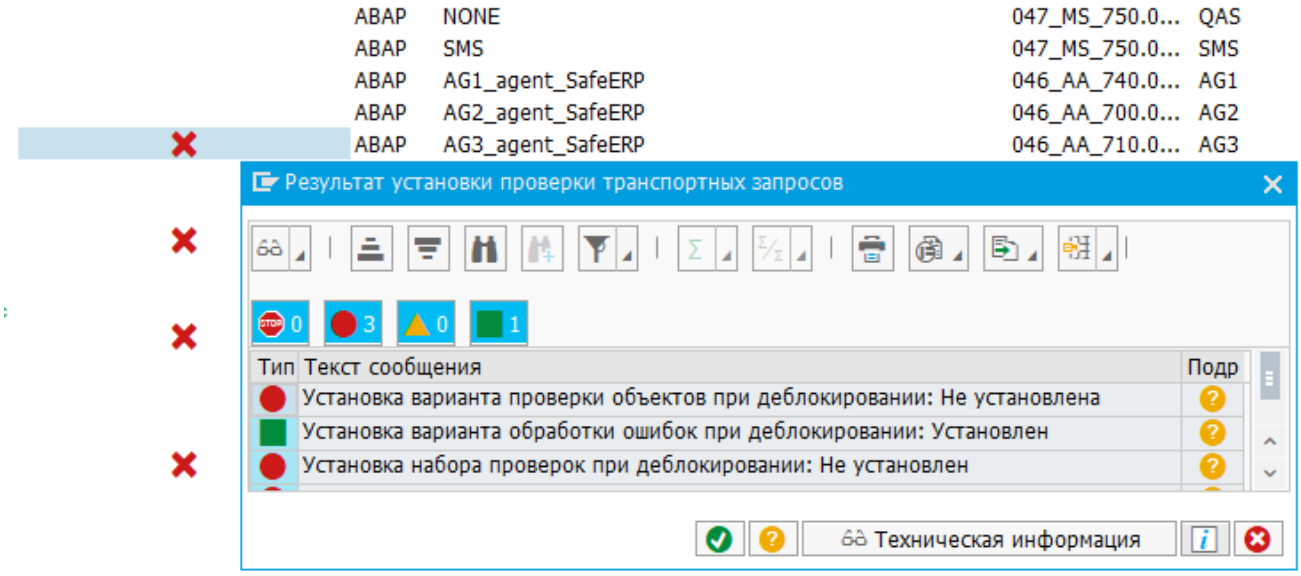


Рисунок 23 – Окно со статусами результатов установки транспортных запросов

4.2 Настройка параметров ПК «SafeERP Security Suite»

Функциональность по настройке параметров ПК «SafeERP Security Suite» предназначена для:

- активации лицензии;
- загрузки файла лицензий;
- определения пользователя для фонового задания;
- настройки параметров модуля SafeERP Code Security;
- настройки параметров модуля SafeERP Platform Security;
- активации карты соединений;
- анализа данных;
- анализ пользователей с помощью Ankey IDM.

Для запуска консоли по настройке параметров ПК «SafeERP Security Suite» необходимо в окне настроек ПК «SafeERP Security Suite» выбрать в основном меню пункты «Дополнительные функции» → «Настройка» → «SafeERP Suite» (рис. 24).

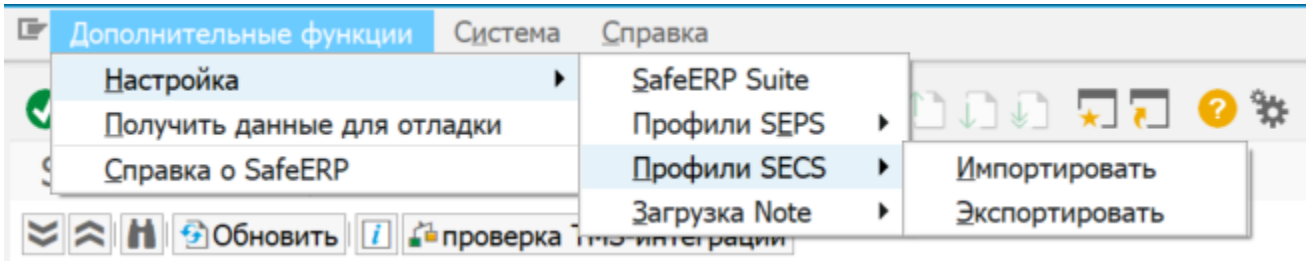


Рисунок 24 – Запуск консоли по настройке параметров ПК SafeERP

Консоль настройки параметров SafeERP Suite представлена на рис. 25.

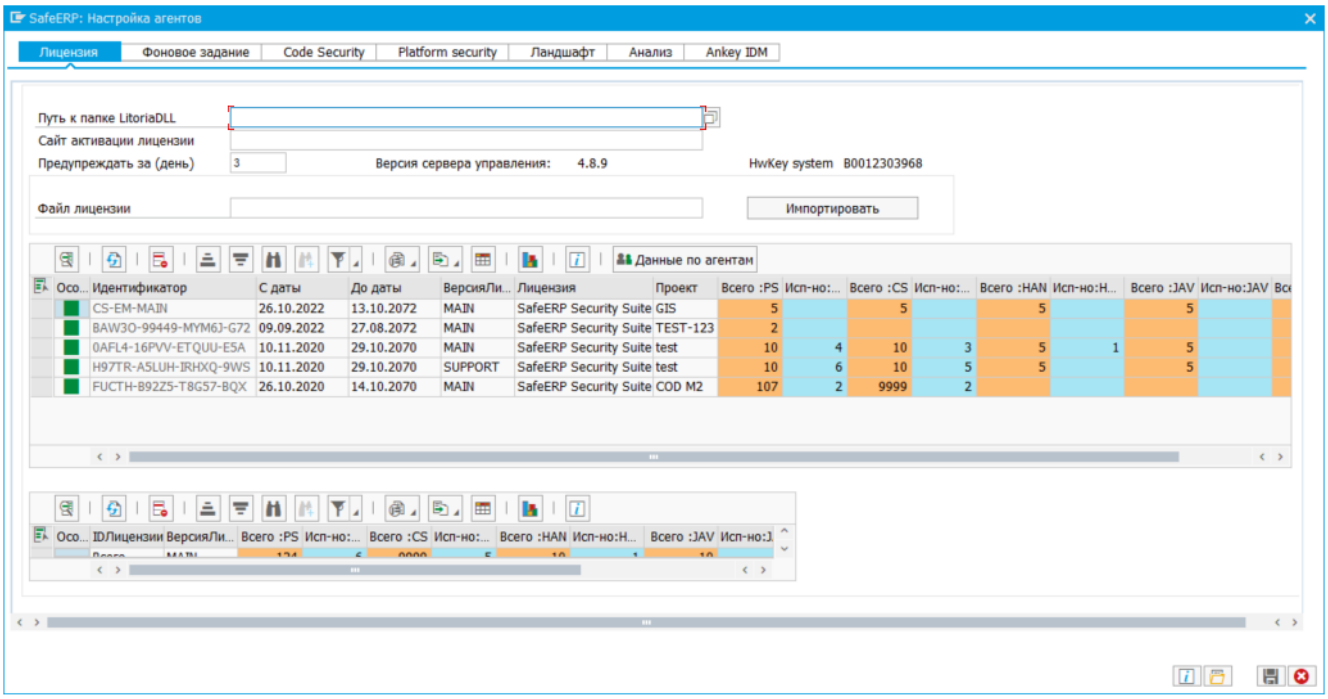


Рисунок 25 – Консоль настройки параметров SafeERP Suite

Консоль настройки параметров SafeERP Suite имеет следующие управляющие элементы (общие для всех вкладок):

- «Справка» – справочная информация по функциональности вкладки;
- «Настройка логических путей» – вызов стандартной транзакции FILE для активации диалогового окна управления файлами;
- «Сохранить» – сохранение настроек;
- «Отмена» – сброс настроек.

4.2.1 Настройки для активации и загрузки лицензий

Для корректной работы активации лицензии необходимо выполнить следующие действия:

1) Настроить физический путь хранения файлов.
2) Настроить логический путь хранения файлов.
3) Присвоить физический путь файла логическому пути.

4.2.1.1 Создание каталога на физическом уровне

Для создания каталога на физическом уровне необходимо обратиться к группе SAP базис.

4.2.1.2 Создание каталога на логическом уровне

Создание каталога на логическом уровне необходимо для корректной работы активации лицензии в интерфейсе SAP GUI, а также в SAP FIORI.

Для создания каталога на логическом уровне необходимо обратиться к транзакции FILE. Окно транзакции представлено на рис. 26.

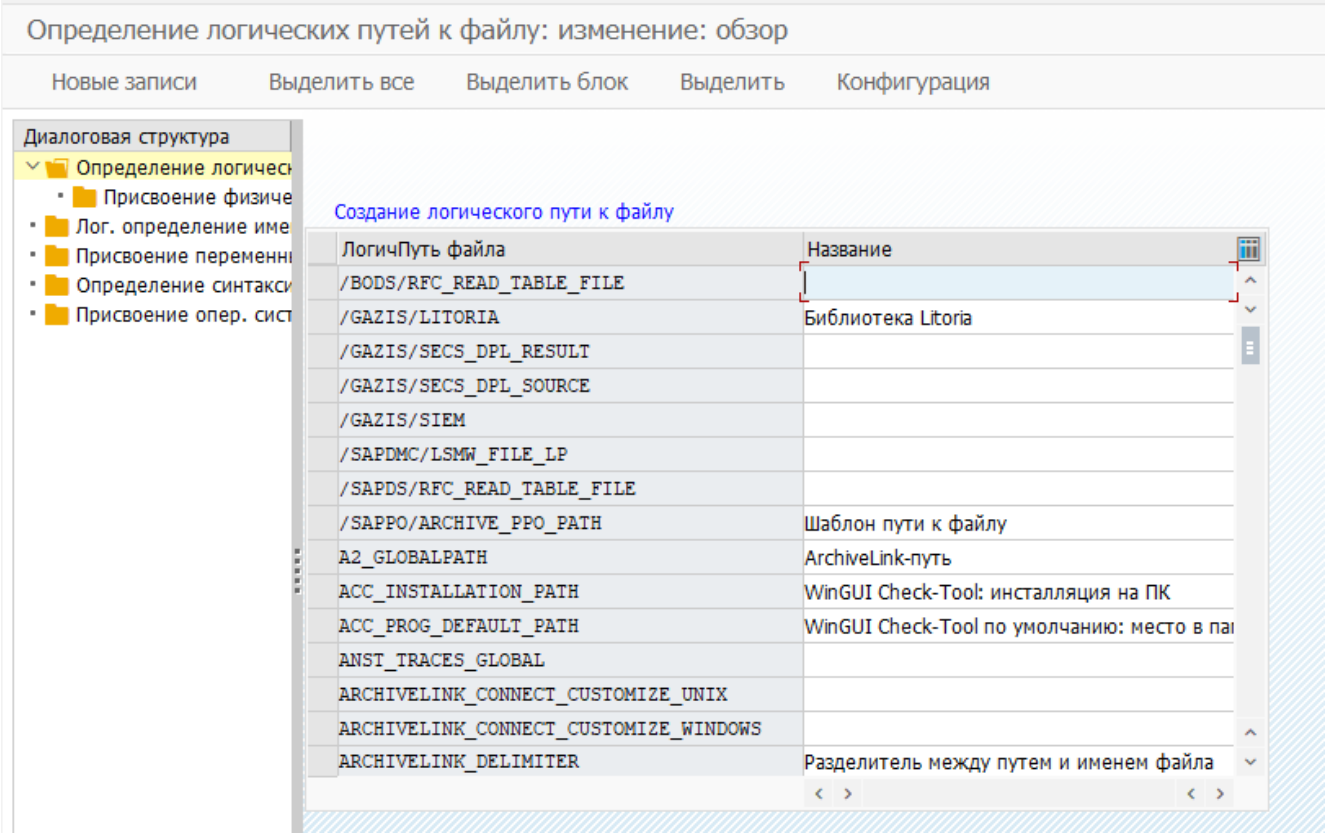


Рисунок 26 – Список каталогов на логическом уровне

Для создания каталога на логическом уровне необходимо нажать кнопку новые записи Новые записи, ввести в столбец «логический путь файла» «/GAZIS/LITORIA» и в столбец «Название» «Папка для лицензий LITORIA». Нажать кнопку .

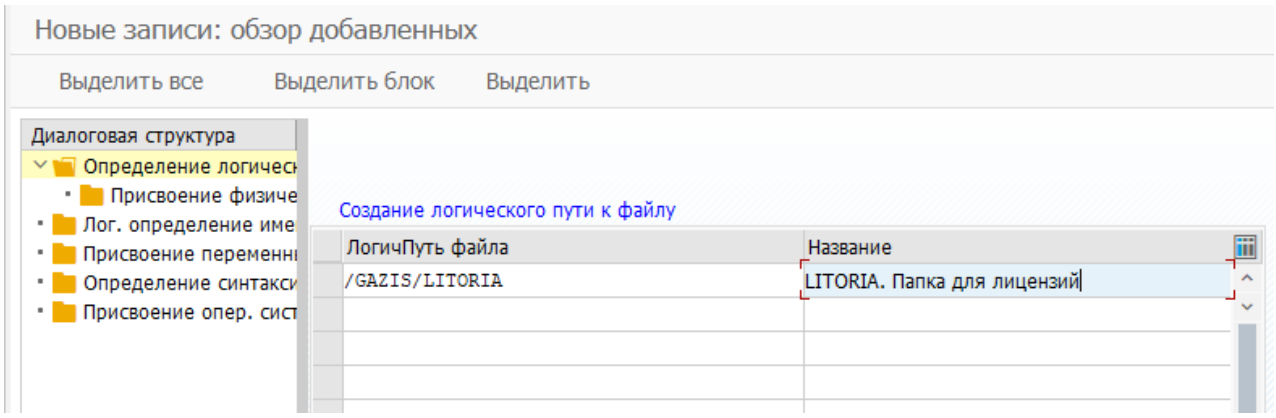


Рисунок 27 – Создание каталога на логическом уровне

4.2.1.3 Генерация запроса на активацию лицензии

Для активации лицензии необходимо установить модуль активации лицензии. Установка представлена в документе «Установка удаление «ПК SafeERP Security Suite».

Для активации лицензии необходимо запустить транзакцию /N/GAZIS/ACTIVATION. Ввести номер ключа лицензии (рис. 28), адрес электронной почты, на которую будет

отправлен ключ активации и файл лицензии, путь для выгрузки файла, а также выбрать имя продукта, нажать кнопку .

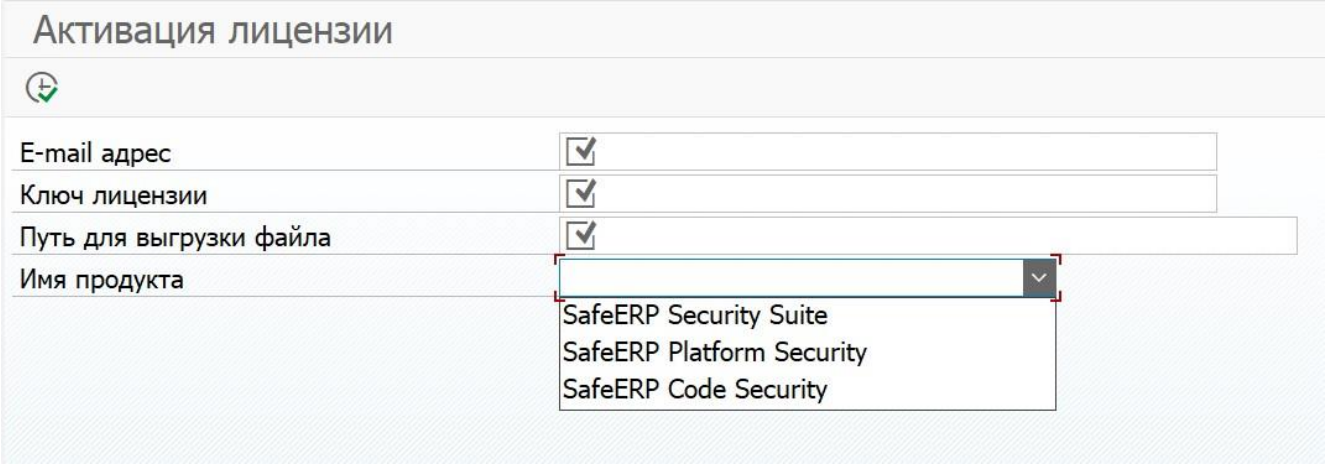


Рисунок 28 – Окно «Активация лицензии»

4.2.1.4 Загрузка файла лицензий

Окно вкладки «Лицензия» консоли настройки параметров SafeERP Suite предназначено для загрузки файла лицензий, в котором определены версии лицензий и доступное количество подключаемых агентов к ПК «SafeERP Security Suite». Файл с лицензиями предоставляется в комплекте поставки ПК «SafeERP Security Suite».

Окно вкладки «Лицензия» представлено на рис. 29.

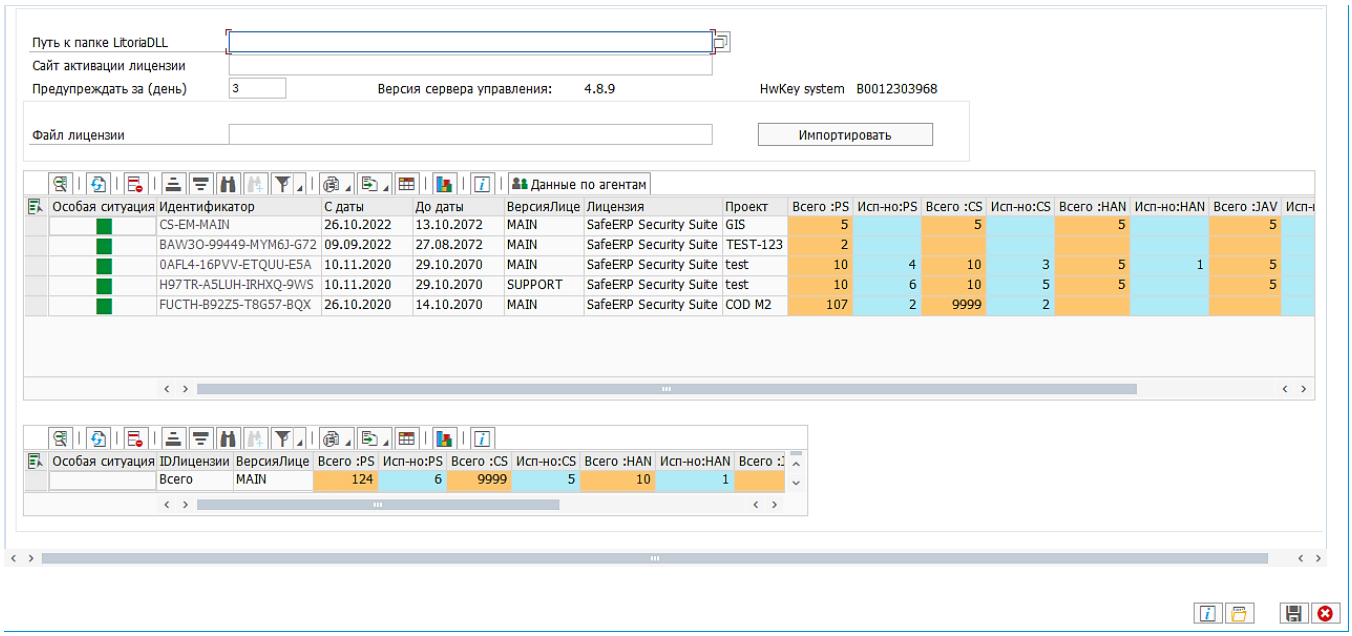


Рисунок 29 – Окно вкладки «Лицензия»

Окно вкладки содержит две области:

1) Загрузка файла лицензии.

В область загрузки файла лицензии включены следующие поля:

— «Путь к папке DLL лицензии» – папка, в которой находятся файлы для активации

лицензии;

— «Сайт активации лицензии» – сайт, на котором необходимо произвести процедуру активации лицензии. Сайт для активации лицензии необходимо уточнить у поставщиков услуг;
— «Файл лицензии» – выбор файла для загрузки лицензии0[1)] (выбор файла осуществляется с помощью кнопки , активация команды импорта файла осуществляется с помощью кнопки Импортировать);
— «Предупреждать за (день)» – выбор периода времени, за который необходимо предупредить об окончании срока действия лицензии;
— «Информация о номере последней установленной версии (релиза) сервера управления ПК SafeERP Security Suite»;
— «Информация о параметре «HwKey system», содержащем хэш-сумму ключа оборудования».

2) Таблицы со списками лицензий.

Первая таблица со списком лицензий содержит в себе информацию о всех приобретённых, действующих и с истекшим сроком действия лицензиях в ПК SafeERP. Вторая таблица содержит общую сумму всех доступных и используемых действительных лицензий (см. рис. 29). Данные в таблице появляются после импорта файла с лицензиями.

В область таблиц включены следующие поля:

— «Особая ситуация» – индикаторы, отображающие статус лицензий: – действительные лицензии, – лицензии с истекающим сроком действия, – с истекшим сроком действия лицензии или лицензии с истекающим сроком действия (время перехода в статус с истекающим сроком действия определяется полем «Предупреждать за (день)»);
— «Идентификатор» – наименование (код) файла лицензии, определяемый при его генерации для таблицы с общей информацией по всем лицензиям, и уточняющая метка «Всего» для таблицы с общей суммой всех доступных и используемых действительных лицензий;
— «С даты» – дата начала действия лицензии;
— «До даты» – дата окончания действия лицензии;
— «Версия лицензии» – определение вида лицензии: «MAIN» – основная лицензия на подключение агентов (может быть двух типов: бессрочная и со сроком действия (временная)) и «SUPPORT» – лицензия на техническую поддержку выбранного программного продукта (как правило, со сроком действия один год);
— «Лицензия» – программный продукт, для которого сформирована лицензия;
— «Имя проекта» – название проекта компании-заказчика, для которого приобретены лицензии на программные продукты SafeERP;
— «Всего: PS количество продуктивных ABAP-агентов» – количество агентов ABAP-системы для проверки программным модулем SafeERP Platform Security;

[1)] Для загрузки лицензии в ПК SafeERP Security Suite используется файл типа «сертификат». Данный файл входит в комплект поставки ПК SafeERP Security Suite

- «Использовано: PS количество продуктивных ABAP-агентов» – количество продуктивных ABAP-системы (количество подключенных систем) для проверки программным модулем SafeERP Platform Security;
- «Всего: CS количество продуктивных ABAP-агентов» – количество агентов на продуктивные ABAP-системы для проверки программным модулем SafeERP Code Security;
- «Использовано: CS количество продуктивных ABAP-агентов» – количество агентов ABAP-системы (количество подключенных систем) для проверки программным модулем SafeERP Code Security;
- «Всего: количество HANA-агентов» – количество агентов на HANA-системы для проверки программным модулем SafeERP Platform Security;
- «Использовано: количество HANA-агентов» – количество агентов на HANA-системы (количество подключенных систем) для проверки программным модулем SafeERP Platform Security;
- «Всего: количество Java-агентов» – количество агентов на Java-системы для проверки программным модулем SafeERP Platform Security;
- «Использовано: количество Java-агентов» – количество агентов на Java-системы (количество подключенных систем) для проверки программным модулем SafeERP Platform Security;
- «Всего: количество BO-агентов» – количество агентов на BO-системы для проверки программным модулем SafeERP Platform Security;
- «Использовано: количество BO-агентов» – количество агентов на BO-системы (количество подключенных систем) для проверки программным модулем SafeERP Platform Security.

4.2.1.5 Загрузка файла с данными по лицензиям

Во вкладке «Лицензии» доступна функция загрузки отчета по лицензиям для агентов.

Для того чтобы скачать отчет по лицензиям необходимо нажать кнопку Данные по агентам (см. рис. 29), выбрать место сохранения excel файла, нажать кнопку «Сохранить».

В файле содержится таблица со следующими столбцами:

- SID – трехзначный идентификатор агента;
- описание – краткое описание агента;
- тип – тип агента, который используется в системе;
- версия – версия агента, который подключен в системе;
- группа – группа, в которую входит агент;
- ID основной лицензии – ключ основной лицензии;
- проект основной лицензии – информационно-управляющая система, к которой подключен агент;
- активность основной лицензии от – дата начала срока действия основной лицензии;

— активность основной лицензии до – дата конца действия основной лицензии;
— ID лицензии поддержки – ключ лицензии поддержки;
— проект лицензии поддержки – информационно-управляющая система, к которой подключен агент;
— активность лицензии поддержки от – дата начала срока действия лицензии поддержки;
— активность лицензии поддержки до – дата конца срока действия лицензии поддержки.

4.2.2 Определение пользователя для сервисного задания

Окно вкладки «Фоновое задание» консоли настройки параметров SafeERP Suite предназначено для определения типа пользователя для запуска фоновых заданий. Окно вкладки «Фоновое задание» представлено на рис. 30.

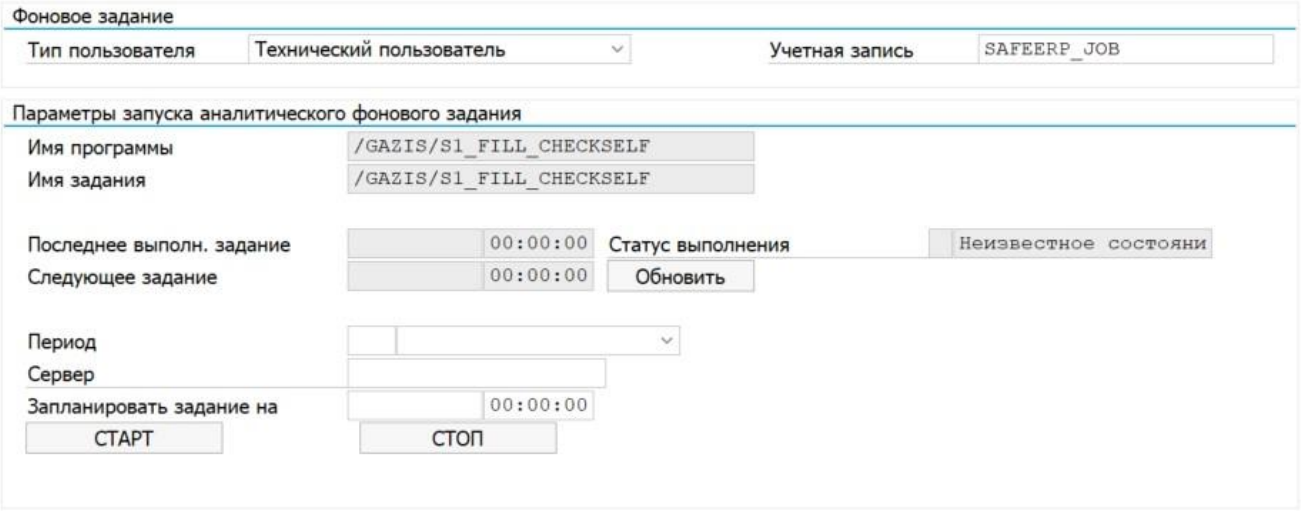


Рисунок 30 – Окно вкладки «Сервисное задание»

Окно вкладки содержит две области:

1) Фоновое задание.

В область фонового задания включены поля:

— «Тип пользователя» – выбор типа пользователя для запуска фоновых заданий: текущий пользователь (учетная запись пользователя, используемая для входа в систему сервера приложения ПК SafeERP Suite), технический пользователь (специальная техническая учетная запись для операций администрирования);
— «Учетная запись» – выбор имени учетной записи пользователя при установке в поле «Тип пользователя» значения «Технический пользователь». Для выбора имени учетной записи необходимо нажать кнопку (рис. 31).

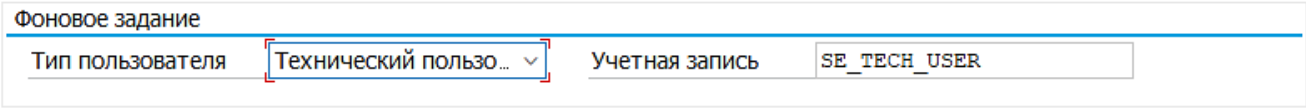


Рисунок 31 – Поле выбора учетной записи технического пользователя

2) Параметры запуска аналитического фонового задания.

В область параметры запуска аналитического фонового задания включены поля:

- «Имя программы» – программа, которая используется в качестве фонового задания;
- «Имя задания» – имя задания, которое используется в качестве фонового задания;
- «Последнее выполн. задание» – дата и время выполнения последнего фонового задания;
- «Статус выполнения» – статус выполнения фонового задания. Статусы бывают следующими: запланирован, загружен, готов, активно, выполнено, прервано;
- «Следующее задание» – дата и время выполнения следующего фонового задания
- «Период» – период запуска фонового задания. Доступны следующие варианты запуска: минута, час, день, неделя, месяц;
- «Сервер» – адрес сервера, через который запускается фоновое задание. Для просмотра необходимо обратиться к транзакции SM36 в SAP GUI.

Примечание. Для обновления задания необходимо нажать кнопку Обновить .

4.2.3 Настройка параметров модуля SafeERP Code Security

Окно вкладки «Code Security» консоли настройки параметров SafeERP Suite предназначено для выбора и определения параметров функционирования модуля SafeERP Code Security.

Окно вкладки «Code Security» представлено на рис. 32.

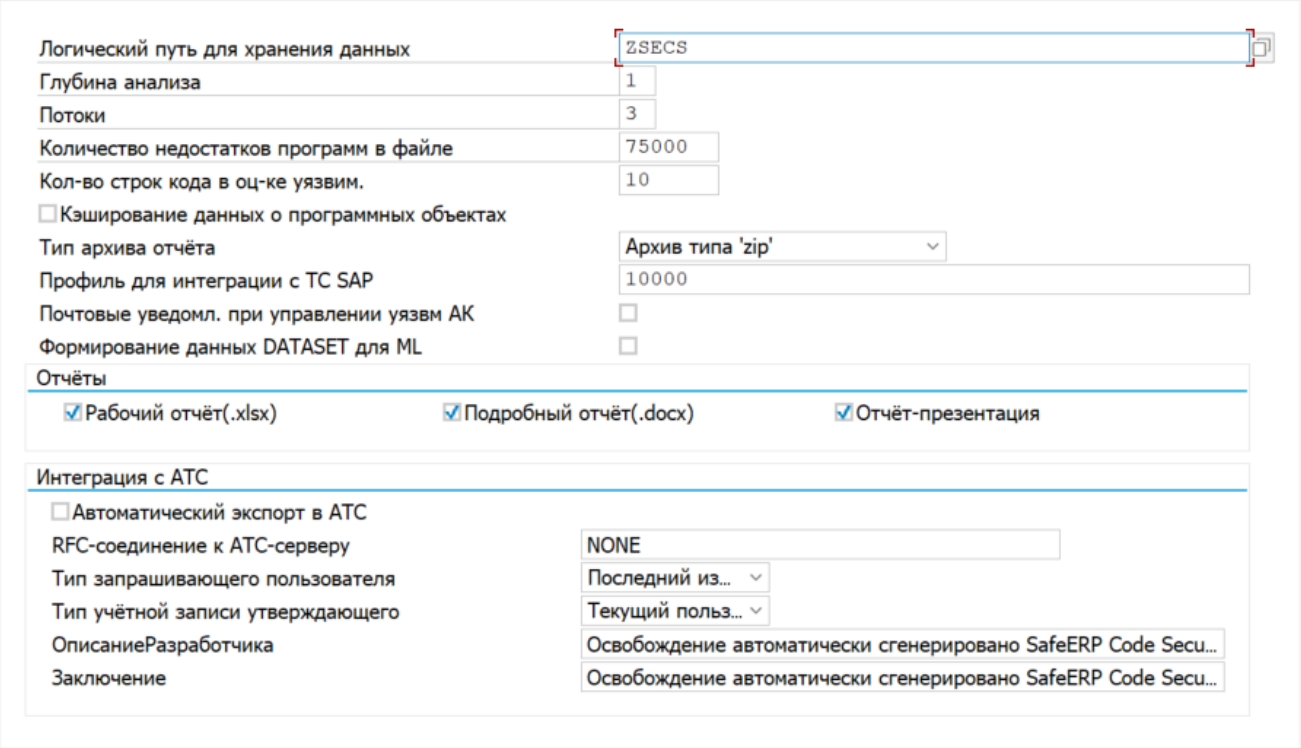


Рисунок 32 – Окно вкладки «Code Security»

Окно вкладки содержит три области:

1) Общие настройки.

В область общих настроек включены поля:

— «Логический путь для хранения данных» – выбор места (имени папки) на дисковом пространстве для выгрузки и хранения отчетов с результатами анализа (выбор осуществляется с помощью кнопки);
— «Глубина анализа» – выбор количества проверяемых цепочек вызовов подпрограмм (при проверке большого количества программ рекомендуемое значение не больше пяти);
— «Потоки» – это последовательность инструкций, которые выполняются параллельно с другими потоками;
— «Количество недостатков программ в файле» – выбор максимального количества строк с перечнем результатов анализа, которое может содержать отчет в формате Excel;
— Элемент выбора «Кэширование данных о программных объектах» отвечает за активацию процедуры сохранения данных о проверяемых программных объектах в базу данных. Кэширование данных позволяет увеличить производительность обработки информации при повторном анализе системы, но при анализе большого количества систем может привести к переполнению базы данных и увеличению требований к ресурсам для ее хранения. Чтобы активировать процедуру кэширования, необходимо установить флаг ☑ в поле элемента;
— «Количество строк кода в оценке уязвимости» – выбор максимального количества строк в программе для анализа кода;
— «Тип архива отчета» – выбор типа архива для сохранения отчета о проверках (типы архива: zip и tar);
— «Профиль для интеграции с ТС SAP» – выбора варианта проверки (профиля), который должен использоваться для анализа кода при деблокировании транспортного запроса на агенте;
— «Почтовые уведомл. при управлении уязвм АК» – активация почтовых уведомлений для инструмента фиксации;
— «Формирование данных DATASET для ML» – активация функциональности по формированию данных для отчета ML в проектах типа АК.

2) Отчеты.

В область отчетов включены элементы выбора:

— «Рабочий отчет (.xlsx)» – активация процедуры сохранения в архив рабочего отчета (в формате .xlsx) для всех итераций анализа. Список документов, формирующихся при активации данной формы отчета, – CHECKS.XLSX, FLAW.XLSX, ITERATION.XLSX, OBJECT.XLSX;
— «Подробный отчет (.docx)» – активация процедуры сохранения в архив подробного отчета (в формате .docx) для всех итераций анализа. Документ, формирующийся при активации данной формы отчета, – REPORT.DOCX;
— «Отчет-презентация (.docx)» – активация процедуры сохранения в архив отчета с

метриками результата анализа по категории «Безопасность» (в формате .docx) для всех итераций анализа. Документ, формирующийся при активации данной формы отчета, – REPORT-METRICS.DOCX.

Чтобы активировать процедуру сохранения отчета, необходимо установить флаг ☑ в поле элемента. Описание отчетов и работы с ними представлено в подпункте 7.1.2.1.4

3) Интеграция с АТС (ABAP Test Cockpit).

В область интеграции с АТС включен элемент выбора «Автоматический экспорт в АТС» для активации процедуры автоматического экспорта данных в АТС. В область интеграции с АТС включены следующие поля настройки интеграции:

— «RFC-соединение к АТС-серверу» – выбор RFC-соединения для подключения к центральной системе проверки АТС (АТС-серверу) (выбор RFC-соединения осуществляется с помощью кнопки);
— «Тип запрашивающего пользователя» – выбор типа пользователя, по действиям которого необходимо формировать уведомления о запросе на утверждение освобождения уязвимости от ложного срабатывания: автор объекта (учетная запись пользователя, под которой создавался программный объект, требующий утверждения), последний изменивший объект (учетная запись пользователя, под которой изменялся программный объект, требующий утверждения), указанный пользователь (выбираемая учетная запись пользователя, от которой разрешается принимать запросы на утверждение освобождений по программным объектам);
— «Тип учетной записи утверждающего» – выбор типа пользователя для получения уведомлений и согласовании запросов на утверждение освобождения уязвимости от ложного срабатывания: текущий пользователь (учетная запись пользователя, используемая для входа в систему сервера приложения ПК SafeERP Suite), указанный пользователь (выбираемая учетная запись пользователя для согласования запросов на утверждение освобождения);
— «Учетная запись» – выбор имени учетной записи пользователя при установке в полях «Тип запрашивающего пользователя» и «Тип учетной записи утверждающего» значения «Указанный пользователь» (рис. 33, 34);

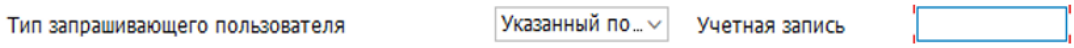


Рисунок 33 – Поле выбора учетной записи для запрашивающего Пользователя

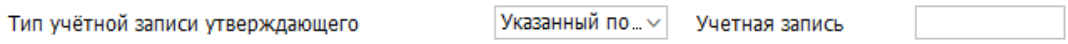


Рисунок 34 – Поле выбора учетной записи для утверждающего Пользователя

— «Описание разработчика» – выбор варианта записи описания разработчика для автоматического заполнения соответствующего поля при утверждении освобождения;
— «Заключение» – выбор варианта записи заключения для автоматического

заполнения соответствующего поля при утверждении освобождения.

4.2.4 Настройка параметров модуля SafeERP Platform Security

Окно вкладки «Platform Security» консоли настройки параметров SafeERP Suite предназначено для выбора и определения параметров функционирования модуля SafeERP Platform Security.

Окно вкладки «Platform Security» представлено на рис. 35.

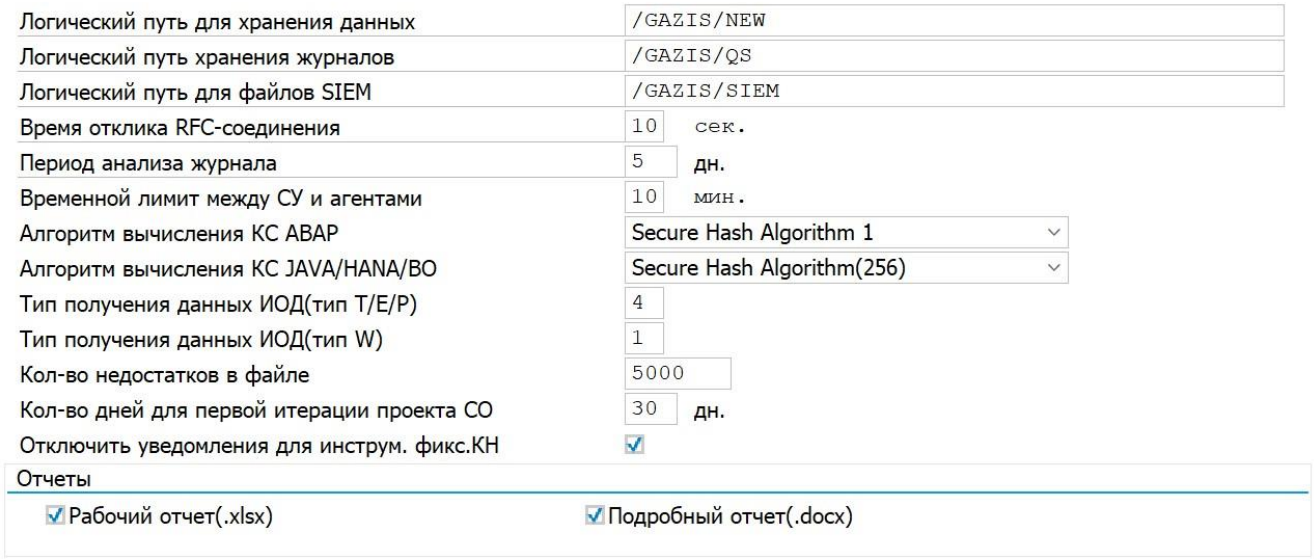


Рисунок 35 – Окно вкладки «Platform Security»

Окно вкладки содержит две области:

1) Общие настройки.

В область общих настроек включены поля:

— «Логический путь для хранения данных» – выбор места (названия папки) на дисковом пространстве для выгрузки и хранения отчетов с результатами анализа;
— «Логический путь хранения журналов» – выбор места (названия папки) на дисковом пространстве для выгрузки и хранения журналов логирования;
— «Логический путь для файлов SIEM» – выбор места (названия папки) на дисковом пространстве для выгрузки и хранения журналов систем;
— «Время отклика RFC-соединения» – выбор максимального времени ожидания проверки отклика от RFC-соединения;
— «Период анализа журнала» – выбор периода чтения лог-файлов из таблиц транзакции SE16 (с момента запуска анализа);
— «Временной лимит между СУ (сервером управления) и агентами» – установка допустимой разницы во времени, установленном на сервере управления и агентах;
— «Алгоритм вычисления КС (контрольных сумм) ABAP» – выбор алгоритма хэширования (вычисления контрольных сумм программных объектов) из пяти представленных вариантов: «ГОСТ Р 34.11-2012», «ГОСТ Р 34.11-94», «СТБ 34.101-2011», «Secure Hash Algorithm 1», «Message Digest 5»;

— «Алгоритм вычисления КС (контрольных сумм) JAVA, HANA, BO» – выбор алгоритма хэширования (вычисления контрольных сумм программных объектов) из двух представленных вариантов: «Secure Hash Algorithm 1» и «Message Digest 5»;
— «Тип получения данных ИОД (тип T/E/P)» – тип получения данных для транзакций, EP Java и программ. Подробное описание представлено в таблице 1;
— «Тип получения данных ИОД (тип W)» – тип получения исходных данных для рабочей книги. Подробное описание представлено в таблице 2;
— «Кол-во недостатков по сценарию в файле» – количество недостатков, которое войдет в отчет Excel;
— «Количество дней для первой итерации проекта CO» – количество дней, за которое будет происходить поиск новых объектов. Минимальное количество дней – 1, максимальное количество дней для первой итерации – 365. По умолчанию задано 30 дней;
— «Отключить уведомления для инструмента фиксации результатов КН» – отключение почтовых уведомлений для инструмента фиксации результатов.

2) История полномочий (отчеты).

В область отчетов включены элементы выбора:

— «Рабочий отчет (.xlsx)» – активация процедуры сохранения в архив рабочего отчета (в формате .xlsx) для всех итераций анализа;
— «Подробный отчет (.docx)» – активация процедуры сохранения в архив подробного отчета (в формате .docx) для всех итераций анализа.

Чтобы активировать процедуру сохранения отчета, необходимо установить флаг ☑ в поле элемента.

Подробное описание алгоритмов работы представлено в таблице 1.

Таблица 1 – Описание алгоритмов для поля «Тип получения данных (тип T/E/P)»

Код	Наименование	Описание
01	Обработка данных на сервере списком ИОД	Алгоритм работы с данными подразумевает чтение лог-файлов с агента на сервер управления и запись их на сервере управления для дальнейшей обработки. После чтения и обработки данные логов удаляются на сервере управления. Это устаревший тип обработки, не рекомендуется к использованию
02	Обработка данных на агенте списком ИОД	С сервера управления посылается список с перечнем объектов: транзакций, программ, BI книг. На агенте собираются данные, которые затем пересылаются на сервер управления. Вариант хорошо работает, когда список ИОД небольшой
03	Обработка данных на агенте по	С сервера управления на агент посылается запрос на получение данных по событиям ИОД. На агенте собираются данные, которые затем пересылаются на

	каждому ИОД на сервере управления	сервер. Данные обрабатываются по одному значению
04	Обработка данных на агенте по каждому ИОД на агенте	С сервера управления посылается список с перечнем объектов: транзакций, программ, BI книг. На агенте собираются данные, которые затем пересылаются на сервер управления. Данные собираются по каждому объекту, объединяются и пересылаются на сервер управления
05	Анализ журнала проверки безопасности, новая версия	Рекомендуется использовать для новых версий SAP-систем. В работе транзакции SM20 произошли изменения: SAP разработал новое ПО, в котором для HANA-систем учитывается также возможность записи событий аудита в БД. Чтение данных в новой версии ПО не совместимы с предыдущими версиями. Рекомендуется использовать только данный тип получения данных ИОД

Подробное описание алгоритмов чтения представлено в таблице 2.

Таблица 2 – Описание алгоритмов для поля «Тип получения данных ИОД (тип W)»

Код	Наименование	Описание
01	Чтение данных из таблиц статистики	Данные событий получают из таблиц БД
02	Данные событий получают из лог-файлов	Данные событий получают из лог-файлов

4.2.5 Активация ландшафта

Окно вкладки «Ландшафт» консоли настройки параметров SafeERP Suite предназначено для настройки параметров карты соединений. Карта соединений представляет собой графическую схему связей (RFC-соединений) всех агент-систем, подключенных к ПК «SafeERP Security Suite».

Окно вкладки «Ландшафт» представлено на рис. 36.

Рисунок 36 – Окно вкладки «Ландшафт»

Окно вкладки содержит две области:

1) Активация карты.

В область активации карты включены элементы и поле выбора:

— элемент «Включить отображение ландшафта в веб-интерфейсе» – активация функции отображения вкладки модуля «Ландшафт» в веб-интерфейсе ПК SafeERP, описание работы с которым приведено в пункте Модуль «Ландшафт» ;

— поле «Имя фонового задания» – установка имени программы с фоновым заданием, выполняющим сбор данных для карты сети (имя программы по умолчанию: /GAZIS/S1_MAP).

Чтобы активировать карту и процедуры сбора данных карты соединений, необходимо установить флаг ☑ в поле элемента.

2) Параметры запуска.

Область параметров запуска содержит следующие поля:

— «Предыдущий запуск» – вывод информации о времени и дате последнего запуска процедуры сбора данных карты соединений;

— «Следующий запуск» – вывод информации о времени и дате следующего запуска процедуры сбора данных карты соединений;

— «Немедленный запуск» – выбор процедуры немедленного запуска сбора данных карты соединений;

— «Период» – период запуска фонового задания. Доступны следующие варианты запуска: минута, час, день, неделя, месяц;

— «Сервер» – адрес сервера, через который запускается фоновое задание. Для просмотра необходимо обратиться к транзакции SM36 в SAP GUI;

— «Дата и время запуска» – дата и время запуска фонового задания.

4.2.6 Анализ данных

Вкладка «Анализ» предназначена для настройки анализа данных, просмотра количества агентов, архивации проекта, временной папки, а также настройки цвета диаграмм во вкладке «Статистика» начальной странице ПК «SafeERP Security Suite».

Вкладка «Анализ» включает в себя три области (рис. 37):

1) Анализ данных.

В область анализа данных включены поля:

— «Период анализа (дней)» – установка периода для сбора и учета данных по результатам анализа систем (по итерациям проектов) для формирования соответствующих аналитик и статистики в панели мониторинга;

— «Период анализа динамический ошибок DUMPs (дней)» – установка периода для сбора и учета данных по дампам (ошибкам) на агенте, связанных с работой ПК «SafeERP Security Suite».

2) Данные по агентам.

Область содержит данные по количеству агентов и количество продуктивных агентов типа ABAP. Отсутствует возможность изменять количество агентов.

3) Архивирование удаленных проекта.

Область содержит данные по времени архивации (дней) – длительность хранения удаленных отчетов о проверках. При превышении заданного времени отчеты о проверках удаляются.

4) Удаление итераций активных проектов.

Временная папка.

В область необходимо указать или выбрать системную папку из списка для временного хранения файлов на сервере приложений.

Примечание. При выборе папки /tmp/ очищение происходит раз в 10 дней. В других случаях необходимо очищать самостоятельно.

5) Настройка цветов.

По умолчанию установлен красный цвет. В области необходимо указать цвет диаграмм, который использует при просмотре стартовой страницы в SAP Fiori. Доступные цвета для настройки: синий (BLUE) и красный (RED).

Примечание. Считывание настройки происходит при первой авторизации или обновлении страницы «SafeERP Security Suite» в браузере.

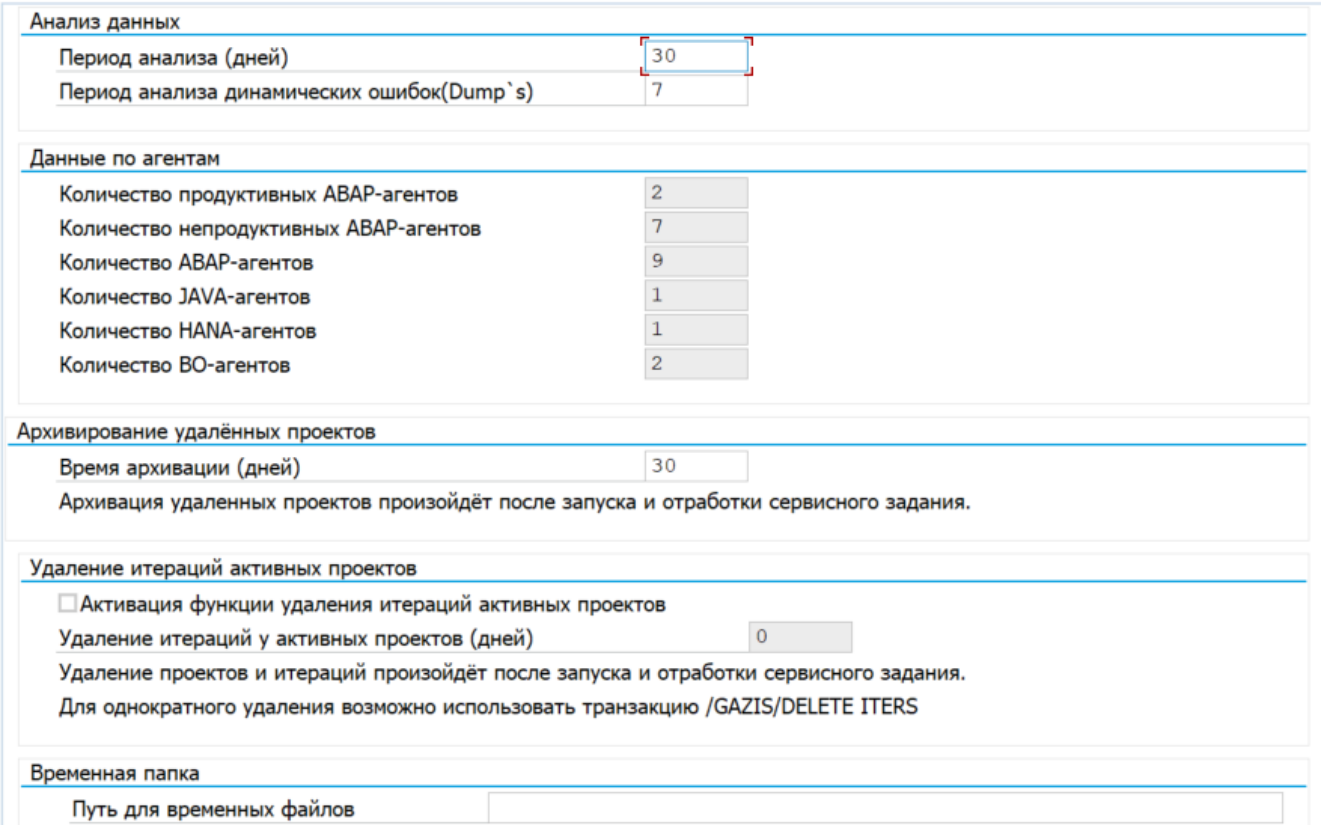


Рисунок 37 – Вкладка «Анализ»

4.2.7 Анализ пользователей с помощью Ankey IDM

Ankey IDM используется для анализа пользователей или ролей с критически важными и потенциально опасными объектами полномочий.

Во время анализа проверяются роли и профили полномочий, присвоенные пользователю.

Для просмотра профиля необходимо выбрать вкладку «Ankey IDM» в консоли настройки параметров SafeERP Suite. Нажать кнопку для выбора профиля (рис. 38).

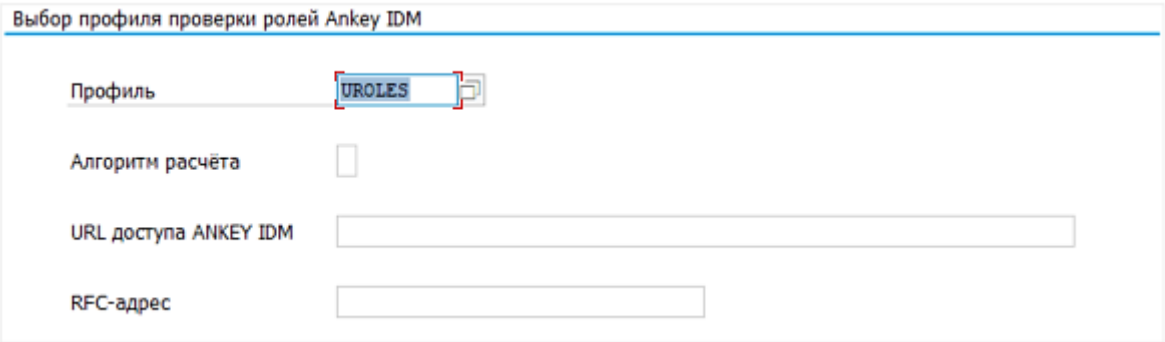


Рисунок 38 – Вкладка «Ankey IDM»

Профиль сканирования (1) 24 Записи найдены

Профиль	ТипСистемы	Описание профиля скан	Профиль по	Кто создал	ДтВрСозд-я	Автор	ДтВрИзм-я
27001	ANY	Профиль стандарта:Инф. тех-ии. М-ды и ср-ва обеспеч. безоп. Системы менеджм. инф. без. требования	✓	HELSHTEYN	26.05.2020 07:35:59		
2SCEN	ANY	2 сценария для теста		NIKANOROVA	13.04.2022 09:22:10		
3SCEN	ANY	3сценария		NIKANOROVA	13.04.2022 09:33:05		
A8_TEST	ANY	тестирование добавления проверок		BICHUK	15.06.2022 12:22:00		
BIZEC_TEC	ANY	Профиль стандарта:BIZEC TEC/11 Версия 2.0	✓	SAFEERP			
CUSTOMS	ANY	пользовательские проверки		ZHDANOVA	22.06.2022 14:17:18		
FSTEC	ANY	Профиль стандарта:Федеральная служба по техническому и экспортному контролю (ФСТЭК России)	✓	SAFEERP			
FZ152	ANY	Профиль стандарта:Федеральный закон РФ от 27 июля 2006 года № 152-ФЗ «О персональных данных»	✓	SAFEERP			
GDPR	ANY	Профиль стандарта:Генеральный регламент о защите данных в ЕС (GDPR)	✓	SAFEERP			
HIPAA	ANY	Профиль стандарта:Акт об ответственности и применимости страхования здоровья	✓	SAFEERP			
ISACA	ANY	Профиль стандарта:ISACA - SAP ERP: Security, Audit and Control Features	✓	SAFEERP			
NIST	ANY	Профиль стандарта:Security and Privacy Controls for Federal Information Systems and Organizations	✓	HELSHTEYN	26.05.2020 07:35:59		
OIL_GAS	ANY	Профиль стандарта:Руководство по безопасности SAP: Нефтегазовая отрасль	✓	SAFEERP			
OWASP	ANY	Профиль стандарта:OWASP Top Ten	✓	SAFEERP			
OWASP_ASVS	ANY	Профиль стандарта:OWASP Application Security Verification Standard	✓	SAFEERP			
PCI_DSS	ANY	Профиль стандарта:Стандарт безопасности данных индустрии платежных карт (PCI DSS)	✓	SAFEERP			
SAP_HANA	ANY	Профиль стандарта:Руководство по безопасности SAP HANA	✓	SAFEERP			
SAP_S_NOTE	ANY	Профиль стандарта:Сервисные ноты SAP	✓	SAFEERP			
SESS_ABAP	ANY	Настройки ППИ согласно ОН ПОИБ для ABAP систем	✓	SAFEERP		DOLGANOVSI	
SESS_BO	ANY	Настройки ППИ согласно ОН ПОИБ для BO систем	✓	SAFEERP			
SESS_HANA	ANY	Настройки ППИ согласно ОН ПОИБ для HANA систем	✓	SAFEERP		SHUBIN	01.10.2020 14:35:59
SESS_JAVA	ANY	Настройки ППИ согласно ОН ПОИБ для Java систем	✓	SAFEERP			
SESS_PRD	PRD	Все сценарии для PRD	✓	SAFEERP			
UROLES	PRD	Ankey IDM		NIKANOROVA	26.03.2022 12:36:29		

24 Записи найдены

Рисунок 39 – Окно «Профиль сканирования»

Консоль Ankey IDM имеет следующие управляющие элементы (рис. 39):

- «Скопировать» – скопировать название профиля во вкладку «Профиль»;
- «Закрыть» – закрыть окно «Профиль сканирования».

В таблицу входят следующие столбцы (рис. 39):

- профиль;
- тип системы;
- описание профиля сканирования;
- профиль полномочий;
- кто создал;
- дата и время создания;
- автор;
- дата и время изменения.

Для анализа пользователей с помощью Ankey IDM необходимо ввести следующие данные:

- профиль – профиль, в котором содержатся проверки для анализа пользователя;
- алгоритм расчета – алгоритм проверок IDM. Алгоритмы подразделяются на следующие типы: общий алгоритм и организационные уровни;
- URL доступа ANKEY IDM – url-адрес, для передачи https post-запроса из Ankey IDM;
- RFC-адрес – RFC-адрес, по которому передаются данные для SAP. Для настройки RFC-соединения необходимо выбирать тип соединения G.

Примечание. Необходимо настроить интеграцию с Ankey IDM для просмотра результатов сканирования.

4.3 Загрузка SAP-нот

Функциональность по загрузке SAP-нот модуля SafeERP Platform Security предназначена для обновления списка SAP-нот на стороне заказчика между обновлениями функциональности (установкой add-on) ПК SafeERP. Файл формируется по запросу и

передается заказчику в формате *sar.

Для запуска консоли по загрузке SAP-нот модуля SafeERP Platform Security необходимо в окне настроек ПК «SafeERP Security Suite» активировать в основном меню пункты «Дополнительные функции» → «Настройка» → «Загрузка Note» (рис. 40).

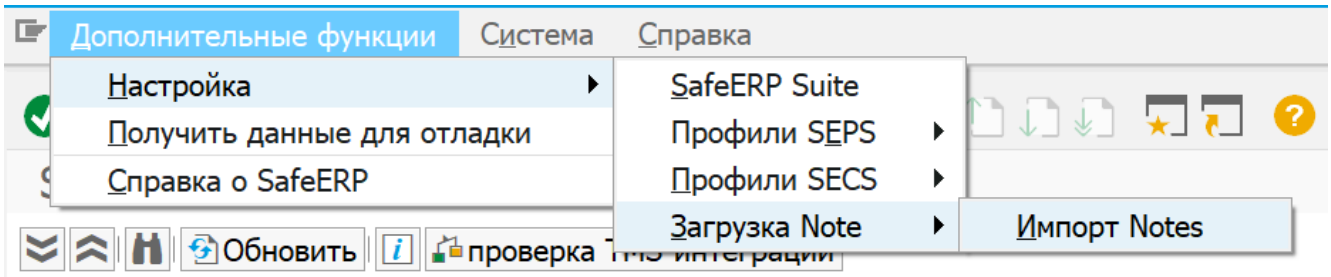


Рисунок 40 – Запуск функциональности по загрузке SAP-нот

При активации пункта меню «Импорт Notes» откроется окно для импорта sar-файла (рис. 41).

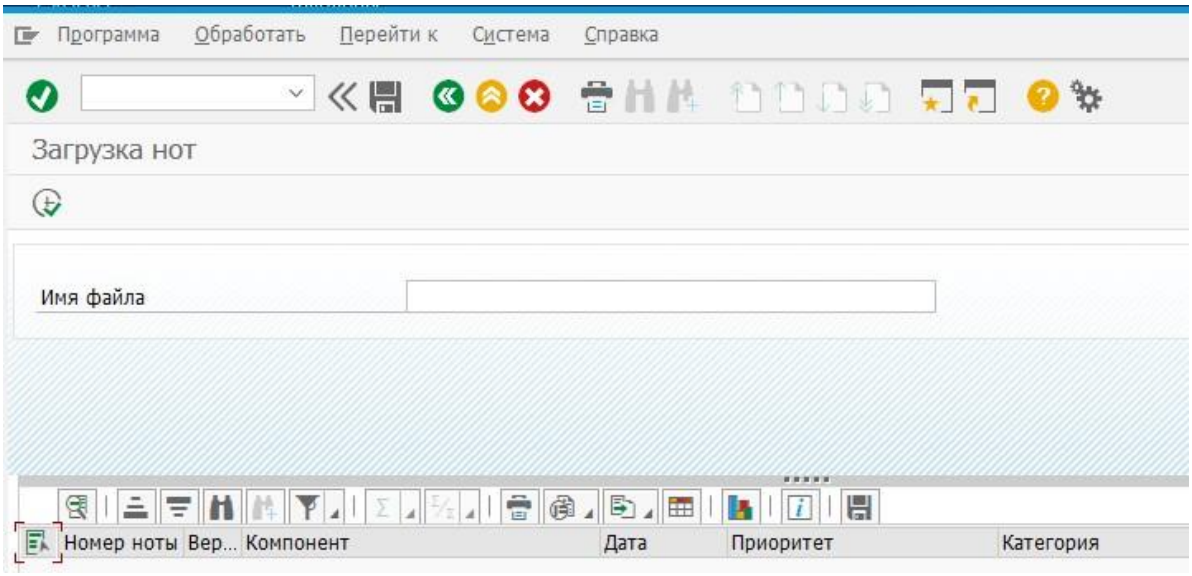
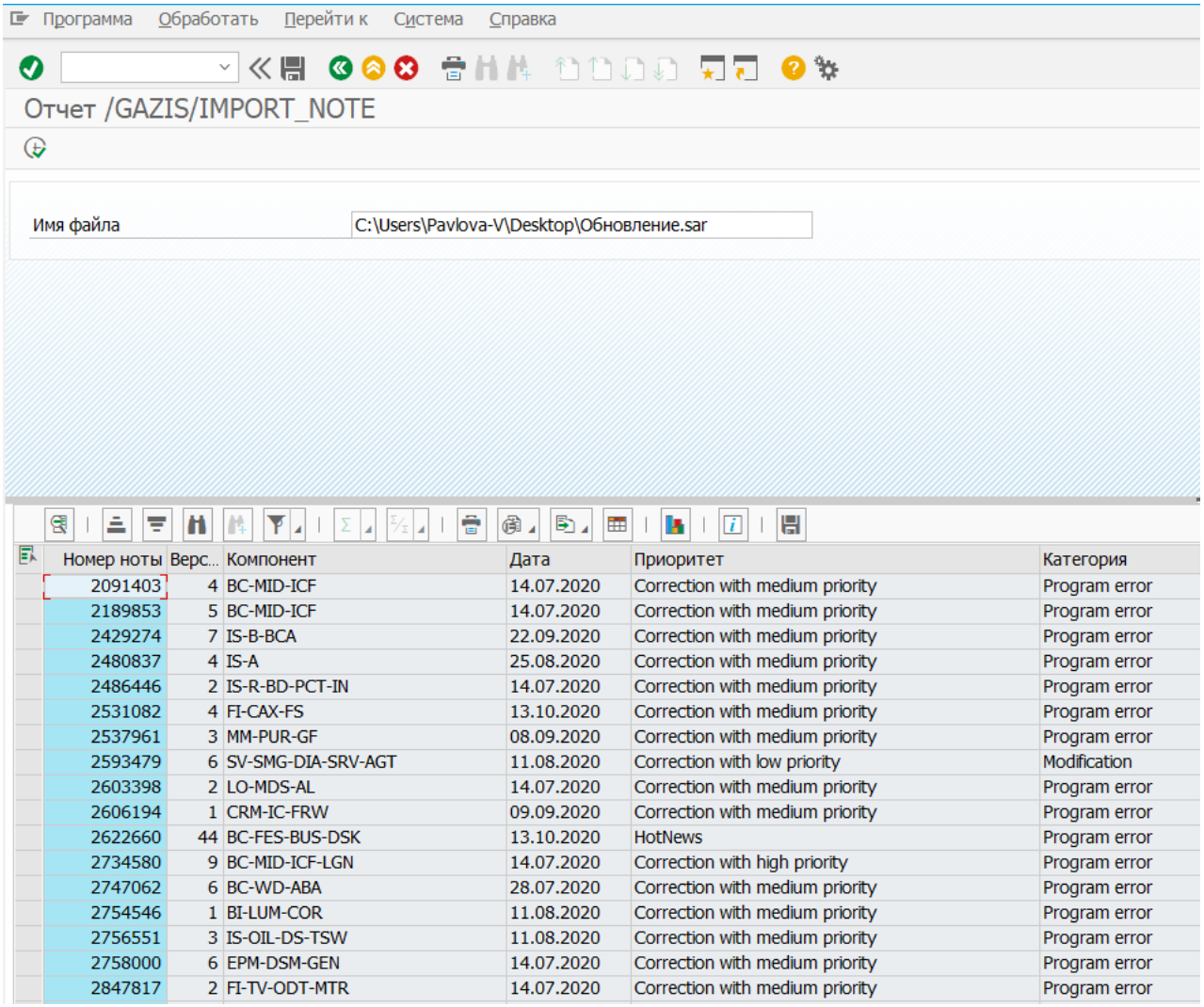


Рисунок 41 – Окно для импорта sar-файла

Для выбора sar-файла необходимо нажать кнопку . Окно выбора sar-файла для импорта аналогично окну загрузки шаблона для импорта профилей, представленного на рис. 40 .

После выбора sar-файла необходимо нажать кнопку «Выполнить» для загрузки списка SAP-нот в таблицу просмотра загружаемых данных, представленную на рис. 42.



Номер ноты	Верс...	Компонент	Дата	Приоритет	Категория
2091403	4	BC-MID-ICF	14.07.2020	Correction with medium priority	Program error
2189853	5	BC-MID-ICF	14.07.2020	Correction with medium priority	Program error
2429274	7	IS-B-BCA	22.09.2020	Correction with medium priority	Program error
2480837	4	IS-A	25.08.2020	Correction with medium priority	Program error
2486446	2	IS-R-BD-PCT-IN	14.07.2020	Correction with medium priority	Program error
2531082	4	FI-CAX-FS	13.10.2020	Correction with medium priority	Program error
2537961	3	MM-PUR-GF	08.09.2020	Correction with medium priority	Program error
2593479	6	SV-SMG-DIA-SRV-AGT	11.08.2020	Correction with low priority	Modification
2603398	2	LO-MDS-AL	14.07.2020	Correction with medium priority	Program error
2606194	1	CRM-IC-FRW	09.09.2020	Correction with medium priority	Program error
2622660	44	BC-FES-BUS-DSK	13.10.2020	HotNews	Program error
2734580	9	BC-MID-ICF-LGN	14.07.2020	Correction with high priority	Program error
2747062	6	BC-WD-ABA	28.07.2020	Correction with medium priority	Program error
2754546	1	BI-LUM-COR	11.08.2020	Correction with medium priority	Program error
2756551	3	IS-OIL-DS-TSW	11.08.2020	Correction with medium priority	Program error
2758000	6	EPM-DSM-GEN	14.07.2020	Correction with medium priority	Program error
2847817	2	FI-TV-ODT-MTR	14.07.2020	Correction with medium priority	Program error

Рисунок 42 – Таблица со списком импортируемых SAP-нот

Для импорта списка SAP-нот в систему необходимо нажать кнопку «Сохранить». В случае успешной загрузки списка SAP-нот будет выведено информационное сообщение (рис. 43).

Рисунок 43 – Информационное сообщение о загрузке SAP-нот

Загруженный список SAP-нот появится в перечне сценариев стандартных проверочных профилей модуля SafeERP Platform Security.

4.4 Запуск ПК SafeERP Platform Security Suite

Для запуска необходимо обратиться к транзакции /N/GAZIS/SEPS.

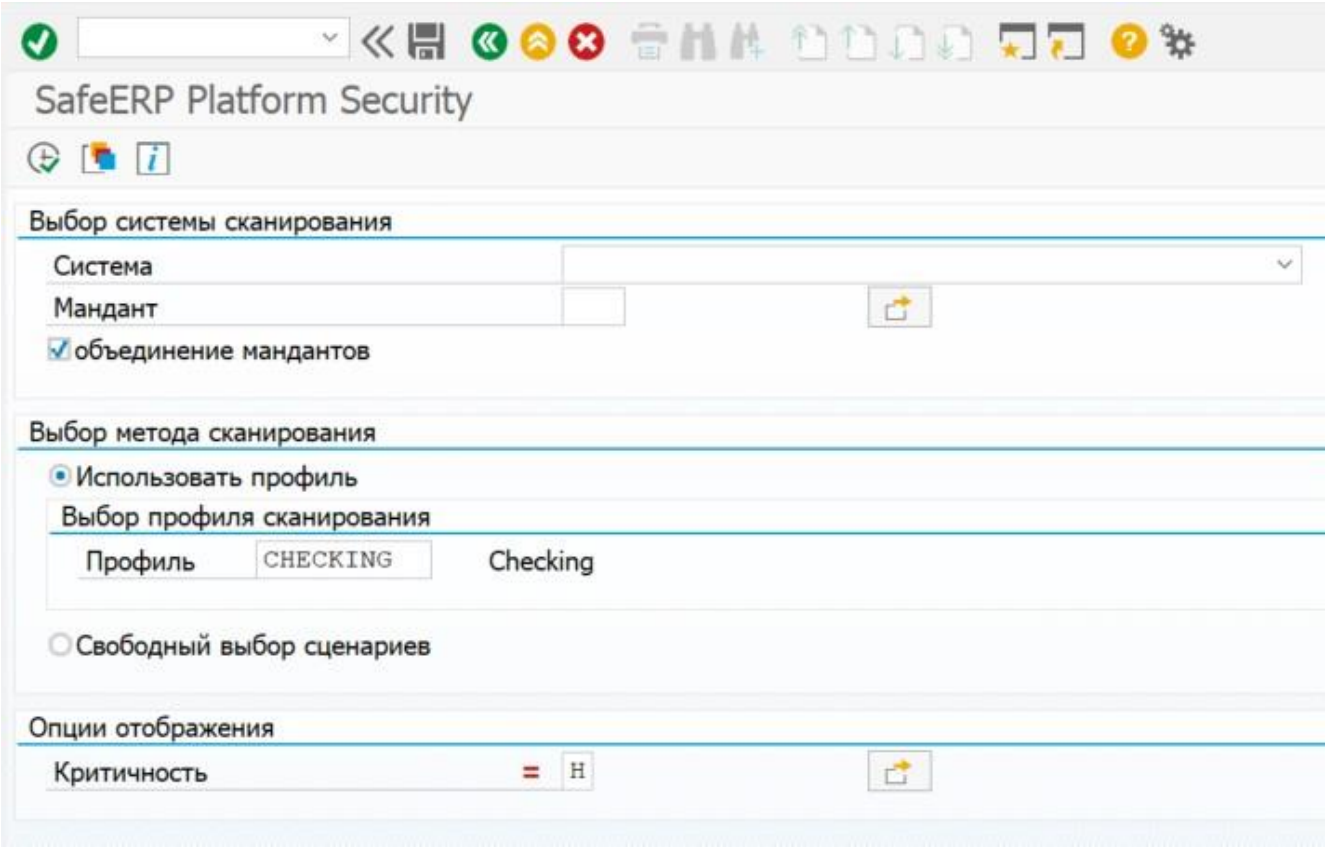


Рисунок 44 – Основная рабочая область транзакции /N/GAZIS/SEPS

В окно транзакции входят следующие области (рис. 44):

— «Выбор системы сканирования». Данная область предназначена для выбора системы и манданта системы.
  Примечание. При выборе манданта доступен множественный выбор. Для множественного выбора необходимо нажать кнопку «Множественный выбор», нажать кнопку *«Многократный выбор…»* в окне «Многократный выбор для Мандант», нажать кнопку «Скопировать» в окне «Многократный выбор для Мандант».
— «Выбор метода сканирования». Данная область предназначена выбора профилей или сценария для сканирования.
  Примечание. При выборе сценария доступен множественный выбор. Для множественного выбора необходимо нажать кнопку «Множественный выбор».
— «Опции отображения». Данная область предназначена для настройки критичности.
  Примечание. При выборе критичности доступен выбор нескольких критериев. Для выбора критичностей необходимо нажать кнопку *«Многократный выбор…»* в окне «Многократный выбор для Критичность», нажать кнопку *«Скопировать»*

в окне «Многократный выбор для Критичность».

Для запуска сканирования системы необходимо выполнить следующие действия:

1) Выбрать систему и мандант в области «Выбор системы сканирования».
2) Выбрать профиль или сценарии для сканирования в области «Выбор метода сканирования».
3) Выбрать критичность в области «Опции отображения». Нажать кнопку *«Выполнить»* .

Примечание. После завершения сканирования оператору доступен просмотр результатов сканирования (рис. 45), а также выгрузка отчета. Для выгрузки отчета необходимо нажать кнопку *«Выгрузка в»* , выбрать место сохранения файла.

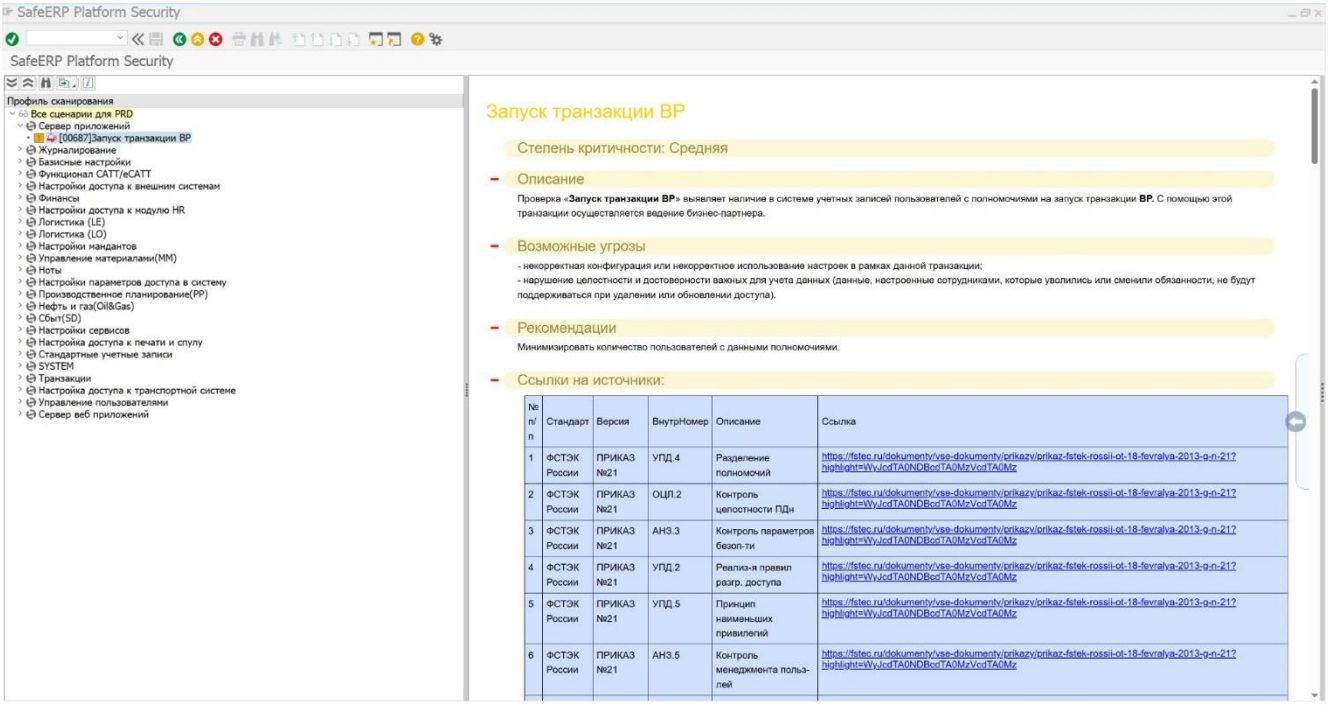


Рисунок 45 – Результаты анализа проекта

4.5 Запуск ПК SafeERP Code Security Suite

Для запуска сканирования проектов типа «Анализ кода» необходимо обратиться к транзакции /N/GAZIS/SECS.

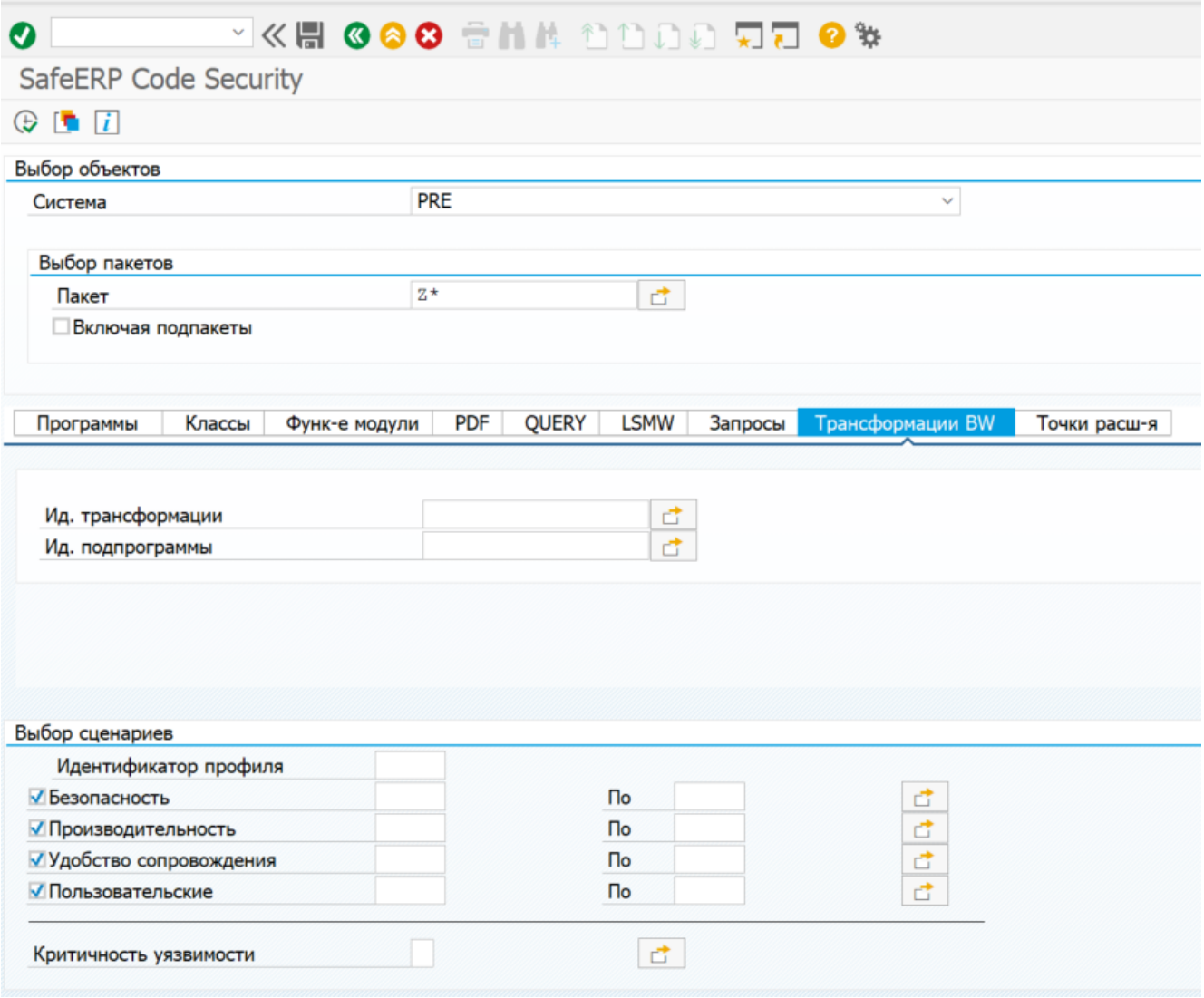


Рисунок 46 – Окно транзакции /N/GAZIS/SECS

В окно транзакции входят следующие области (рис. 46):

- «Выбор объектов». Данная область предназначена для выбора системы;
- «Выбор объектов для анализа». Данная область предназначена для выбора объектов анализа. Доступны следующие объекты: программы, классы, функциональные модули, PDF, QUERY, LSMW, запросы, трансформации BW, точки расширения;
- «Выбор сценариев». Данная область предназначена для выбора профиля сканирования и настройки критичности.

Для запуска анализа необходим выполнить следующие действия:

1) Выбрать систему в области «Выбор объектов». Выбрать пакет в области «Выбор объектов», нажать кнопку *«Enter»* (см. рис. 46).

2) Выбрать тип объекта и ввести данные объектов. Нажать кнопку *«Enter»*.

3) Нажать кнопку *«Выполнить»* .

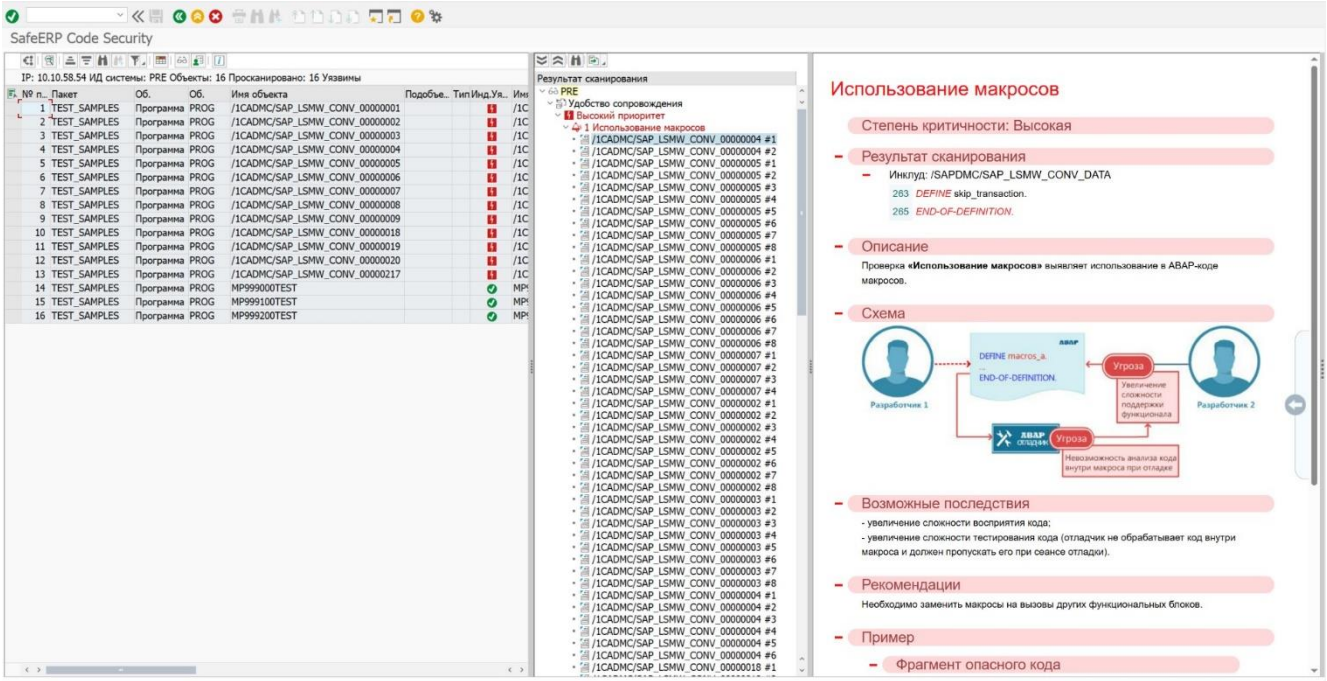


Рисунок 47 – Результаты анализа

Для просмотра найденной уязвимости необходимо выбрать пакет из списка, нажать кнопку «Анализ выбранных объектов» (рис. 47), выбрать группу проверок в области «Результат сканирования», критичность, проверку, уязвимость.

Примечание. После завершения сканирования доступна выгрузка отчета. Для выгрузки отчета необходимо выбрать проверку, нажать кнопку *«Выгрузка в»* (рис. 47), выбрать место сохранения файла.

Анализ трансформаций BW

В ПК «SafeERP Security Suite» реализована функциональность по анализу трансформаций BW. Доступен анализ трансформаций BW как объектов сканирования, а также анализ транспортных запросов, в которые входят объекты трансформации BW.
Анализ трансформаций осуществляется следующими способами:

— через вкладку «Запросы»;
— через вкладку «Трансформации BW».

Для запуска анализа трансформации через вкладку «Запросы» необходимо выполнить следующие действия:

1) Ввести наименование транспортного запроса. Нажать кнопку *«Выполнить»* (рис. 48).

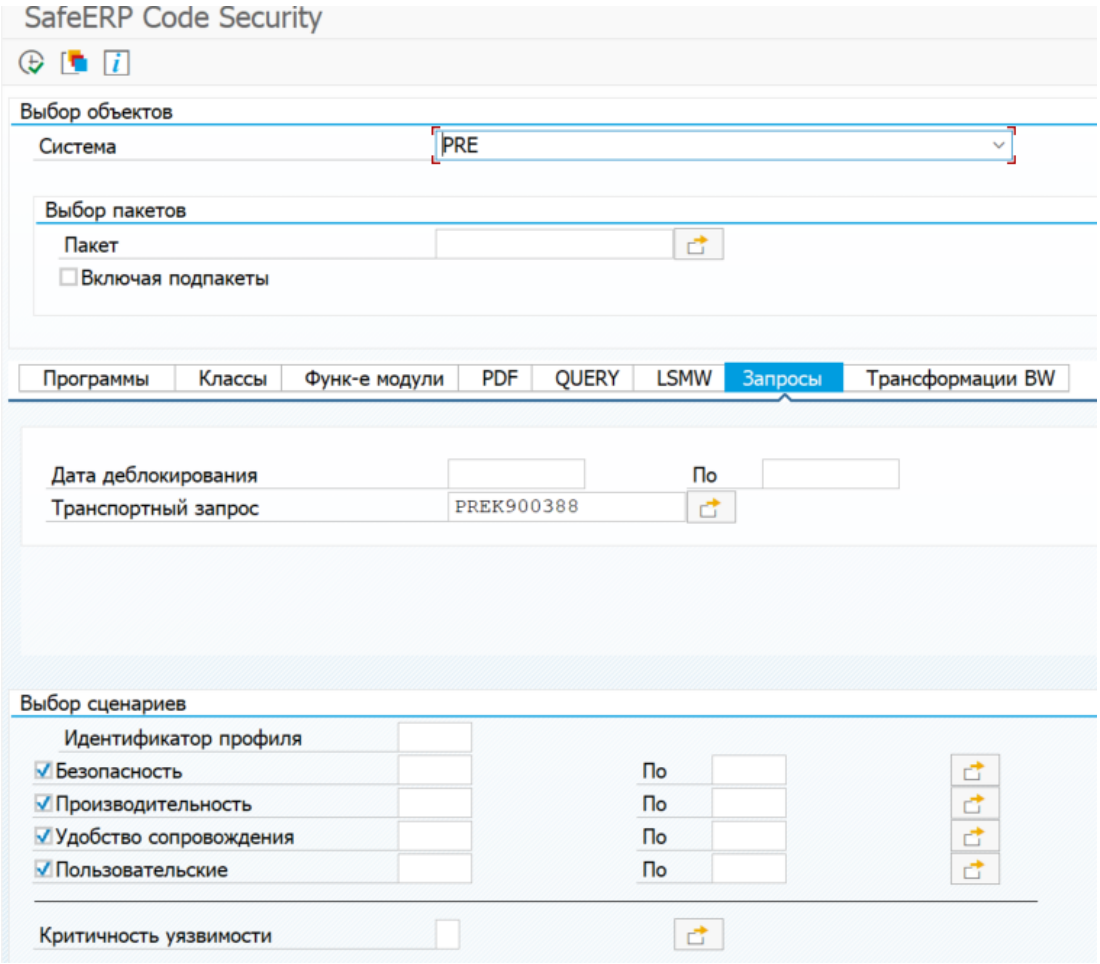


Рисунок 48 – Вкладка «Запросы»

2) Выбрать подпрограмму (ROUT) из списка. Нажать кнопку *«Анализ выбранных объектов»* (рис. 49).

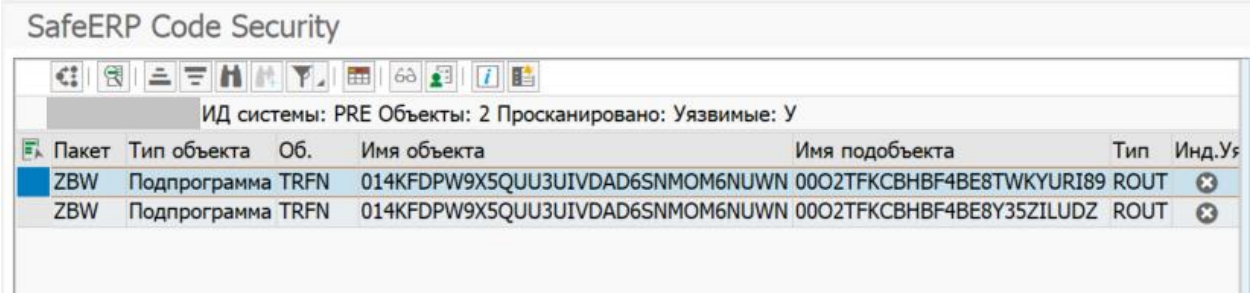


Рисунок 49 – Список подпрограмм (ROUT)

Примечание. При запуске анализа через вкладку «Запросы» статус транспортного запроса не влияет на результат сканирования.

Для запуска анализа трансформации через вкладку «Трансформации» необходимо выполнить следующие действия:

1) Ввести идентификаторы в поля «Ид. трансформации» или «Ид. Подпрограммы» (рис. 50). Нажать кнопку *«Выполнить».*

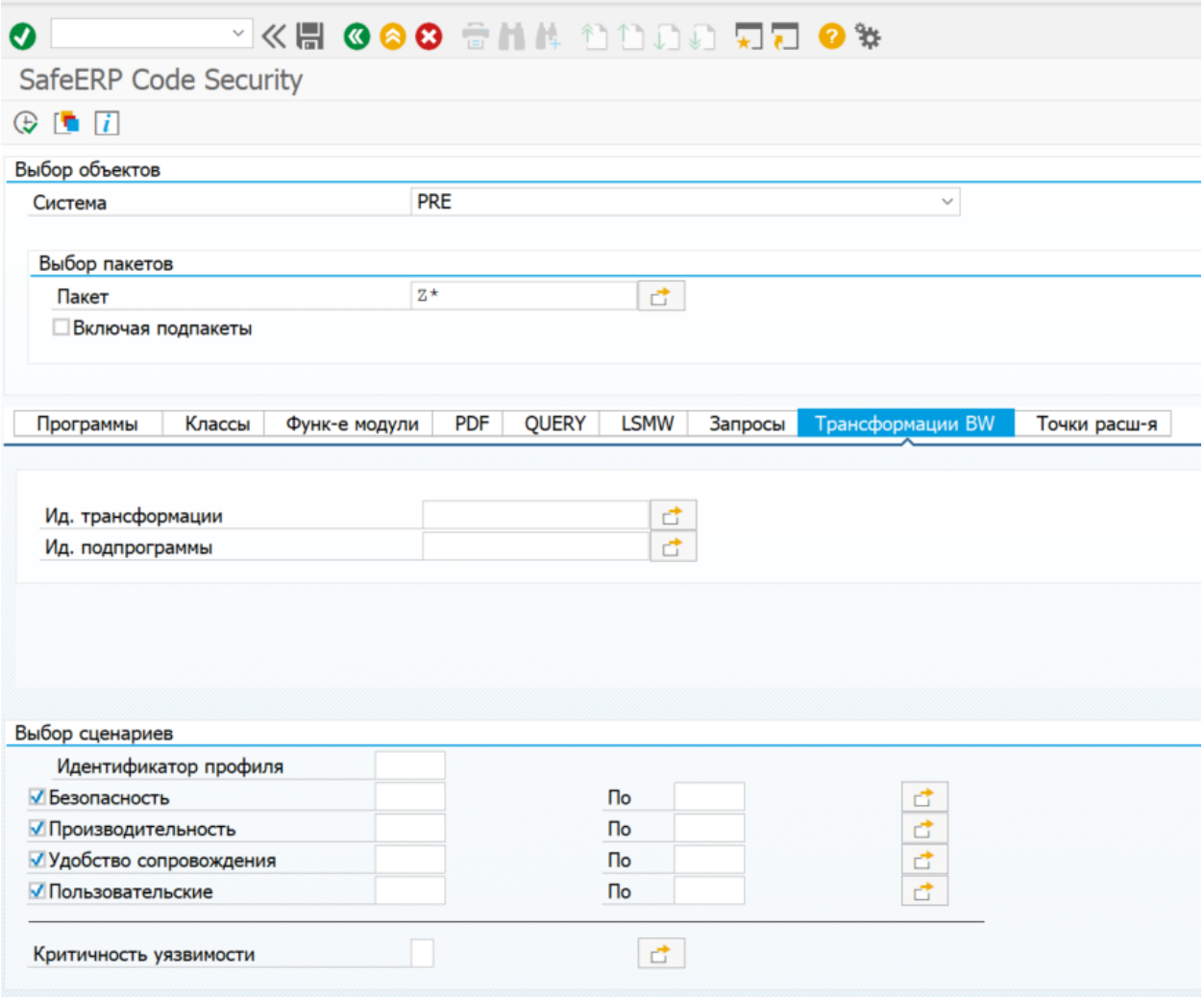


Рисунок 50 – Вкладка «Трансформации BW»

2) Выбрать подпрограмму из списка. Нажать кнопку *«Анализ выбранных объектов»* (см. рис. 49).

Анализ точек расширения (Реализация)

В ПК «SafeERP Security Suite» реализована функциональность по анализу точек расширения. Доступен анализ точек расширения (ENHO) как объектов сканирования, а также анализ транспортных запросов, в которые входят объекты точки расширения.

Анализ точек расширений (реализация) осуществляется следующими способами:

— через вкладку «Запросы»;
— через вкладку «Точки расширения».

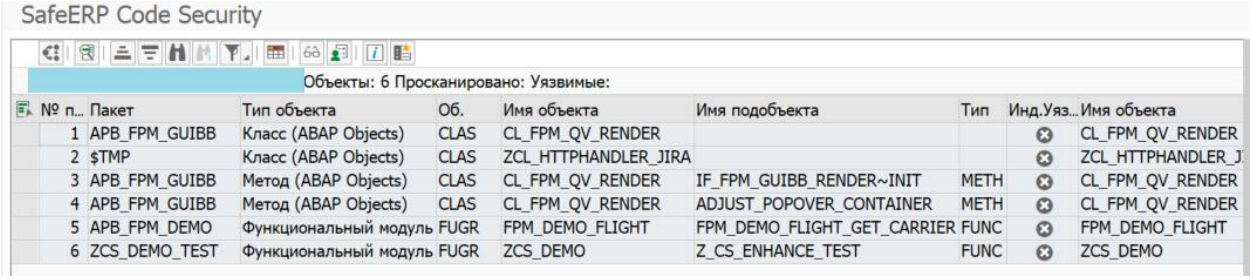
Для запуска анализа точек расширения (реализация) через вкладку «Запросы» необходимо выполнить следующие действия:

1) Ввести наименование транспортного запроса. Нажать кнопку *«Выполнить»* (рис. 48).

2) Выбрать объект сканирования из списка. Нажать кнопку *«Анализ выбранных объектов»* (рис. 49).

Для запуска анализа точек расширения (реализация) через вкладку «Точки расширения» необходимо выполнить следующие действия:

1) Ввести идентификатор в поле «Точки расширения (Реализация)». Нажать кнопку *«Выполнить».*
2) Выбрать объекты из списка. Нажать кнопку *«Анализ выбранных объектов»* (рис. 51).



№ п...	Пакет	Тип объекта	Об.	Имя объекта	Имя подобъекта	Тип	Инд.Уяз...	Имя объекта
1	APB_FPM_GUIBB	Класс (ABAP Objects)	CLAS	CL_FPM_QV_RENDER				CL_FPM_QV_RENDER
2	$TMP	Класс (ABAP Objects)	CLAS	ZCL_HTTPHANDLER_JIRA				ZCL_HTTPHANDLER_J
3	APB_FPM_GUIBB	Метод (ABAP Objects)	CLAS	CL_FPM_QV_RENDER	IF_FPM_GUIBB_RENDER~INIT	METH		CL_FPM_QV_RENDER
4	APB_FPM_GUIBB	Метод (ABAP Objects)	CLAS	CL_FPM_QV_RENDER	ADJUST_POPOVER_CONTAINER	METH		CL_FPM_QV_RENDER
5	APB_FPM_DEMO	Функциональный модуль	FUGR	FPM_DEMO_FLIGHT	FPM_DEMO_FLIGHT_GET_CARRIER	FUNC		FPM_DEMO_FLIGHT
6	ZCS_DEMO_TEST	Функциональный модуль	FUGR	ZCS_DEMO	Z_CS_ENHANCE_TEST	FUNC		ZCS_DEMO

Рисунок 51 – Выбор объектов сканирования

4.6 Настройка почтовых уведомлений

Для уведомления о совершенных действиях пользователя в системах требуется настроить почтовые уведомления.

Для настройки почтовых уведомлений, необходимо ввести транзакцию /N/GAZIS/MAIL в командную строку (см. рис. 121). На рис. 52 представлен интерфейс и данные таблицы «Настройка уведомлений SafeERP».

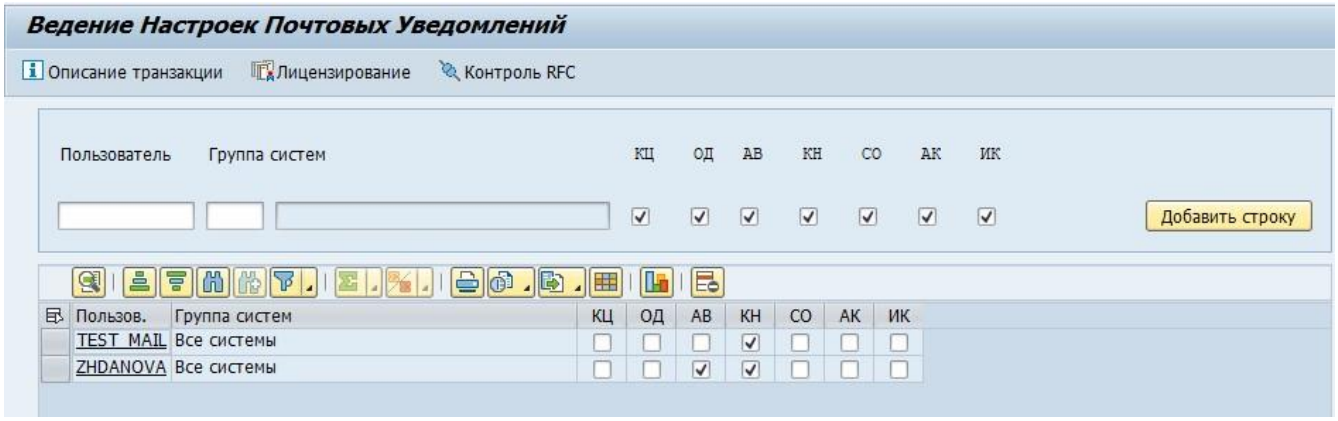


Рисунок 52 – Таблица «Настройка уведомлений SafeERP»

В таблицу «Настройка уведомлений SafeERP» входят следующие столбцы:

- пользователь – пользователи, зарегистрированные в системе;
- группа систем – системы, которые объединены по определенным признакам;
- тип проекта – проекты, которые входят в базу данных. Проекты бывают следующих типов: контроль целостности (КЦ), объекты доступа (ОД), авторизации

(АВ), контроль настроек (КН), создание объектов (СО), анализ кода (АК), инвентаризация кода (ИК).

Почтовые уведомления для модулей «Сканер» и «Анализ кода» поступают в следующих случаях:

- после окончания процедуры сканирования проекта (в том числе и без результатов сканирования);
- при обнаружении ошибок в проекте.

Для того чтобы пользователь получал почтовые уведомления об изменениях в системе или в проектах определенного типа, необходимо нажать кнопку Добавить строку, с помощью кнопки выбрать пользователя и тип проекта в соответствующих столбцах, установить флаг напротив типа проекта установить флаг в поле соответствующего элемента, нажать кнопку «Сохранить» .

Почтовые уведомления для лицензий используются в следующих случаях:

- срок действия основной лицензии истек;
- срок действия лицензии поддержки истек;
- срок действия основной лицензии истекает;
- срок действия лицензии поддержки истекает;
- основная лицензия для агента не присвоена;
- непродуктивный ABAP-агент и ссылки на лицензии были удалены;
- лицензии для агента не обнаружены;
- лицензии для агента были удалены.

Для настройки почтовых уведомлений для лицензии необходимо нажать кнопку Лицензирование, в открывшемся окне нажать кнопку (рис. 53), выбрать пользователя из списка с помощью кнопки (рис. 54), нажать кнопку «Далее» , нажать кнопку «Сохранить» .

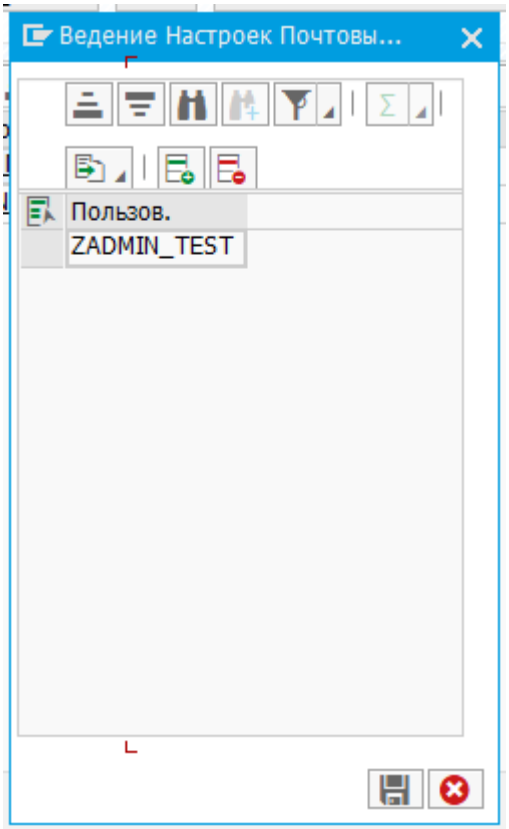


Рисунок 53 – Окно «Ведение настроек почтовых уведомлений»

Рисунок 54 – Окно выбора пользователя

Почтовые уведомления для RFC-соединений поступают в следующих случаях:

- создание RFC соединения (при создании RFC-соединения указывается система, где произошло изменение, RFC-соединение и целевой хост);
- изменении RFC соединения (указывается система, где произошло изменение, RFC-соединение, техническое наименование атрибута и его описание, а также старое и новое значение атрибута);
- удаление RFC соединения (при удалении RFC-соединения указывается система, где произошло изменение, RFC-соединение и целевой хост).

Для настройки почтовых уведомлений для RFC-соединений (модуль «Ландшафт» SAP FIORI) необходимо нажать кнопку Контроль RFC, в открывшемся окне нажать кнопку (рис. 53), выбрать пользователя из списка с помощью кнопки (рис. 54), нажать

кнопку «Далее» , нажать кнопку «Сохранить» .

Примечание. В транзакции предусмотрен настройка получения почтовых уведомлений по степени результата критичности (для проектов типа КН и АК), а также при отсутствии уязвимостей. Для получения почтовых уведомлений по результатам критичности необходимо выполнить следующие действия:

1) Выбрать пользователя в соответствующем столбце (рис. 52).
2) Выбрать тип проекта, критичность в открывшемся окне (рис. 55). Нажать кнопку «Сохранить».

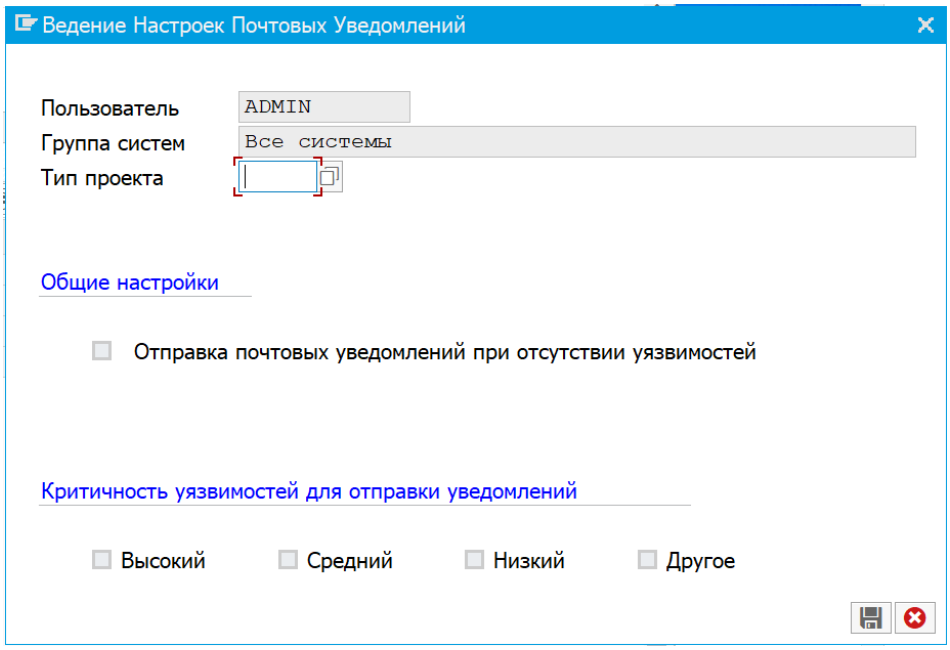


Рисунок 55 – Окно настройки критичности

После того, как пользователь совершил действия, на электронную почту приходят уведомления (см. рис. 56, 57).

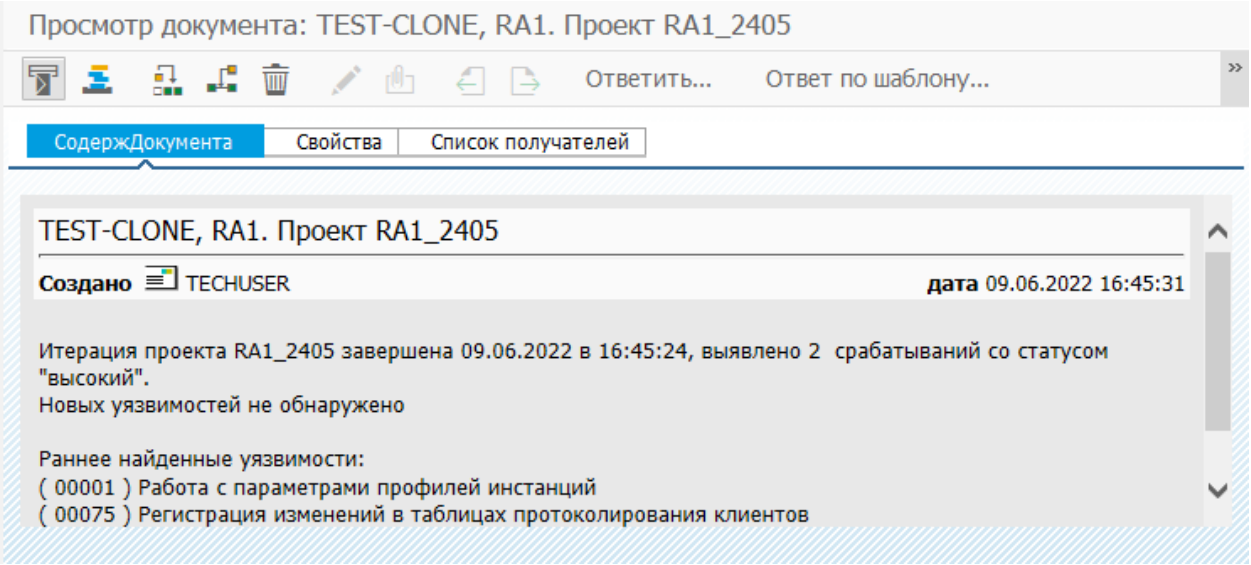


Рисунок 56 – Уведомление в окне «Входящая почта» в SAP GUI

Тема **TEST-CLONE, RA1. Проект RA1_2405**
От TECHUSER
Кому ZHDANOVA
Дата Сегодня 13:45

Итерация проекта RA1_2405 завершена 09.06.2022 в 16:45:24, выявлено 2 срабатываний со статусом "высокий".

Новых уязвимостей не обнаружено

Раннее найденные уязвимости:

(00001) Работа с параметрами профилей инстанций

(00075) Регистрация изменений в таблицах протоколирования клиентов

Рисунок 57 – Уведомление, полученное по электронной почте

SafeERP. Изменения в RFC-соединениях — 1 сообщение

От: "TECHUSER" <safeerp@datagile.ru> — 16 Январь 2024 г. 15:14
Кому: "Алексей Юрьевич Александров" <aleksandrov-ay@datagile.ru>

Добрый день. Были обнаружены изменения в RFC-соединениях.

Созданы новые RFC:

Система	RFC-соединение	Целевой хост
GIS	Test_1	10.10.58.36

Рисунок 58 – Созданное RFC-соединение

SafeERP. Изменения в RFC-соединениях

От: "TECHUSER" <safeerp@datagile.ru>
Кому: "Алексей Юрьевич Александров" <aleksandrov-ay@datagile.ru>

Добрый день. Были обнаружены изменения в RFC-соединениях.

Изменены следующие RFC:

Система	RFC-соединение	Атрибут	Описание атрибута	Старое значение	Новое значение
GIS	Test_1	RFCHOST	Целевой хост	10.10.58.38	10.10.58.95

Рисунок 59 – Измененное RFC-соединение

SafeERP. Изменения в RFC-соединениях — 1 сообщение

От: "TECHUSER" <safeerp@datagile.ru> — 26 Декабрь 2023 г. 13:40
Кому: "Алексей Юрьевич Александров" <aleksandrov-ay@datagile.ru>

Добрый день. Были обнаружены изменения в RFC-соединениях.

Удалены следующие RFC:

Система	RFC-соединение	Целевой хост
TST	TST_Test1	test.host.tst111
	TST_Test3	
	TST_Test5	

Рисунок 60 – Удаленное RFC-соединение

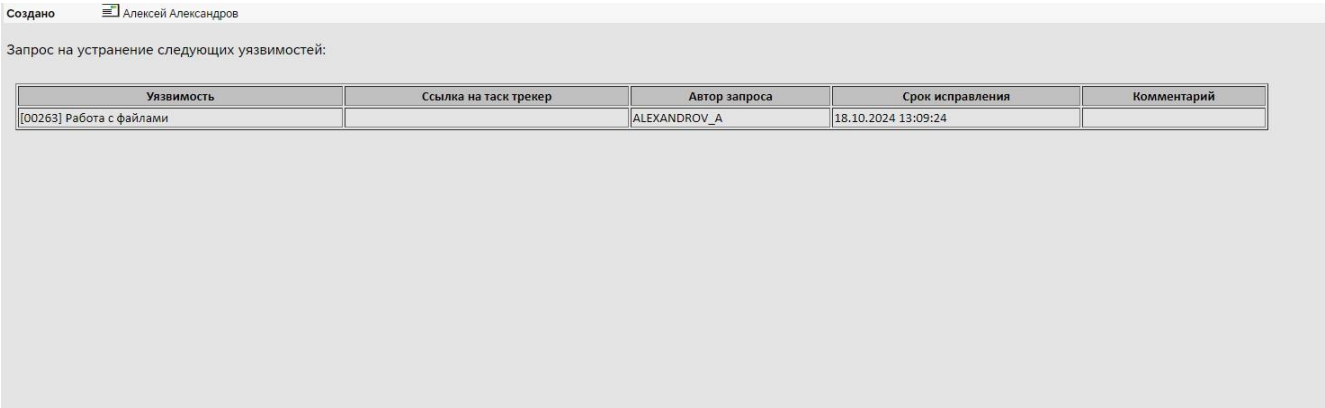


Рисунок 61 – Запрос на устранение выявленной уязвимости

Примечания:

1. Адрес электронной почты пользователя должен находиться в базе данных.
2. Необходимо настроить интеграцию с почтовым сервером компании.

4.7 Мониторинг фоновых заданий

Для отслеживания фоновых заданий используется транзакция /N/GAZIS/MONJOBS.

Для запуска мониторинга фонового задания необходимо ввести /N/GAZIS/MONJOBS в командную строку.

Первоначальный экран представлен на рис. 62.

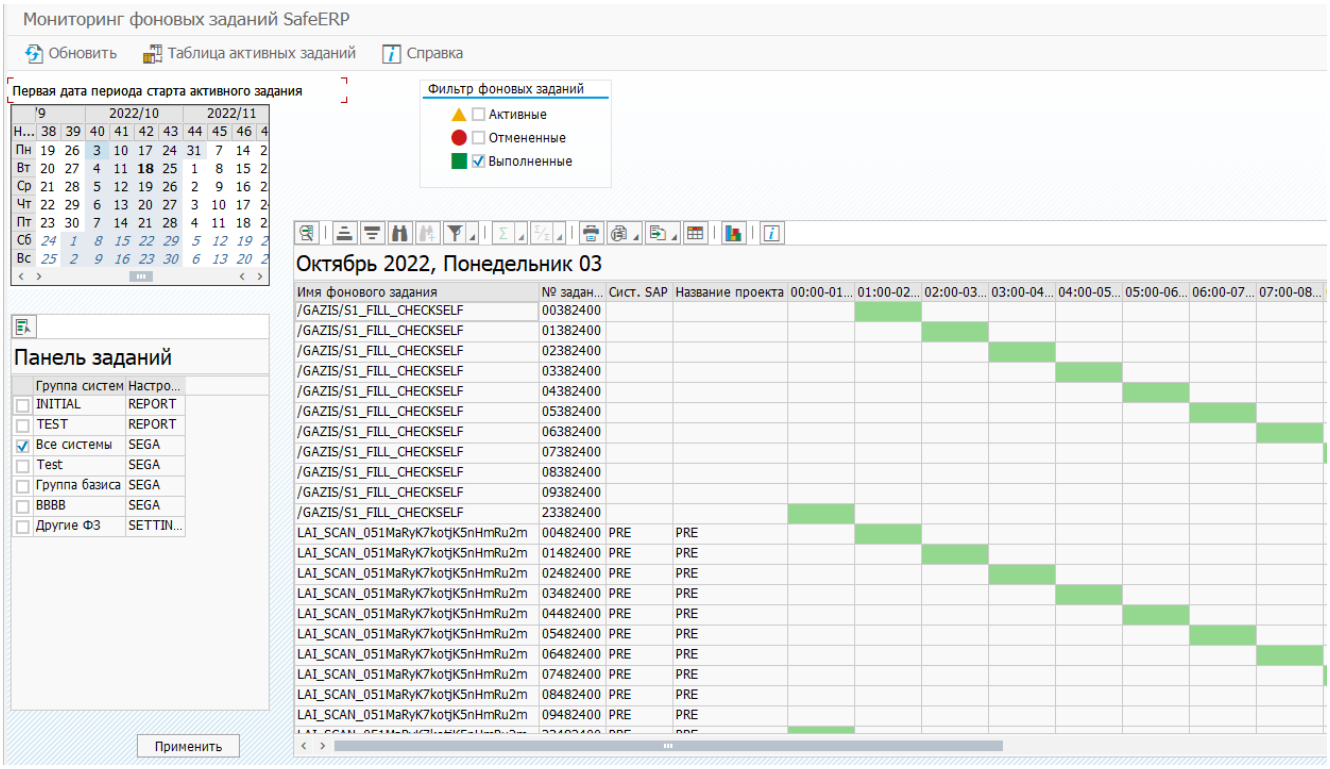


Рисунок 62 – Мониторинг фоновых заданий

В первоначальный экран входят следующие элементы:

- меню;
- первая дата периода старта активного задания;

— фильтр фоновых заданий;
— панель заданий;
— таблица с результатами.

В область «Меню» входят следующие элементы:

— кнопка «Обновить»;
— таблица активных заданий;
— справка.

В область «Фильтр фоновых заданий» входят следующие элементы:

— ▲ «активные»;
— ● «отмененные»;
— ■ «выполненные».

В область «Панель заданий» входят следующие элементы:

— кнопка «Выбрать все/убрать выделенные»;
— группа систем;
— настройка.

В область «Таблица» входят в следующие элементы:

— имя фонового задания;
— номер задания;
— идентификатор системы SAP;
— название проекта;
— временные промежутки с шагом 1 час с 0 до 23.

Индикация временных промежутков представлены в таблице 3.

Таблица 3 – Индикация временных промежутков

Цвет	Описание
	Задание выполнено
	Задание в ходе выполнения
	Задание отменено

Для просмотра фоновых заданий необходимо выполнить следующие действия:

1) Выбрать дату в области «Первая дата периода старта сканирования» (рис. 62).
2) Выбрать тип фонового задания в области «Фильтр фоновых заданий» (рис. 62).
3) Выбрать тип задания в области «Панель заданий» (рис. 62).
4) Нажать кнопку Применить.

4.8 Сравнение двух итераций проекта типа АК

Для запуска сравнений двух итераций проекта типа АК необходимо ввести транзакцию /N/GAZIS/COMPARE_ITERS в командную строку.

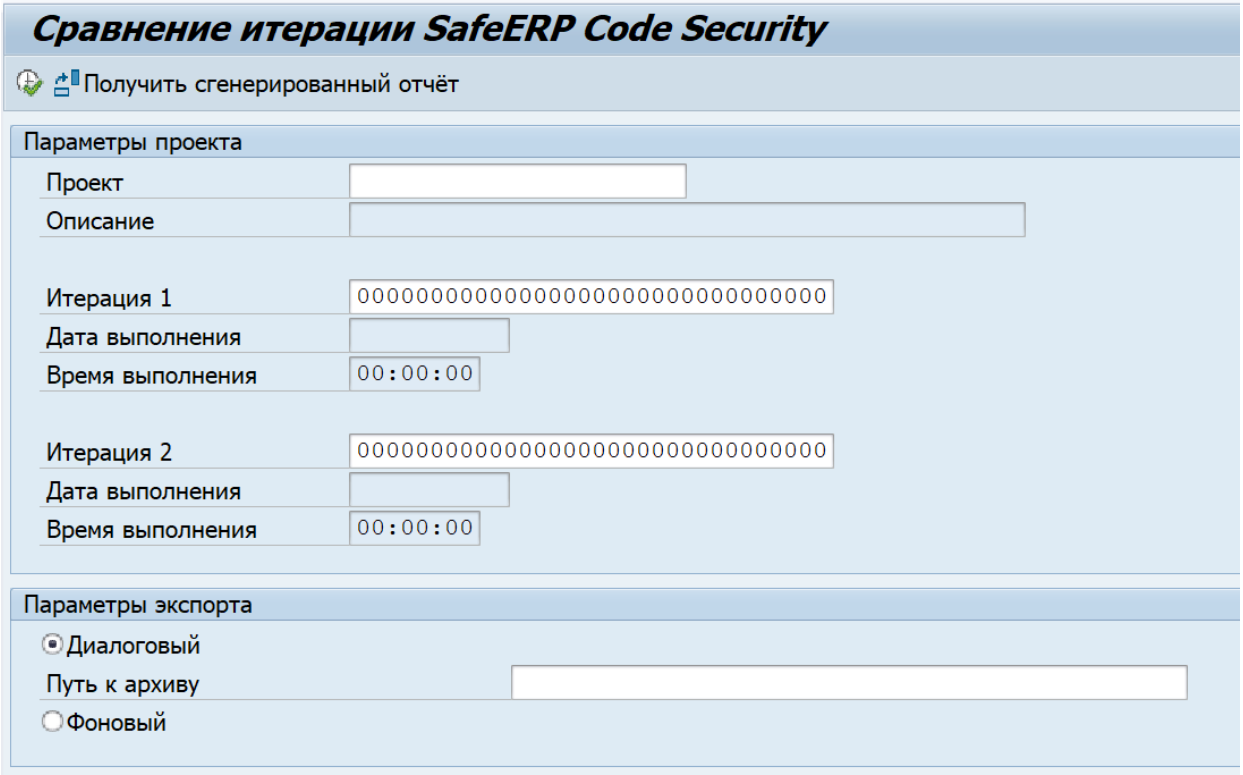


Рисунок 63 – Окно транзакции /N/GAZIS/COMPARE_ITERS

Для сравнения двух итераций необходимо выполнить следующие действия:

1) Нажать кнопку в строке «Проект» (рис. 63).
2) Выбрать проект в открывшемся окне, нажать кнопку .
3) Выбрать итерацию (рис. 64) в открывшемся окне, нажать кнопку .

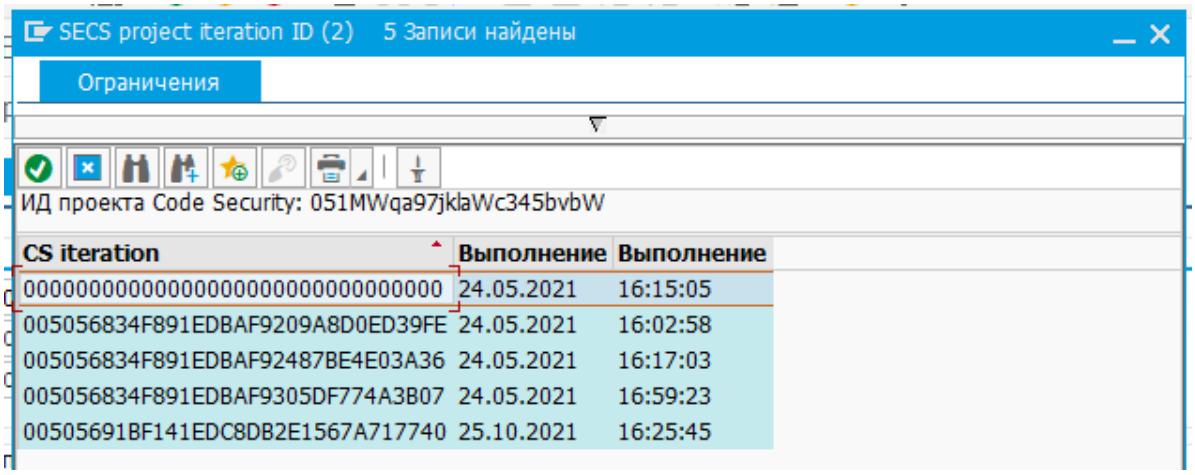
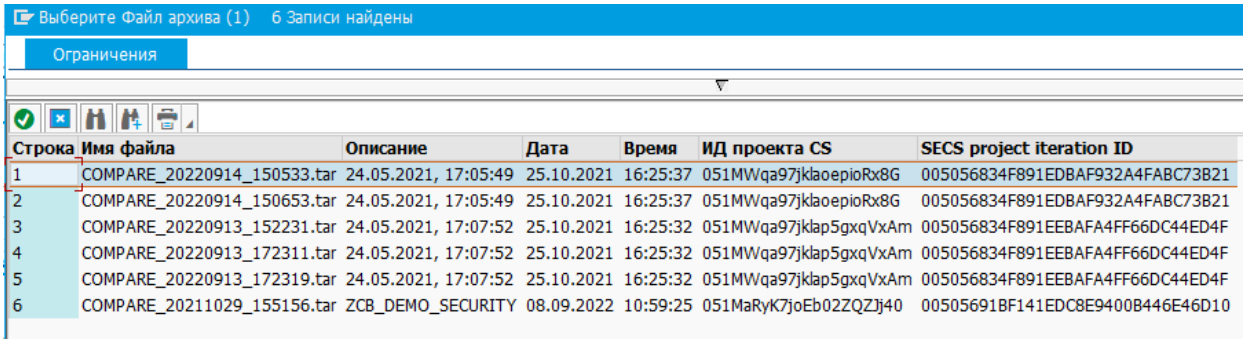


Рисунок 64 – Выбор итерации

4) Нажать кнопку Получить сгенерированный отчёт (рис. 63).
5) Выбрать архив в открывшемся и нажать кнопку (рис. 65).



Строка	Имя файла	Описание	Дата	Время	ИД проекта CS	SECS project iteration ID
1	COMPARE_20220914_150533.tar	24.05.2021, 17:05:49	25.10.2021	16:25:37	051MWqa97jklaoepioRx8G	005056834F891EDBAF932A4FABC73B21
2	COMPARE_20220914_150653.tar	24.05.2021, 17:05:49	25.10.2021	16:25:37	051MWqa97jklaoepioRx8G	005056834F891EDBAF932A4FABC73B21
3	COMPARE_20220913_152231.tar	24.05.2021, 17:07:52	25.10.2021	16:25:32	051MWqa97jklap5gxqVxAm	005056834F891EEBAFA4FF66DC44ED4F
4	COMPARE_20220913_172311.tar	24.05.2021, 17:07:52	25.10.2021	16:25:32	051MWqa97jklap5gxqVxAm	005056834F891EEBAFA4FF66DC44ED4F
5	COMPARE_20220913_172319.tar	24.05.2021, 17:07:52	25.10.2021	16:25:32	051MWqa97jklap5gxqVxAm	005056834F891EEBAFA4FF66DC44ED4F
6	COMPARE_20211029_155156.tar	ZCB_DEMO_SECURITY	08.09.2022	10:59:25	051MaRyK7joEb02ZQZJj40	00505691BF141EDC8E9400B446E46D10

Рисунок 65 – Выбор архива

Примечание. Для сравнения необходимы итерации с одного и того же проекта.

Для просмотра отчета по сравнению двух итераций необходимо скачать архив с результатами сравнения.

Назначение отчетов в архиве *.tar:

- CHECKS.XLSX – сводный список всех сработавших проверок по сравнении двух итераций проекта с указанием их степеней критичности;
- FLAW.XLSX – сводный список всех сработавших проверок по сравнению двух итерации проекта с указанием адреса найденного недостатка кода: пакета, типа объекта, участка кода;
- ITERATION.XLSX – сводная таблица по метрикам сравнении двух итераций проекта;
- OBJECT.XLSX – сводный список всех проверяемых программных пакетов и их объектов.

4.9 Экспорт профилей

Экспорт профилей в интерфейсе SAP GUI осуществляется следующими способами:

- с помощью транзакции /N/GAZIS/SEGA;
- с помощью транзакции /n/gazis/export_seps;
- с помощью транзакции /n/gazis/export_secs.

4.9.1 Экспорт профилей с помощью транзакции /N/GAZIS/SEGA

Для экспорта профилей необходимо выполнить следующие действия:

1) Перейти по следующему пути: Дополнительные функции → Профили SEPS → Экспортировать.
   Примечание. Для экспорта профиля SECS необходимо перейти по следующему пути: Дополнительные функции → Профили SECS → Экспортировать (см. рис. 24).
2) Выбрать «Профиль» (рис. 66).
3) Выбрать действие с профилем («Добавить и обновить профиль» или «Перезаписать данные») (см. рис. 66).

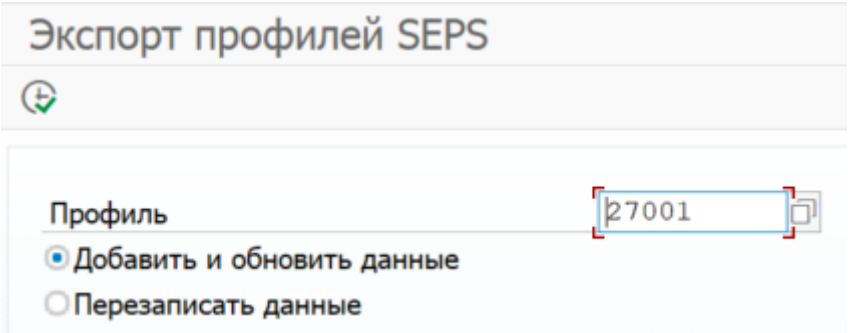


Рисунок 66 – Выбор профиля (для SEPS)

4) Нажать кнопку «Выполнить».

4.9.2 Экспорт профилей с помощью транзакции /n/gazis/export_seps

Транзакция /n/gazis/export_seps предназначена для экспорта профилей SafeERP Platform Security.

Окно транзакции /n/gazis/export_seps представлено на рис. 67.

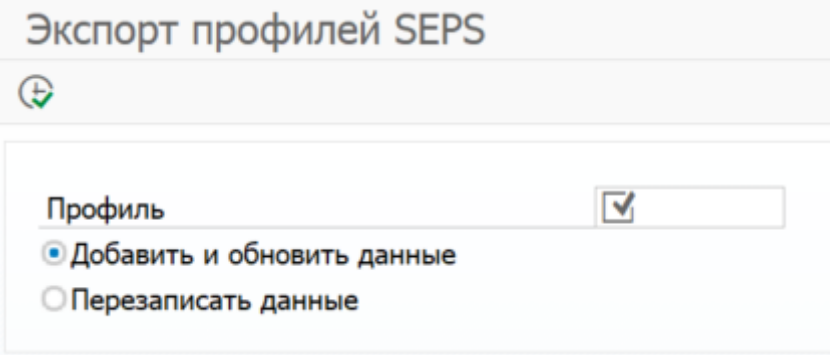


Рисунок 67 – Экспорт профилей (для SEPS)

Для экспорта профилей необходимо выполнить следующие действия:

1) Выбрать профиль для экспорта.
2) Выбрать действие с профилем («Добавить и обновить профиль» или «Перезаписать данные»).
3) Нажать кнопку *«Выполнить»*.
4) Нажать кнопку в окне «Журнал экспорта» (рис. 68).

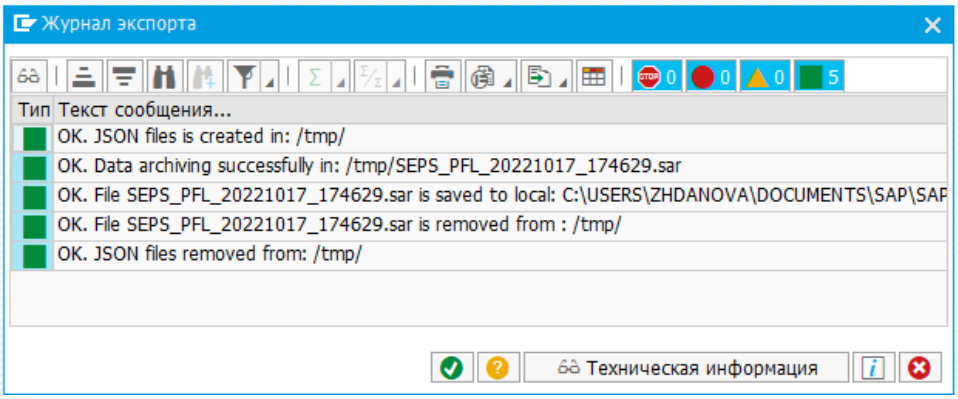


Рисунок 68 – Окно «Журнал экспорта»

4.9.3 Экспорт профилей с помощью транзакции /n/gazis/export_secs

Транзакция /n/gazis/export_secs предназначена для экспорта профилей SafeERP Code Security.

Окно транзакции /n/gazis/export_secs представлено на рис. 69.

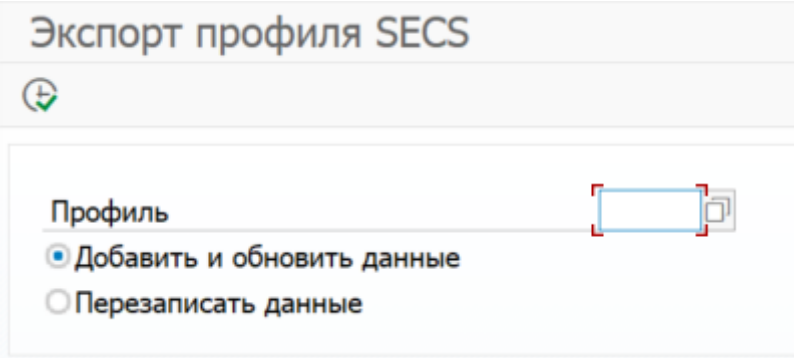


Рисунок 69 – Экспорт профилей (для SECS)

Для экспорта профилей необходимо выполнить действия согласно пункту 4.9.2.

4.10 Импорт профилей

Импорт профилей осуществляется следующими способами:

- с помощью транзакции /N/GAZIS/SEGA;
- с помощью транзакции /n/gazis/import_seps;
- с помощью транзакции /n/gazis/import_secs.

4.10.1 Импорт профилей с помощью транзакции /N/GAZIS/SEGA

Для импорта профилей необходимо выполнить следующие действия:

1) Перейти по следующему пути: Дополнительные функции → Профили SEPS → Импортировать.

   Примечание. Для импорта профиля SECS необходимо перейти по следующему пути: Дополнительные функции → Профили SECS → Импортировать.

2) Выбрать профиль в окне (рис. 70).

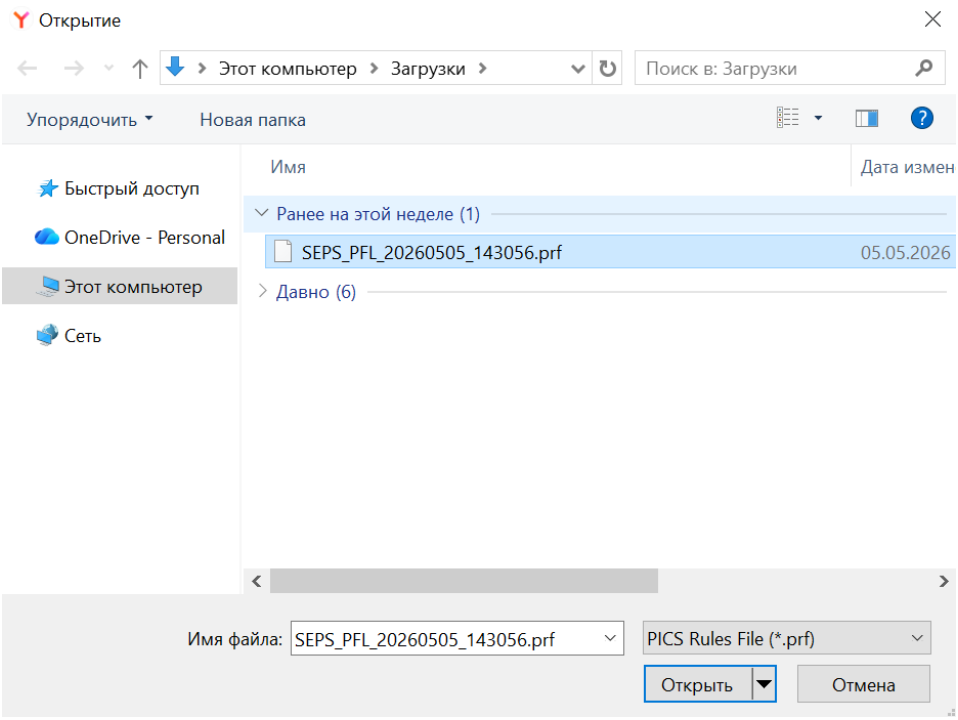


Рисунок 70 – Окно импорта профиля

3) Нажать кнопку *«Открыть»* (см. рис. 70).
4) Нажать кнопку в окне «Журнал импорта» (рис. 71).

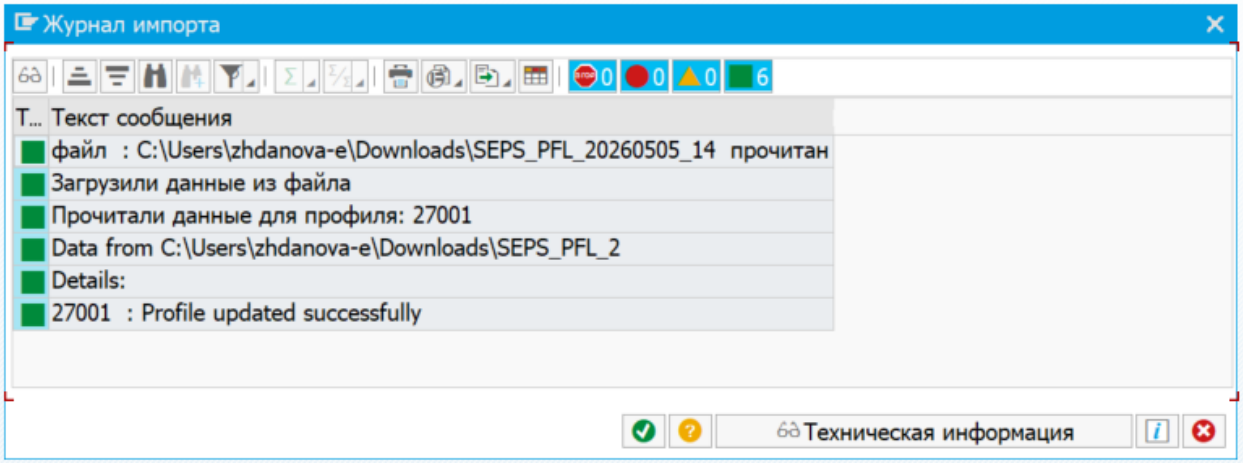


Рисунок 71 – Окно «Журнал импорта»

4.10.2 Импорт профилей с помощью транзакции /n/gazis/import_seps

Транзакция /n/gazis/import_seps предназначена для импорта профилей SafeERP Platform Security.

Для импорта профилей необходимо выполнить следующие действия:

1) Выбрать профиль в дополнительном окне (см. рис. 70).
2) Нажать кнопку *«Открыть»* (см. рис. 70).
3) Нажать кнопку в окне «Журнал импорта» (рис. 71).

4.10.3 Импорт профилей с помощью транзакции /n/gazis/import_secs

Транзакция /n/gazis/import_secs предназначена для импорта профилей SafeERP Code Security.

Для импорта профилей необходимо выполнить действия согласно пункту 4.10.2.

4.11 Проверка системы

Проверка системы служит для проверки количества проверок на агенте и сервере, а также для проверки RFC-соединения.

Для проверки системы необходимо ввести /N/GAZIS/SEGA в командную строку. В открывшемся окне в поле «Компания/Группа/Система» выбрать систему, в контекстном меню выбрать «Изменить систему». В открывшемся окне (рис. 72) нажать кнопку «Проверить систему», ввести логин и пароль от проверяемой системы, нажать кнопку «Ввод».

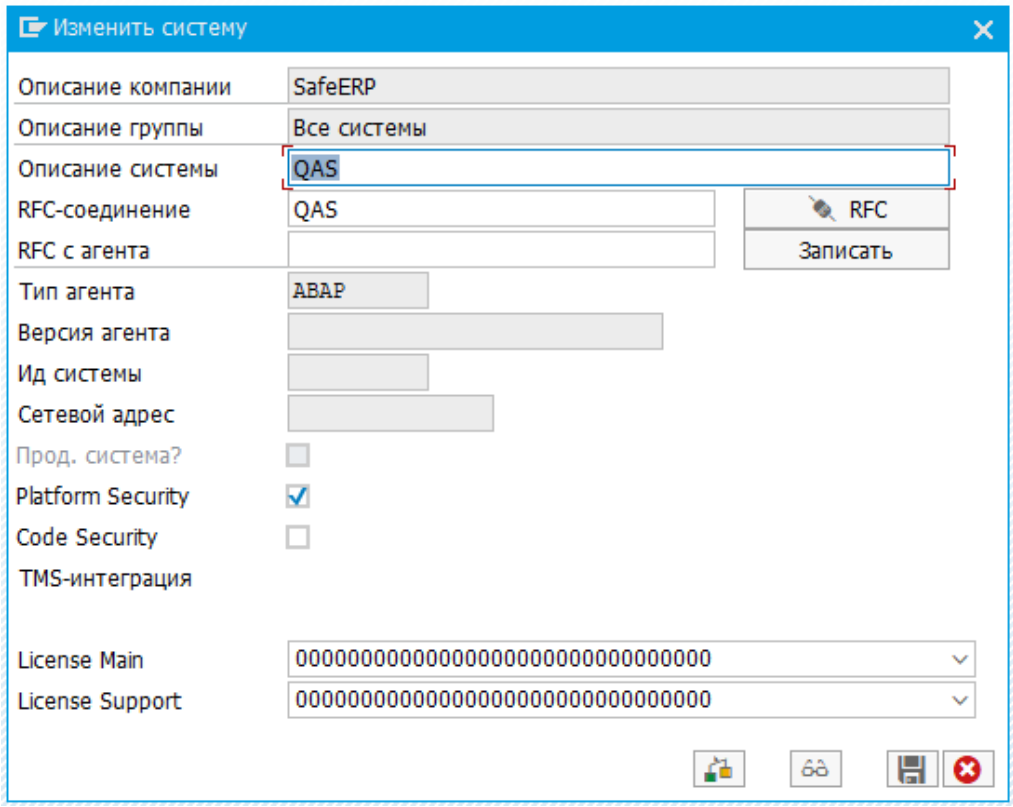


Рисунок 72 – Окно «Изменить систему»

Статус агента после процедуры проверки:

- N – сценарии на агенте отсутствуют;
- L – количество сценариев на сервере, больше чем на агенте;
- M – количество сценариев на агенте, больше чем на сервере;
- A – количество сценариев на агенте = 0 или количество сценариев на агенте = количеству сценариев на сервере;
- I – количество сценариев на сервере и на агенте одинаково, но есть различия в

самих сценариях;

— R – список активных сценариев не соответствует эталонному;
— E – несуществующий профиль для варианта проверок обратного вызова;
— C – ошибка RFC-соединения.

Для выравнивания количества проверок необходимо в окне «Просмотреть систему» (рис. 73) нажать кнопку *«Выравнять»*. Нажать кнопку *«Сохранить»*.

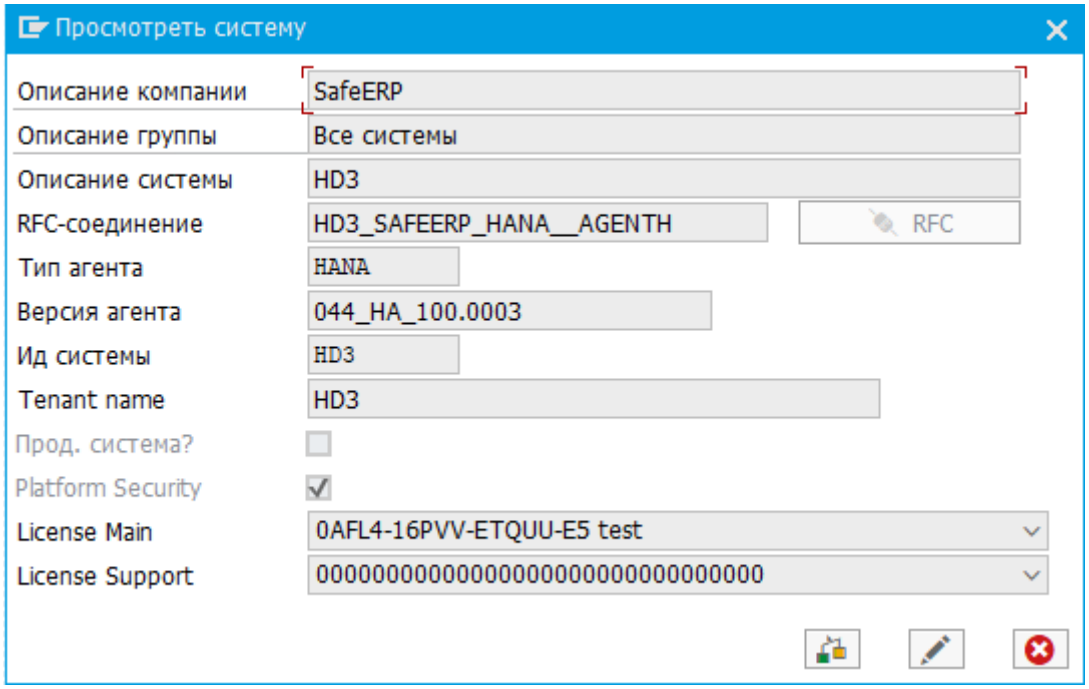


Рисунок 73 – Окно «Просмотреть систему»

Примечание. Функция «Выравнивание» доступна в режиме «Изменить систему».

4.12 Настройка порядка отображений проверок статуса доступности агента в модуле «Панель мониторинга»

Для настройки порядка отображений проверок статуса доступности агента в модуле «Панель мониторинга» (см. рис. 138) необходимо ввести транзакцию /N/GAZIS/MONITOR в командную строку.

Окно транзакции представлено на рис. 74 .

В таблицу настройки входят следующие столбцы:

— «Позиция» – порядковый номер вывода проверки;
— «Параметр» – проверка из списка проверки;
— «Активность» – активность отображения проверки. Для активации отображения проверки необходимо установить флаг ☑.

Вносятся изменения в следующие столбцы:

— «Позиция»;
— «Проверка»;
— «Активность».

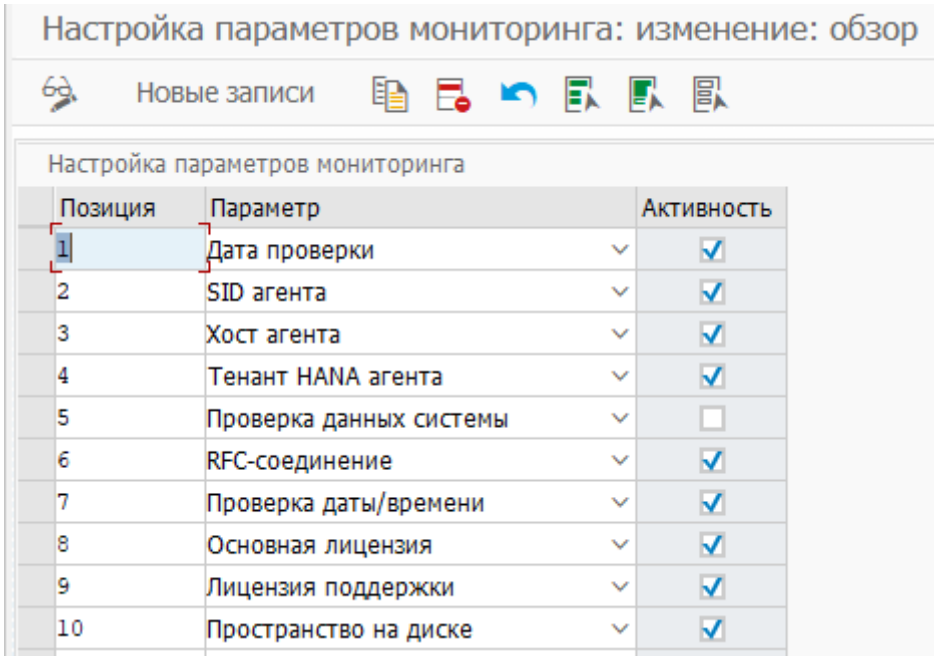


Рисунок 74 – Окно настройки для отображений проверок при просмотре данных об агенте в модуле «Панель мониторинга»

Для добавления проверок в окно «Данные об агенте» необходимо нажать кнопку Новые записи, ввести данные в столбцы «Позиция вывода», «Тип проверок», «Активность», нажать кнопку .

Примечание. Таблица для изменения вывода информации по умолчанию доступна в режиме «Редактирование».

Для редактирования вывода проверок необходимо внести изменения в столбцы, нажать кнопку .

4.13 Поиск псевдокомментариев

Поиск псевдокомментариев доступен в SAP GUI. Вызов функции поиска псевдокомментариев осуществляется с помощью транзакции /N/GAZIS/PSEUDOCOMMENT.

Для работы необходимо заполнить следующие области:

- «Общие настройки» – выбор идентификатора из списка и выбор запуска в фоновом режиме;
- «Выбор объектов» – выбор пакетов и объектов;
- «Выбор сценариев» – выбор данных по безопасности, производительности и удобству сопровождения.

Для поиска псевдокомментариев необходимо ввести в командную строку транзакцию /N/GAZIS/PSEUDOCOMMENT, в открывшемся окне (рис. 75) заполнить области «Общие настройки», «Выбор объектов», «Выбор сценариев», нажать кнопку *«Выполнить»*.

Примечание. Для работы необходимо заполнить все поля. В противном случае поиск псевдокомментариев не будет запущен.

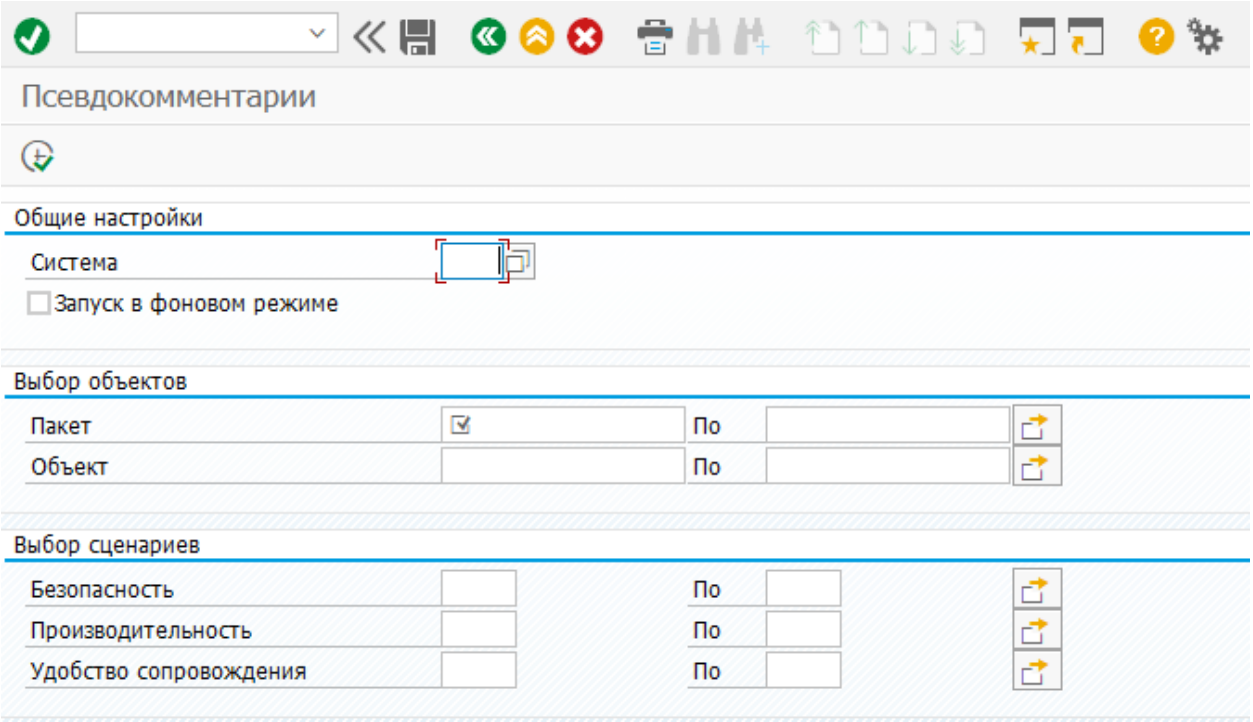


Рисунок 75 – Меню транзакции по поиску псевдокомментариев

4.14 Настройка количества функциональных модулей в функциональной группе

Для проверки количества функциональных модулей в функциональной группе необходимо обратиться к таблице /GAZIS/STCS_CV.

Для настройки количества функциональных модулей в функциональной группе необходимо ввести транзакцию SE11. Необходимо ввести в командную строку транзакцию /GAZIS/STCS_CV, нажать кнопку (рис. 76) в меню, ввести «6» в поле «IND», ввести «3» в поле «POS» и нажать кнопку (рис. 77) в открывшемся окне нажать кнопку , ввести изменения в поля «VALUE LOW» и «VALUE HIGH» (рис. 78), нажать кнопку .

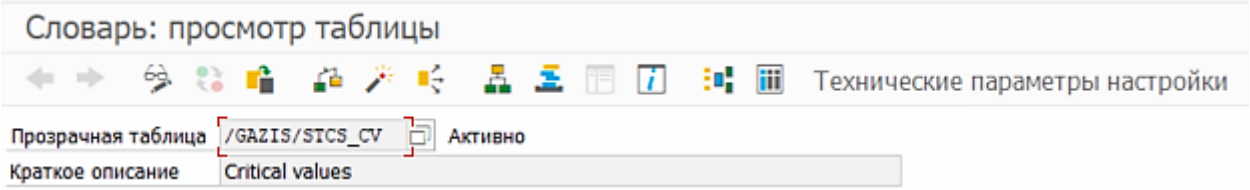


Рисунок 76 – Меню таблицы

Браузер данных: таблица /GAZIS/STCS_CV: экран выбора

Число записей

CMPID		По	
CAT		По	
IND	6	По	
VAR		По	
POS	3	По	
CUSTOM		По	
SPGSC		По	
POLZUK		По	
SIGN		По	
OPT		По	
CHAR_IND		По	
VALUE_LOW		По	
VALUE_HIGH		По	
Ширина списка вывода	250		
МаксЧислоСовпадений	500		

Рисунок 77 – Фильтры для таблиц

Таблица /GAZIS/STCS_CV Изм-ть

Проверочная таблица

MANDT	100
CMPID	1
CAT	M
IND	6
VAR	1
POS	3
CUSTOM	X
SPGSC	M
POLZUK	U
SIGN	I
OPT	BT
CHAR IND	I
VALUE LOW	41
VALUE HIGH	50

Рисунок 78 – Настройка проверок

4.15 Настройка вложенности кода при сканировании

После активации настройки у пользователя при проверке кода будет проверяться 1-й уровень вложенности без учета вложенных вызовов.

Для настройки вложенности необходимо выполнить следующие действия:

1) Ввести транзакцию /N/GAZIS/NEST_SCAN_SET в командную строку.

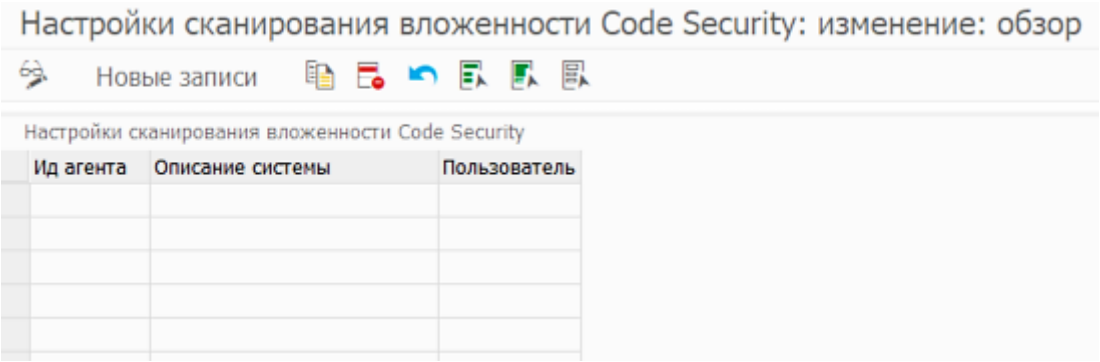


Рисунок 79 – Окно транзакции /N/GAZIS/NEST_SCAN_SET

2) Нажать кнопку Новые записи (рис. 79).
3) Нажать кнопку в столбце «Идентификатор агента». В открывшемся окне выбрать агент. Заполнить столбец «Пользователь» (рис. 79). Нажать кнопку .

Примечания:

1. У пользователей, которые не внесены в настроечный список, будут проверяться все объекты, включая вложенные.
2. Настройка работает в интерфейсе SAP GUI.

4.16 Проверка работы веб-серверов SAP FIORI

Комплекс проверки работоспособности веб-сервисов FIORI в ПК «SafeERP Security Suite».

Для работы с транзакцией необходимо пользователю присвоить следующие полномочия, указанные в приложении 2.

Окно транзакции представлено на рис. 80.

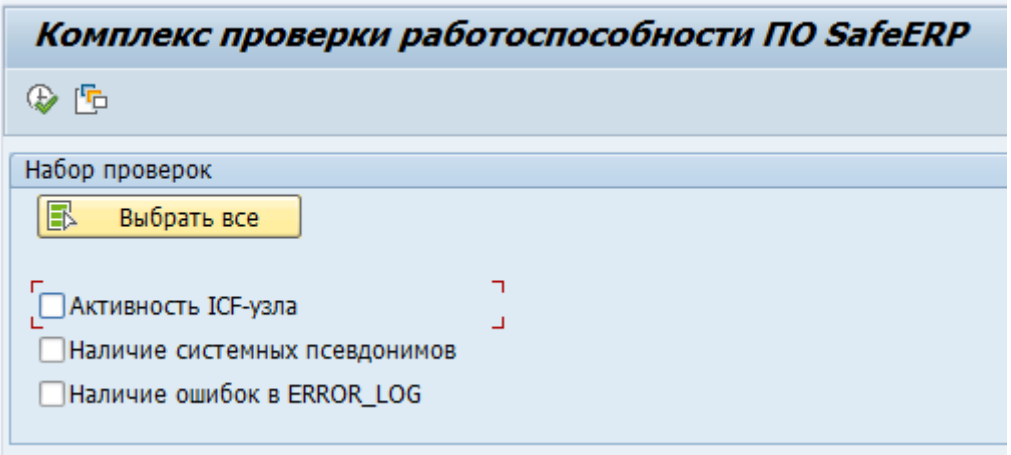


Рисунок 80 – Окно транзакции /N/GAZIS/CHECK_SAFEERP

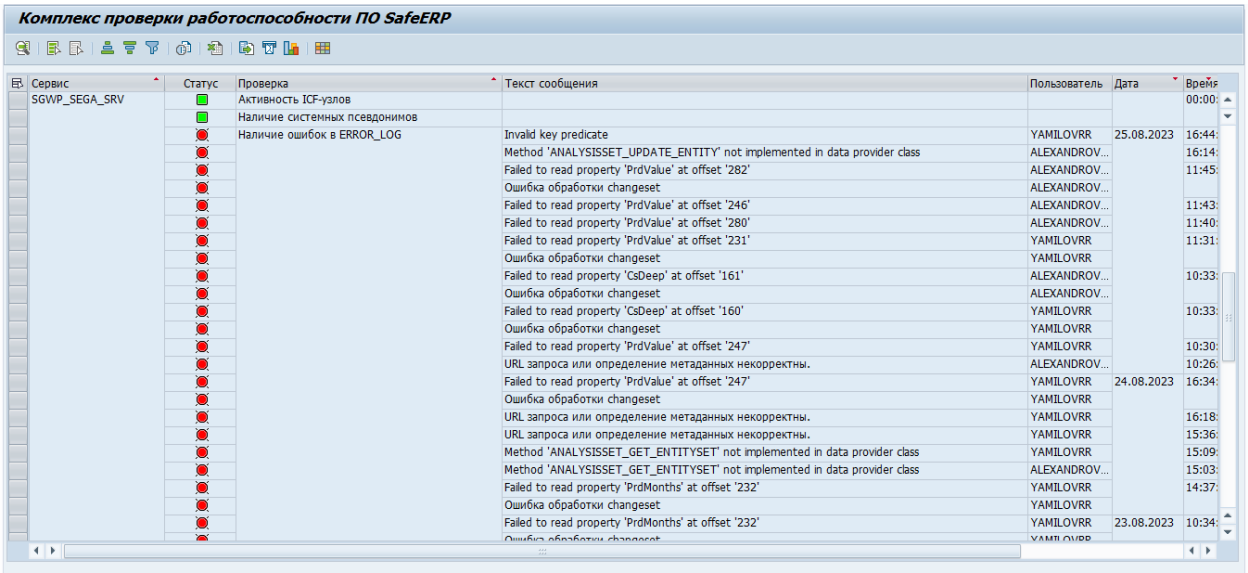
В окно транзакции входят следующие проверки:

- «Активность ICF-узла» – в данной проверке проверяется работоспособность ICF-узла. Узел ICF (Internet Communication Framework) является одним из компонентов серверов для работы abap приложений в веб-интерфейсе;
- «Наличие системных псевдонимов» – в данной проверке проверяется наличие активного системного псевдонима в системе;
- «Наличие ошибок в error_log» – в данной проверке проверяются записи ошибок в логе error_log, связанные с работоспособностью сервисов, которые влияют на работу веб-интерфейса.

Используются следующие статусы для индикации проверок:

- – проверка пройдена. Ошибки не найдены;
- – проверка не пройдена. Подробное описание находится в столбце «Текст сообщения» (см. рис. 81).

Для просмотра мониторинга системы необходимо ввести транзакцию /N/GAZIS/CHECK_SAFEERP в командную строку. Поставить флаг напротив проверки, нажать кнопку .



Сервис	Статус	Проверка	Текст сообщения	Пользователь	Дата	Время
SGWP_SEGA_SRV		Активность ICF-узлов				00:00:
		Наличие системных псевдонимов				
		Наличие ошибок в ERROR_LOG	Invalid key predicate	YAMILOVRR	25.08.2023	16:44:
			Method 'ANALYSISSET_UPDATE_ENTITY' not implemented in data provider class	ALEXANDROV...		16:14:
			Failed to read property 'PrdValue' at offset '282'	ALEXANDROV...		11:45:
			Ошибка обработки changeset	ALEXANDROV...		
			Failed to read property 'PrdValue' at offset '246'	ALEXANDROV...		11:43:
			Failed to read property 'PrdValue' at offset '280'	ALEXANDROV...		11:40:
			Failed to read property 'PrdValue' at offset '231'	YAMILOVRR		11:31:
			Ошибка обработки changeset	YAMILOVRR		
			Failed to read property 'CsDeep' at offset '161'	ALEXANDROV...		10:33:
			Ошибка обработки changeset	ALEXANDROV...		
			Failed to read property 'CsDeep' at offset '160'	YAMILOVRR		10:33:
			Ошибка обработки changeset	YAMILOVRR		
			Failed to read property 'PrdValue' at offset '247'	YAMILOVRR		10:30:
			URL запроса или определение метаданных некорректны.	ALEXANDROV...		10:26:
			Failed to read property 'PrdValue' at offset '247'	YAMILOVRR	24.08.2023	16:34:
			Ошибка обработки changeset	YAMILOVRR		
			URL запроса или определение метаданных некорректны.	YAMILOVRR		16:18:
			URL запроса или определение метаданных некорректны.	YAMILOVRR		15:36:
			Method 'ANALYSISSET_GET_ENTITYSET' not implemented in data provider class	YAMILOVRR		15:09:
			Method 'ANALYSISSET_GET_ENTITYSET' not implemented in data provider class	ALEXANDROV...		15:03:
			Failed to read property 'PrdMonths' at offset '232'	YAMILOVRR		14:37:
			Ошибка обработки changeset	YAMILOVRR		
			Failed to read property 'PrdMonths' at offset '232'	YAMILOVRR	23.08.2023	10:34:

Рисунок 81 – Результаты сканирования

4.17 Проверка RFC соединений агентов

Транзакция /N/GAZIS/CONTROL_RFC предназначена для контроля RFC-соединений и настройки фонового задания для сбора данных о состоянии RFC-соединений агентов.

Для проверки RFC соединений агентов необходимо ввести транзакцию /N/GAZIS/CONTROL_RFC в командную строку.

Окно транзакции представлено на рис. 82.

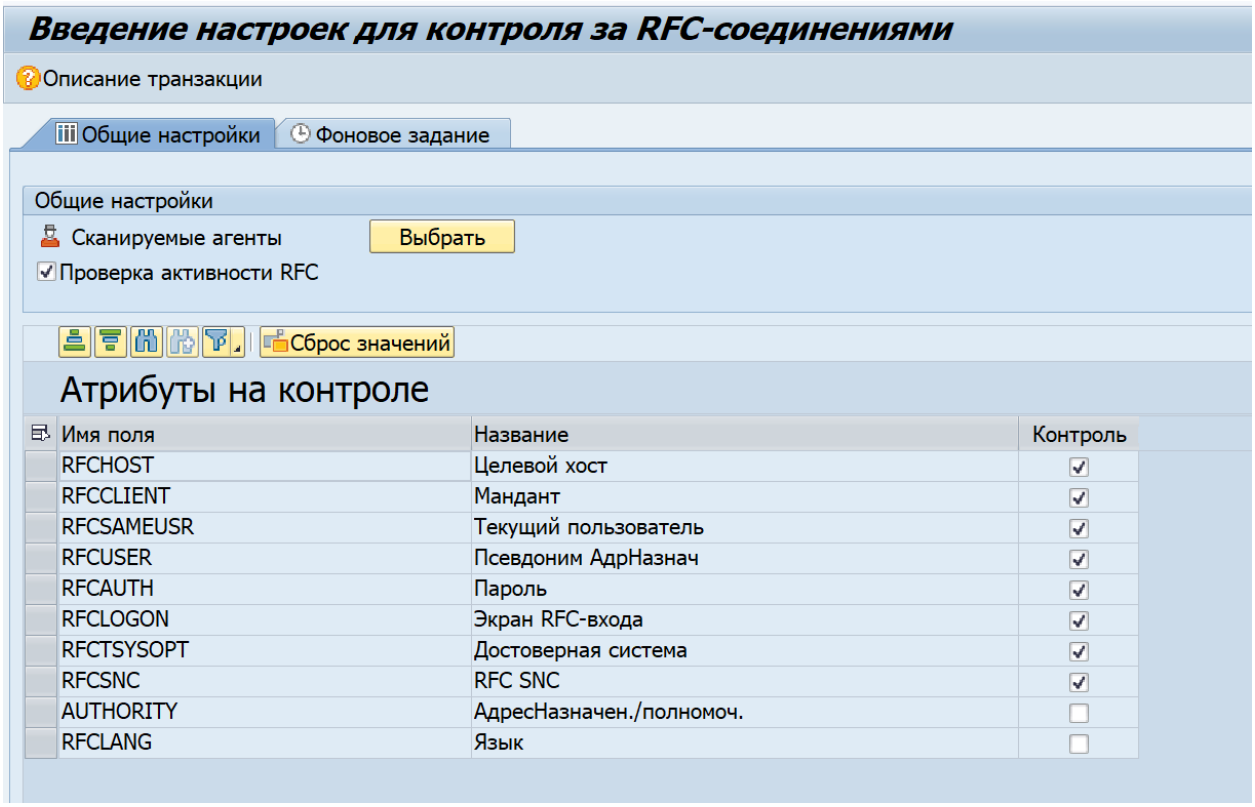


Рисунок 82 – Окно транзакции /n/gazis/control_rfc

В транзакцию входят следующие вкладки:

- «Общие настройки» – настройка RFC-соединений агентов. В данной вкладке предоставляется возможность настройки атрибутов контроля;
- «Фоновое задание» – настройка фоновых заданий.

Во вкладку «Общие настройки» входят следующие области:

- «Общие настройки»;
- «Атрибуты на контроле» – выбор атрибутов для анализа.

В область «Атрибуты на контроле» входят следующие поля:

- «Целевой хост»;
- «Мандант»;
- «Текущий пользователь»;
- «Псевдоним АдрНазначения»;
- «Пароль»;
- «Экран RFC-входа»;
- «Достоверная система»;
- «RFC SNC»;
- «АдресНазначен./полномоч.»;
- «Язык».

Для постановки атрибута на контроль необходимо поставить флаг напротив атрибута, нажать кнопку «Сохранить».

Примечание. Для сброса настроек по умолчанию необходимо нажать кнопку *«Сброс значений».*

Во вкладку «Фоновое задание» входят следующие области:

- «Имя фонового задания» – название программы, которая применяется в качестве фонового задания. По умолчанию стоит программа GAZIS/S1_MAP_RFC_SCAN;
- «Параметры запуска» – параметры запуска фонового задания.

В область «Параметры запуска» входят следующие поля:

- «Последнее выполн. задание» – дата и время выполнения последнего фонового задания;
- «Следующее задание» – дата и время выполнения следующего фонового задания;
- «Статус выполнения» – статус выполнения последнего фонового задания;
- «Период» – период повторения фонового задания;
- «Сервер»;
- «Запланировать задание на» – дата и время выполнения следующего задания.

Доступны следующие статусы выполнения фонового задания:

- R – активно;
- Y – готово;
- P – деблокировано;
- S – запланировано;
- A – отменено;

— F – выполнено;
— X – неизвестное состояние.

4.18 Сравнение двух ролей

Для сравнения двух ролей необходимо обратиться к транзакции /N/GAZIS/COMPARE_ROLE.

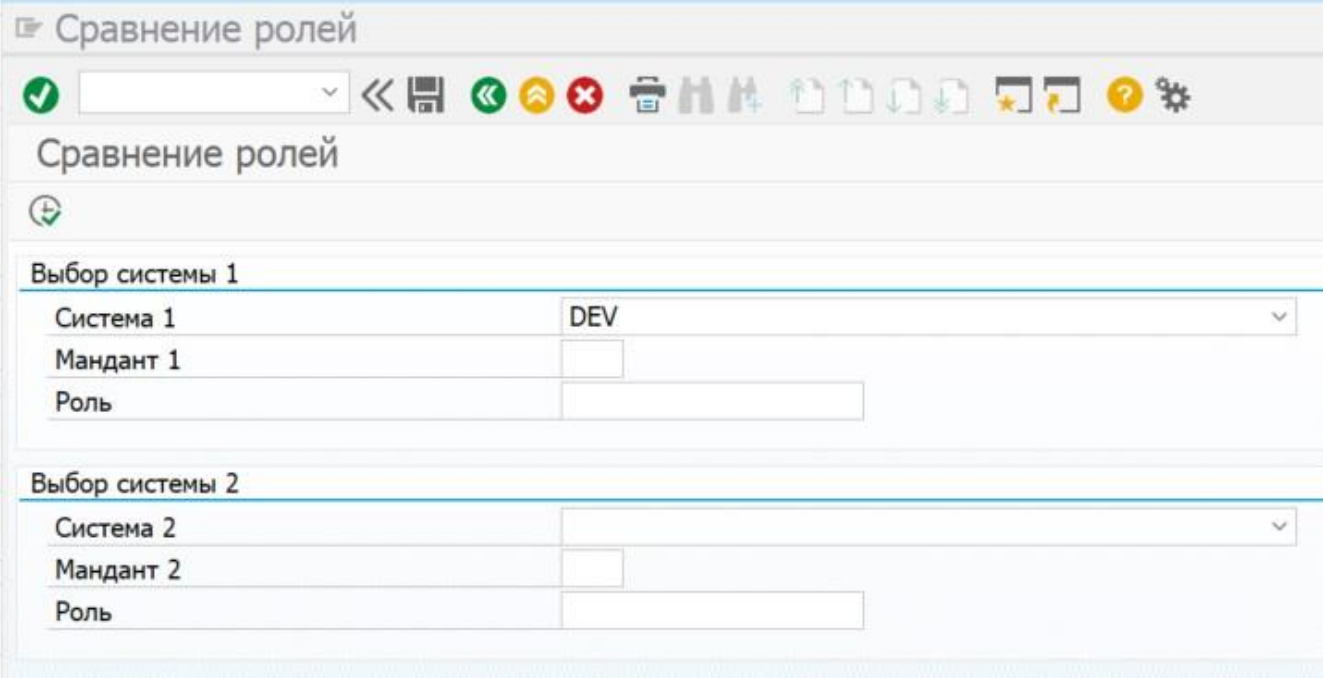


Рисунок 83 – Окно транзакции /N/GAZIS/COMPARE_ROLE

Для сравнения ролей необходимо выполнить следующие действия:

1) Выбрать систему из списка в области «Выбор системы 1» (рис. 83)
2) Нажать кнопку «Enter» в строке «Мандант». Нажать кнопку , выбрать мандант из списка.
3) Нажать кнопку «Enter» в строке «Роль». Нажать кнопку , выбрать роль из списка.
4) Выполнить действия для второй системы указанные в пунктах 1-3.
5) Нажать кнопку «Выполнить» .

После сравнения будет выдан результат сравнения в виде таблицы со следующими столбцами (рис. 84):

— «Особая ситуация» – статус сравнения полномочий. Статусы сравнения имеют следующую индикацию: зелеными (полномочия совпадают) и красными (полномочия не совпадают);
— «Объект» – наименование объекта роли;
— «Поле полномочий» – наименование поля полномочий роли;
— «Со значения» – начальное значение;
— «По значения» – последнее значение;

— «Наименование первой системы» – наименование, мандант и роль первой системы;
— «Наименование второй системы» – наименование, мандант и роль второй системы.

Примечание. При нажатии на роль в окне сравнений ролей (рис. 84) доступен просмотр списка с выбранной системой и мандантом (рис. 85).

Сравнение ролей. Вывод данных.

PRE:000:/AIF/ADMINISTRATOR PRE:000:/AIF/ALL

Особая ситуац...	Объект	Поле полно	Со значения	ПоЗначен...	PRE:000:/AIF/ADMINISTRAT...	PRE:000:/AIF/A...
	/AIF/CFUNC	/AIF/IF			☑	☑
	/AIF/CFUNC	/AIF/IFVER			☑	☑
	/AIF/CFUNC	/AIF/NS			☑	☑
	/AIF/CFUNC	/AIF/NSREC			☑	☑
	/AIF/CFUNC	/AIF/OTHUS	' '		☑	☑
	/AIF/CFUNC	/AIF/OTHUS	*		☑	☑
	/AIF/CFUNC	/AIF/VISI	A		☑	☑
	/AIF/CFUNC	ACTVT	*		☐	☑
	/AIF/CFUNC	ACTVT	03		☑	☑
	/AIF/CFUNC	ACTVT	16		☑	☑
	/AIF/CUST	/AIF/MC	/AIF/ACTIONS		☑	☑
	/AIF/CUST	/AIF/MC	/AIF/ALERT		☑	☑

Рисунок 84 – Список полномочий по ролям

SA1:100:SAP_BC_LVC_ALL

Пользователь	Роль	С даты	По дату
OREHOVA-L	SAP_BC_LVC_ALL	30.09.2024	31.12.9999

Admin.

Рисунок 85 – Список пользователь с выбранной ролью

4.19 Инструмент фиксации результатов

Транзакция /N/GAZIS/SEPS_VULNERS доступна на агенте. Транзакция предназначена для контроля исправления найденных уязвимостей, назначенные на конкретного исполнителя.

Окно транзакции представлено на рис. 86.

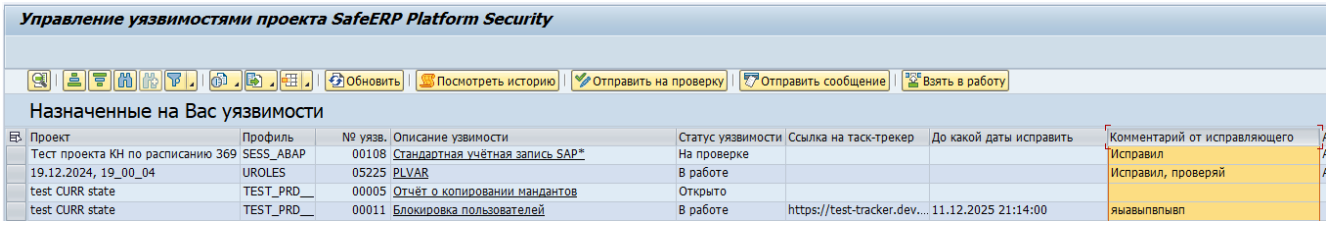


Рисунок 86 – Окно транзакции

Просмотр описания уязвимости

Для просмотра описания уязвимостей необходимо нажать на наименование уязвимости в советующем столбце (см. рис. 86).

Подробное описание уязвимости представлено на рис. 87.

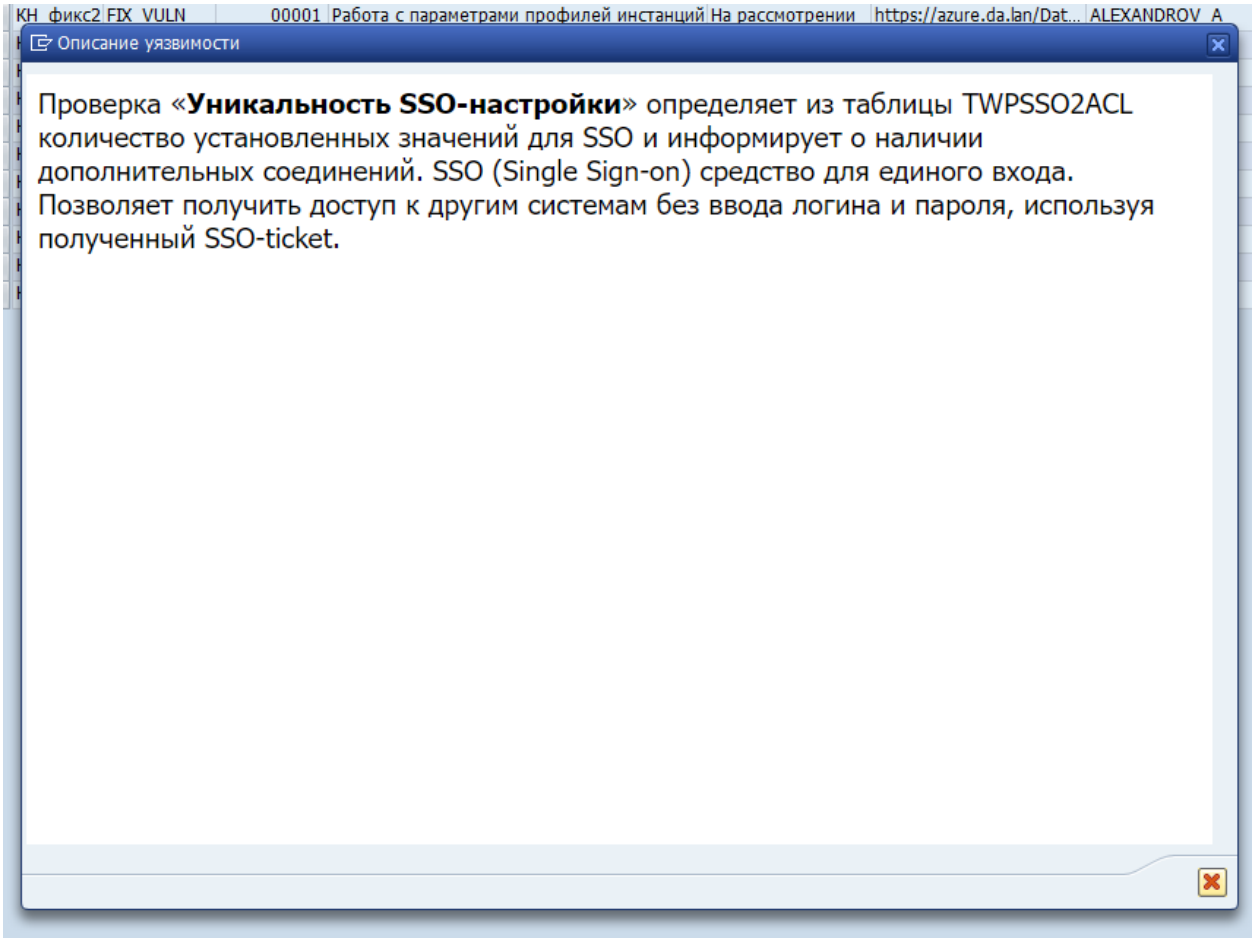


Рисунок 87 – Подробное описание уязвимости

История изменений

Для просмотра истории изменений необходимо выделить строку (см. рис. 86), нажать кнопку *«Просмотреть историю».*

История изменений представлена на рис. 88.

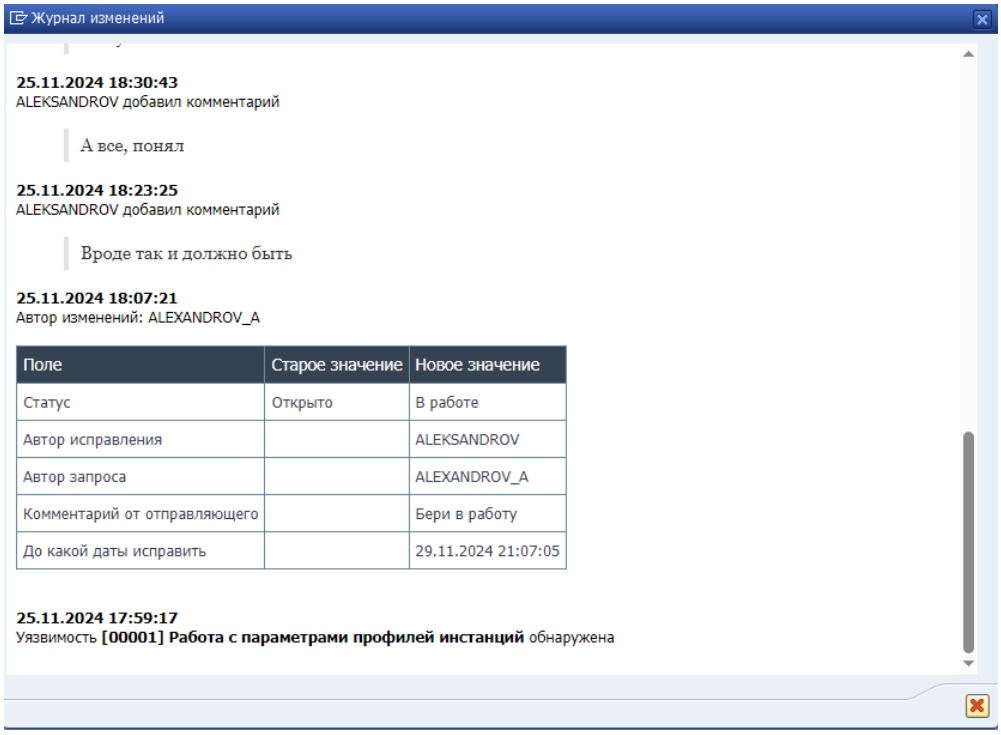


Рисунок 88 – История изменений

Отправить на рассмотрение

Примечание. На рассмотрение отправляются уязвимости со статусом «В работе».

Для отправления уязвимости на рассмотрение необходимо выбрать строку, нажать кнопку *«Отправить на проверку»* (см. рис. 86), заполнить поле в окне «Отправить на рассмотрение», нажать кнопку *«ОК»* (рис. 89).

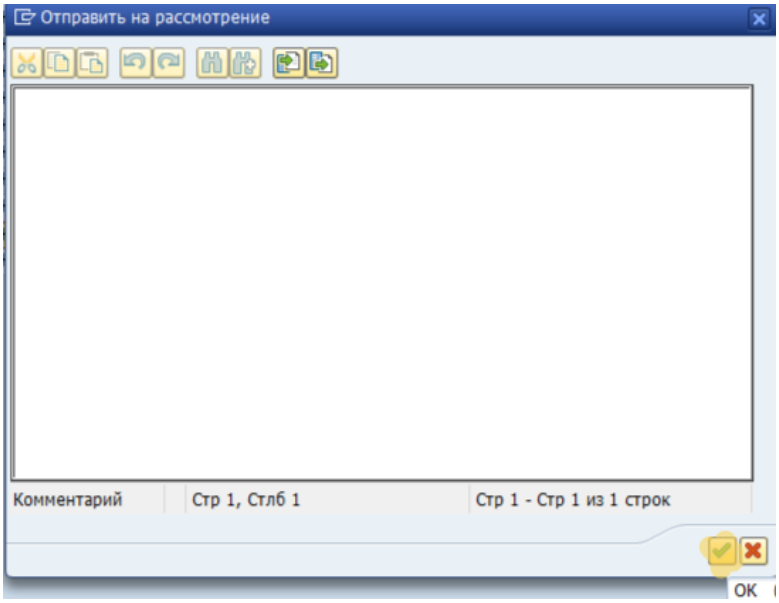


Рисунок 89 – Отправка на рассмотрение

Отправить сообщение

Для отправки сообщения автору запроса необходимо нажать кнопку *«Отправить сообщение»* (см. рис. 86), заполнить поле в окне «Отправить сообщение», нажать кнопку *«ОК»* (рис. 90).

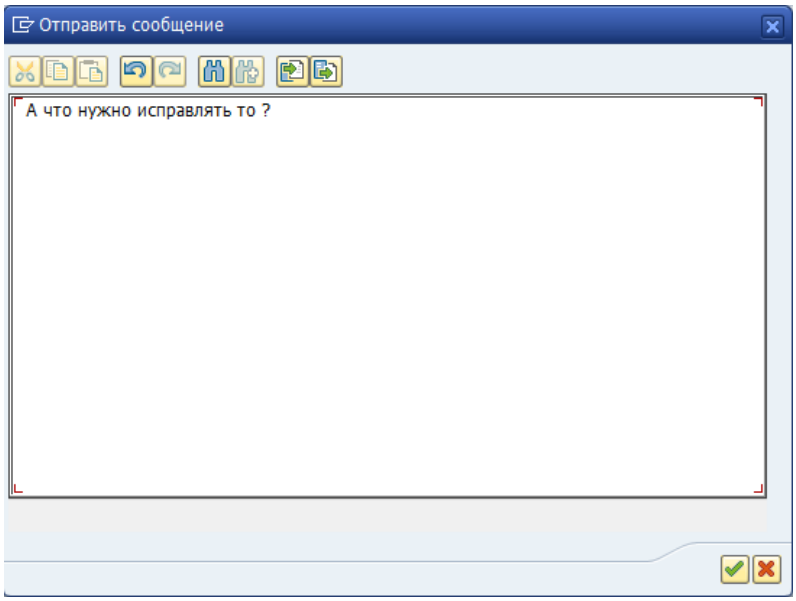


Рисунок 90 – Отправка сообщения

4.20 Выгрузка и загрузка данных освобождений

Для вызова интеграции АТС и SECS, необходимо ввести в командную строку транзакцию /n/gazis/secs_atc.

Содержит следующие виды вкладок (рис. 91):

- «Импорт»;
- «Экспорт».

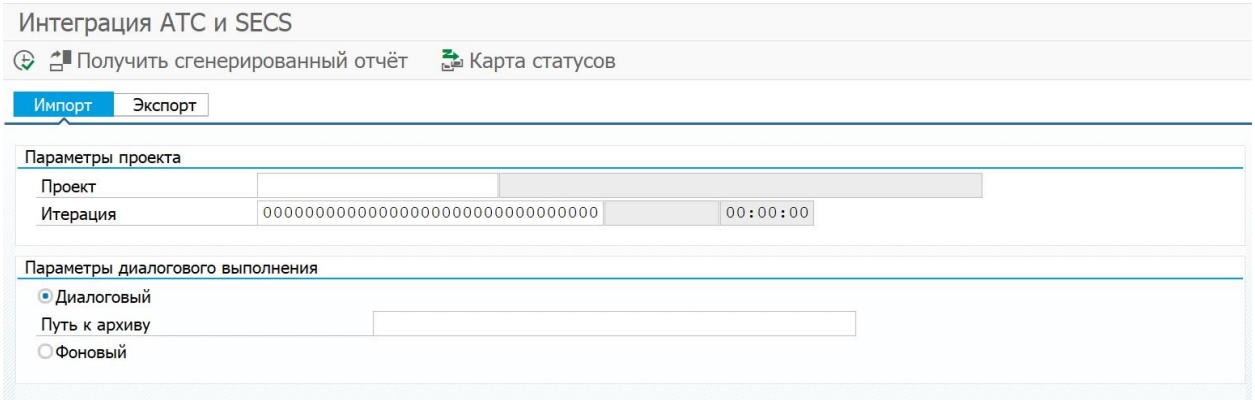


Рисунок 91 – Вкладка «Импорт»

Вкладка «Импорт»

Вкладка «Импорт» предназначена для импорта архива с данными об итерации в формате отчётов EXCEL на локальную машину (считывает с сервера с папки выбранного проекта и выбранной итерации *.sar архив с набором JSON файлов по результатам итерации и преобразует данные в EXCEL, далее упаковывает всё в архив и сохраняет по указанному пути).

Во вкладку импорт входят следующие области:

- «Параметры проекта» – входят строки «Проект» и «Итерация»;
- «Параметры диалогового выполнения» – при выборе типа «Диалоговый» необходимо загрузить zip-архив (рис.94).

Для импорта проекта необходимо выполнить следующие действия:

1) Нажать кнопку в строке «Проект» (см. рис. 91), выбрать проект в открывшемся окне (рис. 92), нажать кнопку .
2) Выбрать итерацию в строке «Итерация», нажать кнопку , выбрать итерацию в открывшемся окне (рис. 93), нажать кнопку .
3) Выбрать параметр диалогового выполнения в соответствующем поле. Нажать кнопку «Выполнить» .

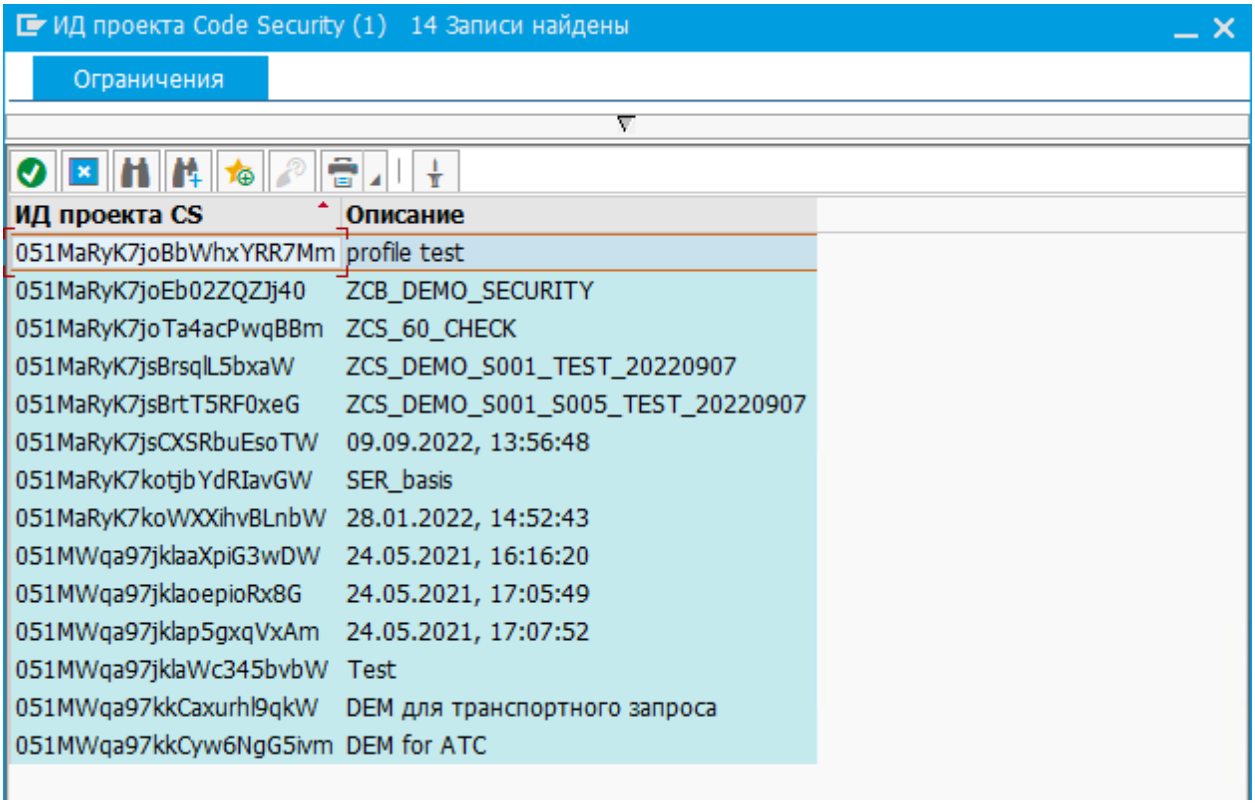


Рисунок 92– Выбор проекта

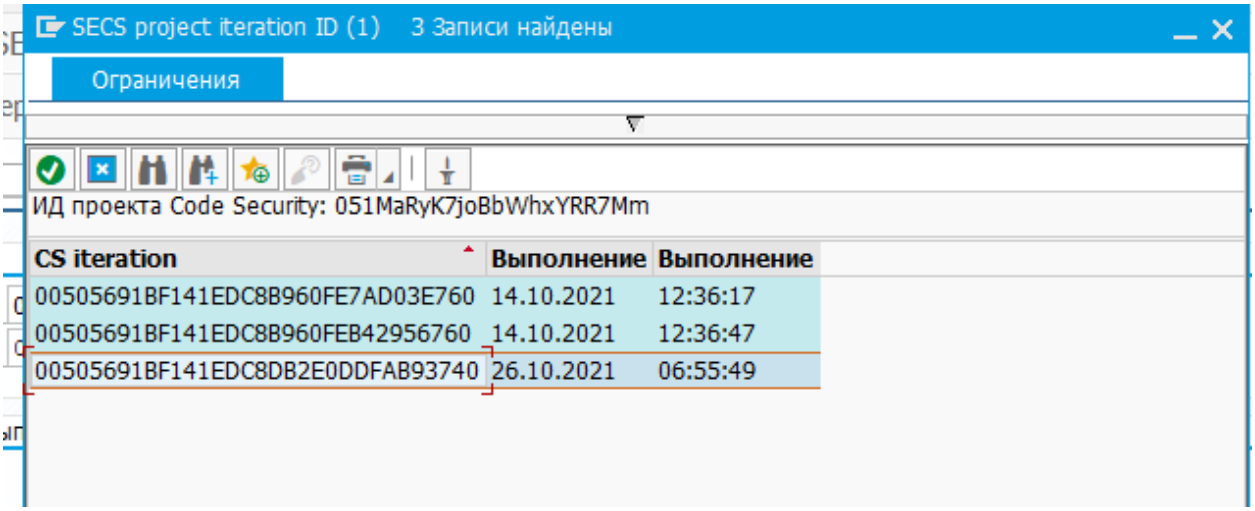


Рисунок 93 – Выбор итераций

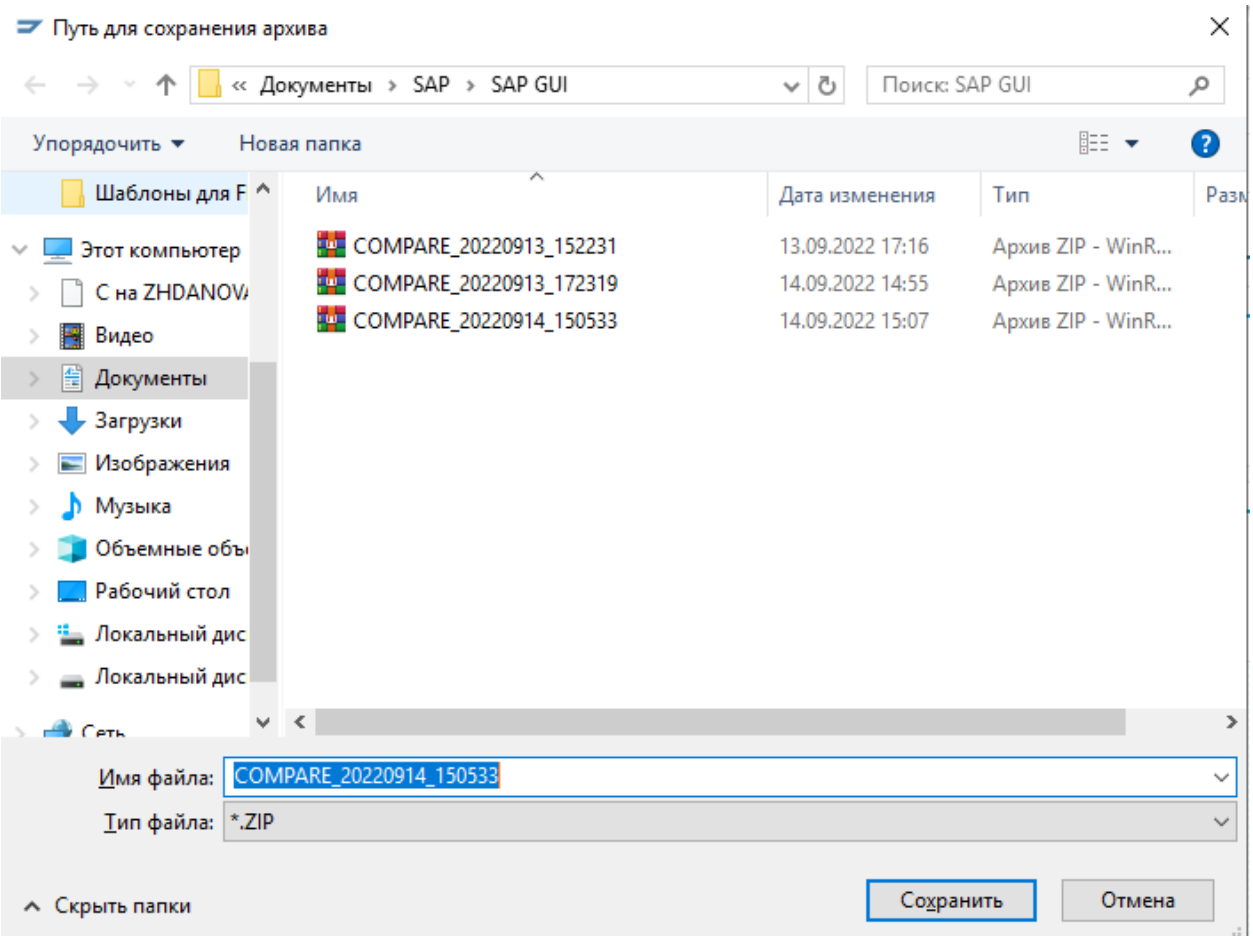


Рисунок 94 – Сохранение архива

Кнопка *«Карта статусов»* предназначена для просмотра статусов запросов, а также для изменений статусов освобождений.

Кнопка *«Получить сгенерированный отчет»* предназначена для выгрузки отчетов на локальную ЭВМ. Для загрузки необходимо выбрать архив в окне, нажать кнопку выполнить.

Вкладка «Экспорт»

Вкладка «Экспорт» предназначена для обновлений освобождений АТС с помощью *zip архива с данными проекта SafeERP Code Security (освобождения считываются из файла FLAWS).

Во вкладку «Экспорт» (рис. 95) входят следующие области:

- «Основные параметры» – выбор *zip архива для экспорта;
- «Параметры освобождения» – параметры, которые необходимо обновить.

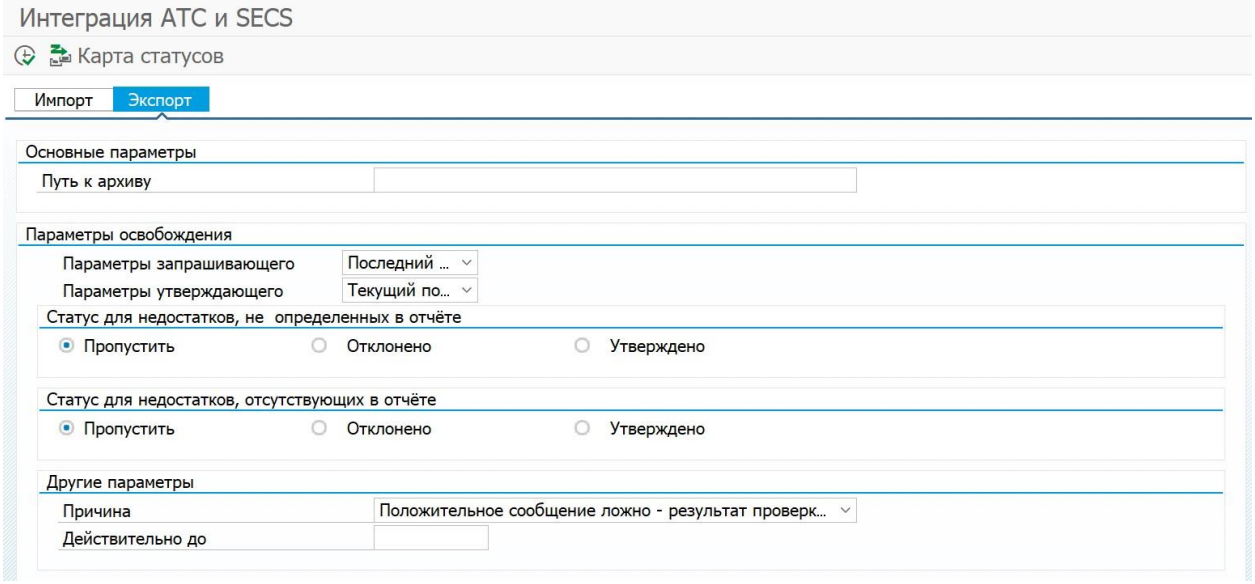


Рисунок 95 – Вкладка «Экспорт»

В область «Параметры освобождения» необходимо указать в:

- поле «Параметры запрашивающего» – пользователь, от которого происходит запрос на освобождение;
- поле «Параметры утверждающего» – пользователь, который утверждает освобождение;
- поле «Статус для недостатков, не определенных в отчете» – статус недостатков, которые не определены в отчете;
- поле «Статус для недостатков, отсутствующих в отчете» – статус недостатков, которые отсутствуют в отчете;
- поле «Другие параметры» – необходимо указать причину, дату и время, до которого действительно освобождение.

Для экспорта проекта необходимо выполнить следующие действия:

1) Выбрать вкладку «Экспорт». Нажать кнопку в поле «Путь к архиву», выбрать архив в открывшемся окне (рис. 96).

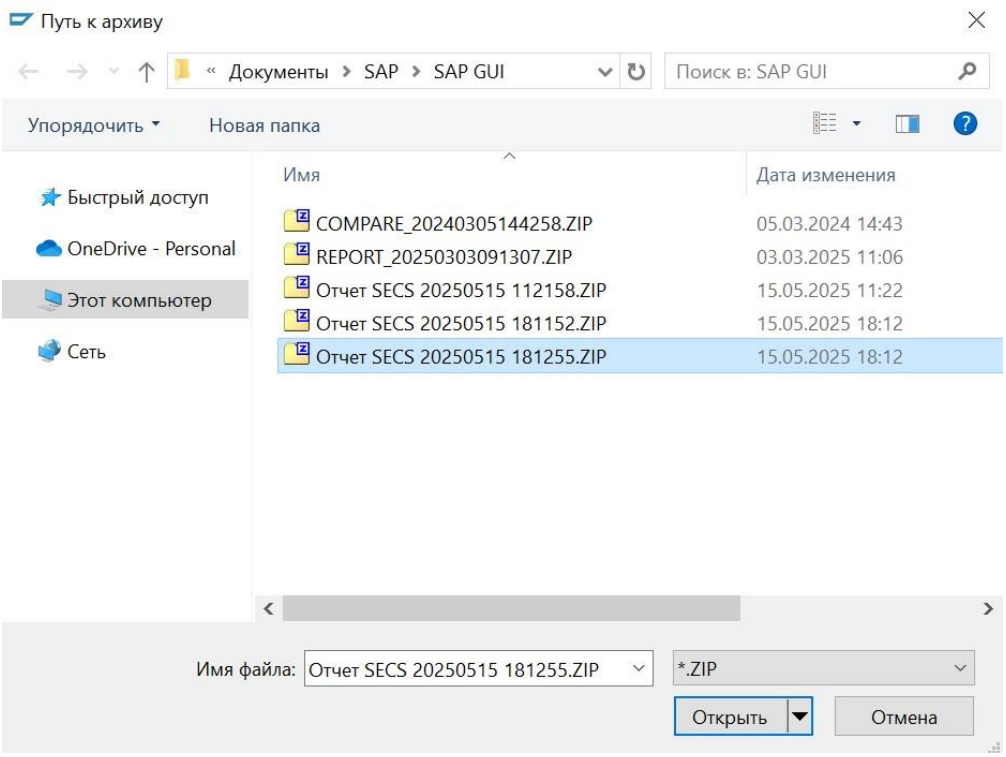


Рисунок 96 – Выбор архива

2) Заполнить поле «Параметры освобождения». Нажать кнопку *«Выполнить»* .

4.21 Подключение к системе отслеживания задач

Для введения настроек для интеграции с системой отслеживания задач необходимо обратиться к транзакции /N/GAZIS/INTEGRAT_TT.

Окно транзакции состоит из следующие областей (рис. 97):

- «Таск-трекер» – предназначен для выбора системы отслеживания задач.
- «Настройки» – предназначен для настройки RFC-соединений для получения информации с агентов.

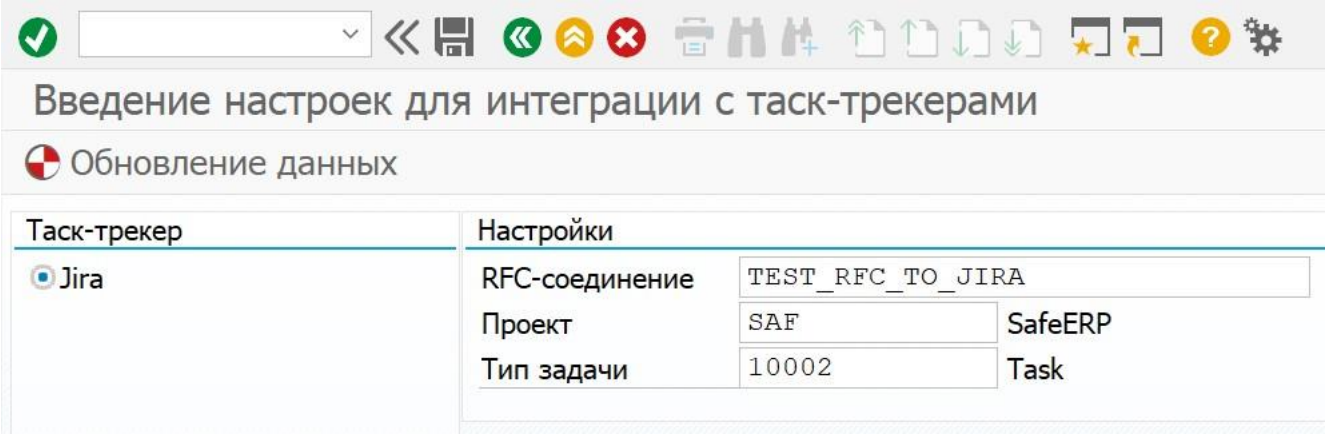


Рисунок 97 – Основная рабочая область транзакции /N/GAZIS/INTEGRAT_TT

В область «Настройки» входят следующие поля (см. рис. 97):

- «RFC-соединение» – выбор RFC-соединения, через который будет осуществляться связь между агентом и таск-трекером. Необходимо выбрать тип соединения G;
- «Проект» – выбор проекта;
- «Тип задачи» – выбор типа задач.

Примечание. Кнопка *«Обновить JIRA-словари»* предназначена для обновление данных на сервере управления: проекты, приоритеты, пользователи, привлеченные на проект, типы задач.

Для синхронизации статуса задач Jira и SAP необходимо выполнить следующие действия:

1) Выбрать RFC-соединения, проект и тип задачи в соответствующих областях (см. рис. 97).
2) Выбрать тип проекта в верхнем меню по следующему пути: «Ведение статусов» → «Анализ кода» (для проектов типа АК) или «Ведение статусов → «Контроль настроек» (для проектов типа КН).
3) Нажать на ячейку в столбце «ID статуса в SAP» (рис. 98, 99). Выбрать статус задачи в окне (рис. 100, 101). Нажать кнопку *«Сохранить».*

Введение статусов для проектов КН

ID статуса в SAP	Описание	ID статуса в Jira	Описание
1	Открыто	10000	New
2	В работе	3	[В работе]
3	Исправлено	10001	Done
4	Безопасно	10001	Done
5	На рассмотрении	3	[В работе]

Рисунок 98 – Список проектов типа КН

Введение статусов для проектов АК

ID статуса в SAP	Описание	ID статуса в Jira	Описание
0	Открыто	10000	New
2	Исправлено	3	[В работе]
3	В работе	3	[В работе]
5	На проверке	3	[В работе]

Рисунок 99 – Список проектов типа АК

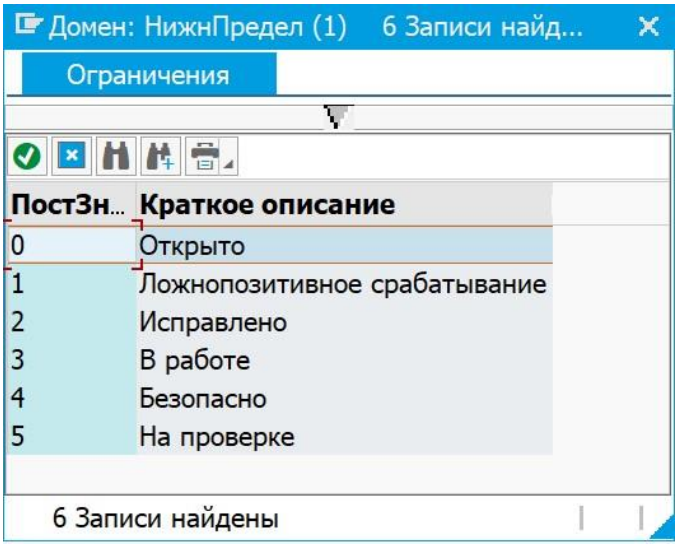


Рисунок 100 – Статусы для проекта типа АК

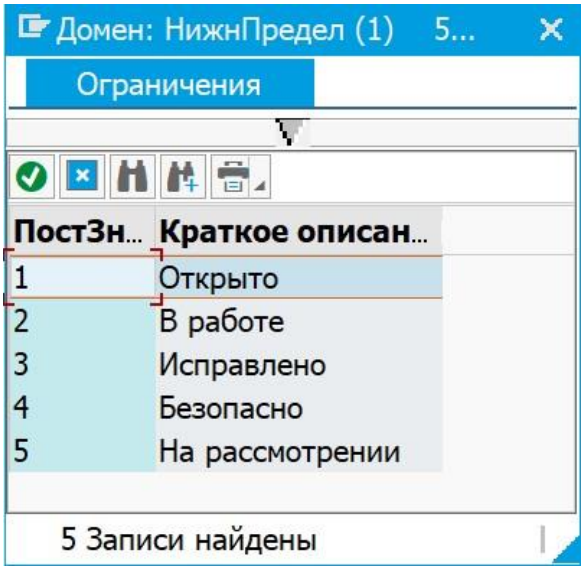


Рисунок 101 – Статусы для проекта типа КН

Примечание. Для столбца «ID статуса в Jira» доступно изменение статуса. Для изменения статуса необходимо нажать на ячейку в столбце «ID статуса в Jira», выбрать статус в окне (рис. 102), нажать кнопку *«Сохранить».*

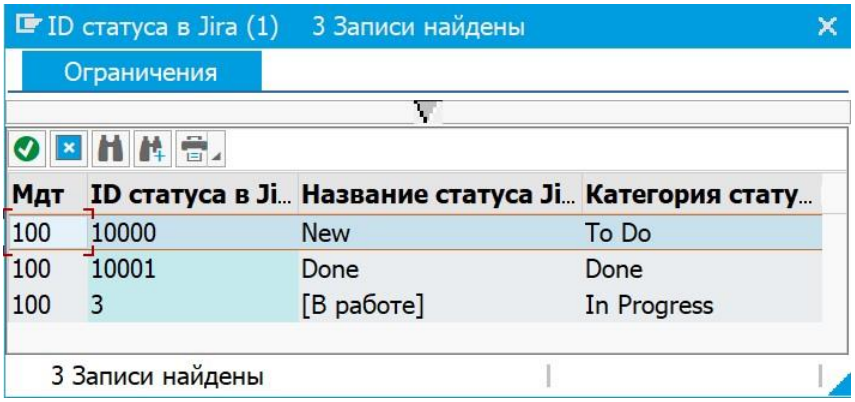


Рисунок 102 – ID статусы Jira

4.22 Управление найденными уязвимостями

Управление уязвимостями осуществляется на агент-системах. Для управления уязвимостями необходимо обратиться к транзакции /N/GAZIS/SECS_VULNERS .
Окно транзакции представлено на рис. 103.

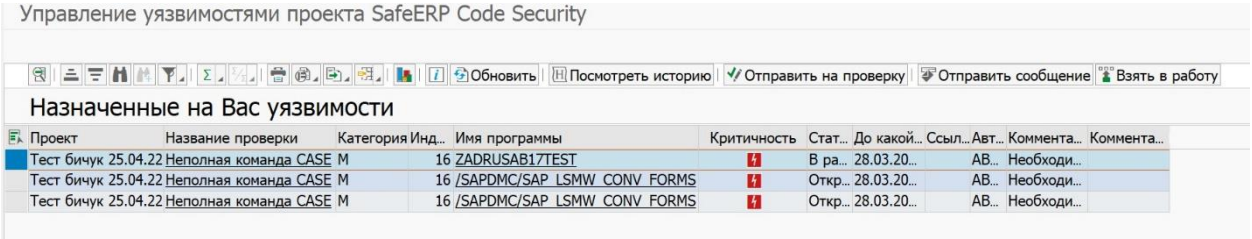


Рисунок 103 – Основная рабочая область

Пользователю доступны следующие действия:

- Обновление информации назначенных уязвимостей. Для обновления информации необходимо нажать кнопку *«Обновить»*.
- Просмотр истории уязвимости. Для просмотра уязвимости необходимо нажать кнопку *«Просмотреть историю»*.
- Отправка на проверку. Для отправки на проверку необходимо нажать кнопку *«Отправить на проверку»*.
- Отправка сообщений.
- Присвоение статуса «Взято в работу».

4.23 История полномочий

Транзакция /n/gazis/history предназначена для просмотра изменений (присвоение, удаление) в ролях.
Основная рабочая область представлена на рис. 104.

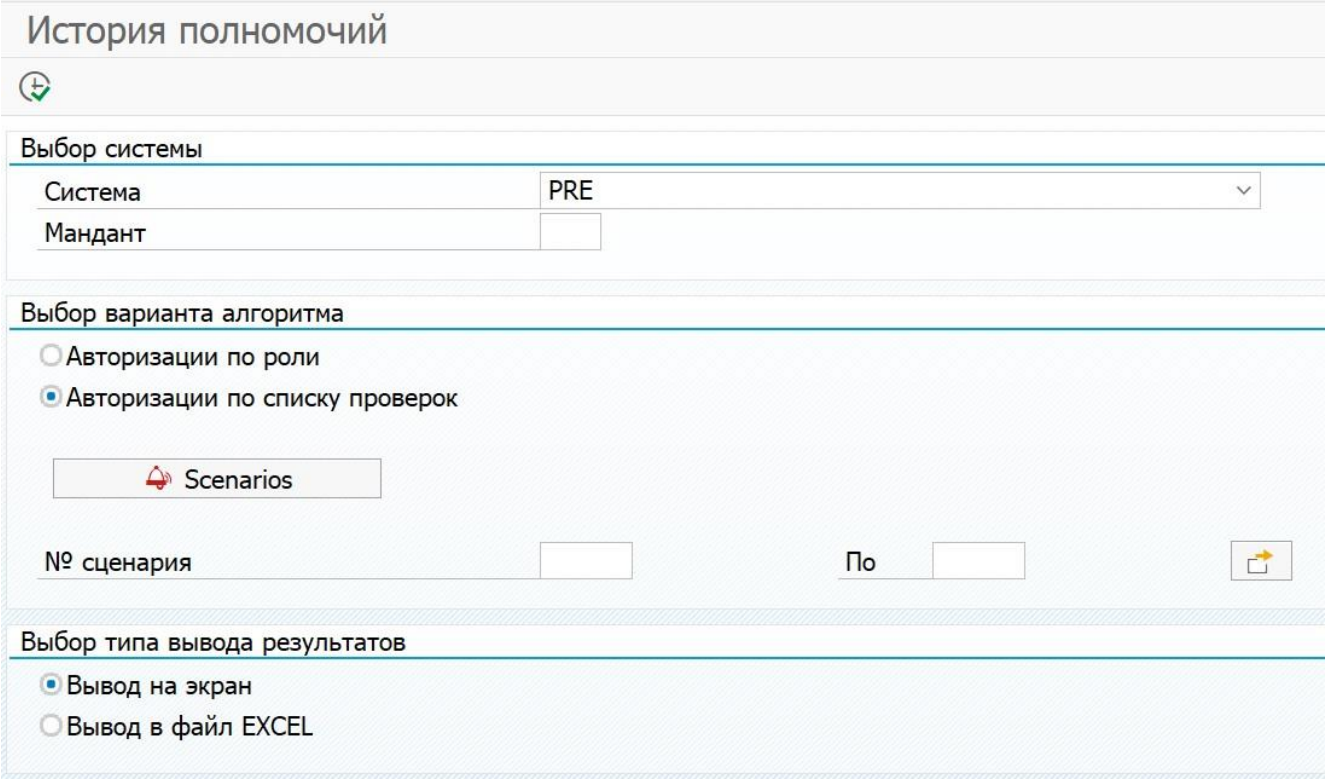


Рисунок 104 – Основная рабочая область транзакции /n/gazis/history

Основная рабочая состоит из следующих областей:

- «Выбор системы» – состоит из полей: «Система» и «Мандант»;
- «Выбор варианта алгоритма» – состоит из полей: «Авторизации по роли» и «Авторизация по списку проверок»;
- «Выбор типа вывода результатов» – состоит из элементов выбора: «Вывод на экран» и «Вывод в файл EXCEL»

Для просмотра истории полномочий необходимо выполнить следующие действия:

1) Выбрать систему в соответствующем поле.
2) Нажать кнопку «Enter» в поле «Мандант». Нажать кнопку , выбрать мандант в новом окне (рис. 105).

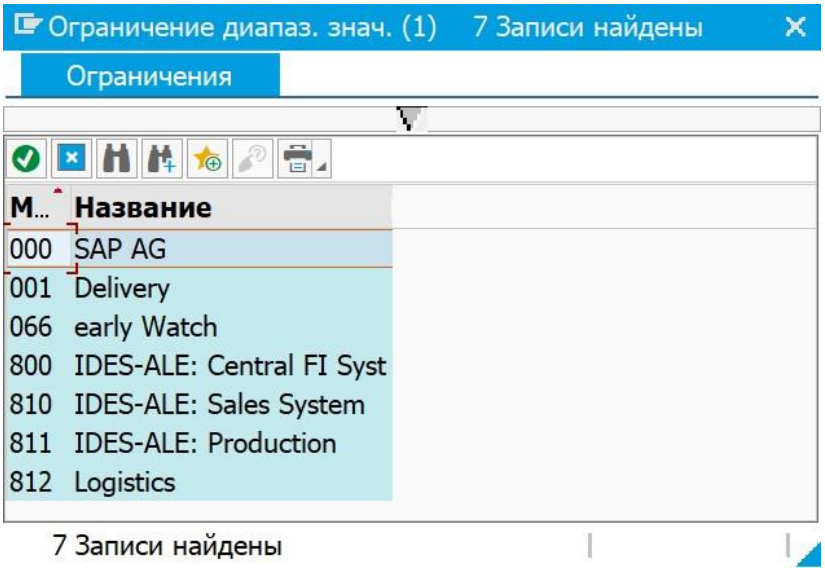


Рисунок 105 – Выбор манданта

3) Выбрать вариант поиска полномочий в области «Выбор варианта алгоритма».
4) Выбрать тип вывода результатов в соответствующей области.
5) Нажать кнопку *«Выполнить».*
6) Выбрать период начала и конца

4.24 Проверка наименований объектов

На всех системах SAP существуют шаблоны наименований объектов и требования к ABAP-разработкам в части наименований сущностей. Требования имеют силу при разработке новых функциональных единиц и корректировке старых, а также учитывают пространство имён, в котором работает система.

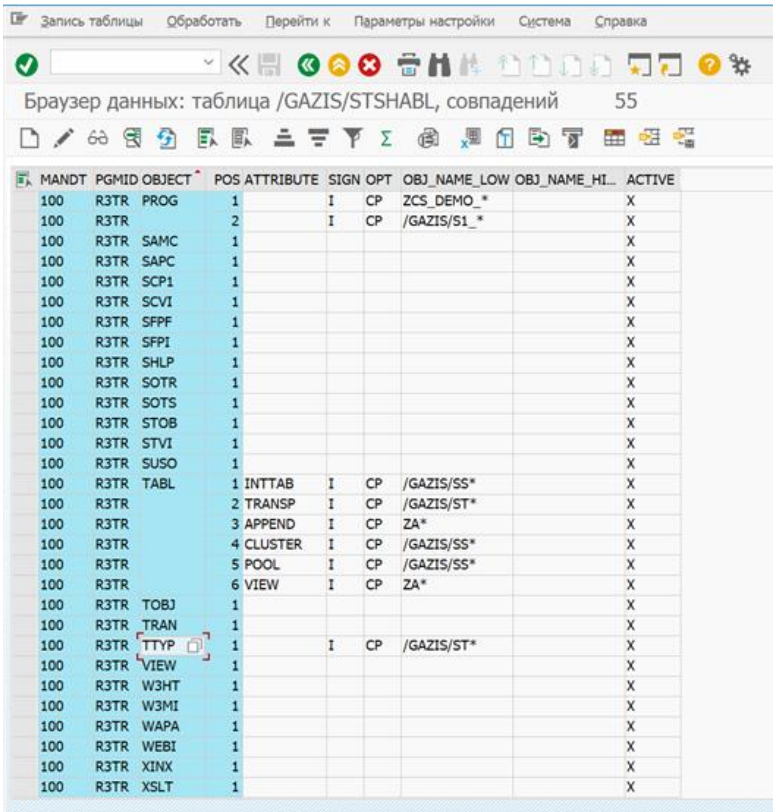
Для проверки наименований объектов необходимо обратиться к транзакции /N/GAZIS/CHECK_NAMES.

4.24.1 Необходимые настройки

Для корректной работы транзакции необходимо настроить шаблон проверки.

Для настройки шаблона необходимо выполнить следующие действия:

1) Запустить транзакцию SE11. В поле «Таблица БД» ввести «/GAZIS/STSHABL». Нажать кнопку *«Просмотр».*
2) Нажать кнопку *«Содержимое»* в открывшемся окне (рис. 106).



MANDT	PGMID	OBJECT	POS	ATTRIBUTE	SIGN	OPT	OBJ_NAME_LOW	OBJ_NAME_HI...	ACTIVE
100	R3TR	PROG	1		I	CP	ZCS_DEMO_*		X
100	R3TR		2		I	CP	/GAZIS/S1_*		X
100	R3TR	SAMC	1						X
100	R3TR	SAPC	1						X
100	R3TR	SCP1	1						X
100	R3TR	SCVI	1						X
100	R3TR	SFPF	1						X
100	R3TR	SFPI	1						X
100	R3TR	SHLP	1						X
100	R3TR	SOTR	1						X
100	R3TR	SOTS	1						X
100	R3TR	STOB	1						X
100	R3TR	STVI	1						X
100	R3TR	SUSO	1						X
100	R3TR	TABL	1	INTTAB	I	CP	/GAZIS/SS*		X
100	R3TR		2	TRANSP	I	CP	/GAZIS/ST*		X
100	R3TR		3	APPEND	I	CP	ZA*		X
100	R3TR		4	CLUSTER	I	CP	/GAZIS/SS*		X
100	R3TR		5	POOL	I	CP	/GAZIS/SS*		X
100	R3TR		6	VIEW	I	CP	ZA*		X
100	R3TR	TOBJ	1						X
100	R3TR	TRAN	1						X
100	R3TR	TTYP	1		I	CP	/GAZIS/ST*		X
100	R3TR	VIEW	1						X
100	R3TR	W3HT	1						X
100	R3TR	W3MI	1						X
100	R3TR	WAPA	1						X
100	R3TR	WEBI	1						X
100	R3TR	XINX	1						X
100	R3TR	XSLT	1						X

Рисунок 106 – Список объектов

3) Поставить «X» в столбце «ACTIVE» для тех параметров, которые должны попасть в проверки.

Примечания:

1. Пользователю предоставляется возможность добавления любого типа объекта, используя таблицу TADIR.
2. В поле «ATTRIBUTE» моно занести дополнительную информацию. Например, для таблиц – тип таблицы (прозрачная таблица, структура и др).

4.24.2 Запуск транзакции

Для проверки наименования объектов необходимо ввести транзакцию /N/GAZIS/CHECK_NAMES в командную строку.

Основная рабочая область транзакции представлена на рис. 107.

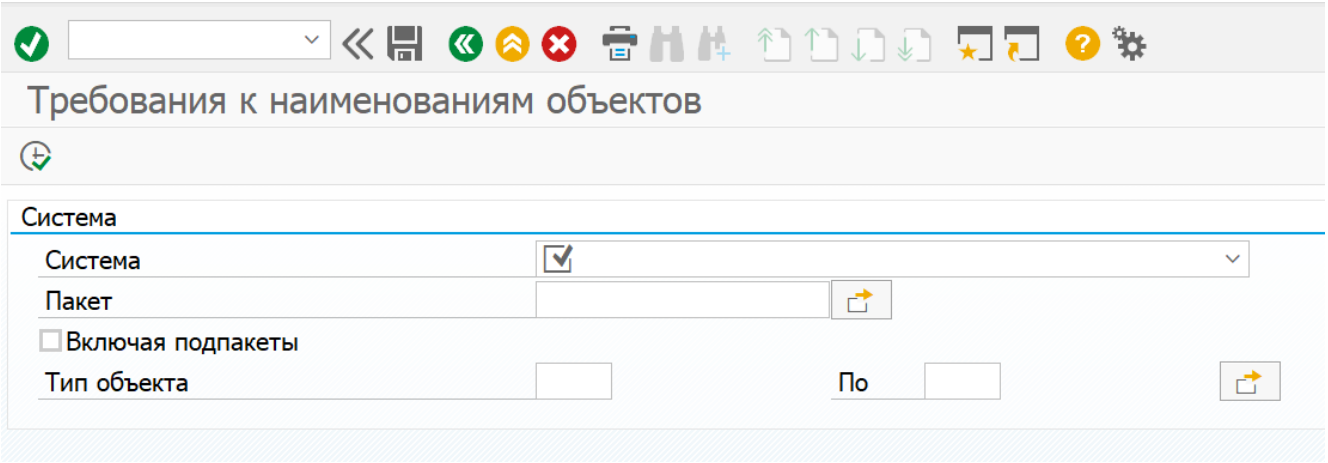


Рисунок 107 – Основная рабочая область транзакции /N/GAZIS/CHECK_NAMES

Основная рабочая область состоит из следующего:

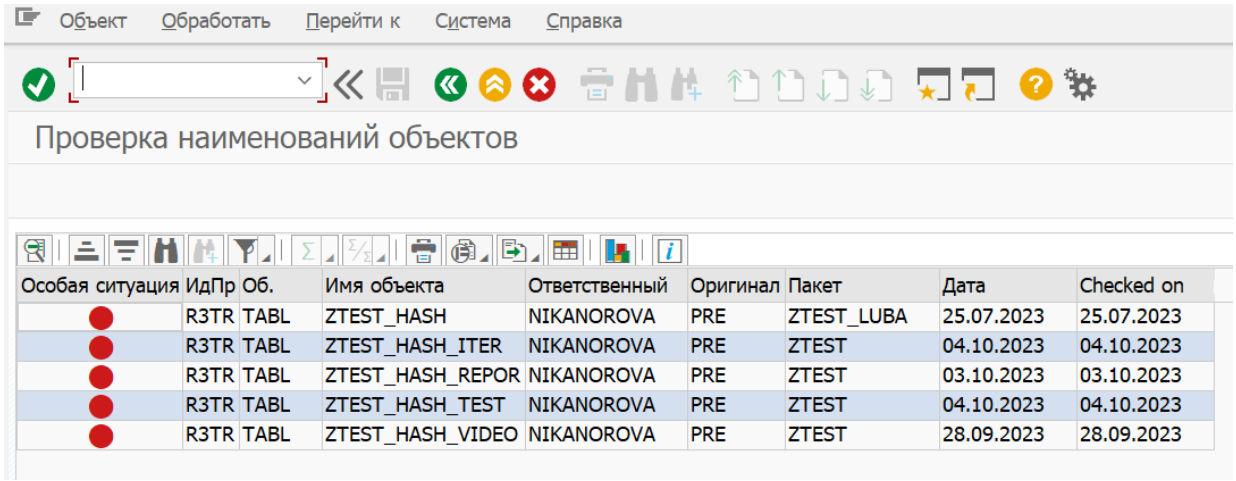
- поле «Система» – выбор системы для сканирования;
- поле «Пакет» – выбор пакета для сканирования;
- элемент выбора «Включая подпакеты» – активация сканирования подпакетов;
- поле «Тип объекта» – выбор тип объекта.

Для проверки наименования объектов необходимо выполнить следующие действия:

1) Заполнить поля «Система», «Пакет», тип объекта.
2) Нажать кнопку *«Выполнить»*.

Примечание. Пакет может содержать много сущностей, то необходимо не загружать выборку большим объемом данных.

Подробный результат представлен на рис. 108.



Особая ситуация	ИдПр	Об.	Имя объекта	Ответственный	Оригинал	Пакет	Дата	Checked on
●	R3TR	TABL	ZTEST_HASH	NIKANOROVA	PRE	ZTEST_LUBA	25.07.2023	25.07.2023
●	R3TR	TABL	ZTEST_HASH_ITER	NIKANOROVA	PRE	ZTEST	04.10.2023	04.10.2023
●	R3TR	TABL	ZTEST_HASH_REPOR	NIKANOROVA	PRE	ZTEST	03.10.2023	03.10.2023
●	R3TR	TABL	ZTEST_HASH_TEST	NIKANOROVA	PRE	ZTEST	04.10.2023	04.10.2023
●	R3TR	TABL	ZTEST_HASH_VIDEO	NIKANOROVA	PRE	ZTEST	28.09.2023	28.09.2023

Рисунок 108 – Результат проверки

Примечание. Красный индикатор в столбце «Особая ситуация» присваивается в том случае, когда проверка не пройдена.

4.25 Иерархия полномочий

Транзакция /n/gazis/hierarchy предназначена для выявления списка пользователей, которым присвоены определенные авторизации.

Основная рабочая область представлена на рис. 109.

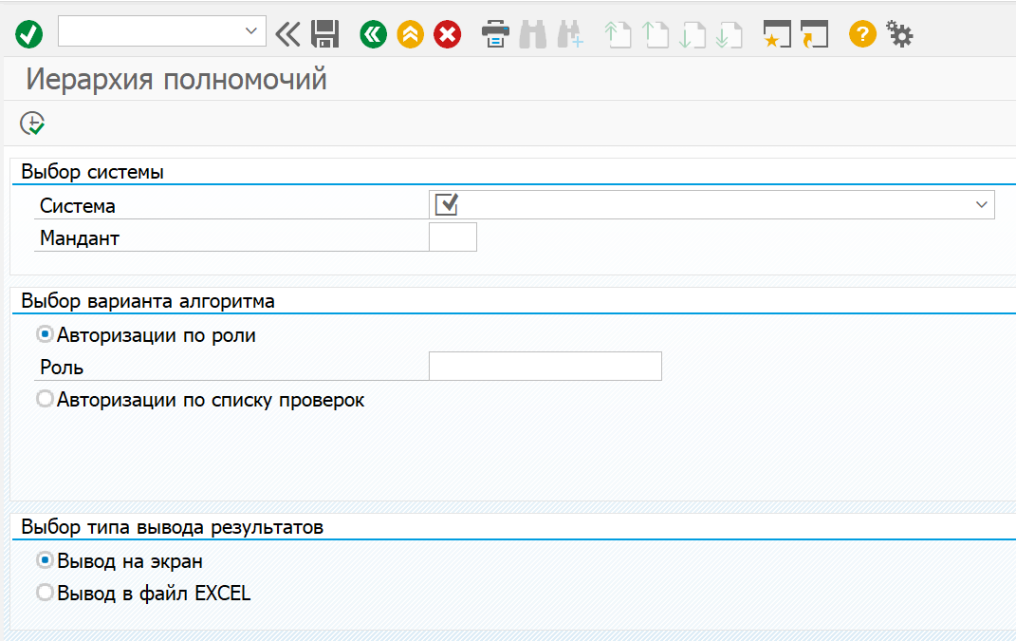


Рисунок 109 – Основная рабочая область транзакции /n/gazis/hierarchy

Основная рабочая область состоит из следующих областей:

- «Выбор системы» – состоит из полей: «Система» и «Мандант»;
- «Выбор варианта алгоритма» – состоит из полей: «Авторизации по роли» и «Авторизация по списку проверок»;
- «Выбор типа вывода результатов» – состоит из элементов выбора: «Вывод на экран» и «Вывод в файл EXCEL».

Для поиска полномочий необходимо выполнить следующие действия:

1) Выбрать систему в соответствующем поле.
2) Нажать кнопку «Enter» в поле «Мандант». Нажать кнопку , выбрать мандант в новом окне (рис. 105).
3) Выбрать вариант поиска полномочий в области «Выбор варианта алгоритма».
4) Выбрать тип вывода результатов в соответствующей области.
5) Нажать кнопку *«Выполнить».*

4.26 Поиск объектов полномочий

Транзакция предназначена для обнаружения полномочий в транзакции согласно выбранной агент-системе.

Основная рабочая область представлена на рис. 110.

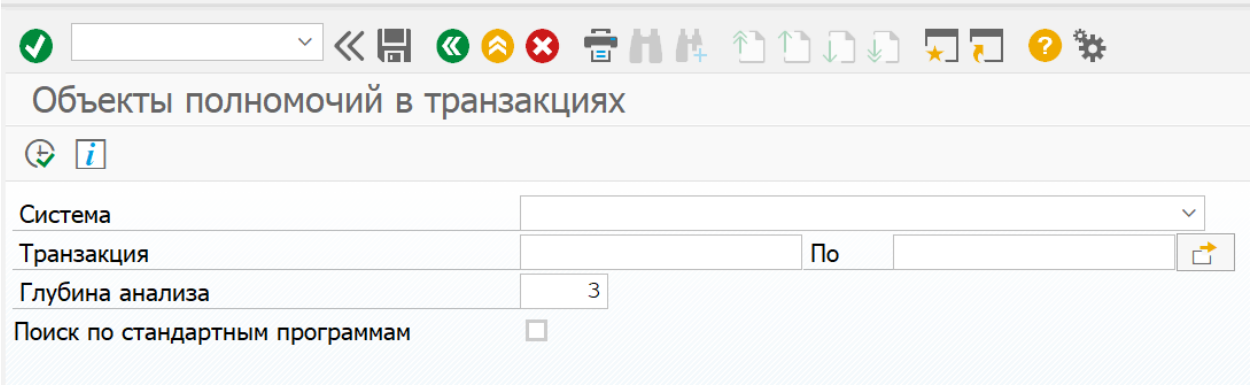


Рисунок 110 – Основная рабочая область транзакции /n/gazis/tran_auth

В основную рабочую область входит следующее:

- поле «Система» – выбор системы для анализа;
- поле «Транзакция» – поле выбора транзакций. Доступен множественный выбор объектов;
- поле «Глубина анализа» – количество вложенных вызов, в которых будет осуществляться поиск объектов полномочий;
- элемент выбора «Поиск по стандартным программам». При установке флага в данной области поиск объектов полномочий (для выбранных транзакций) будут осуществляться в стандартных SAP-программах. По умолчанию поиск объектов полномочий осуществляется в кастомизированных объектах репозитария.

Для поиска объектов полномочий необходимо выполнить следующие действия:

1) Выбрать систему в соответствующем поле
2) Выбрать транзакцию в соответствующем поле.
3) Указать глубину анализа в соответствующем поле.
4) Нажать кнопку *«Выполнить».*

5 Инструменты освобождения

Инструмент освобождений ПК «SafeERP Security Suite» – это инструмент, реализованный на основе SCI (Sap code inspector), являющийся механизмом обработки результатов сканирования статического анализатора кода «SafeERP Security Suite» и предназначенный для более глубокого анализа фиктивных и ложноположительных срабатываний о найденных уязвимостях.

5.1 Полномочия

Для корректной работы инструмента освобождений утверждающий должен иметь полномочия Администратора ПК «SafeERP Security Suite».

5.2 Необходимые настройки

Для корректной работы инструмента освобождений необходимо настроить серверную и агентские части.

5.2.1 Настройка серверной части

Для работы серверной части необходимо проверить следующие данные:

1) Проверяемая система должна быть добавлена в список агентов и иметь действующую лицензию типа Main.

Примечание. Для просмотра и настройки агента необходимо ввести транзакцию /N/GAZIS/SEGA в командную строку.

2) RFC-соединение от сервера к агентской системе должно быть активно
3) Пользователю, под которым настроено RFC-соединение должны быть даны все необходимые полномочия.
4) Пользователь, который будет настраивать и пользоваться транзакцией /GAZIS/SACT должен иметь полномочия администратора ПК «SafeERP Security Suite».

Примечание. TMS-интеграция должна быть правильно настроена.

Для настройки серверной части необходимо выполнить следующие действия:

1) Ввести транзакцию /N/GAZIS/SACT в командную строку.
2) Выбрать раздел «Основные настройки» (рис. 111).

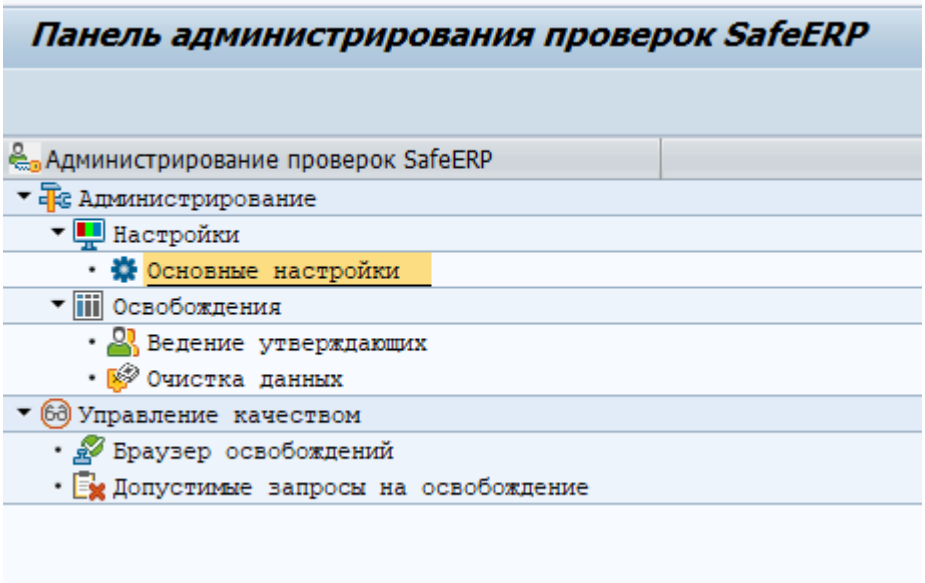


Рисунок 111 – Окно транзакции «/N/GAZIS/SACT»

3) Выбрать глобальный профиль проверки, из которого будет считываться список используемых проверок.
4) Активировать освобождения.
5) Активировать почтовые уведомления для утверждающего (при необходимости). Примечание. Для работы почтовых уведомлений должен быть настроен почтовый сервер и в личных данных утверждающего указан почтовый адрес, на который будут поступать уведомления.
6) Нажать кнопку *«Сохранить».*

5.2.1.1. Настройка утверждающего

Для настройки утверждающего необходимо выполнить следующие действия:

1) Ввести транзакцию /N/GAZIS/SACT в командную строку.
2) Выбрать раздел «Ведение утверждающих».
3) Нажать кнопку Добавить.
4) Выбрать пользователя из списка с помощью кнопки .
5) Нажать кнопку *«Сохранить».*

5.2.2 Настройка агентской части

Для настройки агентской части необходимо проверить следующие данные:

1) В таблице /GAZIS/ATRFS должно быть 1 значение - RFC-соединение от агента к серверу (должно быть активно и настроены все полномочия).
2) В SE03 должны быть активированы проверки при деблокировании запроса.
3) В TRCHECK должна быть настроена блокировка запросов при наличии ошибок.
4) На агентской системе (транзакция SCI) должны быть необходимые проверки (можно выравнять с сервера).
5) Должен быть создан вариант проверки, добавлены в него необходимые проверки либо все и этот вариант необходимо добавить в таблицу SCICHKV_ALTER.

5.2.3 Почтовые уведомления

Для работы почтовых уведомлений необходимо настроить почтовый сервер на сервере управления ПК «SafeERP Security Suite».

Примечание. Для корректной работы функциональности по отправке уведомлений необходимо пользователю, с помощью которого производится RFC-соединение(аутентификация), настроить все необходимые полномочия для работы с почтовым сервером, т.к. именно от его имени будут отправляться уведомления.

Почтовые уведомления для отправляющего приходят в следующих случаях (рис. 112):

- при отклонении;
- при утверждении и отклонении;
- никогда.

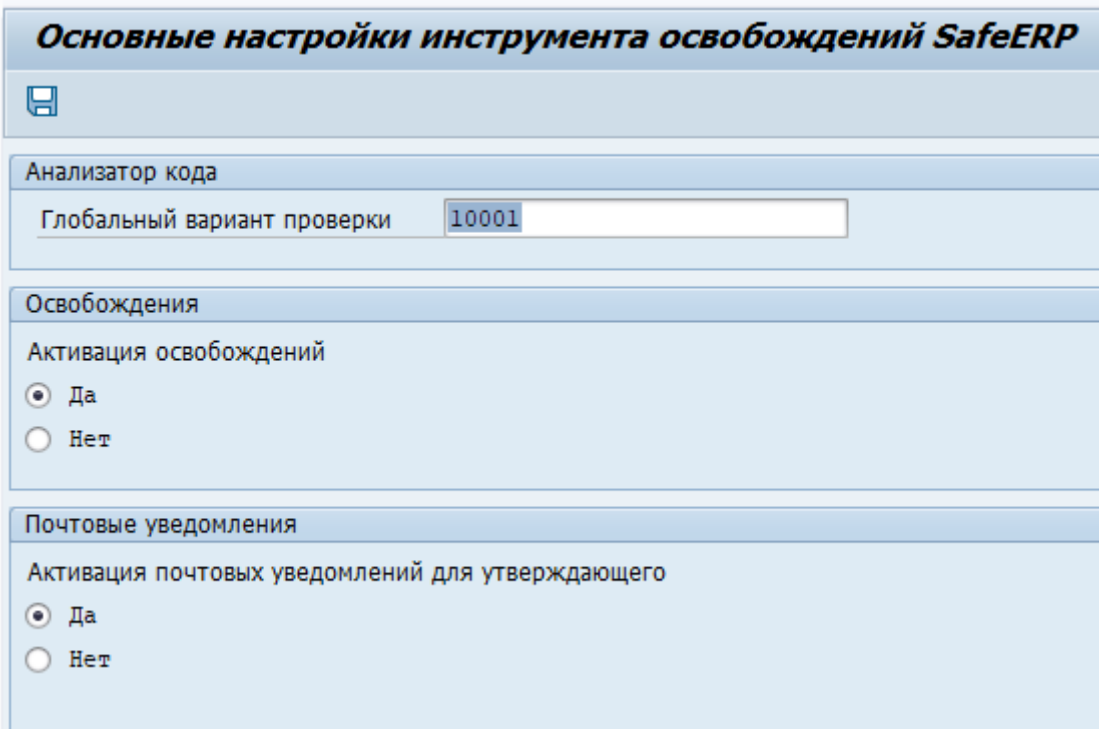


Рисунок 112 – Основные настройки

Для утверждающего почтовые уведомления настраиваются в транзакции /N/GAZIS/SACT в разделе «Основные настройки» (рис. 113).

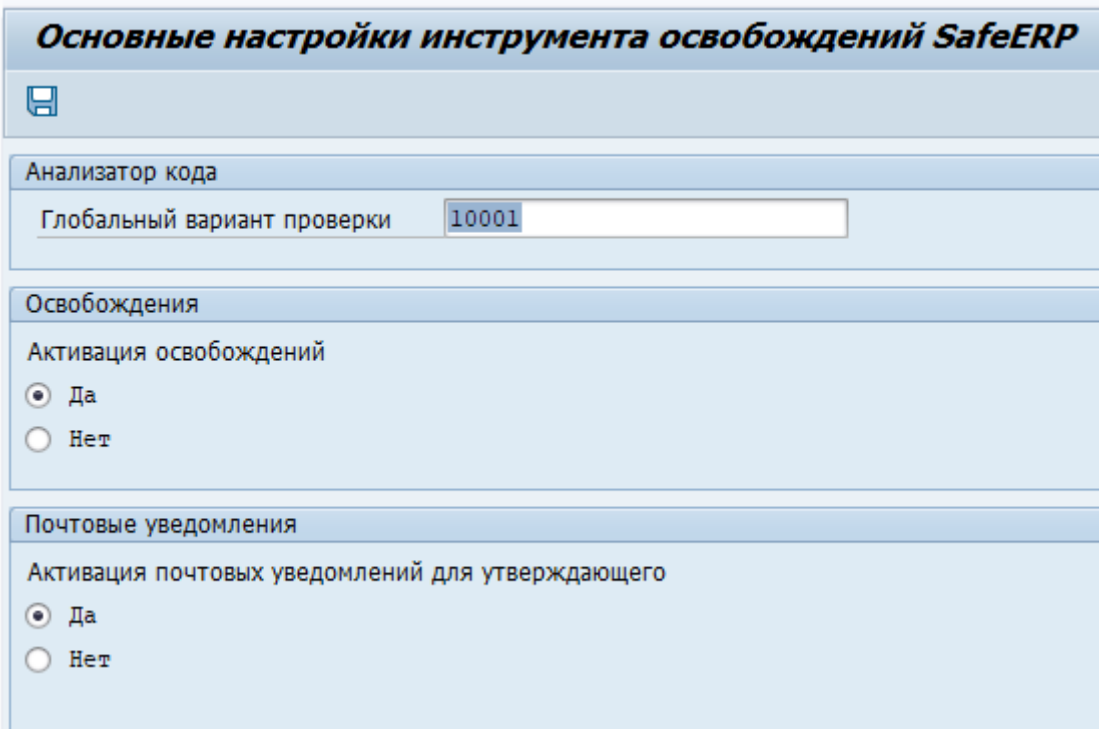


Рисунок 113 – Основное окно

Почтовые уведомления для утверждающего приходят в следующих случаях:

- создании освобождения,
- переходе освобождения в статус «В обработке у утверждающего».

5.3 Статусы освобождений

Статусы освобождений бывают следующими:

- «Открыто»;
- «В обработке у утверждающего»;
- «В обработке у запрашивающего»;
- «Отклонено»;
- «Утверждено».

5.4 Утверждение освобождения

5.4.1 Создания освобождения

Утверждение освобождения для разработчика необходимо выполнить следующие действия:

1) Деблокировать транспортный запрос, который содержит в себе изменения, в транзакции SE09. Запускается процесс анализа исходного кода и считываются освобождения по проверяемым объектам.

   После окончания анализа появляется окно с вопросом о запросе освобождений (рис. 114). В открывшемся окне нажать кнопку *«Да»*.

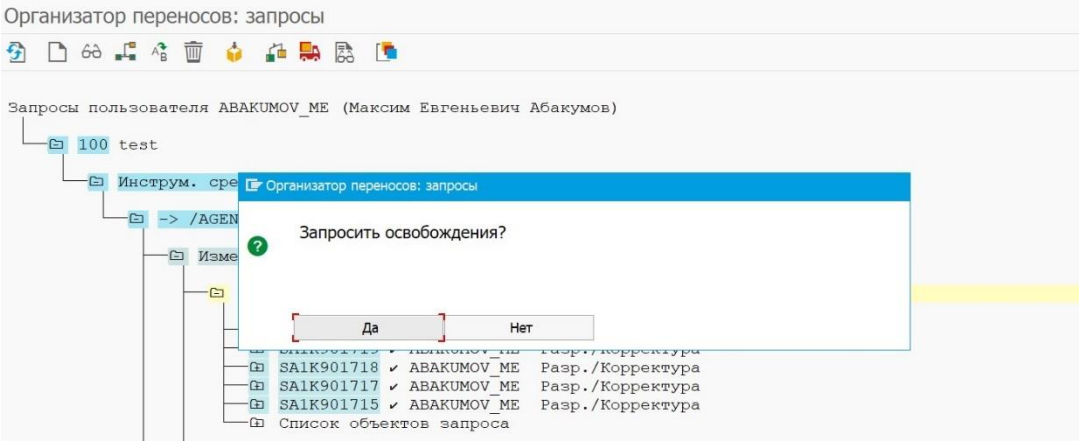


Рисунок 114 – Деблокирование запроса

2) Выбрать в открывшемся окне выбрать уязвимость, нажав на столбец «Поле» (рис. 115).

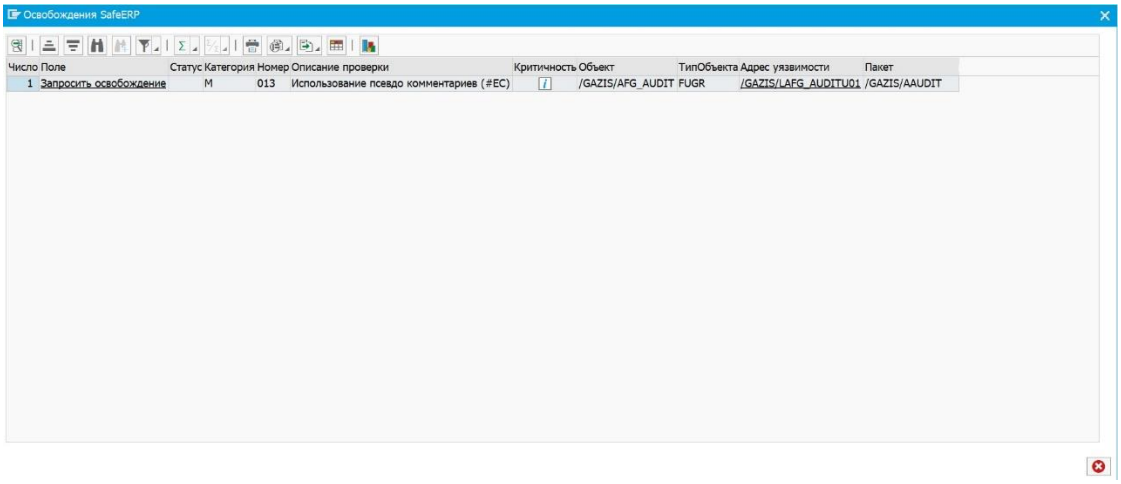


Рисунок 115 – Список уязвимостей

3) На первом шаге «Объем освобождения» доступен просмотр по уязвимости.
4) Выбрать «Утверждающий» и причина». Заполнить поля «Утверждающий», «Причина», «Обоснование», а также настроить уведомления. Нажать кнопку *«Сохранить»* (рис. 116).

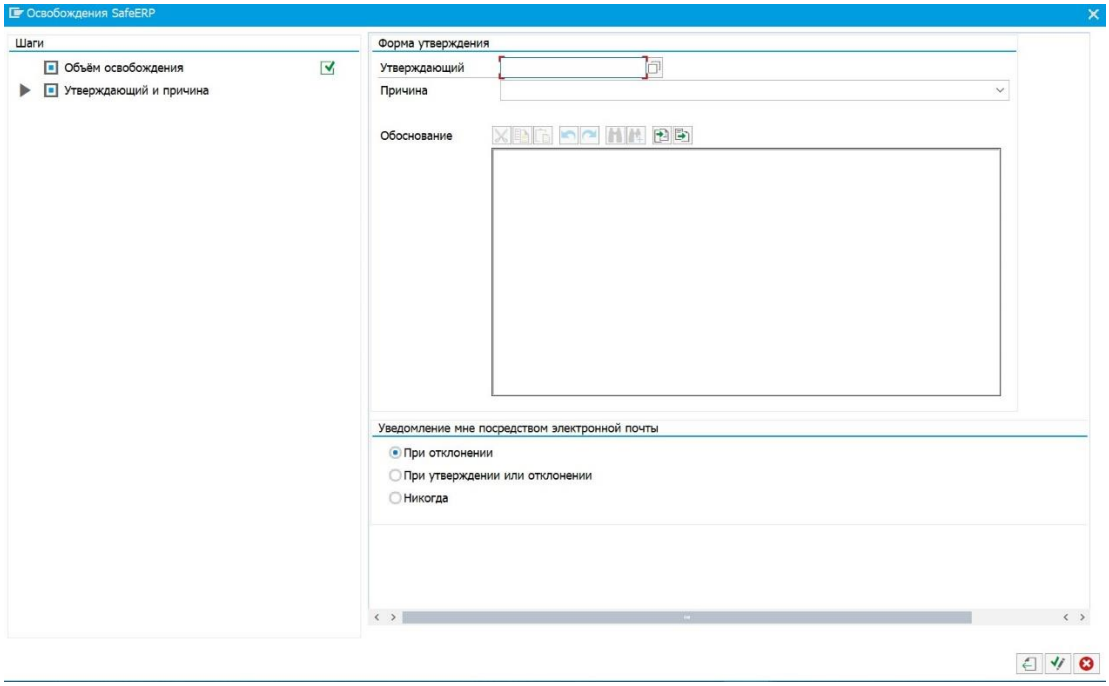


Рисунок 116 – Утверждающий и причина

Для утверждения освобождения необходимо выполнить следующее:

1) Запустить транзакцию /N/GAZIS/SACT на сервере.
2) Выбрать вкладку «Браузер освобождения».
3) Выбрать в открывшемся окне «Утверждающего». Нажать кнопку *«Выполнить»* (рис. 117).

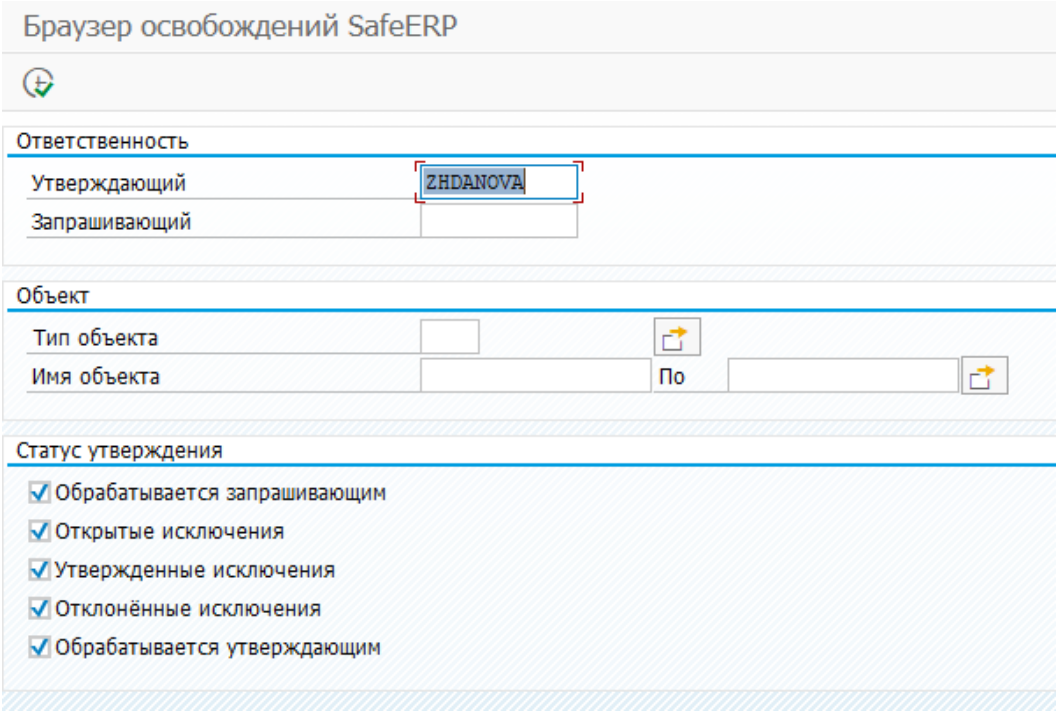


Рисунок 117 – Браузер освобождений

Нажать двойным кликом левой кнопки мыши на освобождение со статусом «Открыто» (рис. 118). Откроется подробное описание выбранного освобождения (рис. 119).

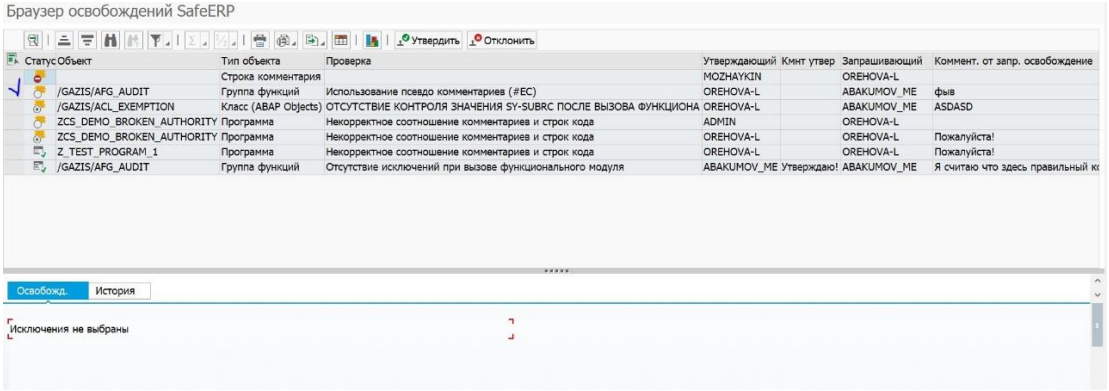


Рисунок 118 – Список освобождений

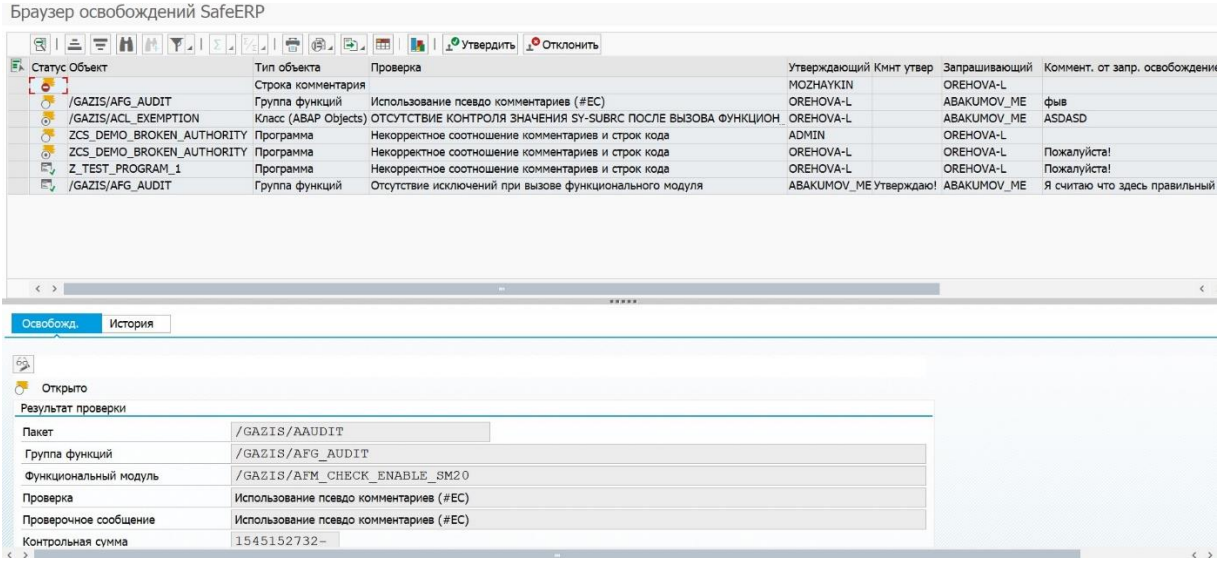


Рисунок 119 – Подробное описание освобождения

4) Нажать кнопку *«Переключить режим»*. Нажать кнопку *«Утвердить»*.

Примечание. При смене режима доступны следующие действия с освобождениями: «Сохранить и закрыть», «Удалить», «Утвердить», «Отклонить», «Вернуть запрашиваемому».

6 Запуск веб-интерфейса администратора ПК «SafeERP Security Suite»

Для работы с веб-интерфейсом функциональности ПК «SafeERP Security Suite» в SAP UI5/Fiori необходимо запустить приложение SAP Fiori из SAP-системы. Доступные способы запуска:

— через вызов из пользовательского меню (рис. 120);

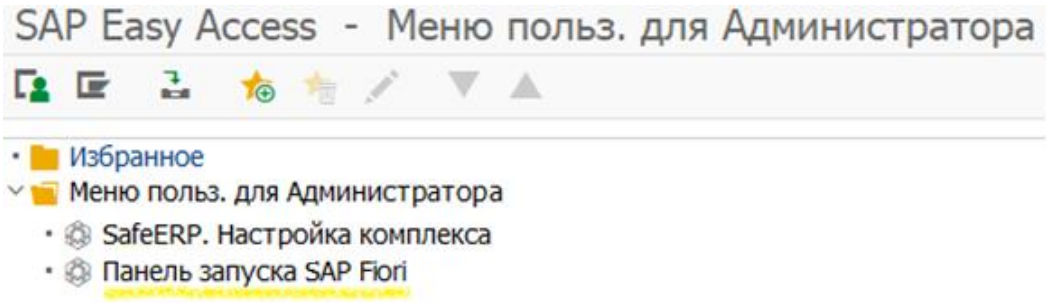


Рисунок 120 – Вызов SAP Fiori из меню системы

— через ввод транзакции «/n/gazis/flp» в командной строке (рис. 121);

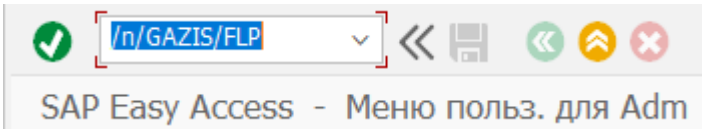


Рисунок 121 – Вызов SAP Fiori Launchpad из командной строки

— через ярлык, расположенный на рабочем столе;
— через панель быстрого доступа в браузере.

Примечания:

1. ПК «SafeERP Security Suite» открывается в браузере по умолчанию, который установлен у пользователя на АРМ.
2. Предполагается, что ПК «SafeERP Security Suite» уже установлен на рабочем месте оператора ПК «SafeERP Security Suite» и соответствующие полномочия ему предоставлены.
3. После активации транзакции /n/gazis/flp/ необходимо повторно авторизоваться в системе.

После регистрации в системе сервера управления ПК «SafeERP Security Suite» развернется стартовая страница (рис. 122).

Информация

О продукте Версии Статистика

Программный комплекс (ПК) «SafeERP Security Suite» предназначен для анализа защищенности и контроля целостности прикладного программного обеспечения многопользовательских автоматизированных систем на базе платформы SAP.

Областью контроля ПК «SafeERP Security Suite» являются:

- программный код ABAP;
- программные объекты;
- пользовательские роли;
- настройки ПО контролируемых систем (ABAP-агентов, Java-агентов, BO-агентов или HANA-агентов).

Функции ПК «SafeERP Security Suite» доступны следующие действия:

- определение небезопасного состояния настроек ПО и средств защиты;
- поиск и выявление изменений контрольных сумм программных объектов;
- фиксация событий по объектам информации ограниченного доступа;
- фиксация событий по объектам авторизаций;
- фиксация событий по созданию новых объектов;
- поиск и выявление небезопасного программного кода, написанного на языке программирования ABAP;
- проверка программного кода на соответствие заданным характеристикам;
- просмотр ландшафта системы;
- просмотр и утверждение RFC-соединений;
- просмотр изменений объектов авторизаций в пользовательских ролях (просмотр истории полномочий, иерархии полномочий, сравнение ролей);

Техническая поддержка: 8-800-700-09-87, support@gaz-is.ru

Скачать документацию

Авторские права (с) ООО «Газинформсервис» 2025. Все права защищены.

Рисунок 122 – Стартовая страница ПК «SafeERP Security Suite»

Примечание. На первоначальной странице доступен просмотр версий агентов (рис. 123) и статистки (рис. 124) в соответствующих вкладках.

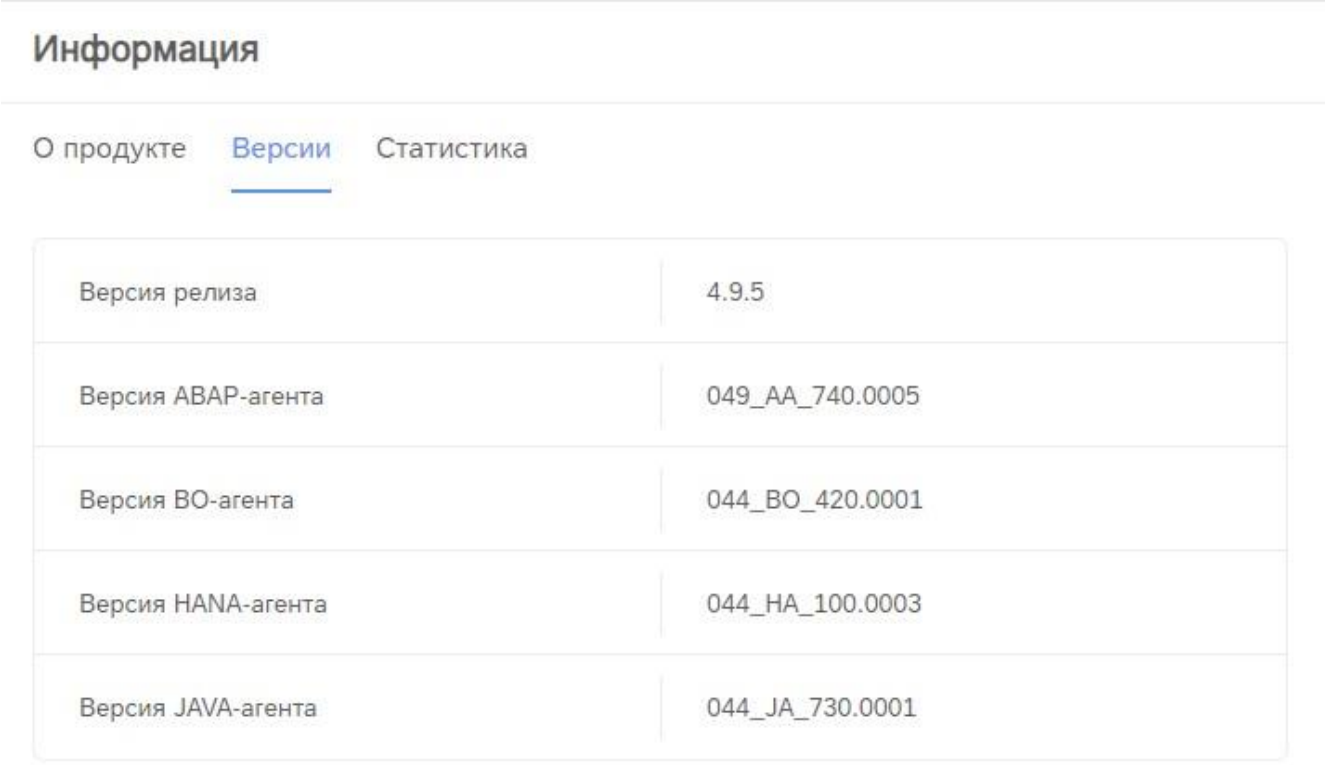


Рисунок 123 – Версия ПК «SafeERP Security Suite» и агентов

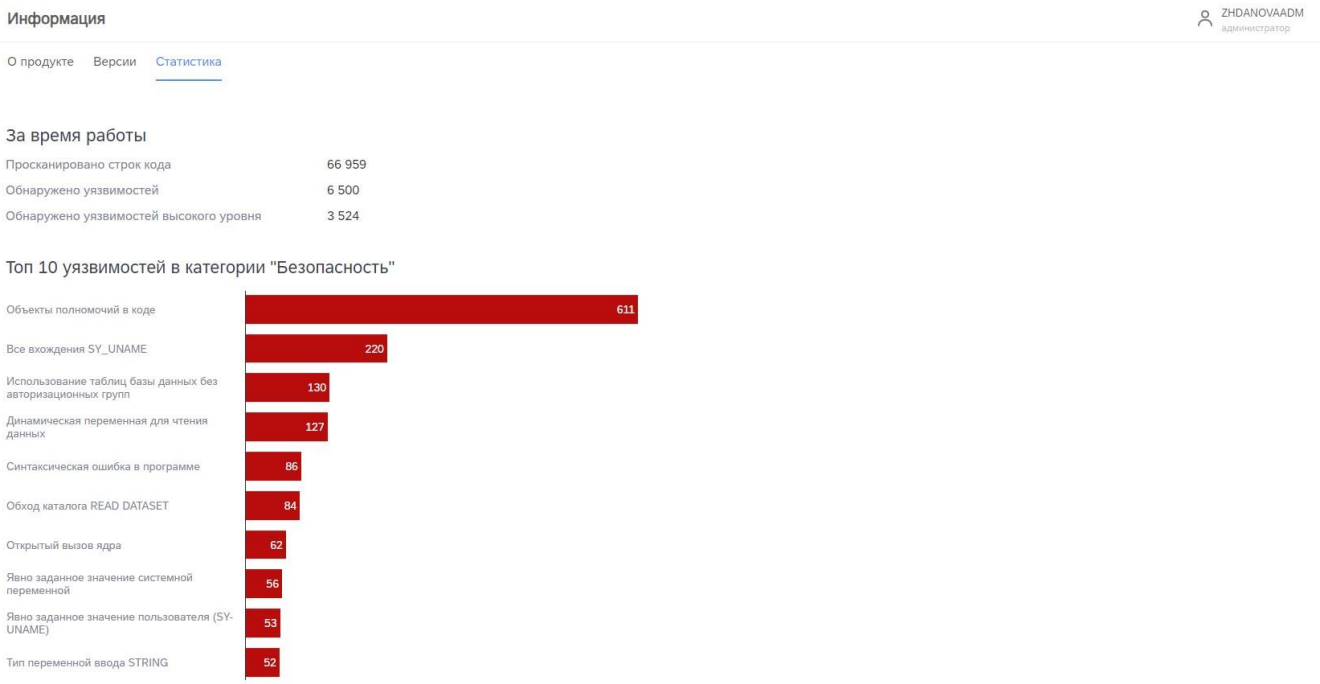


Рисунок 124 – Статистика по найденным уязвимостям

7 Описание веб-интерфейса администратора ПК «SafeERP Security Suite»

7.1. Функциональные модули «SafeERP Security Suite»

После регистрации на сервере управления ПК «SafeERP Security Suite» развернется экран для работы с основной функциональностью ПК «SafeERP Security Suite» – рабочими областями:

- модулем «Панель мониторинга» (рис. 125);
- модулем «Проекты» («Сканер» (SafeERP Platform Security) (рис. 126) и «Анализ кода» (SafeERP Code Security) (рис. 127));
- модулем «Агенты» (рис. 128);
- модулем «Ландшафт» (рис. 129);
- модулем «Контроль RFC» (рис. 130);
- модулем «Профили» (рис. 131);
- модулем «Авторизации» (рис. 132);
- модулем «Контроль качества» (рис. 133);
- модулем «Администрирование» (рис. 134);
- модулем «Аудит»;
- модулем «Уведомления» (рис. 135).

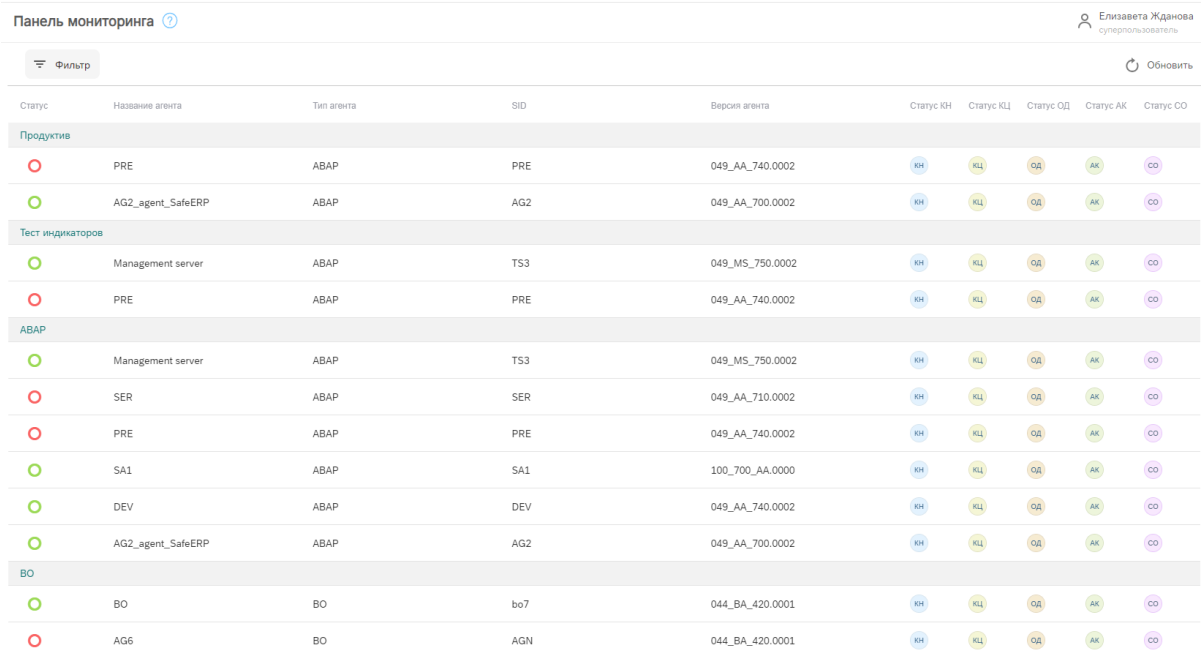


Рисунок 125 – Основная рабочая область модуля «Панель мониторинга»

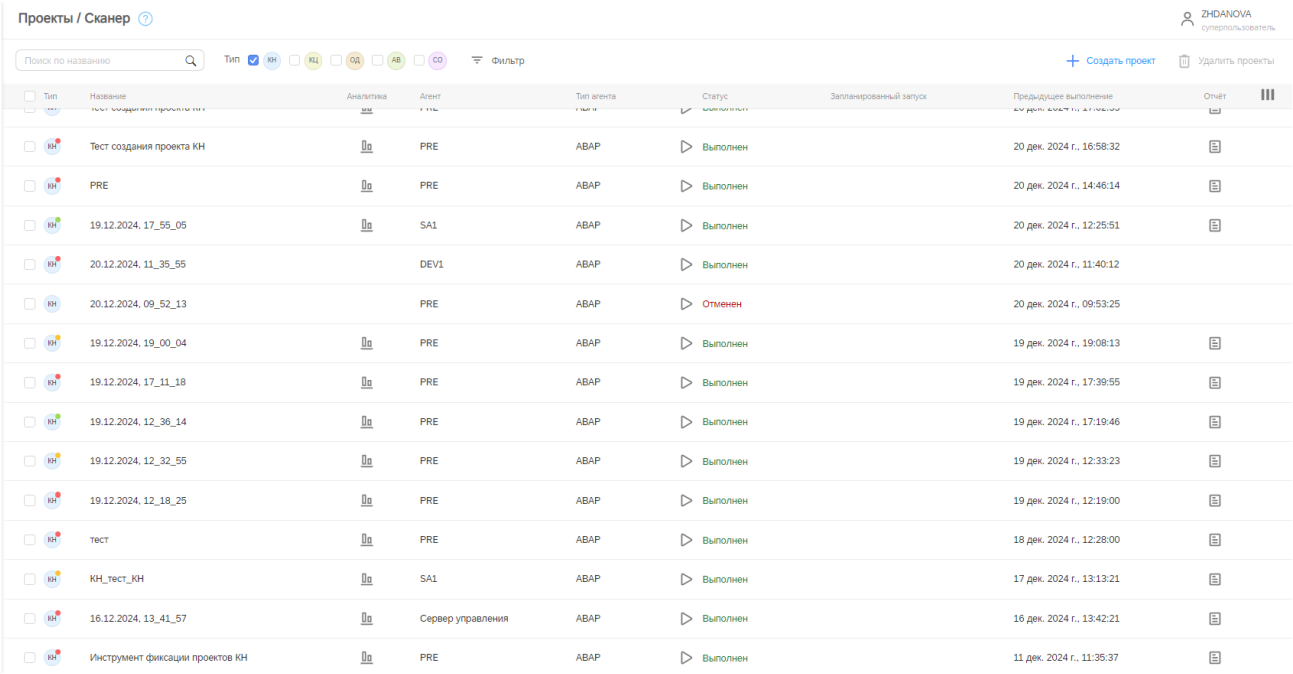


Рисунок 126 – Основная рабочая область модуля «Сканер»

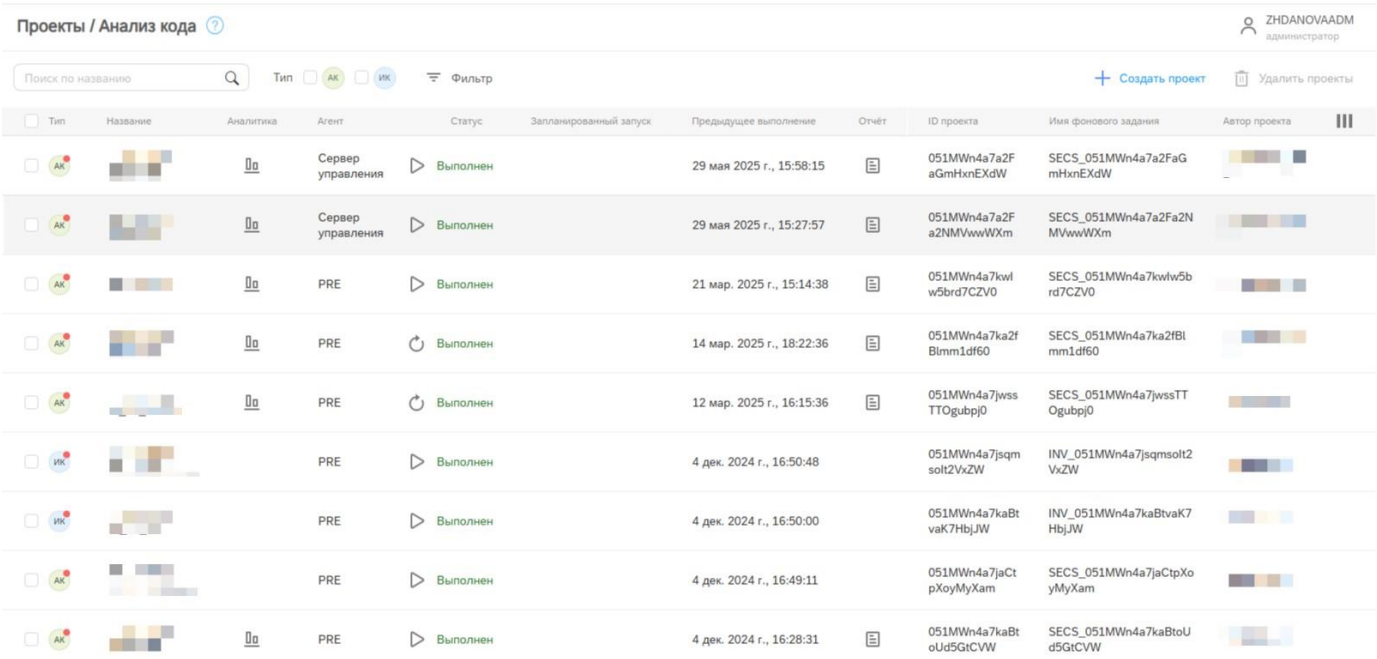


Рисунок 127 – Основная рабочая область модуля «Анализ кода»

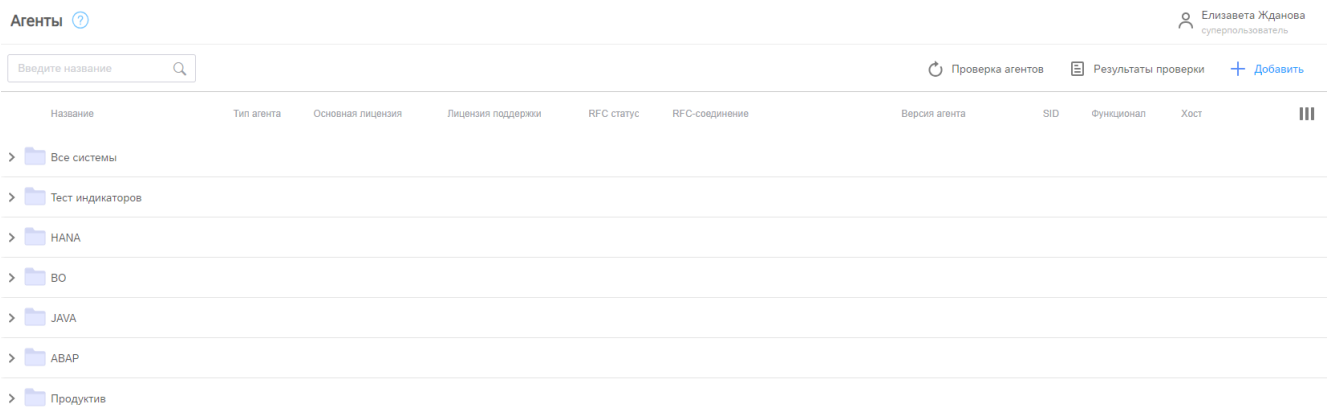


Рисунок 128 – Основная рабочая область модуля «Агенты»

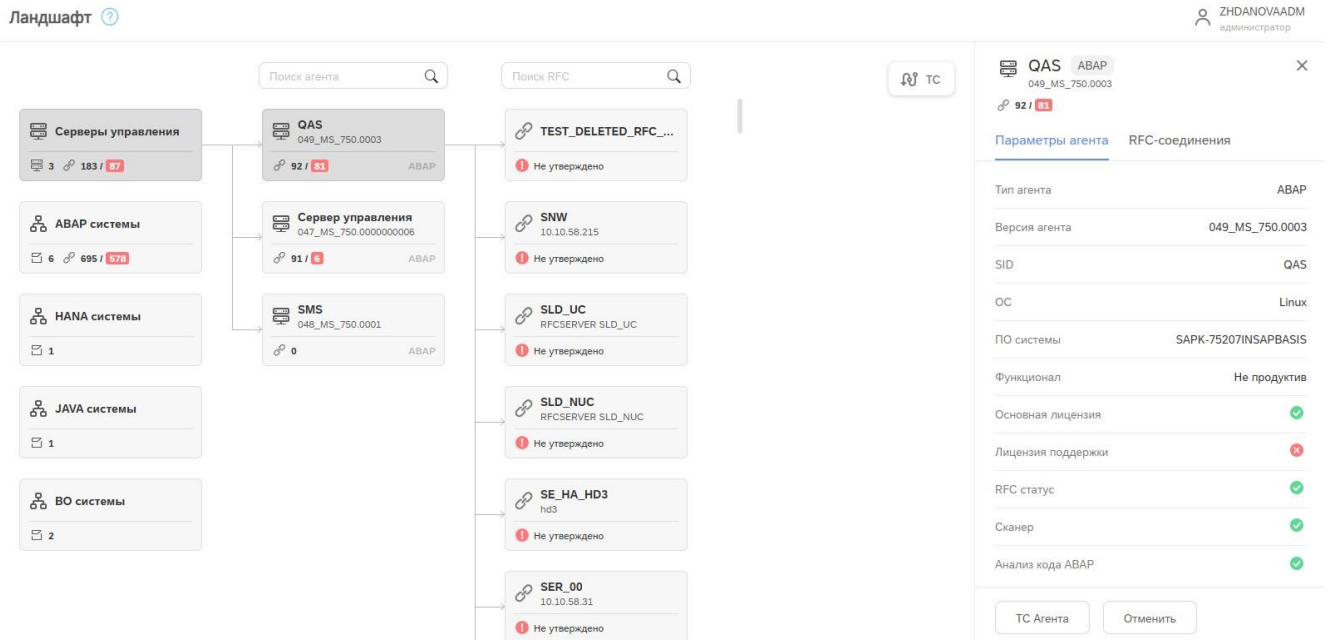


Рисунок 129 – Основная рабочая область модуля «Ландшафт»

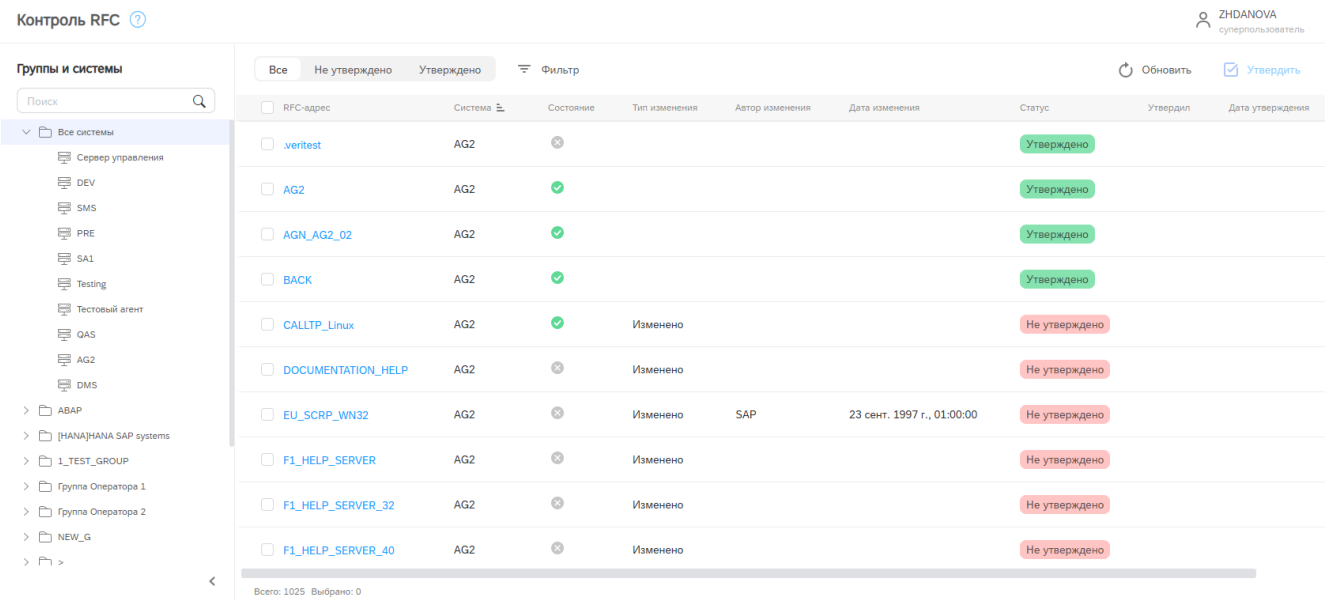


Рисунок 130 – Модуль «Контроль RFC»

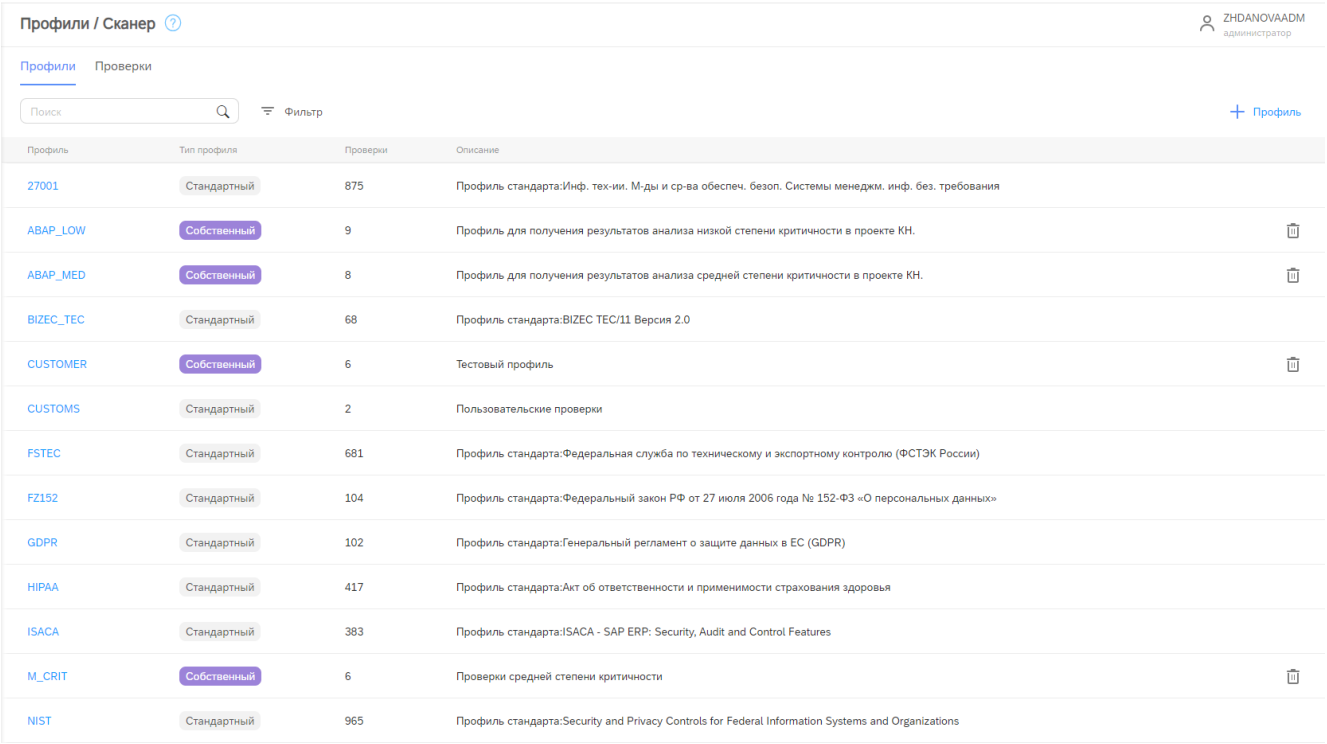


Рисунок 131 – Основная рабочая область модуля «Профили»

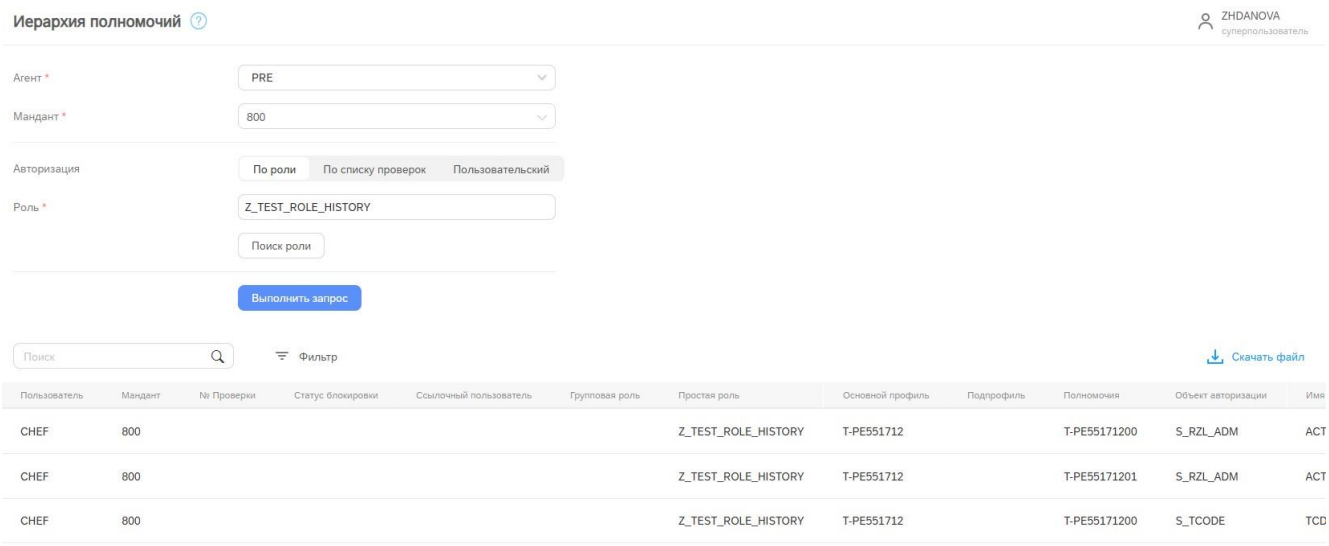


Рисунок 132 – Основная рабочая область модуль «Авторизации»

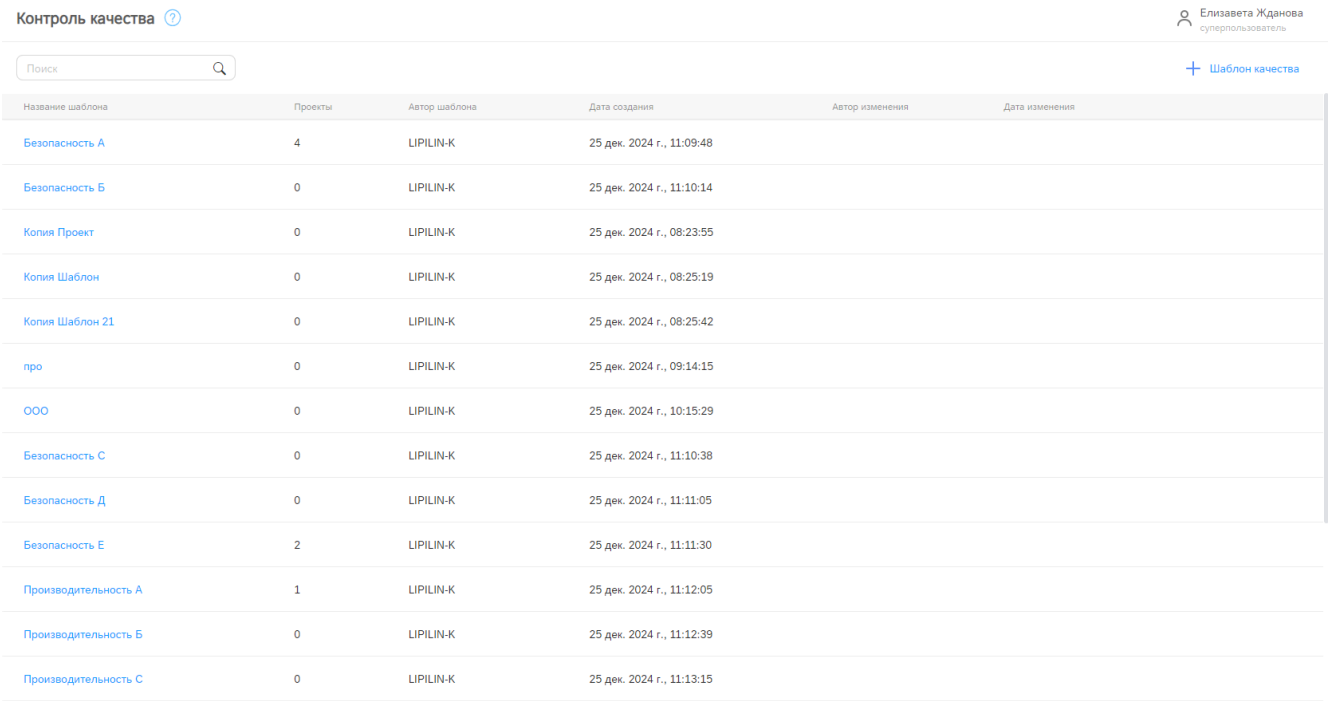


Рисунок 133 – Основная рабочая область модуль «Контроль качества»

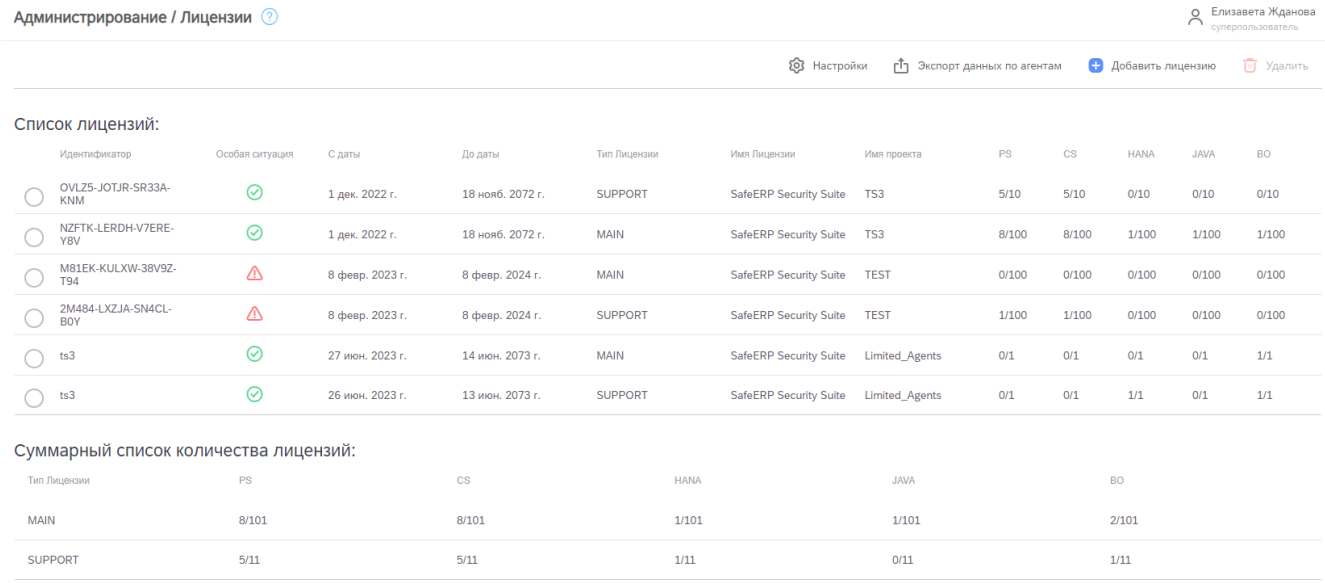


Рисунок 134 – Основная рабочая область модуля «Администрирование»

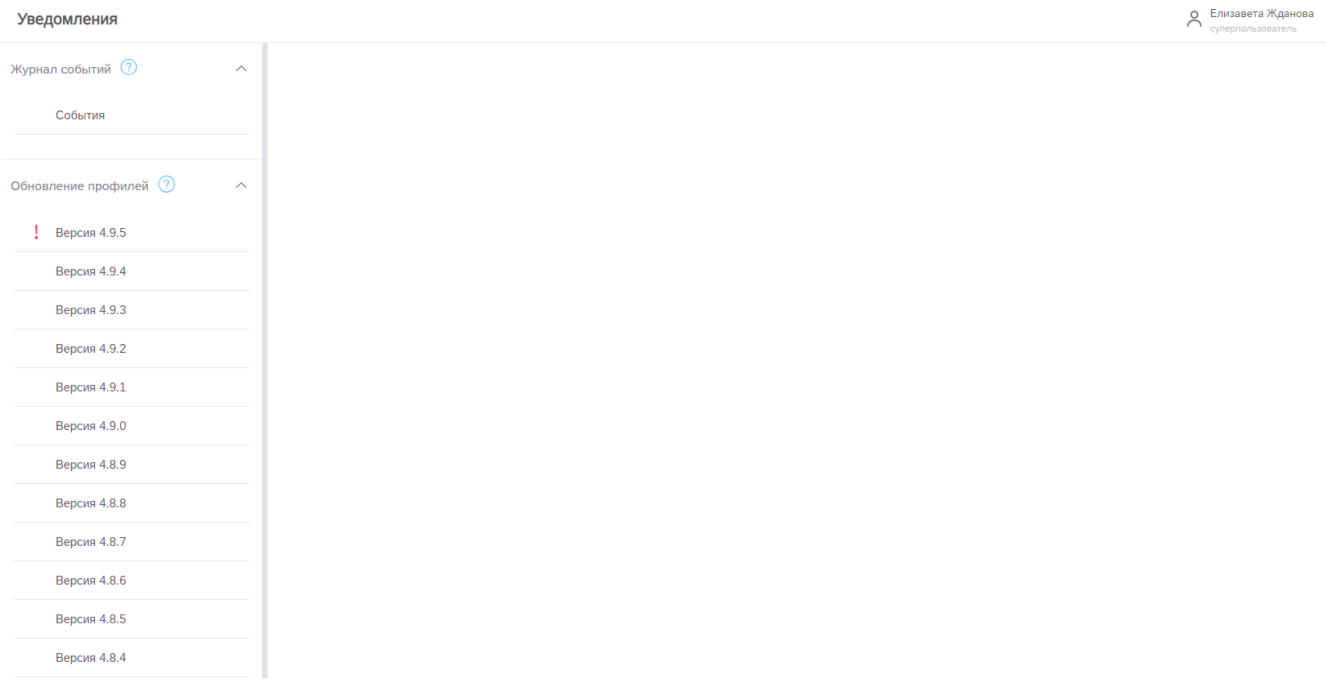


Рисунок 135 – Основная рабочая область модуля «Уведомления»

Примечание. На рисунках 125, 126, 127, 128, 129, 131, 132, 133, 134, 135 приведены примеры основных рабочих областей модулей с информацией об уже созданных проектах[1)] , предназначенных для проведения процедур анализа. При первой настройке функциональности таблицы со списками и статусами проектов будут пустые.

Основные типы проектов для проведения анализа систем:

— контроль настроек (КН) – анализ на наличие небезопасного состояния настроек

[1)] Проект — настраиваемая для проведения процедур анализа систем задача, включающая в себя совокупность объектов анализа, профилей проверок, параметров запуска и результатов анализа (отчетов).

ПО;

— контроль целостности (КЦ) – анализ на наличие изменений контрольных сумм программных объектов;
— объекты доступа (ОД) – анализ на наличие событий доступа к объектам ограниченного доступа;
— авторизации (АВ) – анализ на наличие авторизаций;
— создание объектов (СО) – анализ на наличие истории создания объектов;
— анализ кода (АК) – анализ ABAP-кода на наличие уязвимостей (небезопасных языковых конструкций);
— инвентаризация кода (ИК) – анализ ABAP-кода на подсчет количественных и качественных характеристик.

Столбцы таблицы со списком проектов модулей «Сканер» и «Анализ кода» имеют следующие значения:

1) Тип – иконка с информацией о типе процедуры анализа, осуществляемого данным проектом.
2) Название – наименование проекта.
3) Аналитика – краткий анализ по проекту. Доступна для проектов типа КН и АК.
4) Агент – наименование системы, объекты которой необходимо проанализировать.
5) Кнопки – варианты запуска проекта:

— ▷ – доступна процедура немедленного запуска (перезапуска проекта);
— ↻ – доступна процедура досрочного запуска проекта с запланированным однократным запуском в определённое время (досрочный запуск проекта, выполняемого по расписанию, доступен при изменении типа запуска);
— ↻ – доступна процедура отложенного запуска проекта (однократно в определенное время) или по расписанию (многократно), немедленный запуск невозможен;
— □ – доступна процедура прерывания проекта (при активации пиктограммы будет выведено информационное окно с подтверждением на прерывание процедуры сканирования (рис. 136);

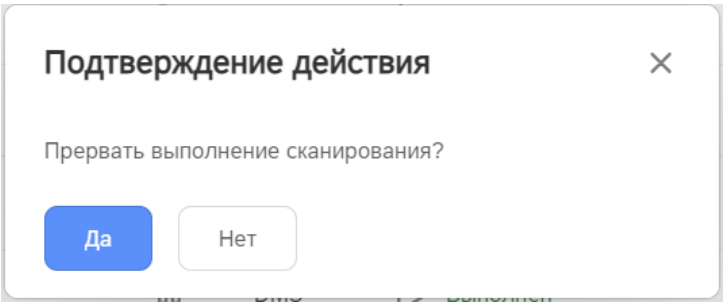


Рисунок 136 – Запрос на прерывание процедуры сканирования

— 11% – режим выполнения проекта (идет анализ).

6) Статус:

— запланирован – запуск проекта по установленному расписанию (наличие уже проведенных итераций анализа или проект был создан и не запускался).

Примечание. Статус Запланирован ● имеют проекты типа КН с прерванным запуском и измененным типом запуска «По расписанию» (однократно);

— выполнен – запуск проекта завершен (анализ выполнен);

— отсутствует – задания на запуск проекта отсутствуют (нет фоновых заданий);

— объекты загружены – объекты для проекта загружены, проект не запускался;

— объекты не загружены – объекты не загружены, проект не запускался;

— отменен – запуск проекта отменен;

— не запущен – объекты для проекта загружены, проект не запускался. Данный статус доступен для проекта типа АК;

— не запущен – проект не запускался (доступен для проектов типа АК).

7) Запланированный запуск – дата и время следующего запуска проекта.

8) Предыдущее выполнение – дата и время последнего запуска проекта.

9) Отчет – кнопка для загрузки документов с результатами анализа.

10) ID проекта – индивидуальный идентификатор проекта.

11) Имя фонового задания – имя фонового задания. Используется в модуле «Анализ кода».

12) Автор проекта – имя пользователя, который создал проект.

Примечание. Для настройки отображения столбцов необходимо активировать кнопку *«Настройка таблицы»*.

Для просмотра содержания проекта необходимо нажать левой кнопкой мыши на строку с названием соответствующего проекта. Справа от таблицы со списком проектов развернется область с его содержанием (рис. 137).

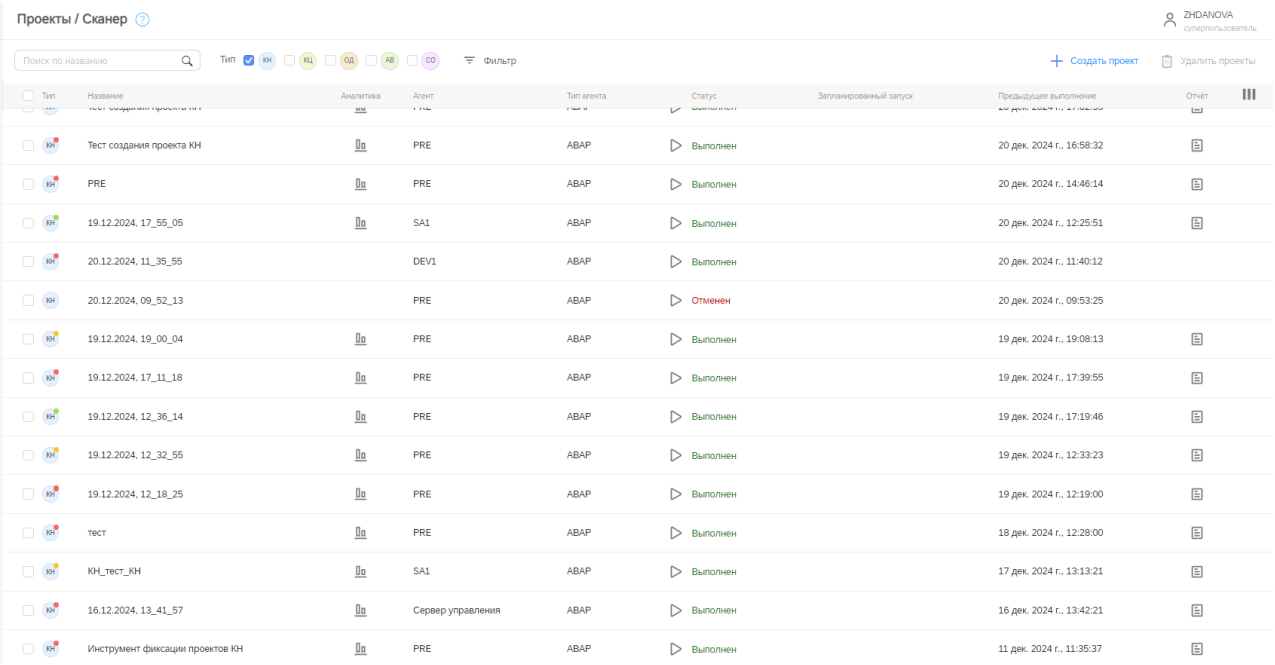


Рисунок 137 – Просмотр содержания проекта типа КН

7.1.1 Модуль «Панель мониторинга»

Веб-интерфейс модуля «Панель мониторинга» предназначен для оперативного мониторинга изменений в статусах (результатах работы) проектов и статусах доступности агентов программного комплекса. Элементы основной рабочей области «Панель мониторинга» представлены на рис. 125.

Столбцы таблицы «Агенты» со списком агентов, поставленных на контроль, имеют следующие значения:

1) Статус – индикатор, информирующий о работоспособности и доступности агента: ○ – ошибки при проверках отсутствуют; ○ – обнаружены ошибки при проверках. (Описание списка проверок, определенных для расчета статуса доступности агента, приведено в подпункте 7.1.1.1).
2) Название агента – наименование системы, объекты которой анализируются.
3) Тип агента – функциональная принадлежность системы (ABAP, Java, BO, HANA).
4) SID – уникальное значение агента, используемое для его идентификации.
5) Версия агента – последняя версия обновления, установленная на агенте.
6) Статус КН – суммарный статус результатов анализа по проектам типа «КН» на агенте (соответствующий индикатор на пиктограмме проекта).
7) Статус КЦ – суммарный статус результатов анализа по проектам типа «КЦ» на агенте (соответствующий индикатор на пиктограмме проекта).
8) Статус ОД – суммарный статус результатов анализа по проектам типа «ОД» на агенте (соответствующий индикатор на пиктограмме проекта).
9) Статус АК – суммарный статус результатов анализа по проектам типа «АК» на агенте (соответствующий индикатор на пиктограмме проекта).
10) Статус СО – суммарный статус результатов анализа по проектам типа «СО» на агенте (соответствующий индикатор на пиктограмме проекта).

Значения статусов (индикаторов) проектов и правила их формирования приведены в подпункте 7.1.1.2.

7.1.1.1 Просмотр данных статуса агента

Список проверок, определенных для расчета статуса агента:

- данные системы;
- проверка данных агентов;
- RFC-соединение;
- пространство на диске;
- статус последнего задания;
- статус последнего задания;
- статус предпоследнего задания;
- статус предпоследнего задания;
- проверка даты/ времени;
- лицензия поддержки;
- общая проверка лицензии у агента;
- наличие дампов в системе;
- статус последнего фонового задания КН;

- статус последнего фонового задания АК;
- статус последнего фонового задания ИОД;
- статус последнего фонового задания КЦ;
- статус последнего фонового задания АВ;
- статус последнего фонового задания СО;
- статус последнего фонового задания логи;
- статус последнего фонового задания ИК;
- статус предпоследнего фонового задания КН;
- статус предпоследнего фонового задания АК;
- статус предпоследнего фонового задания ИОД;
- статус предпоследнего фонового задания КЦ;
- статус предпоследнего фонового задания АВ;
- статус предпоследнего фонового задания СО;
- статус предпоследнего фонового задания логи;
- статус предпоследнего фонового задания ИК;
- дата проверки;
- хост агента;
- SID агента;
- тенант HANA агента.

Для просмотра данных статуса агента необходимо левой кнопкой мыши нажать на соответствующий индикатор. Откроется окно со списком проверок статуса (рис. 138).

Агент: PRE Группа: [CHECK]Like_other_groups RFC соединение: PRE_agent_SafeERP_IDES

Статус	Название проверки	Результат проверки
○	Дата проверки	24.01.2023 13:49:33
○	Лицензия поддержки	SUPPORT лицензия для агента не установлена
○	Наличие дампов в системе	Всего найдено за период с 21.01.2023 по 24.01.2023 11 дампов
○	RFC-соединение	RFC:`PRE_agent_SafeERP_IDES`-Проверка прошла
○	Проверка даты/времени	дата и время синхронизированы
○	Проверка данных системы	048_AA_740.0007 Версия агента валидна
○	Основная лицензия	Срок действия лицензии - лицензия действует.;MAIN лицензия для агента установлена

Рисунок 138 – Просмотр списка проверок статуса агента

Если хотя бы по одной проверке из списка установлено ошибочное значение, общий индикатор системы будет информировать о наличии ошибки (индикатор ○).

7.1.1.2 Значения статусов проектов и правила их формирования

Значения статусов проектов приведены в таблице 4.

Таблица 4 – Значения статусов проектов

Тип проекта	Статус				
	🔴	🟡	🟢	⚪	Пустой
КН	Наличие на агенте корректно отработанных проектов с результатами анализа высокой степени критичности или проектов с неопределенным статусом	Наличие на агенте проектов с результатами анализа средней степени критичности (если нет ни одного проекта с высокой степенью критичности)	Наличие на агенте корректно отработанных проектов с результатами анализа низкой степени критичности (если нет ни одного проекта с высокой или средней степенью критичности)	Наличие на агенте запланированных проектов пока без результатов анализа (после обновления даты ознакомления) для проектов с отложенным запуском	Нет проектов для указанного агента и группы
КЦ	Наличие на агенте корректно отработанных проектов, в которых зарегистрированы события по изменению контрольных сумм объектов, поставленных на контроль	–	Наличие на агенте корректно отработанных проектов, в которых не зарегистрированы события по изменению контрольных сумм объектов, поставленных на контроль	Данный статус к данному типу объекта не применяется	Нет проектов для указанного агента и группы
	Наличие	Наличие на	Наличие на	Данный	Нет

Тип проекта	Статус				
	🔴	🟡	🟢	⚪	Пустой
ОД	проектов с неопределенным статусом	агенте корректно отработанных проектов, в которых зарегистрированы события запуска объектов, поставленных на контроль	агенте корректно отработанных проектов, в которых не зарегистрированы события запуска объектов, поставленных на контроль	статус к данному типу объекта не применяется	проектов для указанного агента и группы
АК	Наличие на агенте корректно отработанных проектов с результатами анализа высокой степени критичности или проектов с неопределенным статусом	Наличие на агенте проектов с результатами анализа средней степени критичности (если нет ни одного проекта с высокой степенью критичности)	Наличие на агенте корректно отработанных проектов с результатами анализа низкой степени критичности (если нет ни одного проекта с высокой или средней степенью критичности)	Данный статус к данному типу объекта не применяется	Нет проектов для указанного агента и группы
СО	Наличие на агенте некорректно отработанных проектов	Наличие на агенте корректно отработанных проектов, в которых зарегистриро-	Наличие на агенте корректно отработанных проектов, в которых не	Данный статус к данному типу объекта не применяется	Нет проектов для указанного агента и группы

Тип проекта	Статус				
	●	●	●	●	Пустой
		ваны события по обнаружению созданных объектов	зарегистри-рованы события по обнаружению созданных объектов		

Примечание. Для обновления статусов всех агентов необходимо нажать кнопку *«Обновить»* (см. рис. 125).

Для просмотра данных по статусам проектов необходимо одним нажатием левой кнопкой мыши активировать соответствующую пиктограмму проекта на выбранном агенте. Развернется окно со списком проектов (рис. 139, 140).

Рисунок 139 – Суммарный статус проектов типа «КН» на агенте PRE

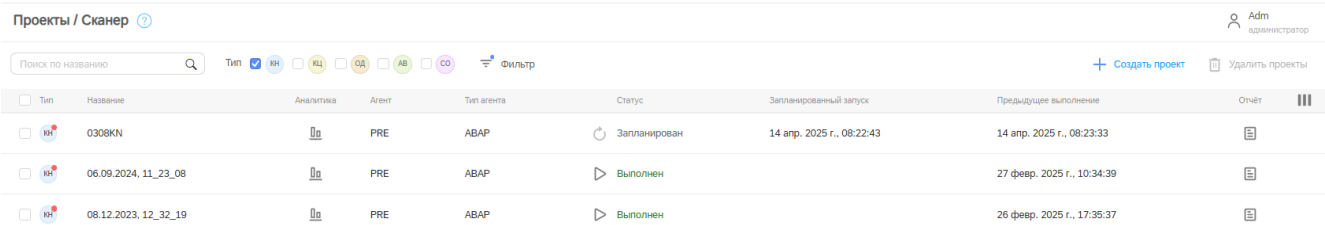


Рисунок 140 – Список всех проектов типа «КН» со статусами на агенте PRE

Общие правила работы в модуле «Панель мониторинга»:

— переход осуществляется к списку проектов только с индикаторами статусов красного, желтого, серого и зеленого цветов (переход не осуществляется к списку проектов с индикаторами статусов серого цвета и пустыми) (рис. 141);

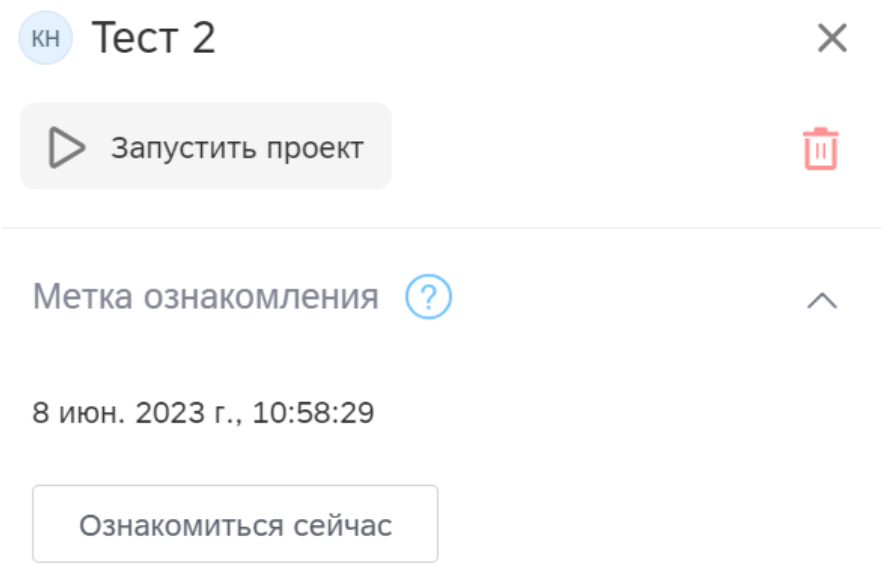


Рисунок 141 – Метка ознакомления для проектов типа «КН»

— для проектов типа «КЦ», «ОД», «АК» и «СО» не предусмотрена метка ознакомления, и статусы проектов в панели мониторинга от действий пользователя не меняются (обновление происходит по истечению установленного периода времени).

7.1.1.3 Фильтрация данных по группам агентов

Фильтрация данных таблицы по группам агентов выполняется с помощи кнопки *«Фильтр»* в основной рабочей области «Панель мониторинга» (см. рис. 125).

Чтобы выбрать группу (группы) нажать кнопку *«Фильтр»*. Для выбора группы в окне «Выбор групп» необходимо установить флаг ☑ в поле соответствующего элемента (рис. 142).

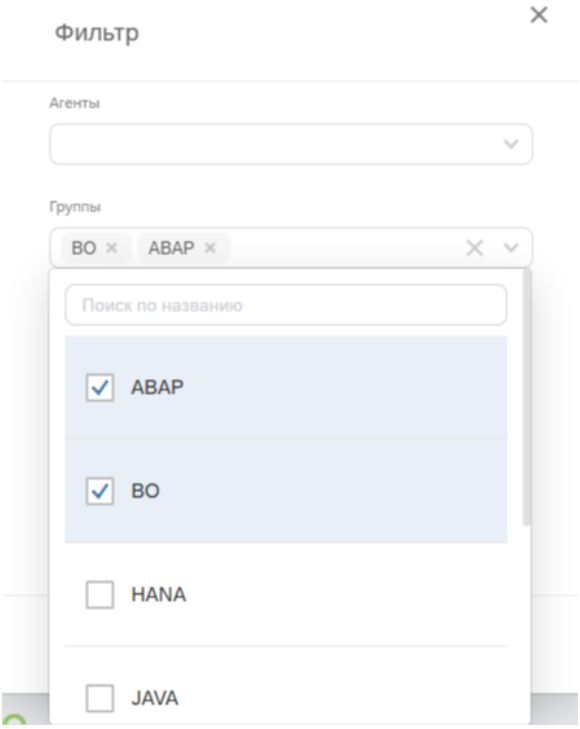


Рисунок 142 – Установка фильтра по группам агента

Чтобы начать поиск группы через форму поиска по названию группы, необходимо ввести название группы в строке поиска и нажать кнопку *«Поиск»*. Для сброса введенных данных предусмотрена кнопка *«Сбросить»* (рис. 143).

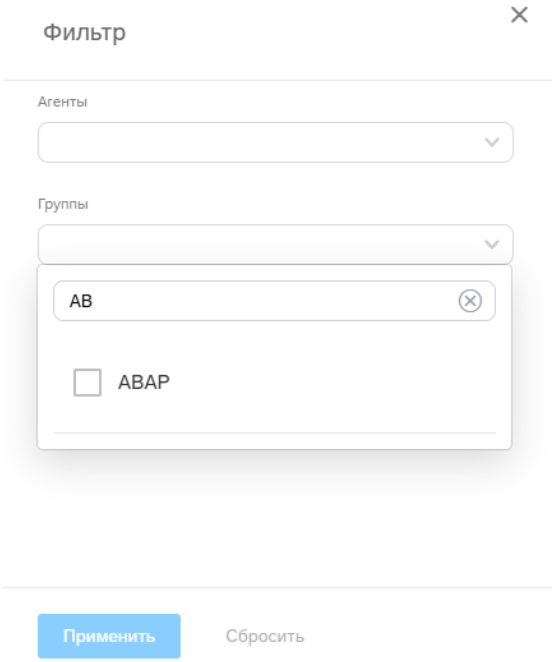


Рисунок 143 – Пример формы поиска группы по его названию

Для завершения установки фильтра по группам в окне «Выбор группы» предусмотрена кнопка *«Выбрать»*. Для сброса выбранных значений предусмотрена кнопка *«Отменить»*.

Отфильтрованный список по группам агентов представлен на рис. 144.

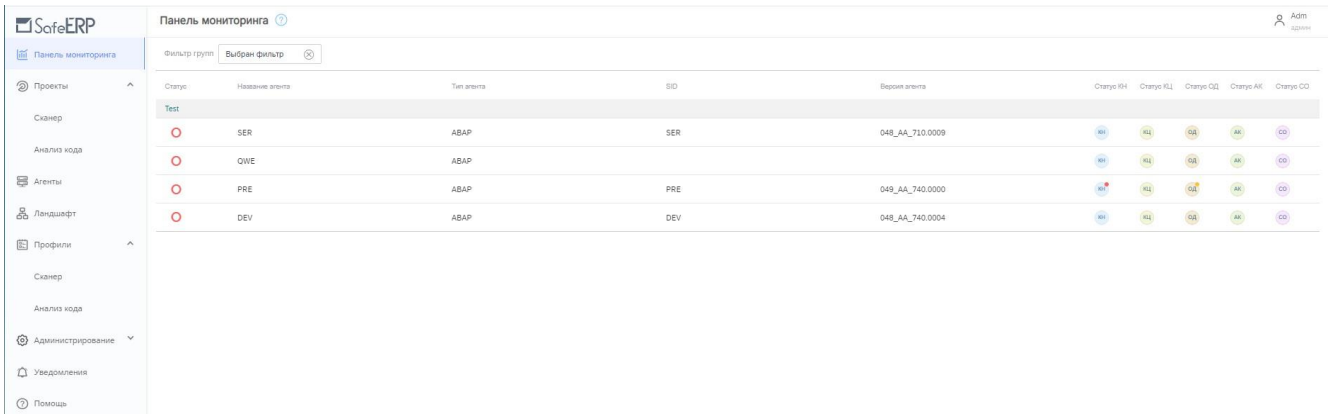


Рисунок 144 – Отфильтрованный список групп агентов

7.1.2 Модуль «Проекты»

7.1.2.1 Модуль «Сканер»

Веб-интерфейс модуля «Сканер» (программный модуль SafeERP Platform Security) предназначен для настройки параметров проектов по проверке настроек ПО на системах-агентах, активации самих операций анализа и получения отчетов. Элементы основной рабочей области модуля «Сканер» представлены на рис. 126.

Основные типы процедур анализа, которые могут быть применены для проверки систем в данном модуле:

- КН – анализ на наличие небезопасного состояния настроек ПО;
- КЦ – анализ на наличие изменений контрольных сумм программных объектов;
- ОД – анализ на наличие событий доступа к объектам ограниченного доступа;
- АВ – анализ авторизаций ролей, профилей и объектов;
- СО – анализ на наличие событий создания новых объектов.

В основной рабочей области «Сканер» доступны следующие действия:

1) Поиск проекта в списке проектов.
2) Добавление проекта.
3) Просмотр/редактирование/запуск/удаление проекта.
4) Просмотр отчетов.

7.1.2.1.1 Поиск проекта

Поиск проекта выполняется через формы поиска в основной рабочей области «Сканер» (см. рис. 126).

Доступные варианты поиска проекта:

- по названию агента (поле «Агент» в окне «Фильтр») (рис. 145);
- по типу процедуры анализа (поля «КН», «КЦ», «ОД», «АВ», «СО»);
- по названию проекта (поле «Название»).

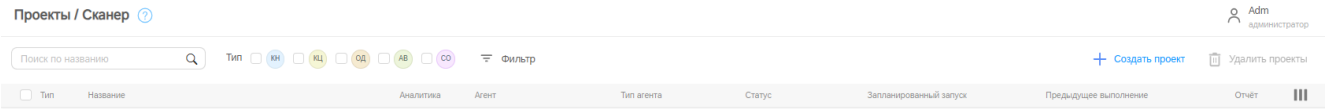


Рисунок 145 – Область поиска проекта

Чтобы начать поиск проекта через форму поиска по названию агента (рис. 146), необходимо нажать кнопку *«Фильтр»*, в открывшемся окне выбрать агента из выпадающего списка или начать вводить название агента в строке поиска.

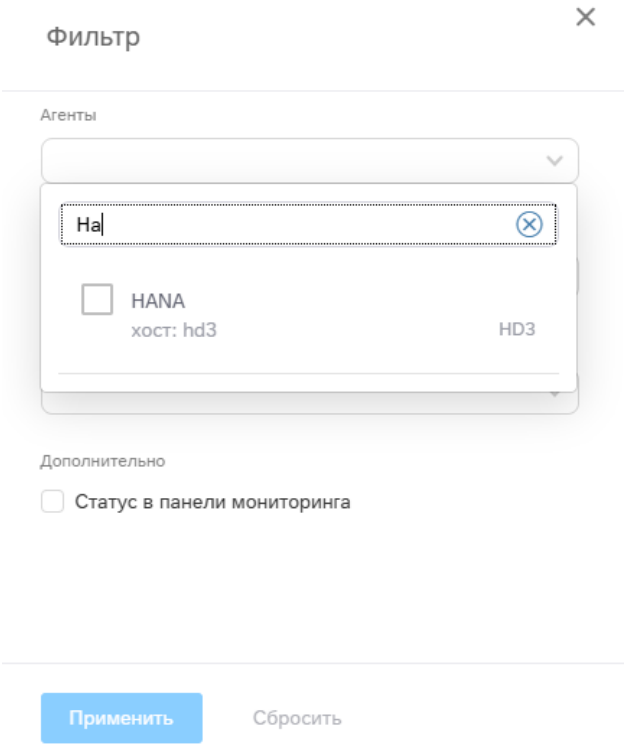


Рисунок 146 – Пример формы поиска проекта по названию агента

Примечание. Через окно «Фильтр» доступен поиск проектов по следующим параметрам:

- агенты;
- группы;
- профили;
- статус в панели мониторинга – поиск проектов статус, которых отображен в модуле «Панель мониторинга».

Чтобы начать поиск проекта через форму поиска по типу проекта (рис. 147), необходимо выбрать тип проекта в соответствующем поле.

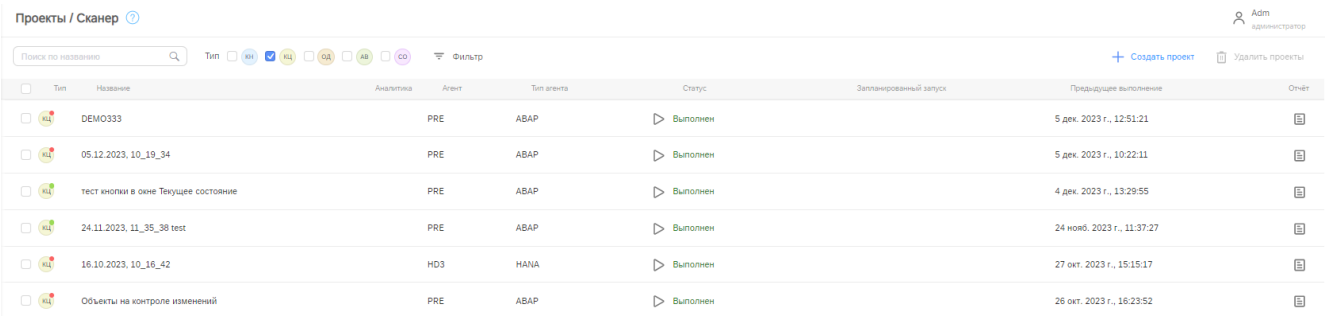


Рисунок 147 – Пример формы поиска проекта по типу процедуры анализа

Чтобы начать процедуру поиска проекта по его названию (рис. 148), необходимо задать символьную маску в соответствующей форме поиска.

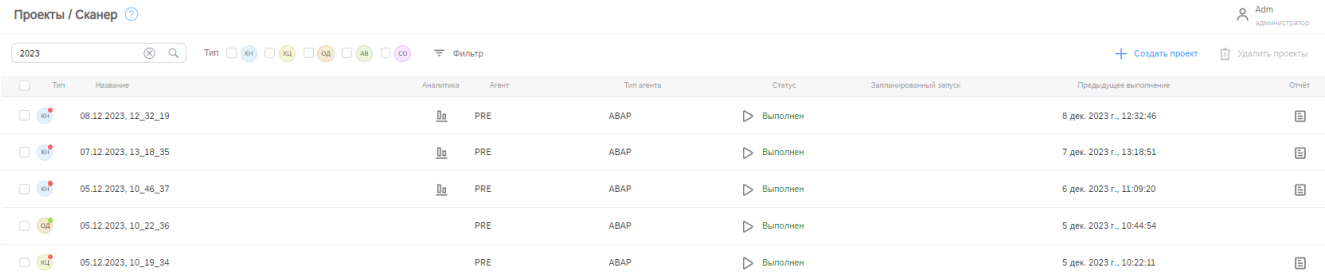


Рисунок 148 – Пример формы поиска проекта по его названию

При вводе маски агента или проекта в соответствующей форме поиска необходимо нажать кнопку *«Поиск».* Для сброса введенных данных предусмотрена кнопка *«Сбросить».*

Для сброса выбранных значений сразу во всех формах поиска предусмотрена кнопка *«Отменить».*

7.1.2.1.2 Создание проекта

Функция создания проекта предоставляется только пользователям с полномочиями на администрирование ПК «SafeERP Security Suite».

Чтобы добавить проект, необходимо нажать кнопку *«+Создать проект»* в основной рабочей области «Сканер» (рис. 126). Появится вкладка «Создать проект» (рис. 149), в котором необходимо определить тип процедуры анализа, осуществляемого данным проектом.

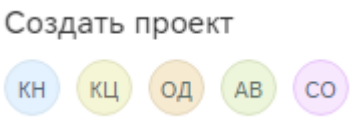


Рисунок 149 – Выбор типа процедуры анализа для проекта

В открывшейся вкладке «Создание проекта» (рис. 150), в зависимости от выбранного типа проекта, необходимо определить параметры проекта.

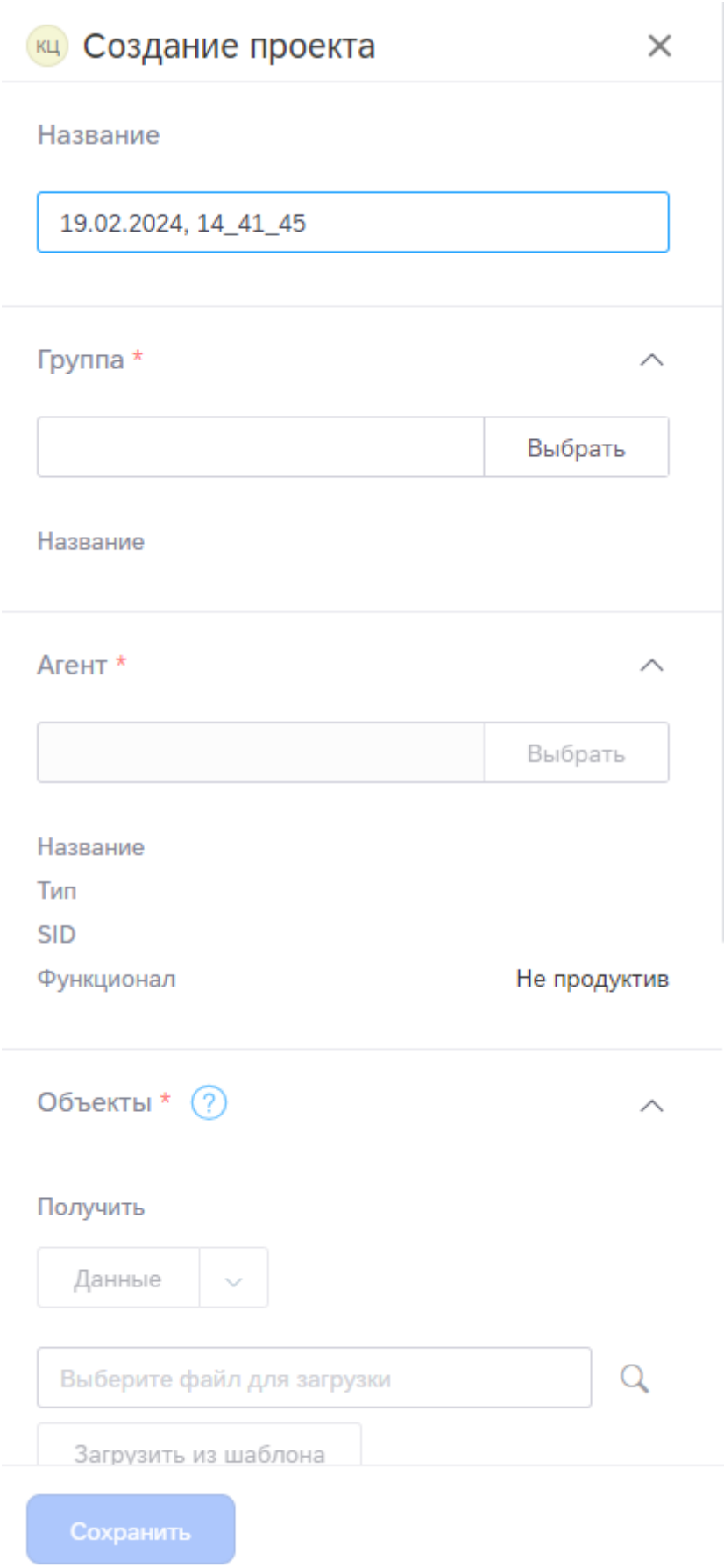


Рисунок 150 – Вкладка «Создание проекта»

После выбора параметров проекта необходимо нажать кнопку сохранения проекта *«Сохранить»*. Кнопка сохранения проекта станет активной только в случае определения всех параметров проекта.

Обязательные для определения параметры проекта приведены в таблице 5.

Таблица 5 – Обязательные для определения параметры проекта

Тип проекта	Название	Группа	Агент	Объекты	Профили	Параметры запуска	Передача данных в SIEM
КН	+	+	+	-	+	+	-
КЦ	+	+	+	+	-	+	Не применяется
ОД	+	+	+	+	-	+	-
АВ	+	+	+	-	-	+	-
СО	+	+	+	+	-	+	Не применяется

Поля «Отчеты» или «История итераций» добавляются в содержимое проекта автоматически после сохранения проекта.

Далее описание параметров проекта будет приведено в той последовательности, в которой происходит их заполнение в окне «Создание проекта» (см. рис. 150), вне зависимости от типа проекта. При работе с определенным типом проекта необходимо ориентироваться на список обязательных для определения параметров проекта и на описание работы с ними, приведенное в подпунктах 7.1.2.1.2.1 – 7.1.2.1.2.7 Выбор

7.1.2.1.2.1 Выбор названия проекта

Поле выбора названия проекта (см. рис. 150) предназначено для определения символьного идентификатора проекта.

При создании проекта доступен ввод его названия (рис. 151).

Рисунок 151 – Пример названия проекта

Процедура переименования проектов не предусмотрена.

7.1.2.1.2.2 Выбор группы агента

Поле выбора группы агента (см. рис. 150) предназначено для назначения агенту идентификатора группы.

До выбора системы-агента необходимо определить для нее группу из разрешенного списка групп для данного агента. Необходимость формирования групп для агентов обусловлена правилами разграничения доступа пользователей к процедурам анализа той или иной системы. Пользователям с полномочиями на одну группу агентов может быть закрыт доступ к другим группам. Данное распределение предварительно устанавливается политикой безопасности компании.

Выбор группы агента необходимо осуществлять из предварительно настроенного списка с помощью нажатия на кнопку *«Выбрать»* (рис. 152). В поле выбора группы агента,

пример которого приведен на рис. 153, доступна функция поиска по названию группы. Для отмены выбора группы необходимо нажать кнопку *«Отменить»*.

Рисунок 152 – Вкладка «Группа»

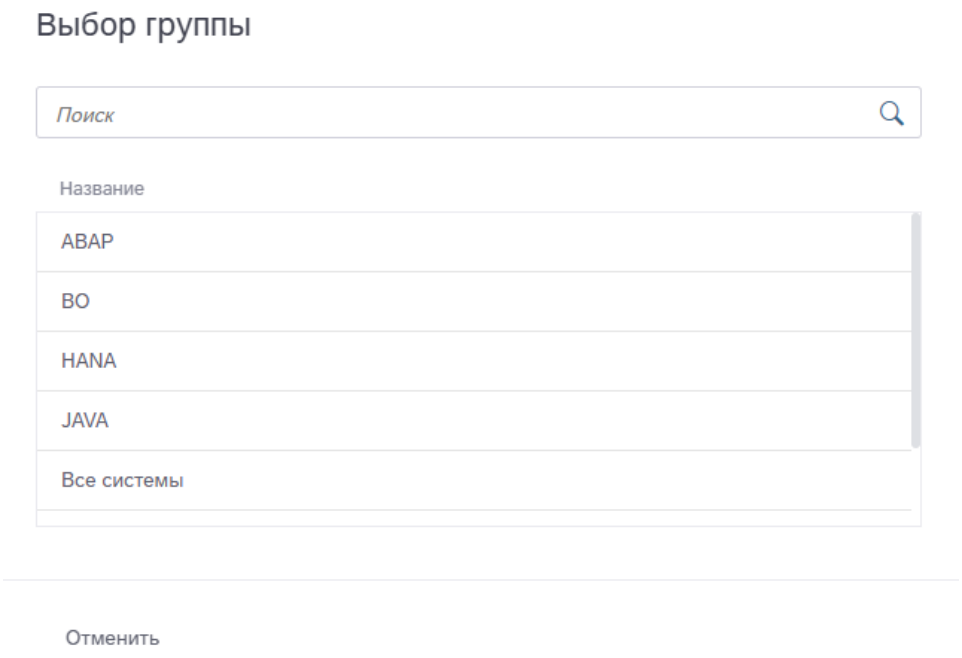


Рисунок 153 – Пример поля выбора группы для агента

7.1.2.1.2.3 Выбор агента

Поле выбора агента (см. рис. 150) предназначено для выбора агента, объекты которого будут анализироваться в создаваемом проекте.

Выбор агента необходимо осуществлять из предварительно настроенного списка с помощью нажатия на кнопку *«Выбрать»*. В поле выбора агента, пример которого приведен на рис. 154 доступна функция поиска по названию агента. Для отмены выбора агента необходимо нажать кнопку *«Отменить».*

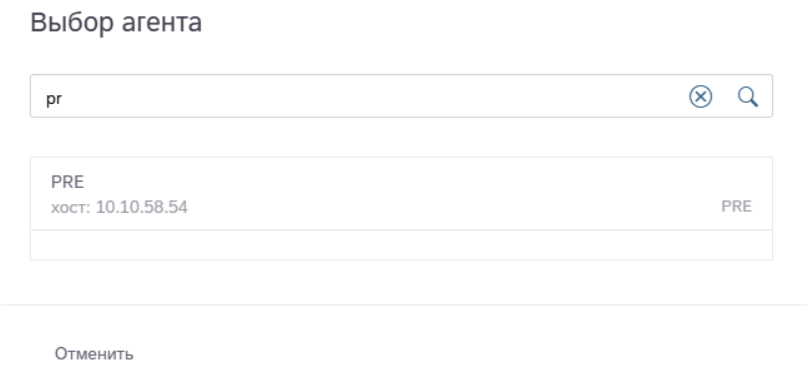


Рисунок 154 – Выбор агента

После выбора агента появится информация о характеристиках агент-системы: название, тип, SID, функционал (рис. 155).

Рисунок 155 – Характеристики агента

Примечание. Для проектов типа КН и КЦ используются агенты следующих типов: ABAP, Java, HANA, BO. Для проектов типа ОД, АВ и СО используются агенты типа ABAP.

7.1.2.1.2.4 Выбор объектов для анализа (проекты КЦ, ОД и СО)

Область выбора объектов (см. рис. 150) предназначено для выбора программных объектов агента, которые будут анализироваться в создаваемом проекте.

В модуле «Сканер» выбор объектов для анализа осуществляется для проектов типа КЦ, ОД и СО.

Для проектов типа КЦ объектами анализа могут быть:

- ABAP-агент: пакеты (DEVC, DEVP), группа функций (FUGR, FUGS), параметры функциональных модулей (FUNC), интерфейс (INTF), логическая база данных (LDBA), пакетный интерфейс (PINF), программа (PROG), программа, выполненная после переноса (XPRA), классы (CLAS);
- Java-агент: файлы, объекты EP, объекты MII;
- BO-агент: объекты инструментов Universe, CrystalRep, WebIntel;
- HANA-агент: объекты репозиторий базы данных.

Для проектов типа ОД объектами анализа могут быть:

- транзакции;
- программы;
- рабочие книги BI-системы;
- Java-приложения, связанные с данной ABAP-системой.

Для проектов типа СО объектами анализа могут быть:

- класс (CLAS);
- пакет (DEVC);
- дистанционный функциональный модуль (FRFC);
- стандартный функциональный модуль (FUNC);
- индекс (INDX);
- веб-сервис (IWPR);
- таблица БД (TABL);
- транзакции (TRAN).

Примечание. В первой итерации проектах типа СО берутся объекты, созданные за последние 30 дней. В последующие итерации берутся события создания объектов, созданные в период от последнего сканирования до текущего (между итерациями). Для корректировки периода необходимо обратиться к пункту 4.2.4 или подпункту 7.1.9.4.

7.1.2.1.2.4.1 Выбор объектов анализа при создании проекта

Процедура выбора объектов анализа доступна только после определения группы для агента и самого агента. Работа с объектами анализа осуществляется в поле «Объекты» (рис. 156).

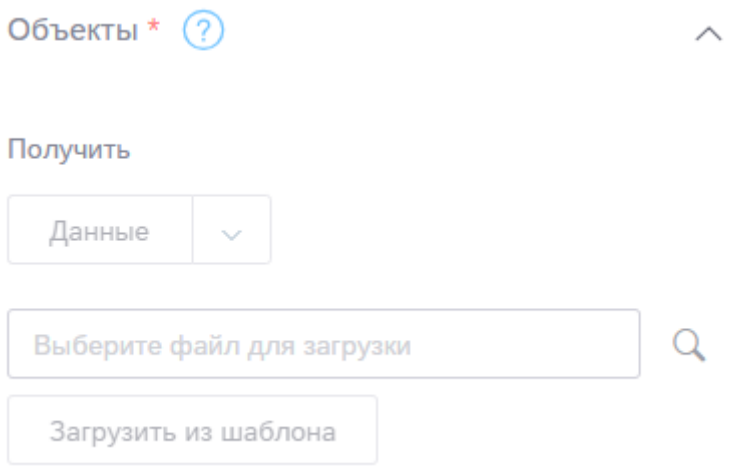


Рисунок 156 – Поле выбора объектов анализа

Для работы с объектами анализа доступны следующие действия:

1) Получить шаблон. Чтобы получить форму для внесения данных по объектам анализа, необходимо активировать соответствующее поле в пункте «Данные» (рис. 157). (Поле «Получить данные» станет активным только после проведения первой итерации проекта).

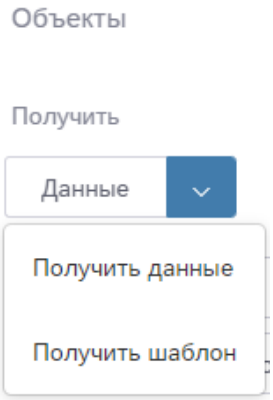


Рисунок 157 – Получение шаблона

2) Загрузить из шаблона. Чтобы выбрать и загрузить объекты анализа с локального компьютера из шаблона, необходимо в поле «Выберите файл для загрузки» нажать кнопку для вызова стандартной формы загрузки файла с локального компьютера. После выбора файла его название появится в поле выбора (рис. 158) и далее нажать на соответствующую кнопку *«Загрузить из шаблона»*.

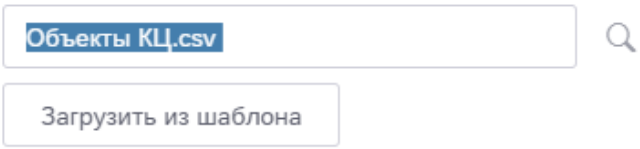


Рисунок 158 – Загрузка объектов анализа из шаблона

Шаблоны для определения списка объектов анализа проектов типа ОД и КЦ приведены на рис. 159, 160 соответственно.

Шаблон для объектов анализа типа проекта ОД содержит следующие столбцы:

- имя КТ(KT_NAME) – имя объекта, который требуется добавить в процедуру анализа.
- критичность(ETYPE) – уровень критичности объекта. Уровни критичности подразделяются на: ERROR, WARNING, INFORMATION.
- уровень конфиденциальности (PRIVACY_LEVEL) – уровень конфиденциальности объекта, который требуется ввести для процедуры анализа. Уровни конфиденциальности подразделяются на: PERSDATA – персональные данные, TRADESECR – коммерческая тайна, INTUSE – информация для служебного пользования, NLAI – информация неограниченного доступа, PERS_TRADE – персональные данные и коммерческая тайна.
- тип ПС(SWT) – тип данных объектов, которые необходимо включить в отчет. Необходимо ввести символ для включения T – для транзакции, W – рабочей книги, E – EP Java, P – программы.

— описание(DESCRIPTION) – подробное описание объекта. Данное поле является необязательным для заполнения.
— техническое имя(TECH_NAME) – имя BiW-объекта. Данное поле является необязательным для заполнения.

Шаблон для объектов анализа типа проекта КЦ содержит следующие столбцы:

— тип объекта (OBJECT) – тип объекта, который требуется добавить в процедуру анализа.
— объект (OBJ_NAME) – имя объекта, который требуется добавить в шаблон.

Имя КТ(KT_NAME)	Критичность(ETYPE)	Уровень конфиденциальности (PRIVACY_LEVEL)	тип ПС(SWT)	Описание(DESCRIPTION)	Техническое имя(TECH_NAME)

Рисунок 159 – Шаблон для объектов анализа проекта типа ОД

Тип Объекта(OBJECT)	Объект(OBJ_NAME)

Рисунок 160 – Шаблон для объектов анализа проекта типа КЦ

7.1.2.1.2.4.2 Контроль качества

Поле «Контроль качества» предназначено для анализа готовности проектов типа КН проекта, а также для соответствия проекта заданными характеристикам.

Для активации контроля качества необходимо поставить флаг напротив «Активировать», выбрать шаблон из списка, нажать кнопку «Сохранить».

Примечания:

1. Для создания шаблона необходимо обратиться к модулю «Контроль качества».
2. Уязвимости со статусом «Закрыто» не учитываются при подсчете метрик в поле «Контроль качества».

Статусы метрик

В поле «Контроль качества» доступны следующие статусы метрик:

— «Пройдена» – рассчитанная метрика соответствует заданной метрике;
— «Не пройдена» – рассчитанная метрика не соответствует заданной метрике;
— невозможно рассчитать метрику.

Примечание. Невозможно рассчитать метрику в следующих случаях:

— для расчета метрики применяются проверки, тип инстанции которых отличается от типа инстанции в проекте КН;
— для расчета метрики применяются проверки, которые не включены в профиль, выбранный в проекте КН.

Статусы контроля качества

В поле «Контроль качества» доступны следующие статусы контроля качества:

— «Пройден» – проект соответствует заданным метрикам;
— «Не пройден» – проект не соответствует заданным метрикам.

Доступные метрики

В поле «Контроль качества» доступны следующие метрики:

— «Требования ФСТЭК России» – при расчете данной метрики применяются уязвимости, у которых есть ссылка на требования ФСТЭК России. У метрики «Требования ФСТЭК России» по умолчанию задано значение 100;
— «Уязвимости в базисных настройках» – при расчете данной метрики применяются уязвимости, которые относятся к группе «Базисные настройки»;
— «Уязвимости в настройках параметров доступа в систему» – при расчете данной метрики применяются уязвимости, которые относятся к группе «Настройки параметров доступа в систему»;
— «Уязвимости в статусе «Открыто» – при расчете данной метрики применяются все уязвимости со статусом «Открыто». Метрика «Уязвимости в статусе «Открыто» задается при добавлении или редактировании шаблона;
— «Рейтинг безопасности» – при расчете данной метрики применяются критичности всех уязвимостей, выявленных в проекте КН, независимо от группы или подгруппы проверок;
— «Уязвимости в полномочиях» – при расчете данной метрики применяются уязвимости, которые относятся ка к подгруппе «Полномочия»;
— «Уязвимости в параметрах профилей инстанции» – при расчете данной метрики применяются уязвимости, которые относятся к подгруппе «Параметры профилей инстанций».

Для метрик «Уязвимости в базисных настройках», «Уязвимости в настройках параметров доступа в систему», «Рейтинг безопасности», «Уязвимости в полномочиях», «Уязвимости в параметрах профилей инстанций» доступны следующие значения:

— A – уязвимости не найдены;
— B, C, D – принадлежит полуинтервалу найдены уязвимости со степенями критичности «Низкая», «Средняя», или «Высокая».

Условия прохождения метрик

Метрика «Требования ФСТЭК России» считается пройденной, если критичность всех уязвимостей равна «Информация» или «Корректно».

Метрика «Уязвимости в базисных настройках» считается пройденной, когда результат метрики равен A.

Метрика «Уязвимости в настройках параметров доступа в систему» считается пройденной, когда результат метрики равен A.

Метрика «Уязвимости в статусе «Открыто» считается пройденной, если количество уязвимостей в статусе «Открыто» меньше или равно значению в поле «Условие» из шаблона контроля качества.

Метрика «Рейтинг безопасности» считается пройденной, когда результат метрики равен A.

Метрика «Уязвимости в полномочиях» считается пройденной, когда результат метрики

равен А.

Метрика «Уязвимости в параметрах профилей инстанций» считается пройденной, когда результат метрики равен А.

7.1.2.1.2.4.3 Просмотр/изменение объектов анализа в уже созданных проектах

Для доступа к объектам анализа в уже созданных проектах необходимо выбрать проект из списка проектов (рис. 126) и одним нажатием левой кнопки мыши на строке с названием проекта активировать окно с содержанием проекта (см. рис. 150). Работа с объектами анализа осуществляется в области «Объекты» (рис. 161).

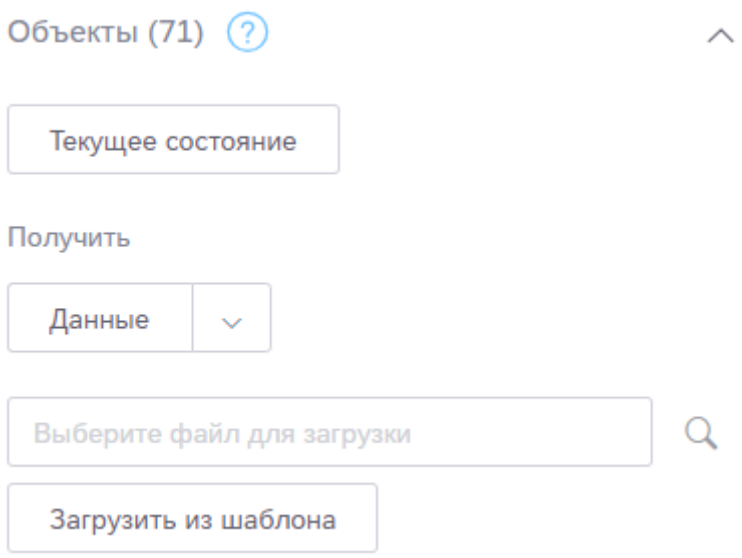


Рисунок 161 – Область для работы с объектами анализа

Для работы с объектами анализа доступны следующие действия:

1) Текущее состояние. Чтобы получить подробную информацию о проверке объектов анализа, необходимо активировать поле «Текущее состояние», описание работы с которым приведено в подпункте 7.1.2.1.2.4.4
2) Получить данные. Чтобы получить установленный для проекта список объектов анализа в формате *.csv, необходимо активировать соответствующее поле в пункте «Данные» (см. рис. 157).
3) Получить шаблон. Чтобы получить форму для внесения данных по объектам анализа, необходимо активировать соответствующее поле в пункте «Данные» (см. рис. 157).
4) Загрузить из шаблона. Для выбора и загрузки шаблона с объектами анализа с локального компьютера (изменение списка объектов анализа) необходимо нажать на соответствующую кнопку *«Загрузить из шаблона»* (см. рис. 161).

7.1.2.1.2.4.4 Текущее состояние объектов анализа в созданных проектах

Просмотр текущего состояния объектов доступен для проектов следующего типа:

- КН;
- КЦ;
- ОД;
- СО.

7.1.2.1.2.4.4.1 Текущее состояние объектов анализа в созданных проектах типа КН

Окно «Текущее состояние» доступно после первого запуска сканирования проекта.

В окно «Текущее состояние» входят следующие области (рис. 162):

- информационная – содержит информацию о системе, профиле, количестве и критичности уязвимостей, дате и времени сканирования;
- меню – содержит поисковую строку, кнопки «Фильтр» «Управление уязвимостями»;
- таблица уязвимостей.

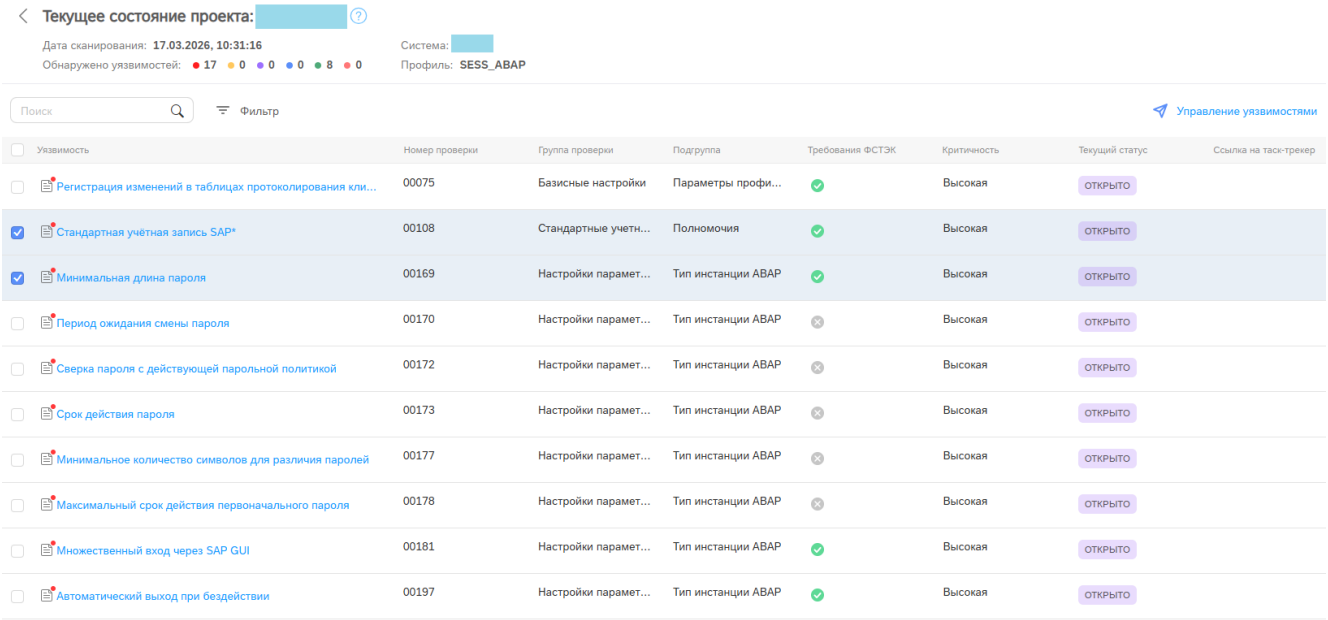


Рисунок 162 – Окно «Текущее состояние» (для проектов типа КН)

Примечание. В окне «Текущее состояние» доступен фильтр по следующим параметрам:

- критичность
- статус уязвимости;
- наличие ссылки на таск-трекер;
- требования ФСТЭК России;
- ID задачи;
- группы проверок;
- подгруппы проверок;
- ключевые параметры проверки.

Найденные уязвимости могут приминать следующие статусы (рис. 162):

- красный цвет – высокая критичность;
- оранжевый цвет – средняя критичность;
- фиолетовый цвет – низкая критичность;
- синий цвет – информация;

— зеленый цвет – корректно;
— коралловый цвет – не определено.

Примечание. Статус «Не определено» присваивается тем уязвимостям, которые не соответствуют заданным параметрам критичности. Для просмотра параметров критичности необходимо обратиться к вкладке «Критичность» при подробном просмотре найденной уязвимости.

Функциональность «Управление уязвимостями»

В ПК «SafeERP Security Suite» реализована функциональность по управлению уязвимостями.

Вызов функциональности управления уязвимостями осуществляется следующими способами:

— через окно «Текущее состояние»;
— через окно просмотра найденной уязвимости в текущей итерации проекта.

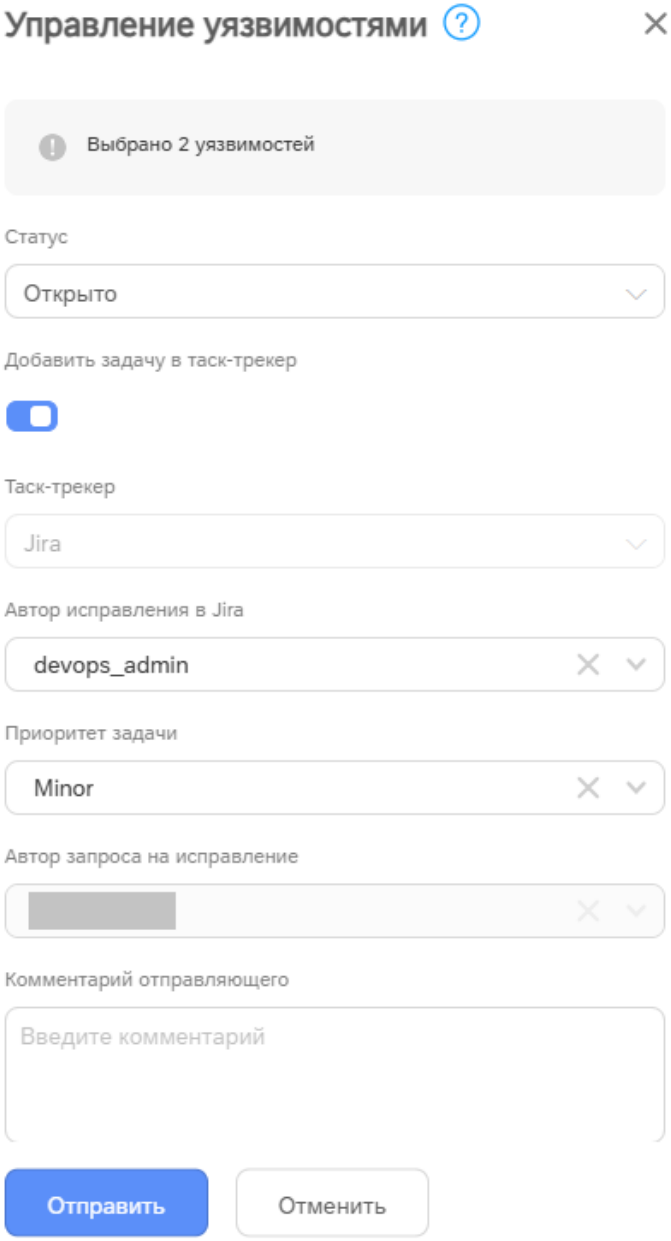


Рисунок 163 – Окно «Управление уязвимостями» (для проекта типа КН)

В окно «Управление уязвимостями» доступно следующее (рис. 163):

- поле «Статус» – статус обнаруженной уязвимости. Данное поле является необходимым.
- переключатель «Добавить задачу в таск-трекер» – после активации переключателя автоматически создается в таск-трекере;
- поле «Таск-трекер» – тип таск-трекера. Доступна система отслеживания задач «Jira»;
- поле «Автор исправления в Jira» – список пользователей, подключенного таск-трекера;
- поле «Приоритет задачи» – приоритет задачи в системе отслеживания задач

«Jira»;

- поле «Автор запроса на исправления» – автор запроса на исправление заполняется автоматически текущим пользователем, который изменяет статус уязвимости. Если автор запроса уже заполнен, то при изменении статуса он поменяется на текущего пользователя. Данное поле является обязательным;
- поле «Комментарий исправляющего» – комментарий от пользователя, отправляющего запрос на исправление. При необходимости, заполнить дополнительную информацию про данную уязвимость для исправляющего. Заполняет автор запроса;
- поле «Система исправления» – система, на которой необходимо устранить выбранную уязвимость;
- поле «До какой даты исправить» – дата, до которой необходимо исправить текущую уязвимость.

Во окне «Управление уязвимостями» (см. рис. 163) доступны следующие статусы для уязвимостей:

- «Открыто» – уязвимость найдена после сканирования;
- «В работе» – находится в процессе исправления у назначенного лица;
- «На проверке» – ожидает проверки инициатором или согласующим;
- «Закрыто» – уязвимость исправлена.

Для изменения статусов найденных уязвимостей необходимо выполнить следующие действия:

1) Выбрать уязвимости. Нажать кнопку «Управление уязвимостями».
2) Заполнить поля в окне «Управление уязвимостями», нажать кнопку *«Отправить».*

Примечание. При редактировании полей в окне «Управление уязвимостями» сохраняются изменения в тех полях, в которые были внесены изменения. Поля без изменений не меняются. Количество измененных уязвимостей выводится в информационное сообщение.

Для настройки почтовых уведомлений по проекту типа КН необходимо обратиться к транзакции /N/GAZIS/MAIL.

Почтовые уведомления приходят в следующих случаях:

- автору исправления, когда уязвимость имеет статус «В работе»;
- автору запроса, когда уязвимость имеет статус «Исправлено»;
- автору запроса, когда уязвимость имеет статус «Безопасно».

Примечание. Настройка по отключениям почтовых уведомлений для инструмента фиксации результатов производиться в транзакции /n/gazis/sega (во вкладке «Platform Security») или в модуле «Администрирование» (в разделе «Сканер»).

Во окне «Текущее состояние» доступен просмотр информации об уязвимости.

Для просмотра истории необходимо нажать на наименование уязвимости.

Окно просмотра уязвимости содержит следующее:

- поле «Информация» – содержит информацию о номере проверки, текущем статусе, ссылке на таск-трекер.

Примечание. Ссылка на таск-трекер формируется после активации переключателя «Добавить задачу в таск-трекер» в окне «Управление уязвимостями»;

— вкладка «Информация об уязвимости» – содержит дочерние вкладки «Описание», «Результат», «Ссылки», «Схема», «Возможные последствия», «Рекомендации», «Критичность» (рис. 164);

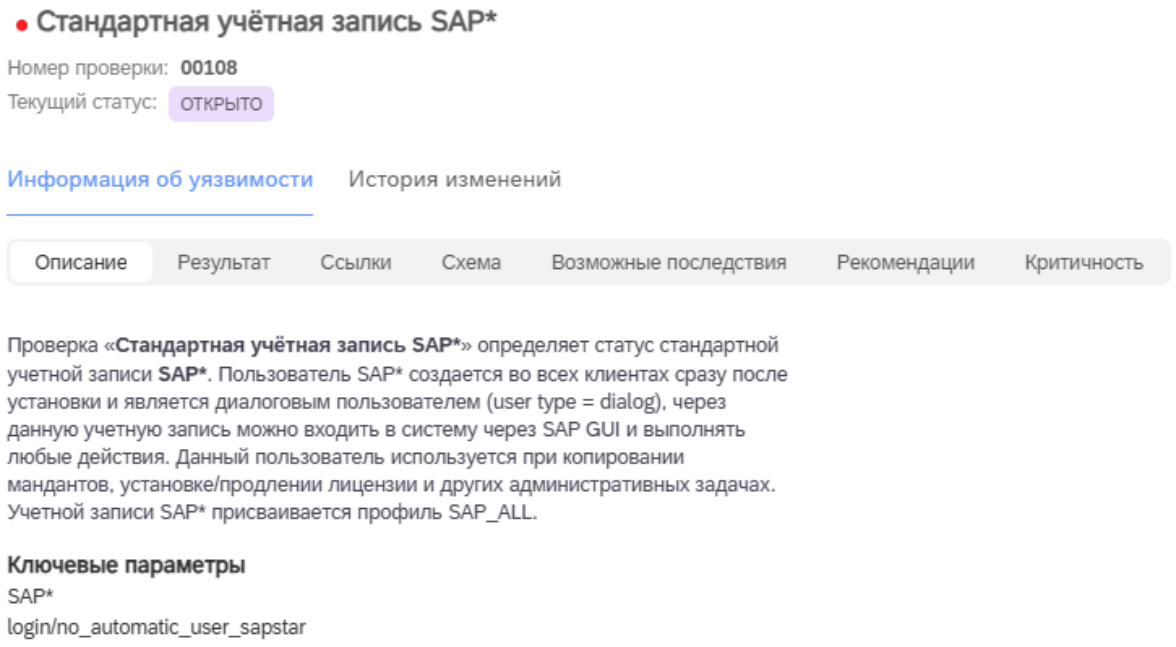


Рисунок 164 – Вкладка «Информация об уязвимости»

— вкладка «История изменений» – содержит историю изменений уязвимости. Доступно добавление комментария. Для добавления комментария необходимо нажать кнопку *«Добавить комментарий»*, внести информацию в окне «Добавить комментарий», нажать кнопку *«Отправить»*.

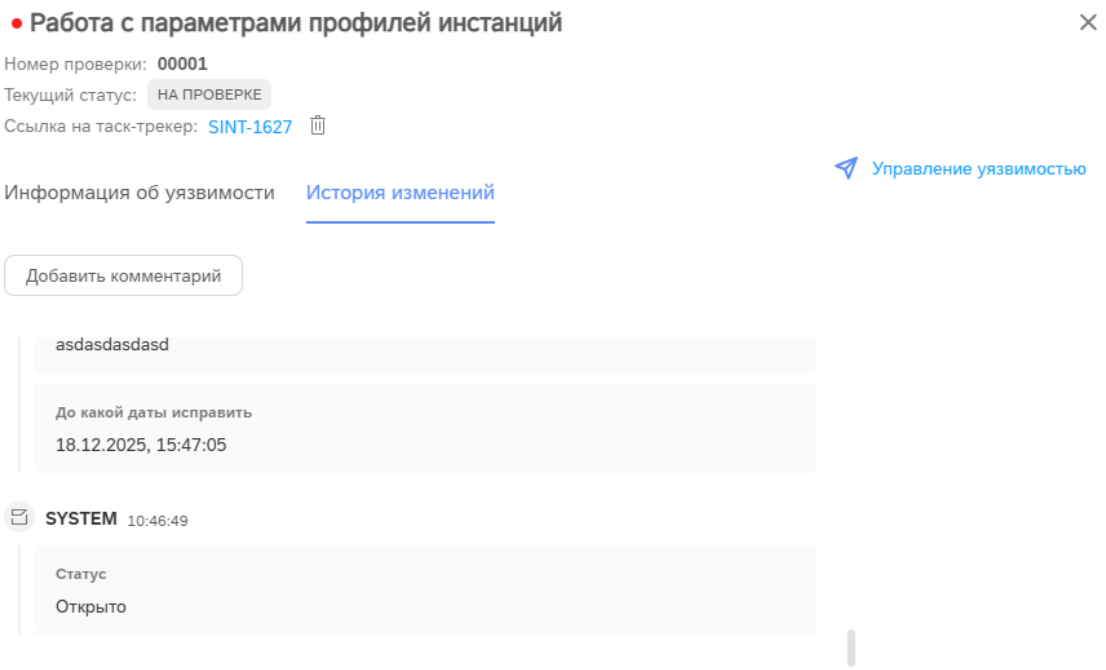


Рисунок 165 – Вкладка «История изменений»

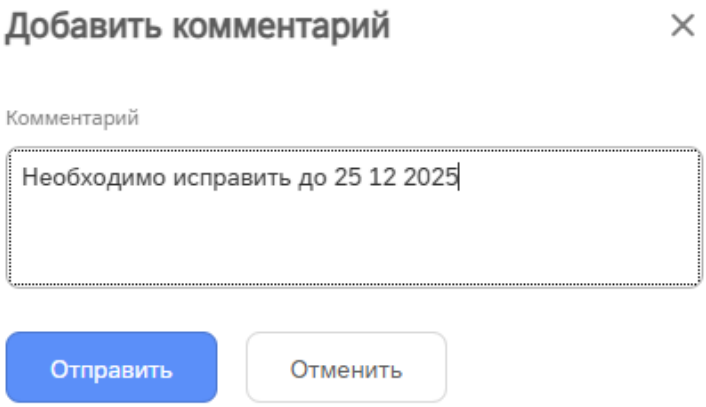


Рисунок 166 – Окно «Добавить комментарий»

Почтовые уведомления

Администратору ПК «SafeERP Security Suite» поступают почтовые уведомления по проектам типа КН в случаях, которые указаны в таблице 6.

Таблица 6 – События для проектов типа КН

Источник изменений	Событие	Отправитель	Получатель
Сервер управления(FIORI)	Добавлен комментарий	Тех.пользователь	Автор исправления
	Изменены данные	Тех.пользователь	Автор исправления

Агент (транзакция /n/gazis/seps_vulners)	Добавлен комментарий	Тех.пользователь	Автор запроса
	Изменен статус (->На рассмотрение)	Тех.пользователь	Автор запроса

Примечания:

1. Предварительно должна быть отключена настройка в разделе «Сканер». Для настройки необходимо обратиться к модулю «Администрирование» или к транзакции /N/GAZIS/SEGA.
2. Адрес электронной почты пользователя находится в разделе «Коммуникация». Для просмотра раздела «Коммуникация» необходимо обратиться к транзакции SU01.
3. Необходимо настроить интеграцию с почтовым сервером компании.

7.1.2.1.2.4.4.2 Текущее состояние объектов анализа в созданных проектах типа КЦ

При нажатии кнопки *«Текущее состояние»* в поле выбора объектов в созданных проектах типа КЦ откроется окно, содержащее две области: «Статусы объектов в списке» и «Статусы объектов на агенте».

Пример окна «Текущее состояние объектов» для проектов типа КЦ представлен на рис. 167.

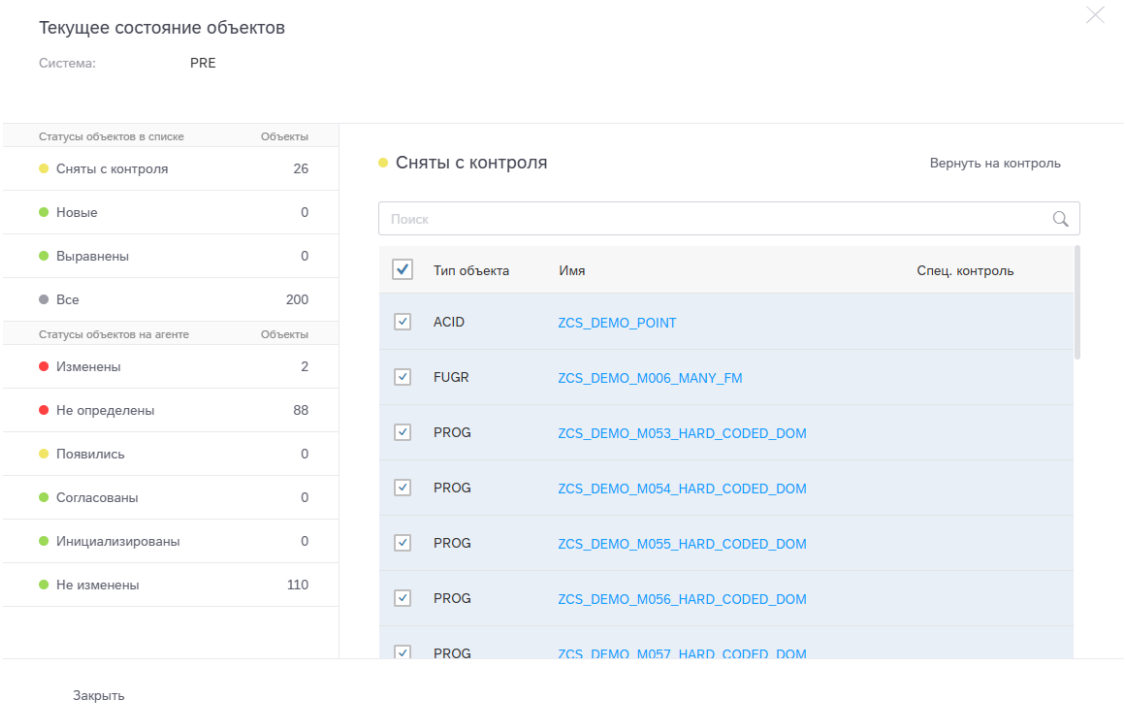


Рисунок 167 – Пример окна текущего состояния объектов анализа проекта типа КЦ

Область «Статусы объектов в списке» содержит отображение текущего состояния списка объектов на сервере управления (система, с которой производится контроль):

- «Сняты с контроля» – состояние объектов не отслеживается проектом;
- «Новые» – объекты, впервые поставленные на контроль;
- «Выравнены» – объекты, выравненные оператором;
- «Все» – все объекты в загруженном на контроль целостности списке.

Для просмотра списка объектов необходимо одним нажатием левой кнопки мыши активировать соответствующий статус в списке (рис. 168).

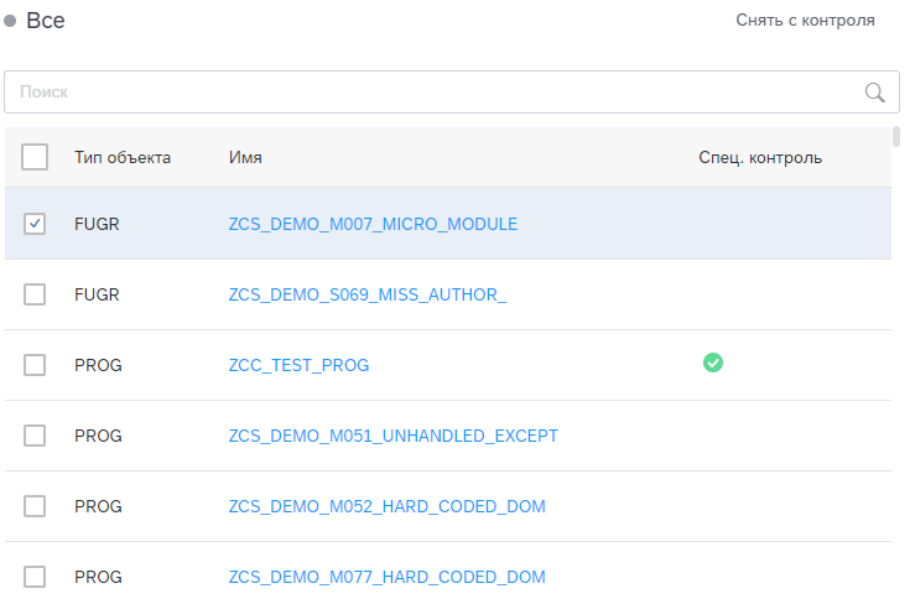


Рисунок 168 – Просмотр списка объектов КЦ

Область «Статусы объектов на агенте» содержит отображение состояний объектов после последнего запуска проекта:

- «Изменены» – объекты с зафиксированным изменением контрольной суммы;
- «Не определены» – объекты не определены;
- «Появились» – объекты, поставленные ранее на контроль и появившиеся на агенте;
- «Согласованы» – объекты согласованы;
- «Инициализированы» – объекты, впервые поставленные на контроль, контрольные суммы для которых успешно рассчитаны;
- «Не изменены» – объекты без изменения контрольных сумм с момента последней итерации проекта (рис. 169).

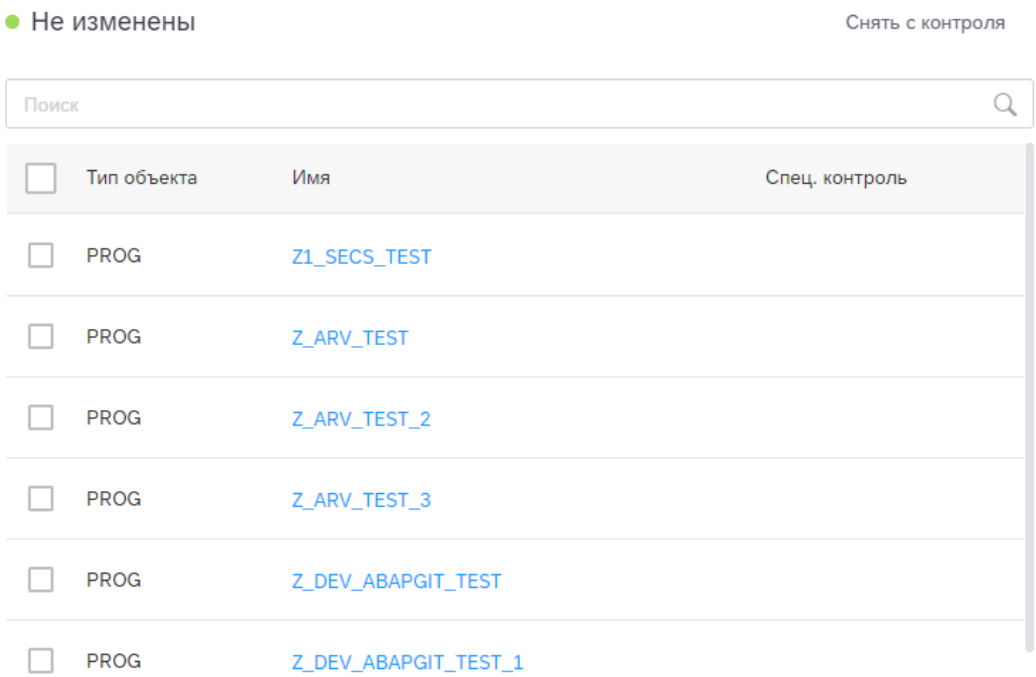


Рисунок 169 – Список объектов КЦ без изменения контрольных сумм

В окне «Текущее состояние объектов» для проектов типа КЦ доступны следующие действия:

1) Поиск по названию объекта. Чтобы выполнить поиск объекта в списке объектов (область с результатами проверки событий по объектам), необходимо ввести маску или название объекта в форму поиска над таблицей объектов (рис. 170).

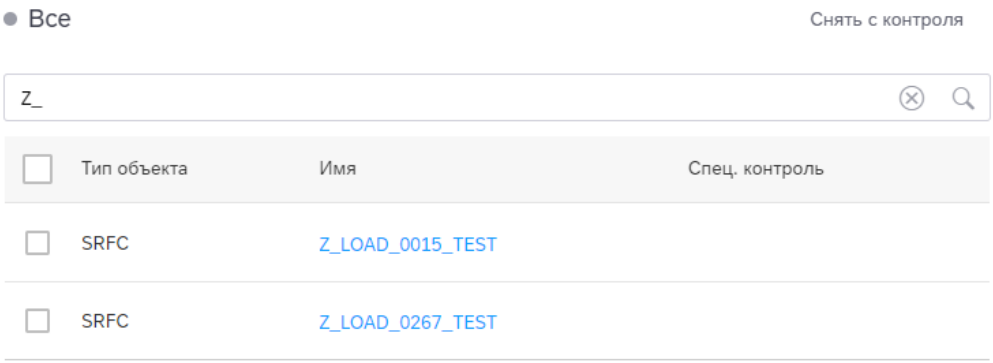


Рисунок 170 – Форма поиска по названию объекта анализа

2) Просмотр истории запросов по объектам анализа. Чтобы выполнить просмотр истории запросов, необходимо выбрать объекты анализа из списка объектов. Откроется окно «История транспортных запросов» (рис. 171).

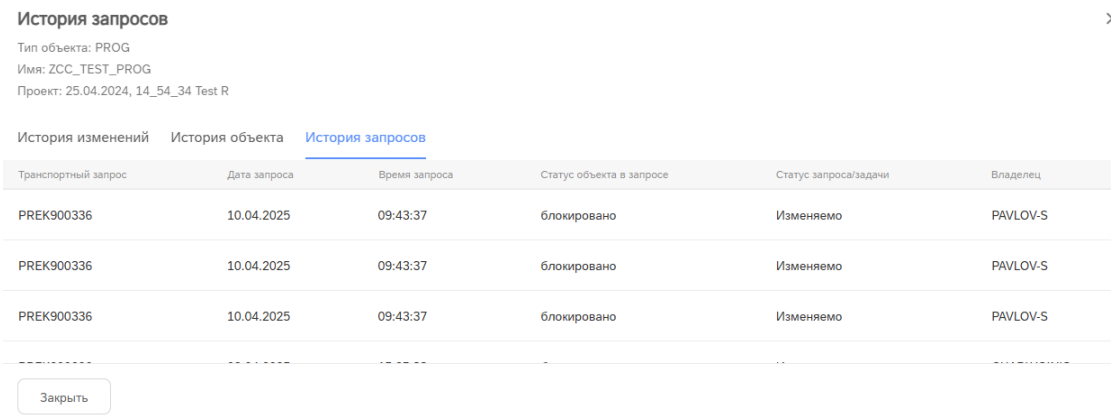


Рисунок 171 – История транспортных запросов

3) Просмотр истории по объектам анализа. Чтобы выполнить просмотр истории, необходимо выбрать объекты анализа из списка объектов, нажать на наименование объекта. В открывшемся окне «История объекта» (рис. 172), нажать на вкладку История объекта .

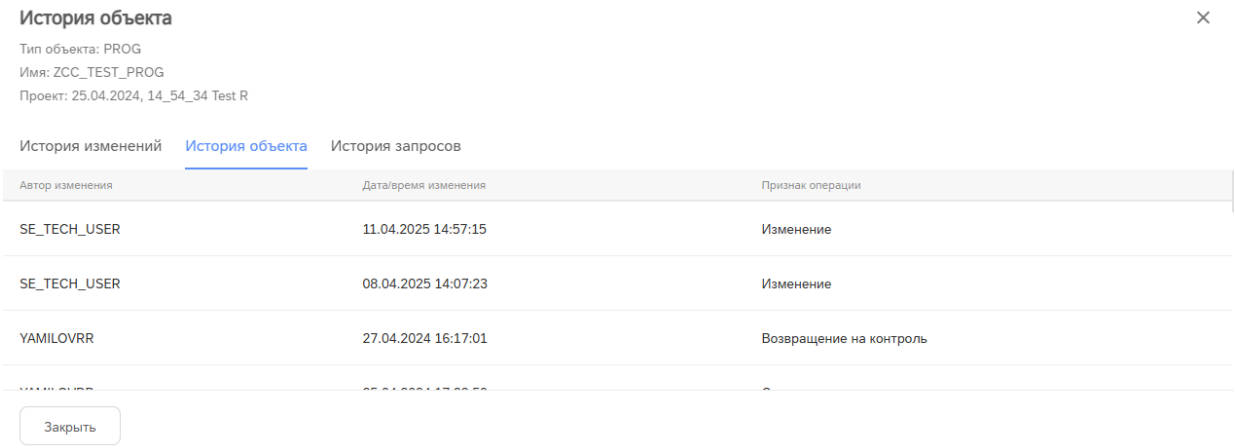


Рисунок 172 – Просмотр истории по объекту анализа

4) Снятие объекта с контроля. Чтобы снять объект с контроля, необходимо выделить объект или объекты в списке объектов (рис. 173) и нажать соответствующую кнопку «Снять с контроля» над таблицей объектов.

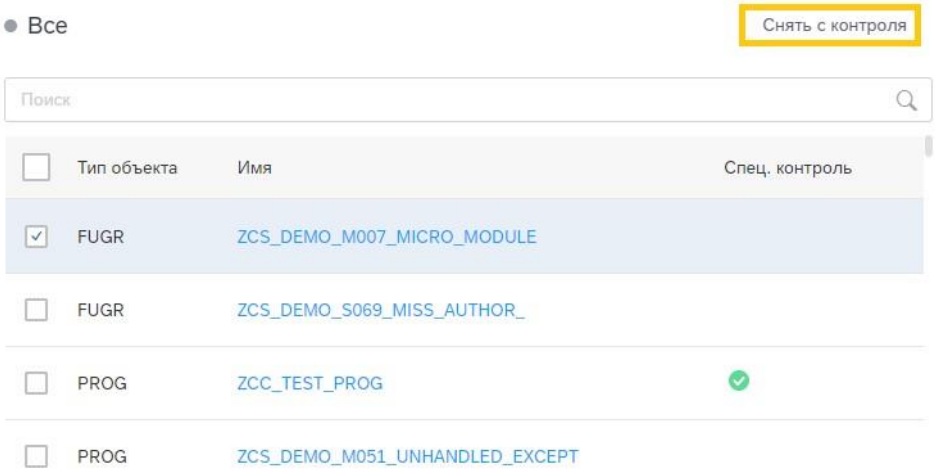


Рисунок 173 – Снятие объекта с контроля

Объект будет удален из списка и перенесен в список объектов со статусом «Сняты с контроля» (рис. 174).

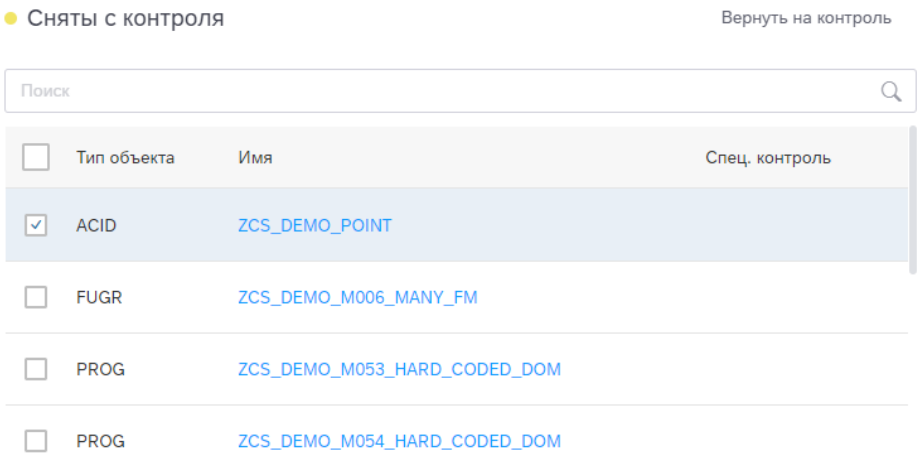


Рисунок 174 – Определение объекта в список «Сняты с контроля»

5) Возвращение объекта на контроль. Для того чтобы вернуть объект на контроль, необходимо в списке объектов со статусом «Сняты с контроля» установить флаг ☑ напротив объекта/объектов, нажать соответствующую кнопку «Вернуть на контроль» над таблицей объектов (рис. 175).

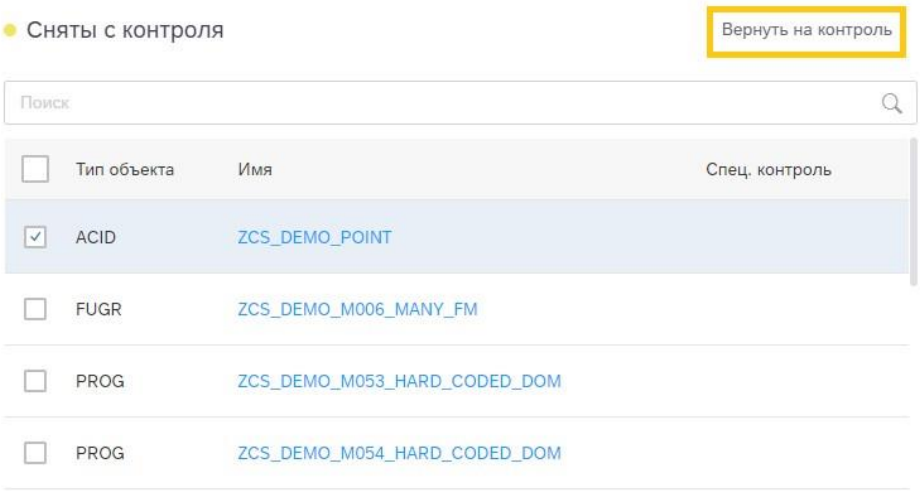


Рисунок 175 – Возврат объектов на контроль

6) Выравнивание объекта. Выравнивание объекта – это процедура, подтверждающая легитимность изменения контрольной суммы объекта. Чтобы выровнять объект/объекты, необходимо в списке объектов со статусом «Изменены» выделить объект/объекты с измененной контрольной суммой и нажать на соответствующую кнопку «Выровнять» (рис. 176).

Рисунок 176 – Активация процедуры выравнивания объекта КЦ

После активации процедуры выравнивания объект КЦ удаляется из списка измененных объектов.

7.1.2.1.2.4.4.1.1 Метка «Спец. контроль»

Метка «Спец. контроль» предназначена для просмотра изменений объектов в проекте (рис. 177).

Для просмотра изменения объекта необходимо нажать на метку в столбце «Спец контроль».

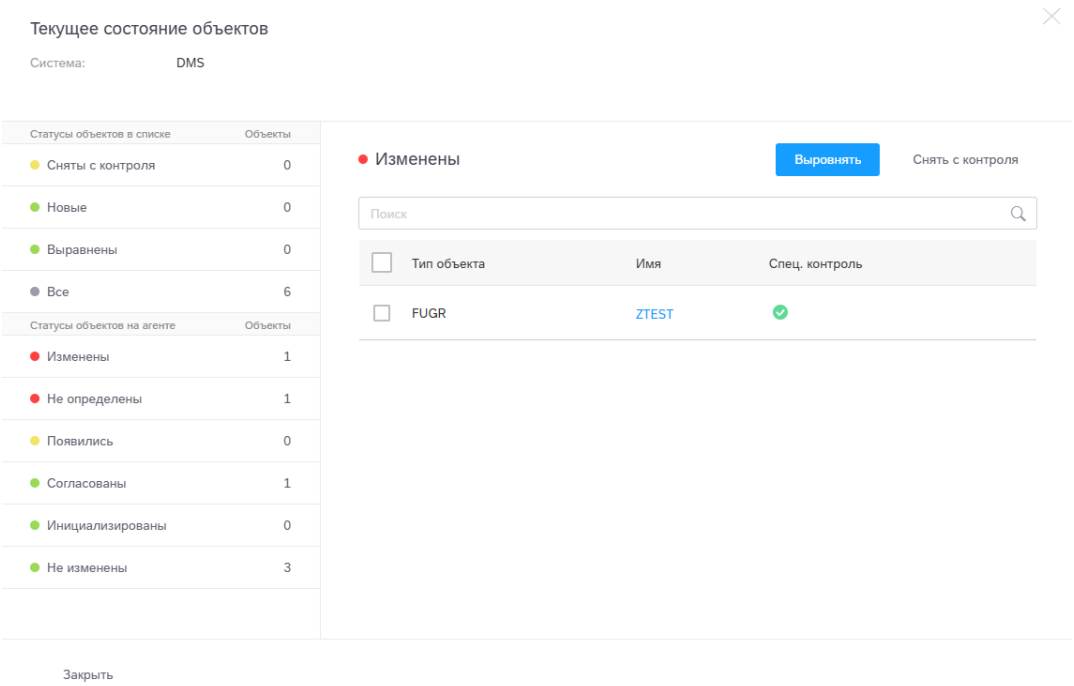


Рисунок 177 – Список объектов с меткой «Спец. контроль»

Окно «История изменений» предназначено для просмотра истории изменений в объекте.

В окно «История изменений» входят следующие вкладки:

- «История изменений» – дата и время запуска итераций проекта;
- «История объекта» – история изменений объекта. Вкладка содержит следующее данные: автор изменения (пользователь, который внес изменения в объект), дата и время изменения и признак операции (действия, которые были выполнены с объектом);
- «История запросов» – список транспортных запросов, которые содержат изменения, а также статус транспортных запросов.

Примечание. Если объект используется в нескольких проектах КЦ, то данные не удаляются. Данные удалятся только после удаления всех проектов, где используется объект.

Для просмотра изменений объекта необходимо выбрать объект с меткой «Спец контроль» в окне «Текущее состояние», выбрать вкладку «История изменений» в открывшемся окне, нажать на итерацию проекта, нажать на объект в столбце «Объекты кода».

Просмотр статусов объектов осуществляется в столбце «Объекты кода». Статусы объектов представлены в таблице 7 .

Таблица 7– Статусы объектов кода

Статус	Значение
	Строки кода были удалены
	– строки кода были добавлены;

	– строки кода были изменены
	Строки кода были удалены, а также изменены или добавлены

При просмотре изменений в окне выделяются строки кода следующими цветами:

- красный – строки кода были удалены (рис. 178);
- зеленый – строки кода были добавлены или изменены (рис. 179).

Примечание. Для просмотра измененного кода необходимо выбрать вкладку «Изменено» в окне «Сравнение версий».

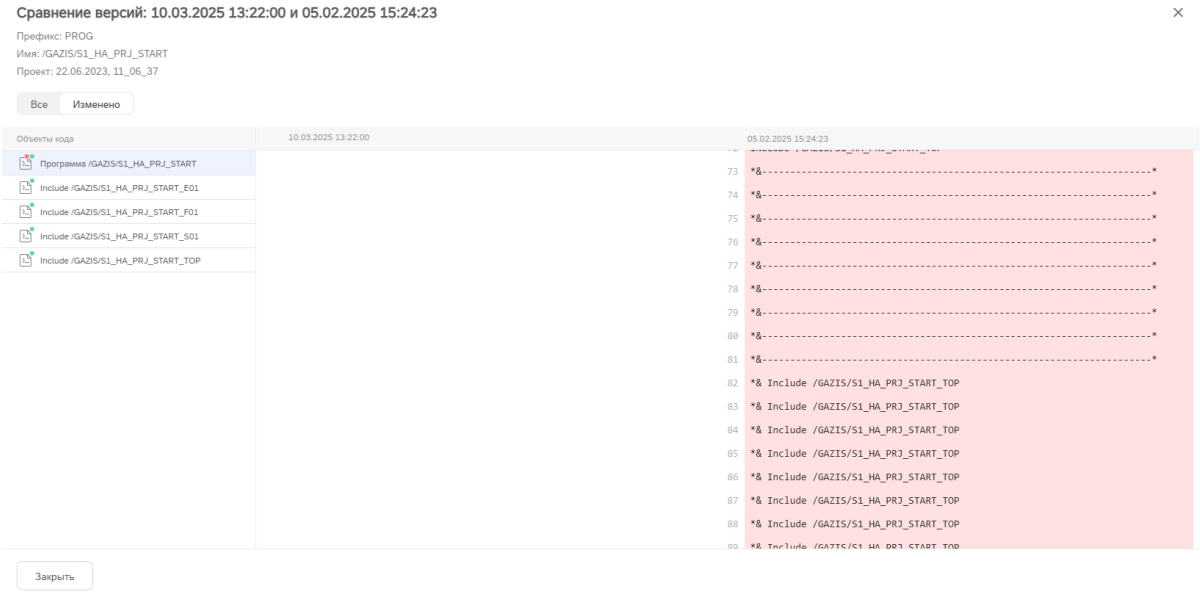


Рисунок 178 – Строки с удаленным кодом

Рисунок 179 – Добавленные строки кода

Метка «Спец.контроль» для типа объектов «TABL»

При выборе типа объекта «TABL» необходимо выбрать 2 итерации проекта для сравнения, нажать кнопку «Сравнение версий» (рис. 180). В отдельном окне откроется

список с параметрами изменения.

Доступен просмотр по следующими параметрам:

- тип изменения;
- таблица изменений;
- описание таблицы изменений;
- поле ID;
- описание поля ID;
- атрибут;
- описание атрибута;
- новое значение;
- старое значение;
- язык;
- позиция;
- позиция индекса.

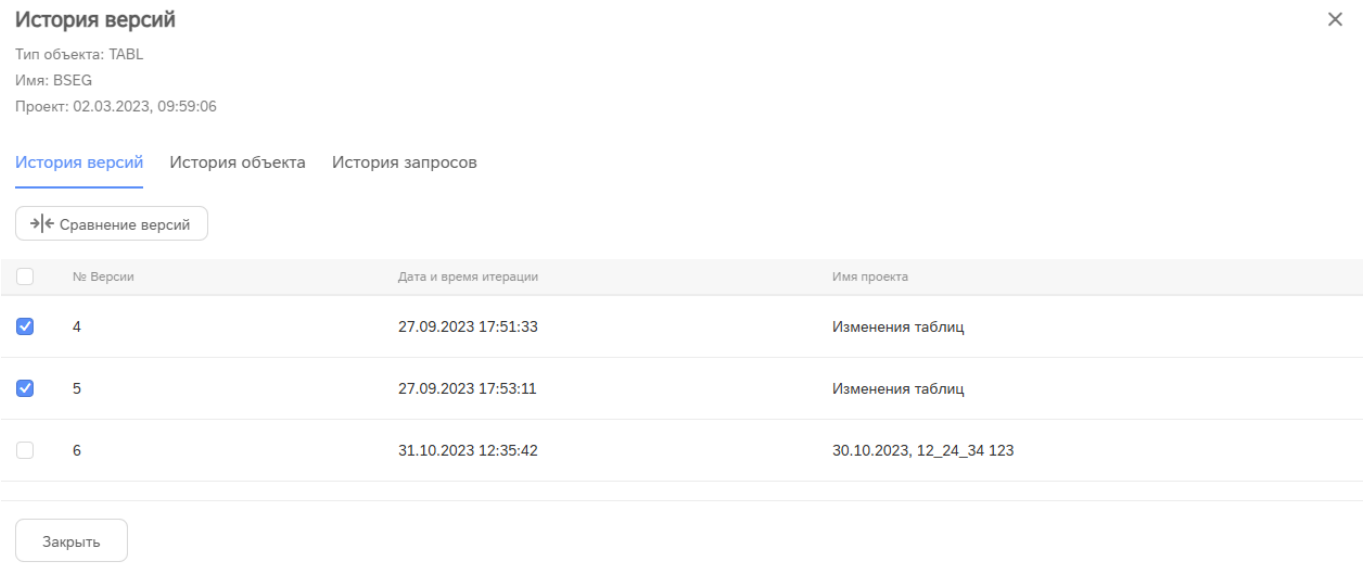


Рисунок 180 – Список итераций с изменениями для объектов типа «TABL»

Примечание. Настройка отображение параметров происходит с помощью кнопки *«Настройки»* (рис. 181).

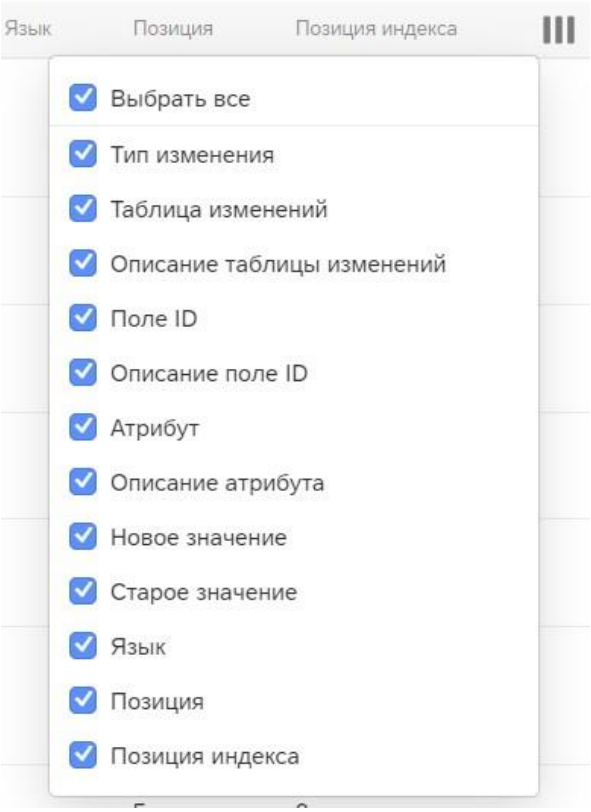
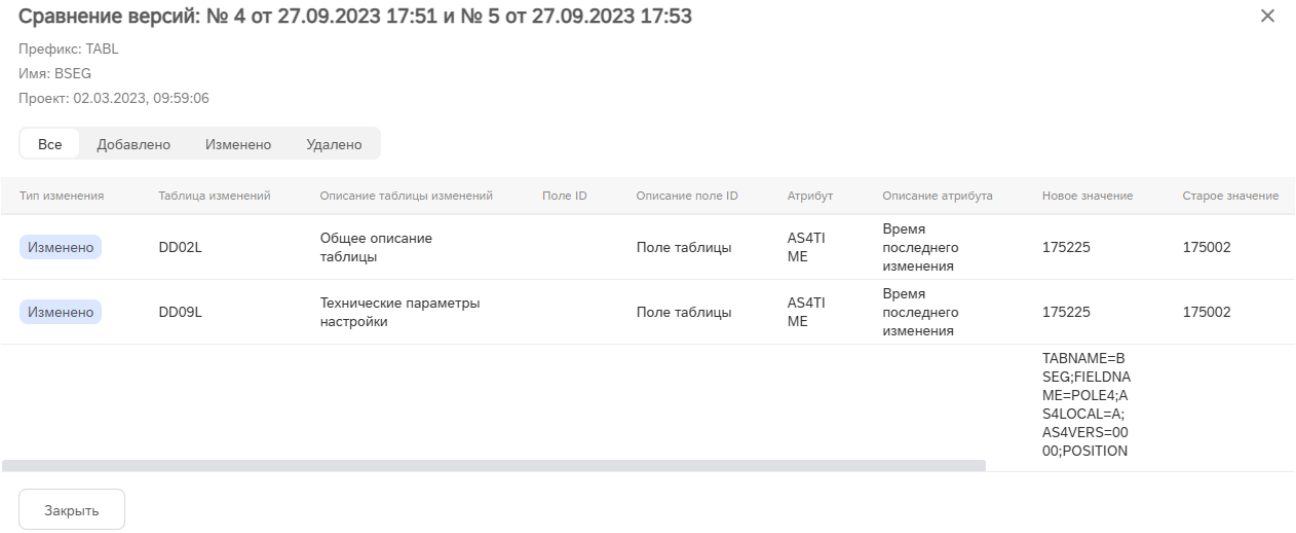


Рисунок 181 – Настройка отображение параметров

Доступные статусы изменений для объекта типа «TABL» (рис. 182):

- «Все»;
- «Добавлено»;
- «Изменено»;
- «Удалено».



Сравнение версий: № 4 от 27.09.2023 17:51 и № 5 от 27.09.2023 17:53

Префикс: TABL
Имя: BSEG
Проект: 02.03.2023, 09:59:06

Все | Добавлено | Изменено | Удалено

Тип изменения	Таблица изменений	Описание таблицы изменений	Поле ID	Описание поле ID	Атрибут	Описание атрибута	Новое значение	Старое значение
Изменено	DD02L	Общее описание таблицы		Поле таблицы	AS4TIME	Время последнего изменения	175225	175002
Изменено	DD09L	Технические параметры настройки		Поле таблицы	AS4TIME	Время последнего изменения	175225	175002
							TABNAME=BSEG;FIELDNAME=POLE4;AS4LOCAL=A;AS4VERS=0000;POSITION	

Закрыть

Рисунок 182 – Объекты типа «TABL» с изменениями

7.1.2.1.2.4.4.2 Текущее состояние объектов анализа в созданных проектах типа ОД

Пример окна «Текущее состояние объектов» для проектов типа ОД приведен на рис. 183.

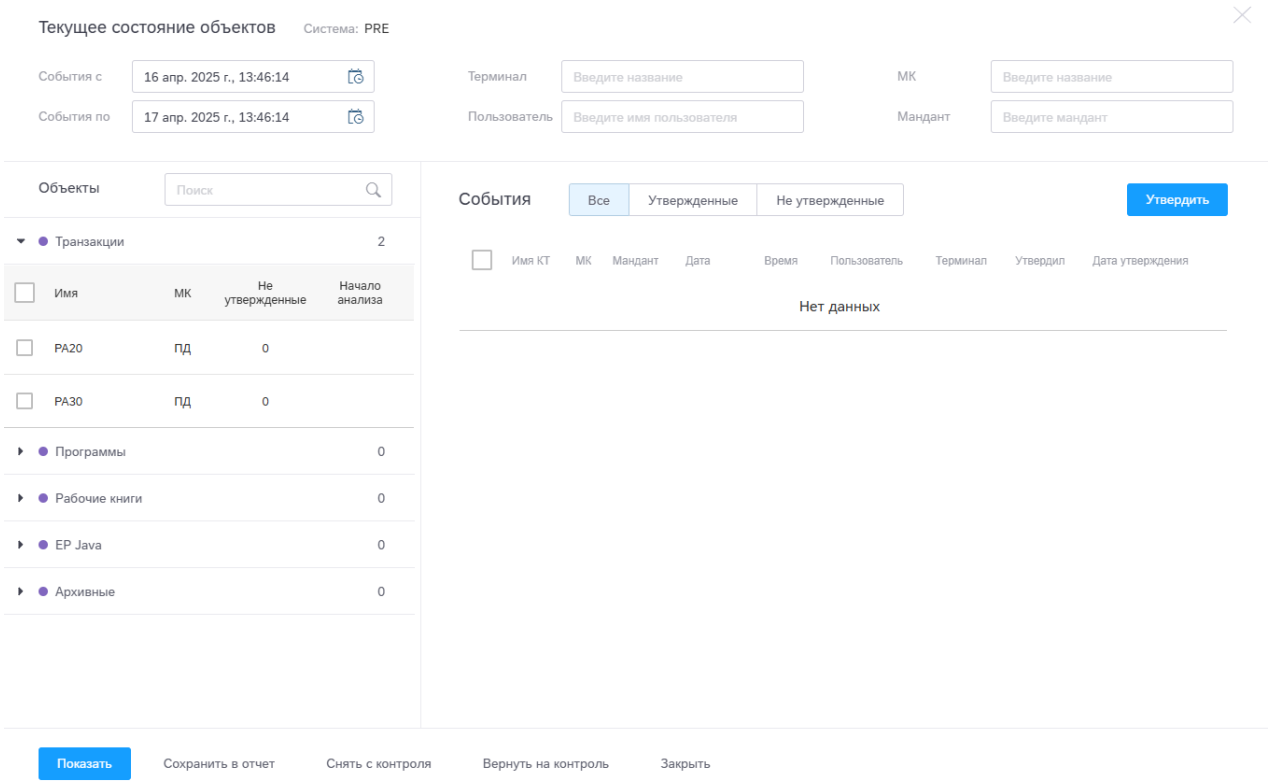


Рисунок 183 – Пример окна текущего состояния объектов анализа проекта типа ОД

В окне «Текущее состояние объектов» для проектов типа ОД доступны следующие действия:

1) Выбор периода просмотра информации по объектам анализа. Чтобы отредактировать дату и время отчетного периода или выбрать дату и время из календаря, необходимо нажать кнопку и указать их в полях «Начало» и «Конец» (рис. 184).

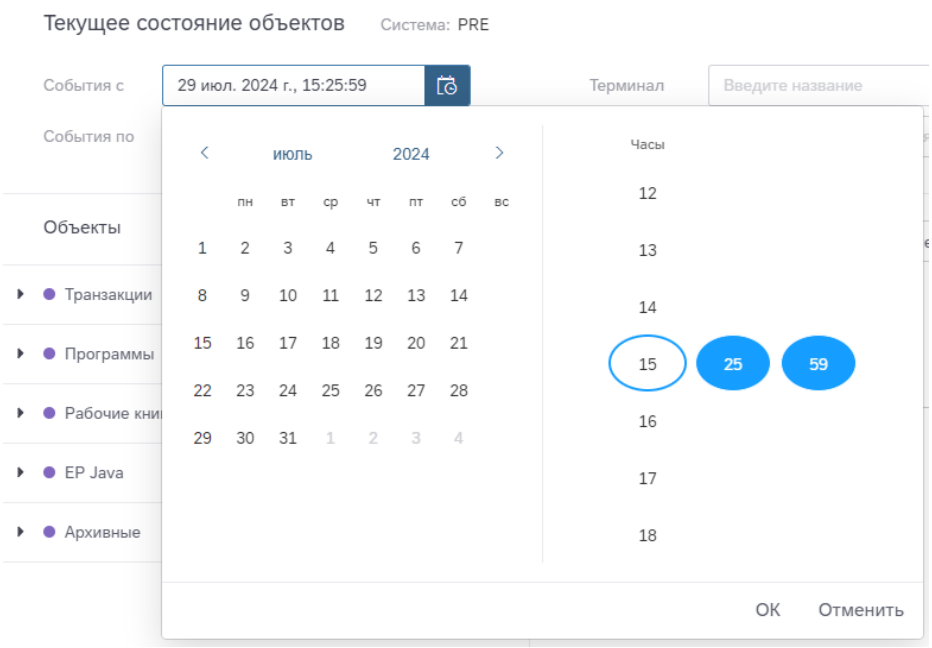


Рисунок 184 – Выбор периода просмотра информации

2) Поиск по названию объекта. Чтобы осуществить поиск объекта в списке объектов, необходимо ввести маску или название объекта в форму поиска над таблицей объектов (рис. 185).

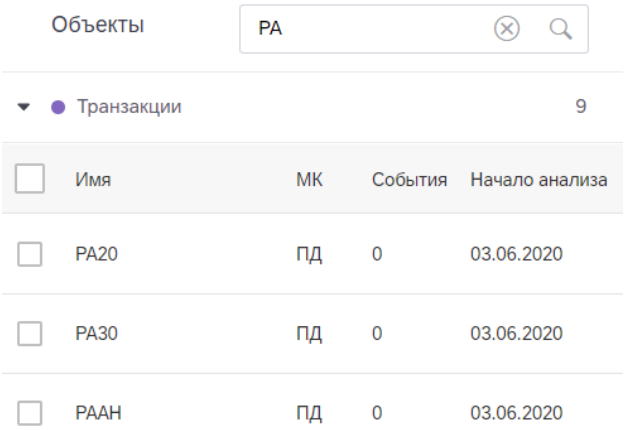


Рисунок 185 – Область поиска по названию объекта анализа

3) Просмотр событий по объектам анализа. Чтобы осуществить просмотр событий по объектам анализа, необходимо выбрать объекты анализа из списка объектов и нажать кнопку «Показать». В шаблоне таблицы вывода данных по событиям объектов анализа отобразится подробная информация (рис. 186).

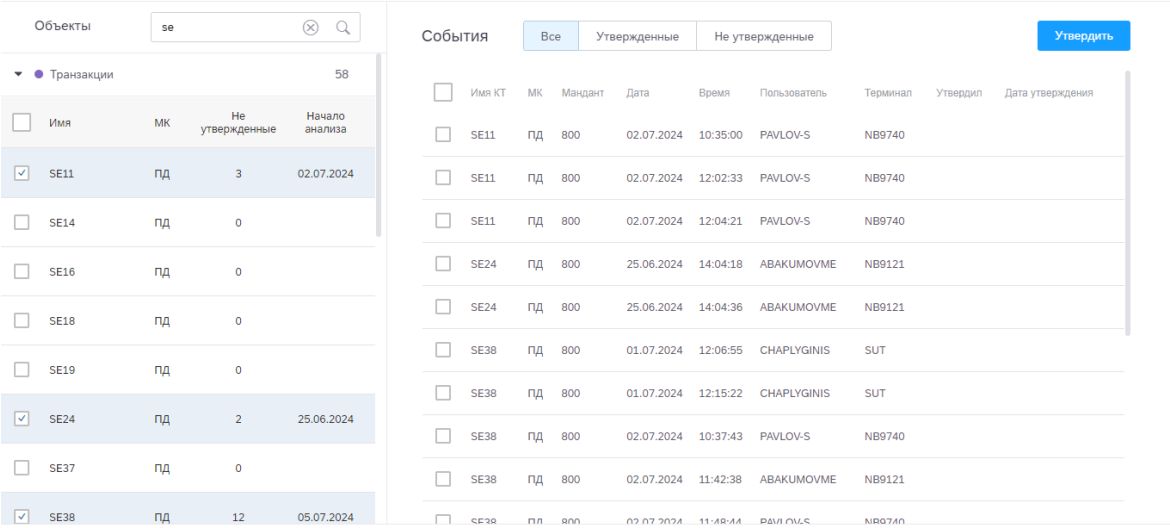


Рисунок 186 – Просмотр информации по событиям объектов анализа

Значения столбца «МК» (Маркер конфиденциальности) представлены в таблице 8.

Таблица 8 – Значения столбца «МК»

Значение столбца МК	Описание
СП	Для служебного пользования
ИНОД	Информация неограниченного доступа
ПД	Персональные данные
ПД+КТ	Персональные данные+Коммерческая тайна
КТ	Коммерческая тайна

4) Поиск информации в таблице событий объектов анализа. Чтобы выполнить поиск необходимой информации в таблице, необходимо ввести искомые данные в формы поиска над таблицей событий (рис. 187).

Рисунок 187 – Формы поиска информации в таблице событий

5) Сохранение в отчет. Чтобы выгрузить данные из таблицы событий объектов анализа в файл в формате Excel, необходимо нажать соответствующую кнопку «Сохранить в отчет» под списком объектов (см. рис. 183).
6) Снятие объекта с контроля. Чтобы снять объект с контроля, необходимо выделить объект/объекты в списке объектов и нажать на соответствующую кнопку «Снять с контроля» под списком объектов (рис. 188).

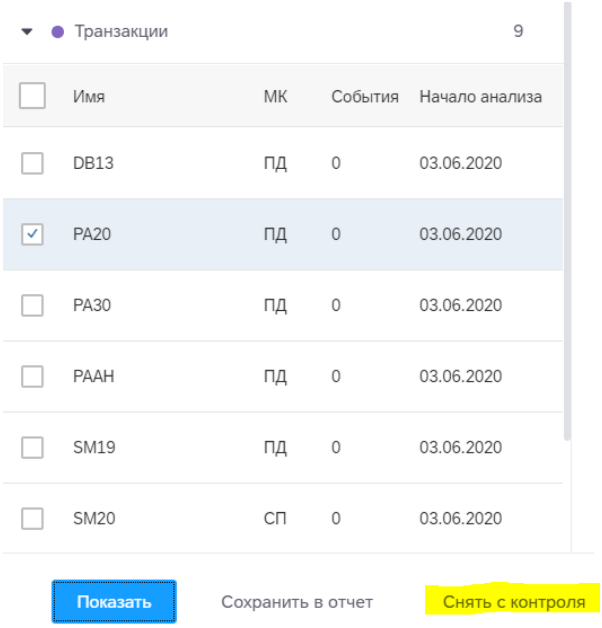


Рисунок 188 – Снятие объекта с контроля

Объект будет удален из списка и перенесен в папку «Архивные» (рис. 189).

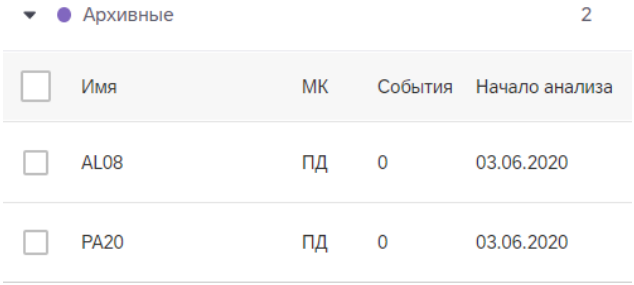


Рисунок 189 – Определение объекта в архив

7) Возврат объекта на контроль. Чтобы вернуть объект на контроль, необходимо выделить объект/объекты в списке «Архивные» и нажать на соответствующую кнопку «Вернуть на контроль» под списком объектов. Объект будет возвращен из архива в список объектов для контроля (рис. 190).

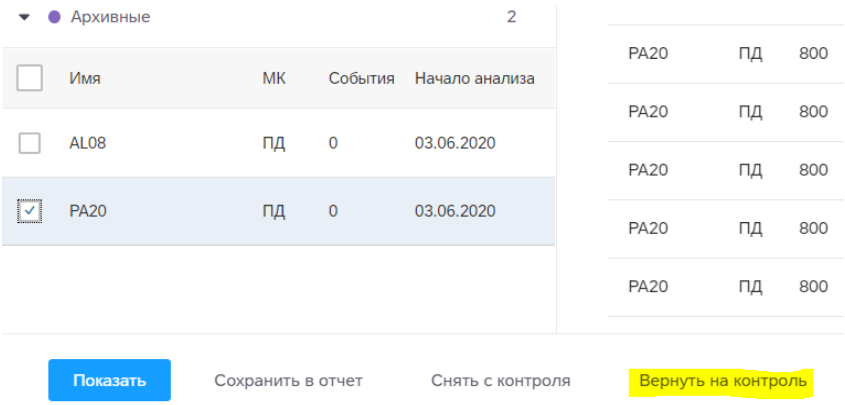


Рисунок 190 – Возвращение объекта на контроль

8) Утверждение события. Утверждение события – это процедура, подтверждающая обработку события доступа к объекту ограниченного доступа. Чтобы утвердить события, необходимо нажать кнопку «Текущее состояние» во вкладке «Объекты». В открывшемся окне необходимо выбрать период и объекты. В области «Объекты» необходимо выбрать данные, нажать кнопку «Утвердить» (рис. 191). В поле «События» необходимо выбрать события, которые требуется утвердить, нажать кнопку «Утвердить». Для просмотра утверждённых событий, необходимо нажать на вкладку «Утвержденные». Для закрытия окна просмотра текущего состояния объектов необходимо нажать кнопку «Закрыть».

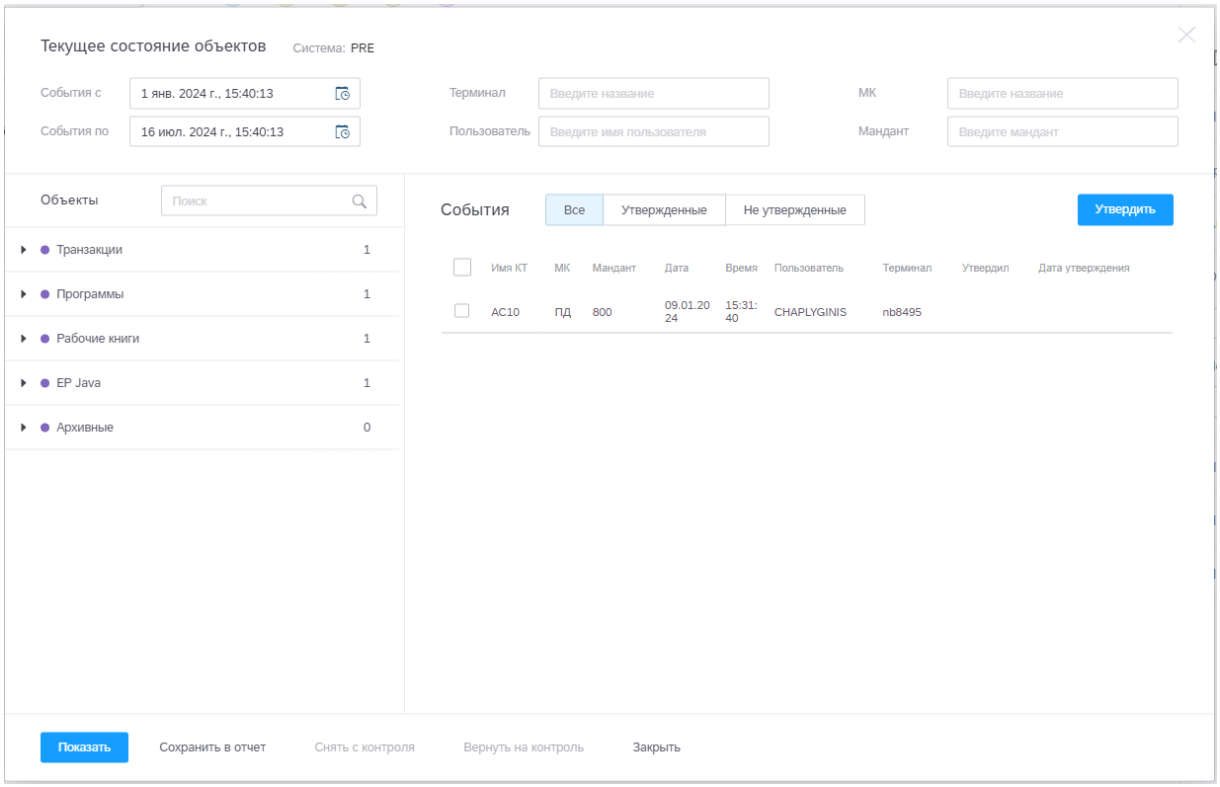
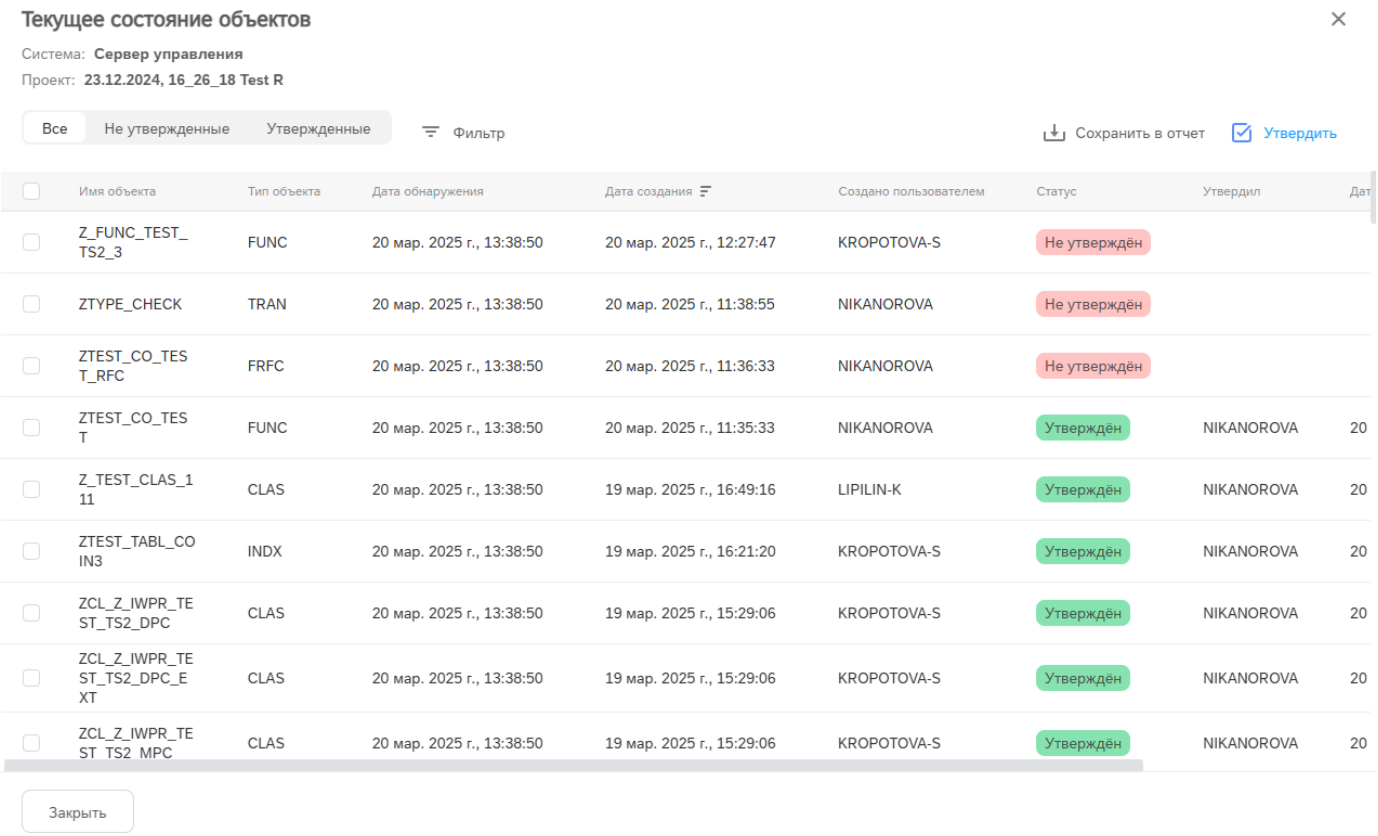


Рисунок 191 – Пример окна текущего состояния объектов анализа проекта типа ОД

7.1.2.1.2.4.4.3 Текущее состояние объектов анализа в созданных проектах типа СО

Пример окна «Текущее состояние объектов» для проектов типа СО представлен на рис. 192.



Имя объекта	Тип объекта	Дата обнаружения	Дата создания	Создано пользователем	Статус	Утвердил	Дат
Z_FUNC_TEST_TS2_3	FUNC	20 мар. 2025 г., 13:38:50	20 мар. 2025 г., 12:27:47	KROPOTOVA-S	Не утверждён		
ZTYPE_CHECK	TRAN	20 мар. 2025 г., 13:38:50	20 мар. 2025 г., 11:38:55	NIKANOROVA	Не утверждён		
ZTEST_CO_TEST_RFC	FRFC	20 мар. 2025 г., 13:38:50	20 мар. 2025 г., 11:36:33	NIKANOROVA	Не утверждён		
ZTEST_CO_TEST	FUNC	20 мар. 2025 г., 13:38:50	20 мар. 2025 г., 11:35:33	NIKANOROVA	Утверждён	NIKANOROVA	20
Z_TEST_CLAS_111	CLAS	20 мар. 2025 г., 13:38:50	19 мар. 2025 г., 16:49:16	LIPILIN-K	Утверждён	NIKANOROVA	20
ZTEST_TABL_COIN3	INDX	20 мар. 2025 г., 13:38:50	19 мар. 2025 г., 16:21:20	KROPOTOVA-S	Утверждён	NIKANOROVA	20
ZCL_Z_IWPR_TEST_TS2_DPC	CLAS	20 мар. 2025 г., 13:38:50	19 мар. 2025 г., 15:29:06	KROPOTOVA-S	Утверждён	NIKANOROVA	20
ZCL_Z_IWPR_TEST_TS2_DPC_EXT	CLAS	20 мар. 2025 г., 13:38:50	19 мар. 2025 г., 15:29:06	KROPOTOVA-S	Утверждён	NIKANOROVA	20
ZCL_Z_IWPR_TEST_TS2_MPC	CLAS	20 мар. 2025 г., 13:38:50	19 мар. 2025 г., 15:29:06	KROPOTOVA-S	Утверждён	NIKANOROVA	20

Рисунок 192 – Пример окна «Текущее состояние объектов» для проектов типа СО

В окне «Текущее состояние объектов» для проектов типа СО доступны следующие действия:

1) Просмотр информации по объектам анализа в соответствии с заданными параметрами фильтра. Чтобы просмотреть информацию по объектам анализа в соответствии с заданными параметрами фильтра необходимо нажать кнопку «Фильтр» (рис. 192) и заполнить поля «Имя объекта», «Тип объекта», «Создано пользователем», «Дата обнаружения с», «Дата обнаружения по», «Дата создания с» , «Дата создания по», «Создано пользователем», «Утвердил», «Дата утверждения с», «Дата утверждения по» (рис. 193), нажать кнопку *«Применить».*

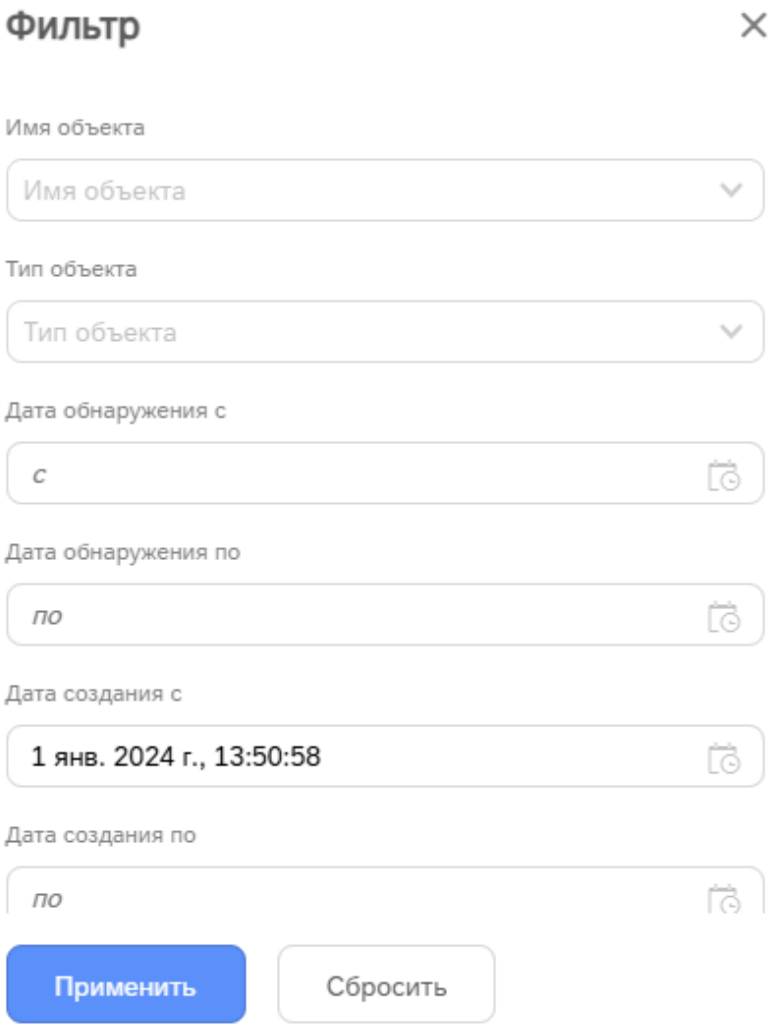


Рисунок 193 – Окно «Фильтр» для окна «Текущее состояние» объектов типа СО

2) Загрузка отчета. Для загрузки отчета на локальную ЭВМ необходимо поставить флаг напротив объектов, нажать кнопку *«Сохранить в отчет»* (рис. 192).
3) Утверждение объектов. Утверждение объекта – это процедура, подтверждающая создания объекта. Для утверждения объектов необходимо поставить флаг напротив объектов, нажать кнопку *«Утвердить»* (рис. 192).
   Примечание. После утверждения всех созданных объектов индикация проекта в столбце «Тип» измениться на зеленую.

7.1.2.1.2.5 Выбор профиля для проекта типа КН

Поле выбора профиля объектов предназначено для определения набора проверок (сценариев), которые будут применены к выбранной агент-системе.

В модуле SafeERP Platform Security параметр проекта «Профили» необходимо заполнить для проектов типа КН (рис. 194).

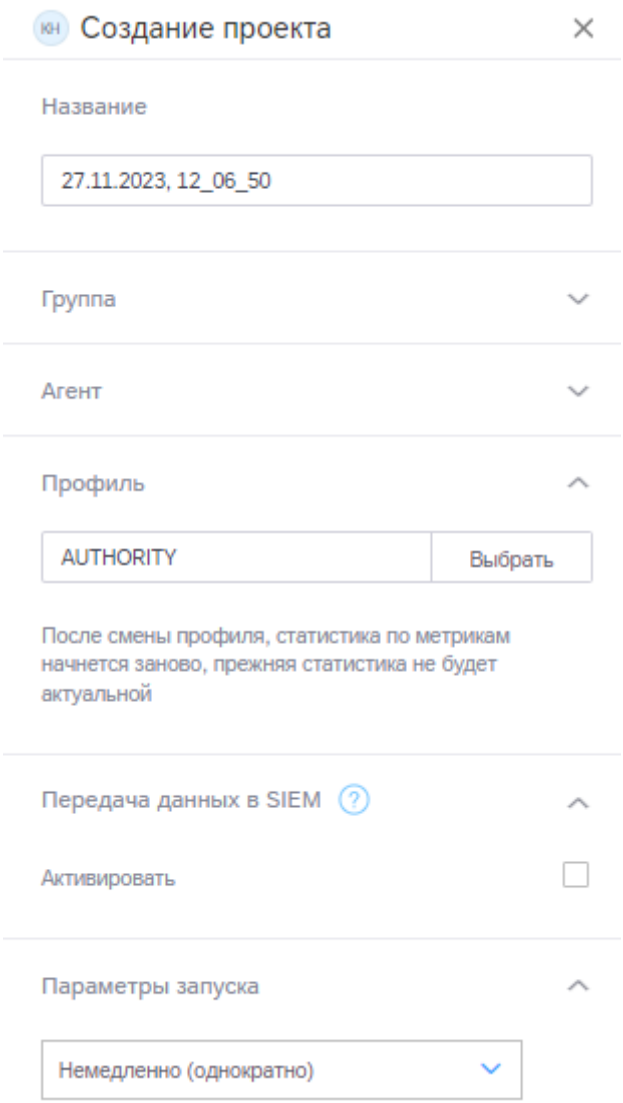


Рисунок 194 – Поле «Профили» для проектов типа КН

Чтобы выбрать профиль из предварительно настроенного списка, необходимо нажать кнопку *«Выбрать».* В поле выбора профиля, пример которого приведен на рис. 194, доступна функция поиска по наименованию профиля. Для добавления профиля в проект необходимо выделить профиль из списка. Для отмены выбора профиля необходимо нажать кнопку *«Отменить»* (рис. 195).

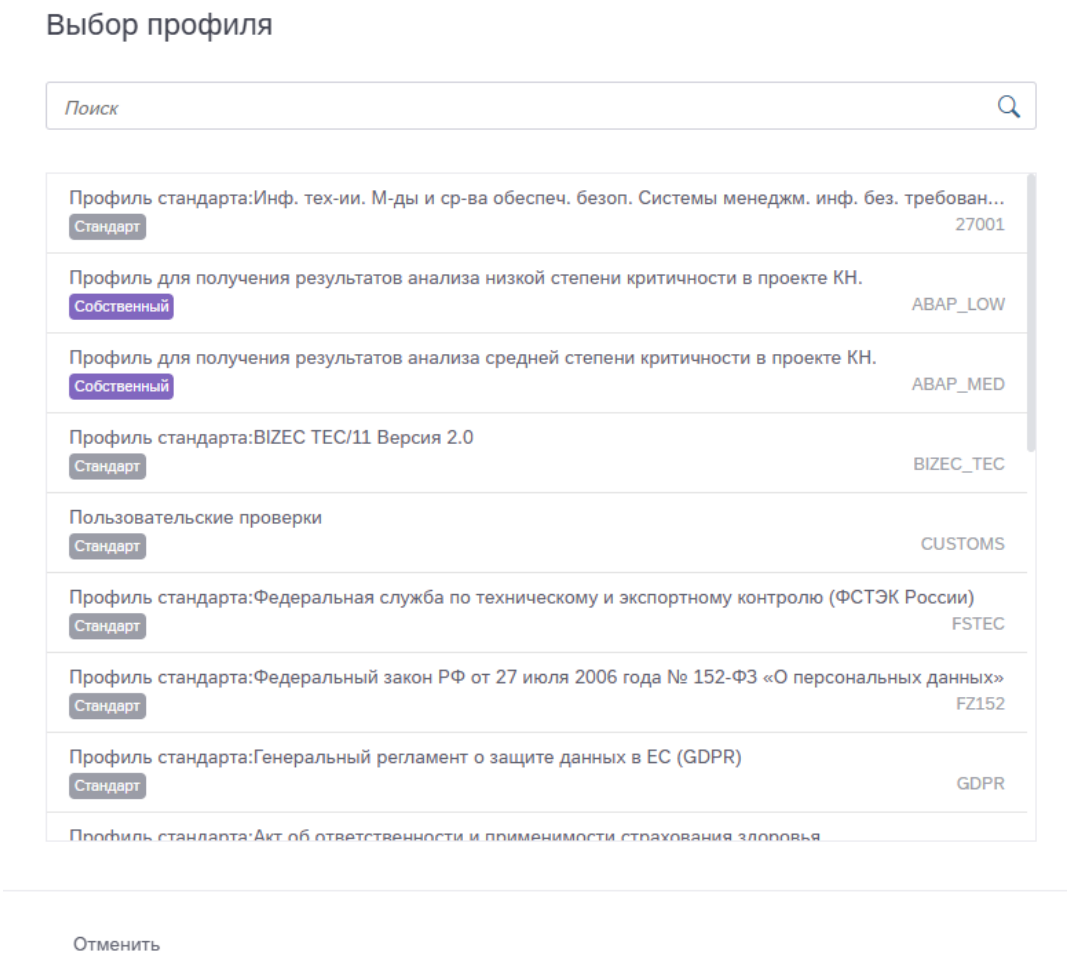


Рисунок 195 – Выбор профиля из преднастроенного списка

Настройка пользовательских профилей осуществляется администратором ПК в интерфейсе SAP graphical user interface (GUI) с помощью транзакции /N/GAZIS/SEGA (см. пункте 4.2.7) или в модуле «Администрирование» (см. в подпункте 7.1.9.8).

7.1.2.1.2.6 Исключения

Поле «Исключения» (рис. 196) предназначено для выбора объектов или пользователей для исключения из анализа. Исключенные объекты или пользователи не входят в отчет о проверках. Доступна данная функция для проектов типа ОД и агентов типа ABAP.

Поле «Исключения» находится во вкладке «Проект типа ОД» на рис. 197.

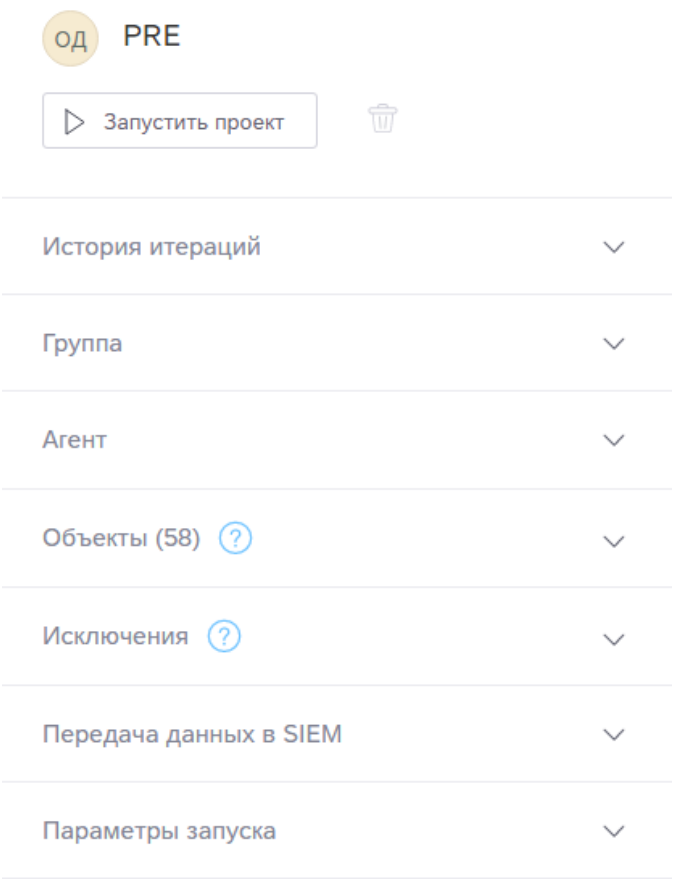


Рисунок 196 – Вкладка «Проект типа ОД»

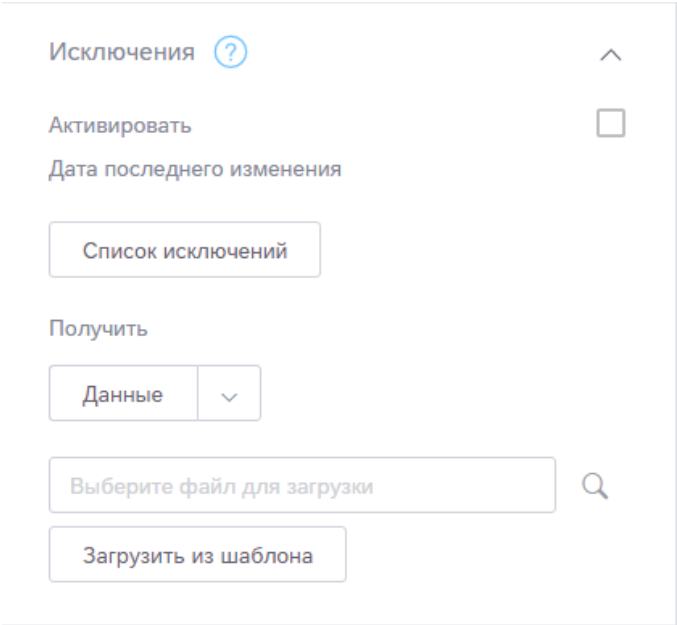


Рисунок 197 – Поле «Исключения»

Для работы с полем «Исключения» доступны следующие действиям:

1) Активация. Чтобы активировать процедуру исключения, необходимо установить флаг ☑ в поле элемента.
2) Просмотр исключений. Чтобы просмотреть исключения, необходимо нажать

кнопку *«Список исключений»*. В открывшемся окне появятся данные об исключенных объектах (рис. 198).

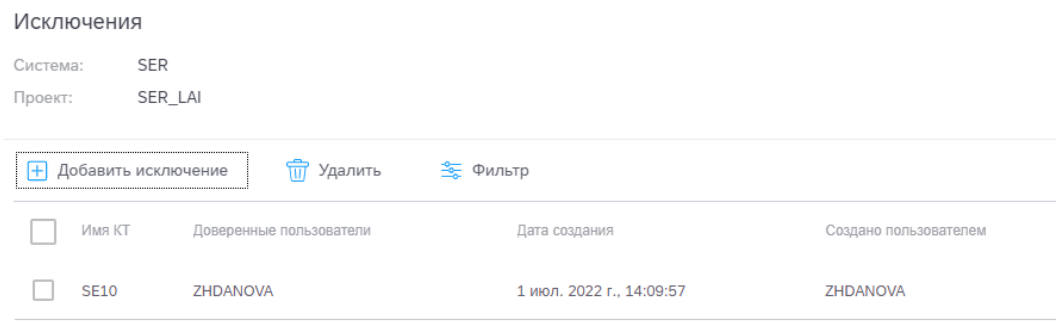


Рисунок 198 – Исключенные объекты

3) Добавление исключений. Чтобы добавить исключения, необходимо нажать кнопку *«Список исключений»*. В открывшемся окне необходимо нажать кнопку *«Добавить исключение»*, затем ввести имя КТ и имя доверенного пользователя (рис. 199), нажать кнопку *«Создать исключение»*.

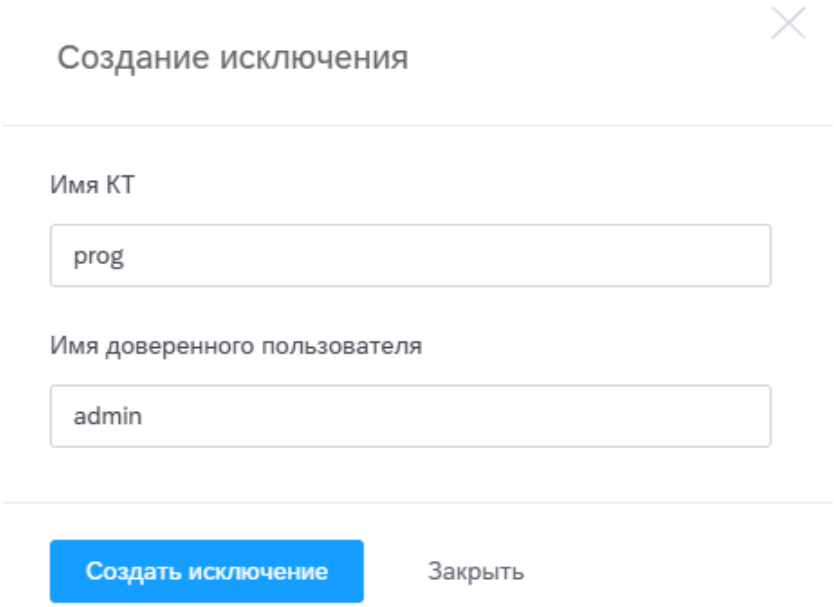


Рисунок 199 – Создание исключения

4) Удаление исключений. Чтобы удалить исключение, необходимо нажать кнопку *«Список исключений»*. В открывшемся окне необходимо установить флаг ☑ в поле объекта, нажать кнопку *«Удалить»*, в открывшемся окне подтвердить удаление (рис. 200).

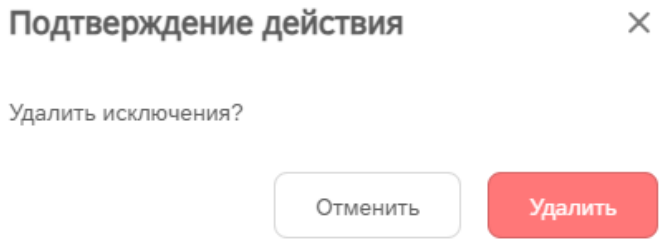


Рисунок 200 – Подтверждение удаление исключения

5) Получить шаблон. Чтобы получить шаблон в поле «Получить», выбрать пункт Получить шаблон (рис. 201).

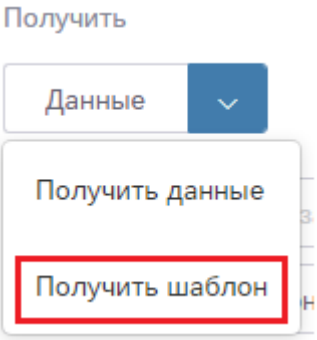


Рисунок 201 – Получить шаблон

В открывшемся файле необходимо ввести (рис. 202):

— имя КТ(KT_NAME) – имя объекта, который требуется исключить.
— пользователь(BNAME) – имя пользователя, который обращался к объекту.
— исключить(EXTENDED) – символ, который требуется ввести для подтверждения исключения из отчета. Ввести «X» для исключения.
— тип ПС (SWT) – тип данных объектов, которые необходимо исключить из отчета. Необходимо ввести символ для исключения T – для транзакции, W – рабочей книги, E – EP Java, P – программы.
— описание(DESCRIPTION) – подробное описание объекта. Данное поле является необязательным для заполнения.
— техническое имя(TECH_NAME) – имя BiW-объекта. Данное поле является необязательным для заполнения.

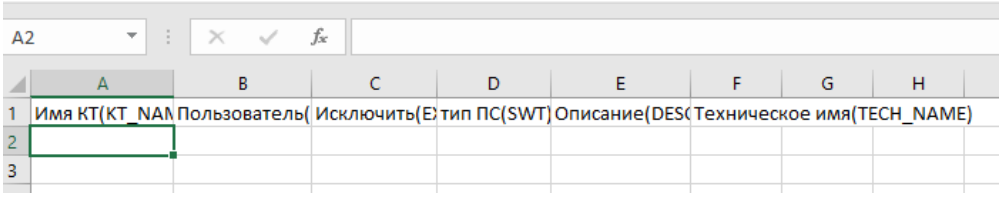


Рисунок 202 – Шаблон для «Исключений»

6) Получить данные. Чтобы получить данные, необходимо в поле «Получить»

выбрать пункт Получить данные (рис. 203).

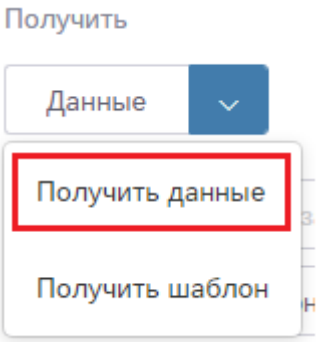


Рисунок 203 – Получить данные

7) Загрузить из шаблона. Чтобы загрузить данные из шаблона, необходимо нажать кнопку . В открывшемся окне необходимо выбрать файл формата .csv для загрузки, нажать кнопку *«Загрузить из шаблон»* (см. рис. 197).

7.1.2.1.2.7 Выбор параметров запуска

Поле выбора параметров запуска (см. рис. 150) предназначено для определения временных характеристик и режима запуска проекта.

Чтобы выбрать параметры запуска из предварительно настроенного списка, необходимо нажать кнопку (рис. 204).

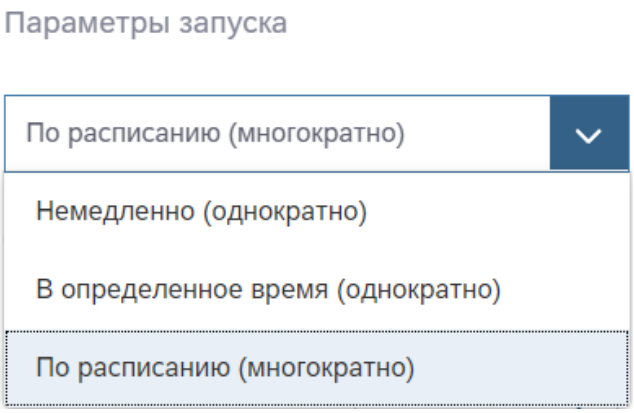


Рисунок 204 – Выбор параметров запуска

В списке параметров запуска доступны следующие режимы:

- немедленно (однократно) – запуск анализа выбранных объектов сразу после сохранения проекта;
- в определенное время (однократно) – запуск анализа выбранных объектов в установленное время (рис. 205).

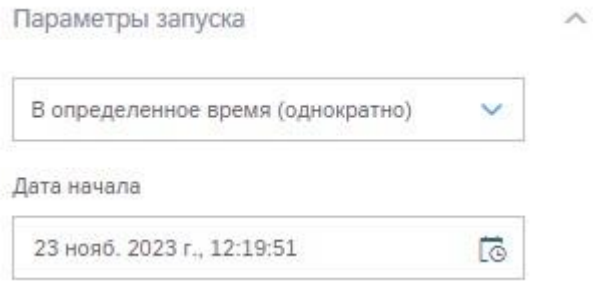


Рисунок 205 – Выбор отложенного режима (однократно)

— по расписанию (многократно) – запуск анализа выбранных объектов в установленное время по расписанию (рис. 206).

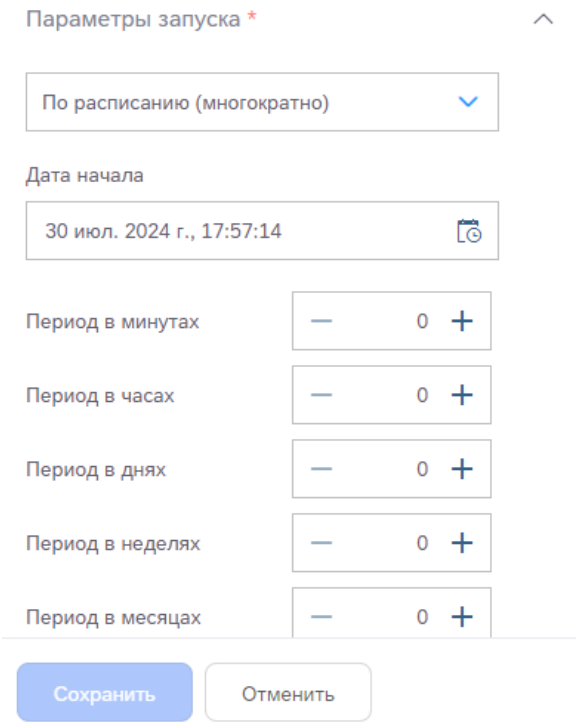


Рисунок 206 – Выбор отложенного режима (многократно)

7.1.2.1.3 Просмотр/редактирование/запуск/удаление проекта

Чтобы просмотреть, отредактировать, запустить, прервать или удалить проект, необходимо открыть область свойств проекта, нажав один раз левой конки мыши на строчку соответствующего проекта (название проекта). При активации области параметров проекта (см. рис. 150), в зависимости от типа процедуры анализа, появится возможность:

— активировать запуск проекта (кнопка *«Запустить проект»*);
— просмотреть отчеты по результатам анализа;
— просмотреть настройки параметров проекта;
— изменить профиль проверок;
— внести изменения в список объектов проекта и исключений;

— изменить параметры запуска;
— изменить настройку «Передача данных в SIEM» (для проектов типа КН, ОД, АВ);
— удалить проект (кнопка *«Удалить»*) (для администратора).

Примечания:

1. Во время выполнения сканирования проекта кнопка *«Сохранить»* остается активной. Если проект запущен, то будет выводиться следующее сообщение (рис. 207):

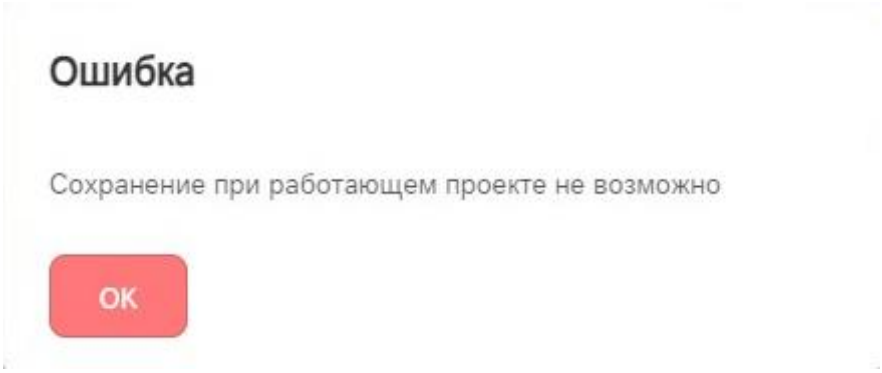


Рисунок 207 – Сообщение при активном проекта

2. После активации кнопки *«Отменить»* после внесения изменений в проекте, будет показано следующее сообщение (рис. 208):

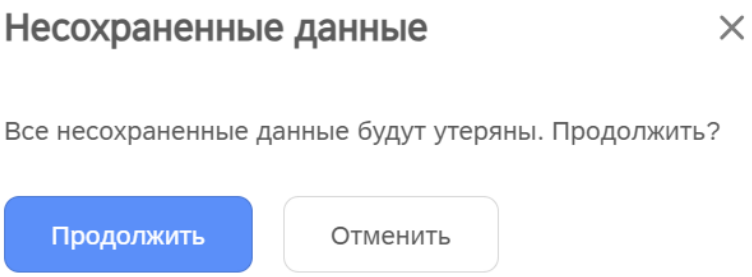


Рисунок 208 – Сохранение изменений

3. После внесения в проект и активации кнопки *«Сохранить»* будет показано следующее сообщение (рис. 209):

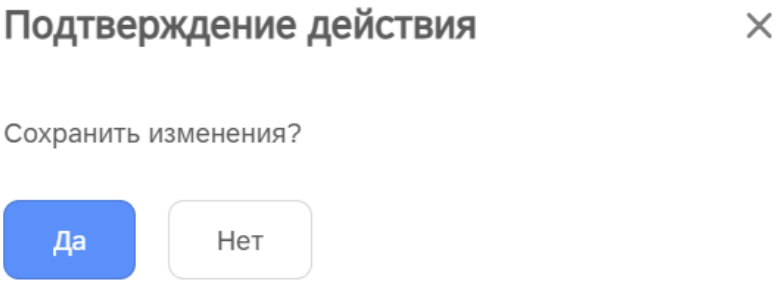


Рисунок 209 - Подтверждение изменений в проекте

7.1.2.1.4 Просмотр отчетов

Описание просмотра отчетов по итерациям проектов представлено в подпунктах 7.1.2.1.4.1 - 7.1.2.1.4.3.

Индикация итераций проекта представлена в таблице 9.

Индикация историй итераций представлена в таблице 10.

Таблица 9 – Индикация итераций отчетов в модуле «Сканер»

Индикатор итерации	События индикатора	
	КЦ	КН
	Ошибка при формировании отчета	Ошибка при формировании отчета
	Фоновое задание отработало успешно. В результатах есть критические события	Фоновое задание отработало успешно. В результатах есть критические события
	Фоновое задание отработало успешно. Целостность объектов не нарушена	Фоновое задание отработало успешно. В результатах есть события со средней степенью критичности или ниже

Таблица 10 – Индикация итераций в модуле «Сканер»

Индикатор итерации	События индикатора		
	ОД	АВ	СО
	Ошибка при RFC-соединении; Некорректное завершение итерации	Ошибка при RFC-соединении; Некорректное завершение итерации	Ошибка при RFC-соединении; Некорректное завершение итерации
	Фоновое задание отработало успешно. Пользователи обращались к информации типа ПД, ИНОД, СП, КТ	Фоновое задание отработало успешно. В результатах есть события, связанные с авторизациями	Фоновое задание отработало успешно. В результатах есть события, связанные с созданием объектов

7.1.2.1.4.1 Просмотр отчетов по проектам типа КН

Просмотр отчета осуществляется следующими способами:

- по последней итерации проекта (без предварительного просмотра результатов). Для загрузки архива на локальную ЭВМ необходимо нажать кнопку в строке проекта в основной рабочей области модуля «Сканер» (рис. 126);
- из списка отчетов по всем итерациям проекта (с возможностью предварительного

просмотра результатов) (рис. 210).

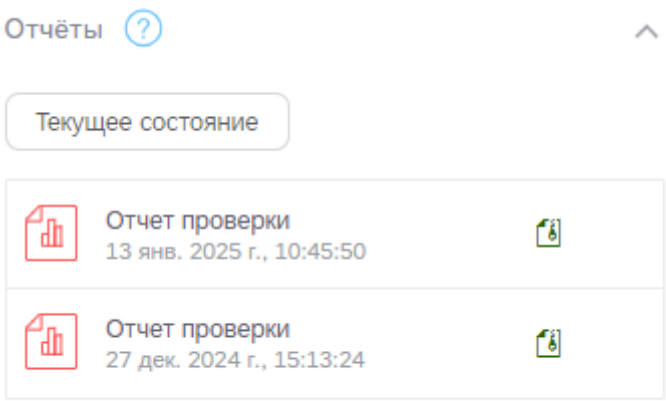


Рисунок 210 – Список отчетов по итерациям проекта типа КН

В окно найденных уязвимостей входят следующие поля (рис. 211):

- основная – содержит информацию о системе, профиле, количестве и критичности уязвимостей, дата и время сканирования;
- уязвимости – содержит поисковую строку, фильтр, список найденных уязвимостей;
- подробное описание уязвимости – содержит вкладку «Информация об уязвимости» с подробным описанием найденной уязвимости.

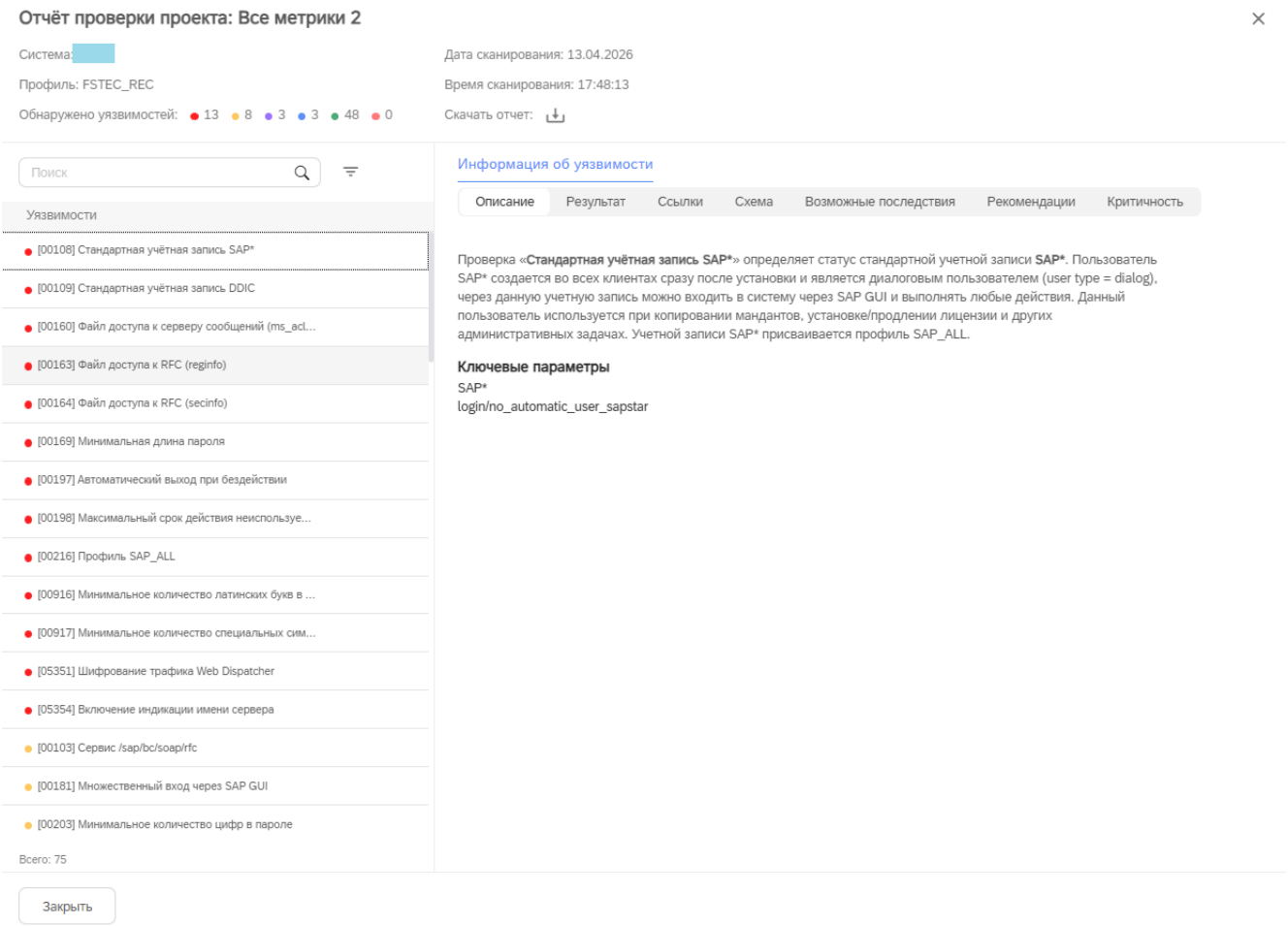


Рисунок 211 – Окно просмотра найденных уязвимостей проекта типа КН

Примечание. Доступен фильтр по следующим параметрам:

- критичность;
- ключевые параметры проверки.

Найденные уязвимости в окне просмотра могут приминать следующие статусы (см. рис. 211):

- красный цвет – высокая критичность;
- оранжевый цвет – средняя критичность;
- фиолетовый цвет – низкая критичность;
- синий цвет – информация;
- зеленый цвет – корректно;
- коралловый цвет – не определено.

Примечание. Статус «Не определено» присваивается тем уязвимостям, которые не соответствуют заданным параметрам критичности. Для просмотра параметров критичности необходимо обратиться к вкладке «Критичность» при подробном просмотре найденной уязвимости.

Вкладка «Информация об уязвимости» содержит следующие дочерние вкладки (см. рис. 211):

- результат – отчет с результатами проверки;

— описание – краткое описание проверки и ключевые параметры;
— ссылки – ссылки на внешние источники, которые применялись при создании проверки;
— схема – схема работы обнаруженной уязвимости;
— возможные последствия – указаны возможные последствия, если уязвимость не будет исправлена;
— критичность – указаны критичность проверки и название профиля проверок.

7.1.2.1.4.1.1 Аналитика для проектов типа КН

Для просмотра аналитики проектов типа КН необходимо нажать кнопку в соответствующей строке проекта в столбце «Аналитика» в основной рабочей области модуля «Сканер» (см. рис. 126).

В окно «Метрики проекта» (рис. 212) входят следующие поля:

— метрики проекта;
— распределение проверок по критичности – количество проверок каждого типа;
— сравнение итераций – сравнение двух последних итераций для каждого типа проверок;
— динамика уязвимостей – построения графиков для каждого типа проверок по результатам итерациям.

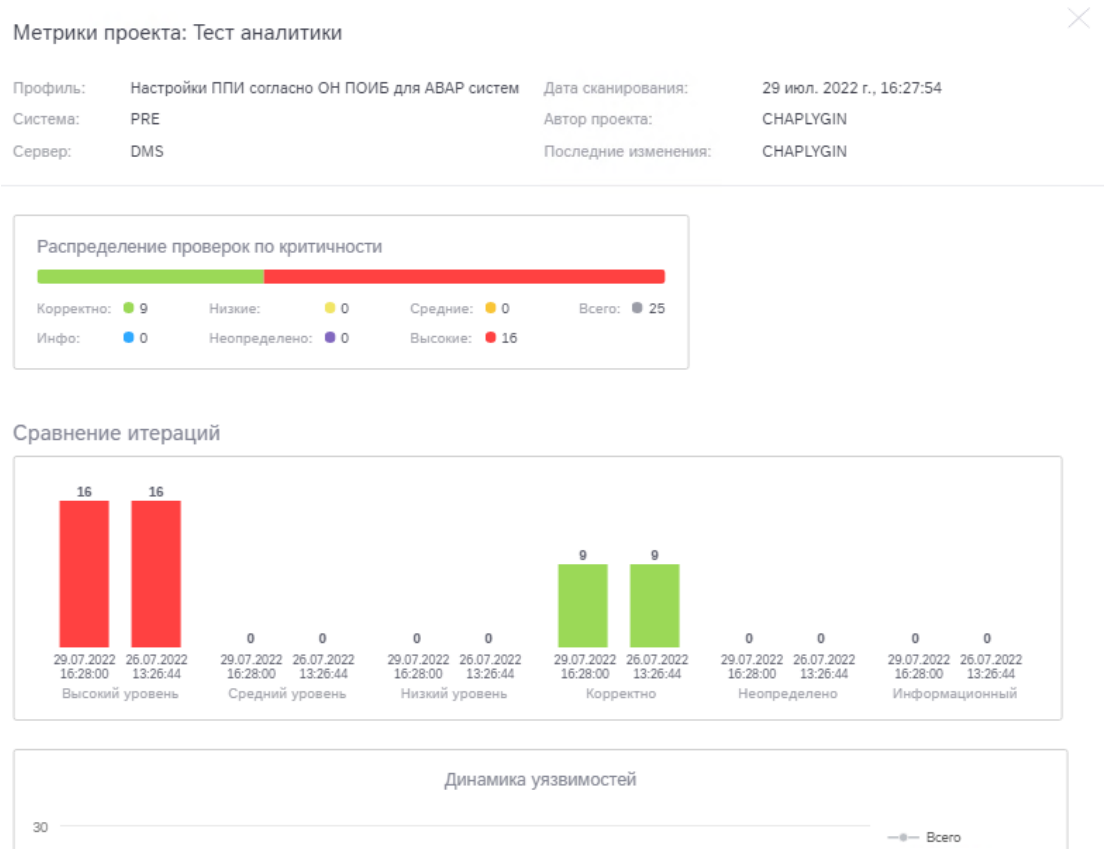


Рисунок 212 – Окно «Метрики проекта» для проектов типа КН

Примечания:

1. Аналитика производится для последних двух итераций проекта типа КН.
2. После смены профиля, статистика по метрикам будет рассчитана заново.

7.1.2.1.4.2 Просмотр отчетов по проектам типа КЦ

Процедуру просмотра отчетов по проектам типа КЦ осуществляют двумя способами:

1) По последней итерации проекта (без предварительного просмотра результатов).
   Чтобы просмотреть отчет по последней итерации проекта, необходимо нажать кнопку основной рабочей области модуля «Сканер» в соответствующей строке проекта в таблице со списком проектов (см. рис. 126).
   В поле «Отчет». Далее отчет можно выгрузить на локальный компьютер для просмотра в формате *.xlsx.
2) Из списка отчетов по всем итерациям проекта (с возможностью предварительного просмотра результатов).
   Чтобы просмотреть список отчетов по всем итерациям проекта, необходимо развернуть поле «Отчеты» в области параметров проекта (рис. 213).

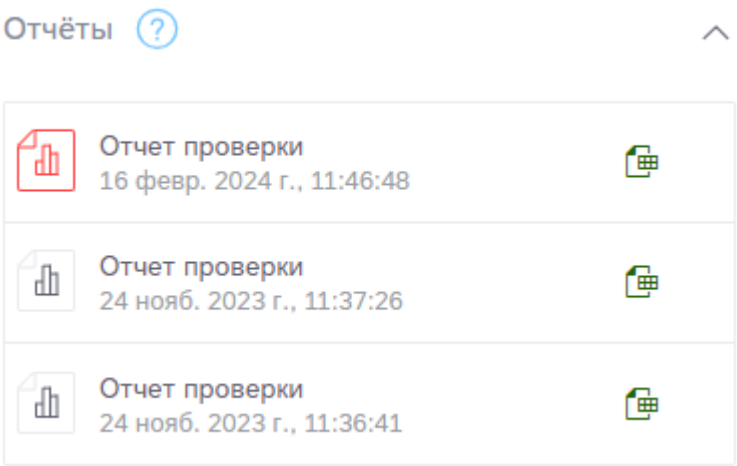


Рисунок 213 – Список отчетов по итерациям проекта типа КЦ

Для выполнения процедуры выгрузки отчета по итерации проекта без предварительного просмотра результата необходимо нажать кнопку *«Скачать Excel-отчет»* в соответствующей строке итерации проекта.

Данное окно аналогично окну «Текущее состояние объектов» для объектов КЦ (см. рис. 167), однако в нем отсутствует возможность проведения операции выравнивания объектов и снятия с контроля.

Для выгрузки отчета по итерации проекта на локальный компьютер в формате *.xlsx, необходимо нажать кнопку *«Скачать Excel-отчет».*

7.1.2.1.4.3 Просмотр отчетов по проектам типа ОД

Просмотр и выгрузка отчетов по проектам типа ОД осуществляются в окне «Текущее состояние объектов» для объектов проекта согласно подпункте. 7.1.2.1.2.4, описание действия – «Сохранение в отчет».

Поле «Анализ транзакций»

Страница «Анализ транзакций» предназначена для просмотра статистики удачных и неудачных запусков транзакции на агенте. Страница «Анализ транзакций» доступна после двух итераций.

На странице «Анализ транзакций» доступны следующие действия:

- просмотр списка транзакций, которые были запущены на агенте;
- просмотр подробной информации о транзакции;
- постановка транзакций на контроль;
- выгрузка шаблона;
- выгрузка отчета.

Страница «Анализ транзакций» состоит из следующего (рис. 214):

- области «Данные для выполнения запроса»;
- основная рабочая область.

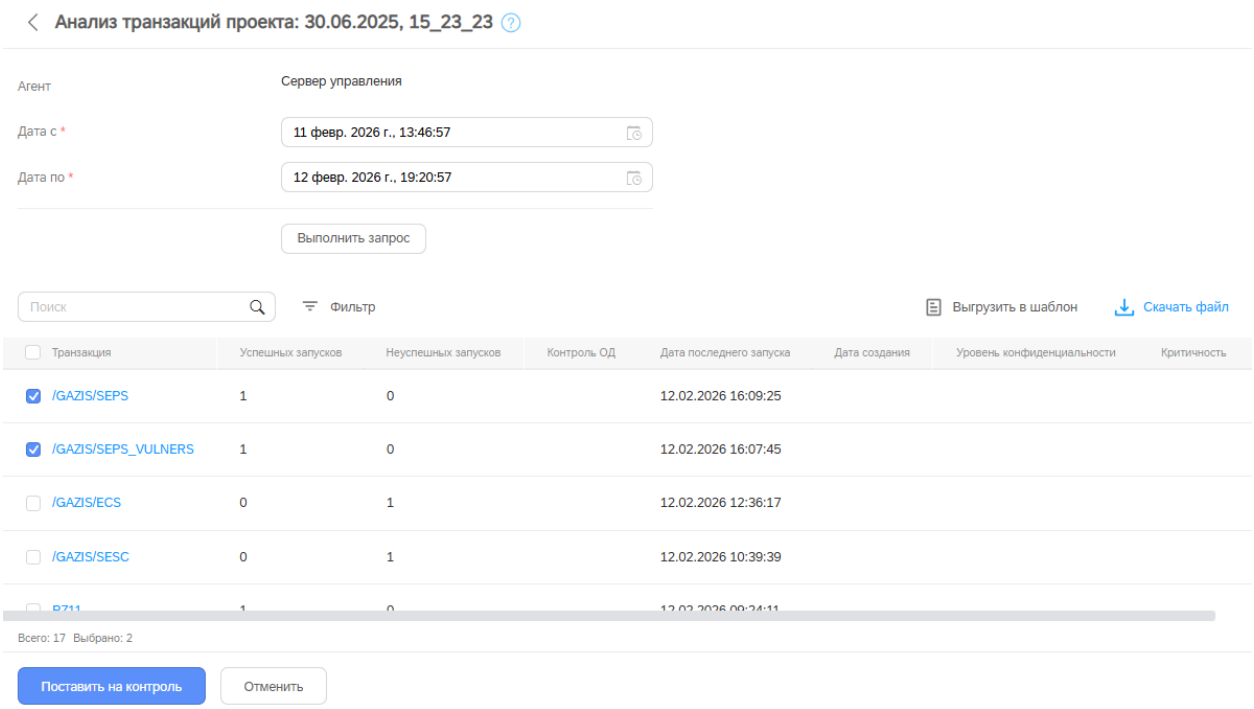


Рисунок 214 – Окно «Анализ транзакций»

Область «Данные для выполнения запроса» состоит из следующих полей:

- «Агент» – агент, на котором была запущена транзакция. Данное поле заполняется автоматически;
- «Дата с» – дата начала периода поиска;
- «Дата по» –- дата конца периода поиска;

Основная рабочая область состоит из столбцов:

- «Транзакция» – наименование транзакции;
- «Успешных запусков» – количество успешных запусков транзакций;
- «Неуспешных запусков» – количество неспешных запусков;
- «Контроль ОД» – метка о постановке транзакции на контроль;

— «Дата последнего запуска» – дата и время последнего запуска транзакции;
— «Дата создания» –дата создания новой транзакции. Стандартные транзакции SAP системы не имеют дату и время создания;
— «Уровень конфиденциальности» – уровень конфиденциальности объекта. Уровни конфиденциальности подразделяются на: PERSDATA – персональные данные, TRADESECR – коммерческая тайна, INTUSE – информация для служебного пользования, NLAI – информация неограниченного доступа, PERS_TRADE – персональные данные и коммерческая тайна.
— «Критичность» – уровень конфиденциальности объекта. Уровни критичности подразделяются на: ERROR, WARNING, INFORMATION.

Примечание. Поля «Дата с» и «Дата по» заполняются автоматически. Также пользователю доступен выбор периода начала и конца периода поиска.

Просмотр подробной информации по транзакции

Модальное окно «Подробная информация» состоит из следующих областей (рис.215):

— «Информационной» – содержит информацию об агенте, транзакции, метки «Контроль ОД», уровень конфиденциальности, критичность;
— «Основной рабочей» – содержит информацию о событии, статусе запуска, критичности, манданте, дате, пользователе, терминале.

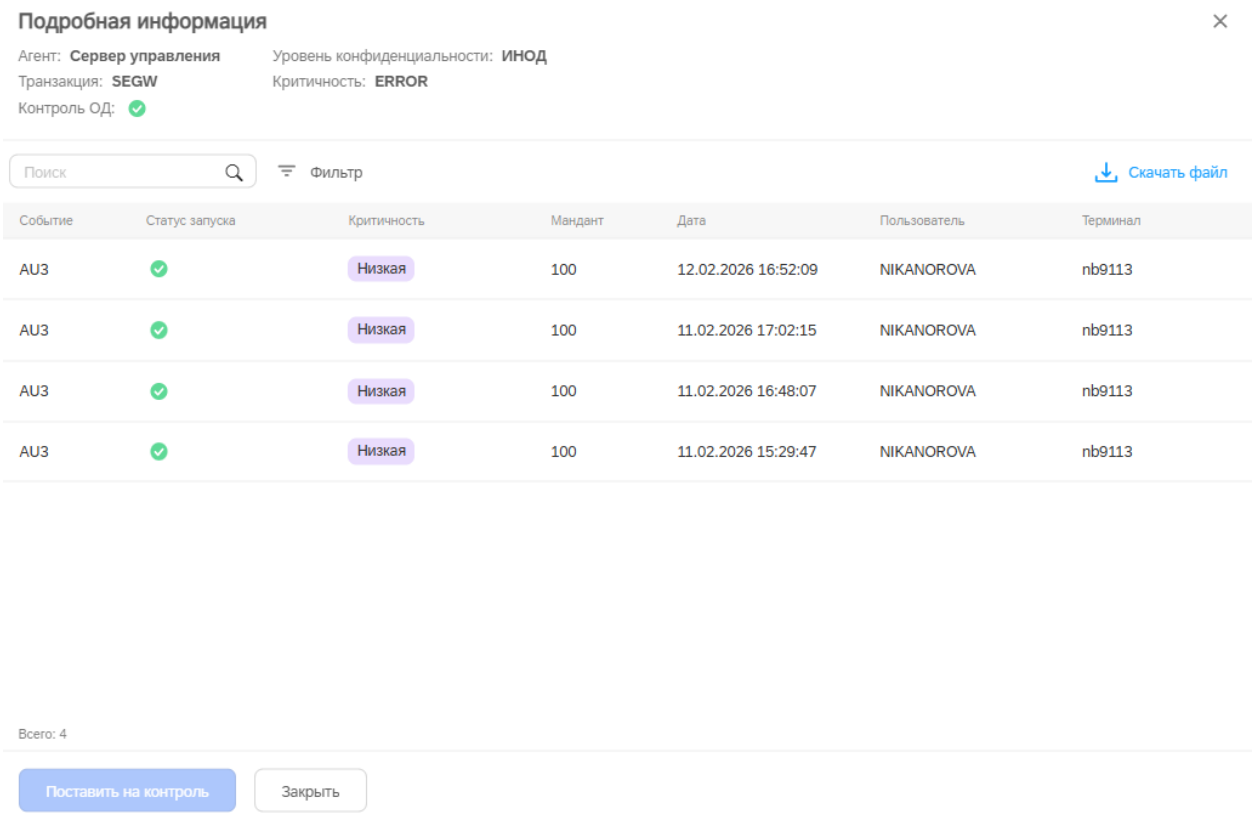


Рисунок 215 – Модальное окно «Подробная информация»

Основная рабочая область состоит из следующих столбцов:

— «Событие»;

— «Статус запуска»;
— «Критичность»;
— «Мандант»;
— «Дата»;
— «Пользователь»;
— «Терминал».

В модальном окне «Подробная информация» пользователю доступны следующие действия:

— постановка транзакции на контроль;
— выгрузка отчёта по транзакции.

В модальном окне «Подробная информация» доступен поиск событий с помощью кнопки «Фильтр». Доступен поиск по следующим параметрам:

— «Событие»;
— «Статус»;
— «Критичность»;
— «Мандант»;
— «Дата последнего запуска с»;
— «Дата последнего запуска по»;
— «Терминал».

Выполнение запроса

Для выполнения запроса необходимо выполнить следующие действия:

1) Заполнить дату начала и конца периода.
2) Нажать кнопку «Выполнить запрос».

После выполнения запроса пользователю доступен фильтр по следующим событиям:

— контроль ОД;
— Дата последнего запуска с;
— Дата последнего запуска по.

Постановка транзакций на контроль

Постановка транзакций на контроль осуществляется следующими способами:

— во вкладке «Объекты»;
— через кнопку «поставить на контроль»;
— в модальном окне «Подробная информация».

Примечание. Снятие транзакции с контроля не предусмотрено.

Для постановки транзакции на контроль во вкладке «Объекты» необходимо выполнить следующие действия:

1) Выполнить запрос.
2) Поставить флаг напротив транзакций, нажать кнопку «Выгрузить в шаблон».
3) Заполнить загруженную таблицу.
4) Выбрать вкладку «Объекты», нажать на поле «Выберите файл для загрузки», выбрать файл, нажать кнопку «Загрузить из шаблона».
5) Нажать кнопку «Сохранить».

Для постановки транзакции на контроль через кнопку «Поставить на контроль необходимо выполнить следующие действия:

1) Выполнить запрос.
2) Поставить флаг напротив транзакций, нажать кнопку «Поставить на контроль».
3) Выбрать уровень конфиденциальности и критичность в окне «Поставить на контроль». Нажать кнопку «Применить» (рис. 216).

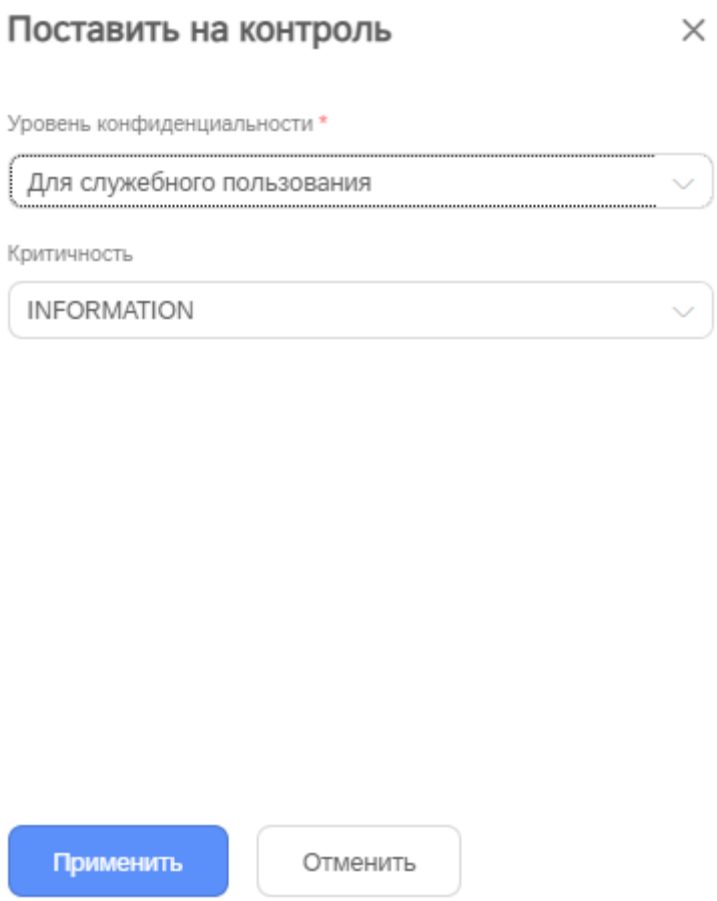


Рисунок 216 – Окно «Поставить на контроль»

7.1.2.1.4.4 Просмотр отчетов по проектам типа АВ

Просмотр отчетов по проектам типа АВ не предусмотрено.

7.1.2.1.4.5 Просмотр историй итераций по проектам типа СО

Просмотр историй итераций по проектам типа СО осуществляется во вкладке «Объекты» (рис. 217).

Для просмотра отчетов по проектам типа СО необходимо раскрыть вкладку «Объекты», нажать кнопку *«Текущее состояние»* (рис. 217, 218).

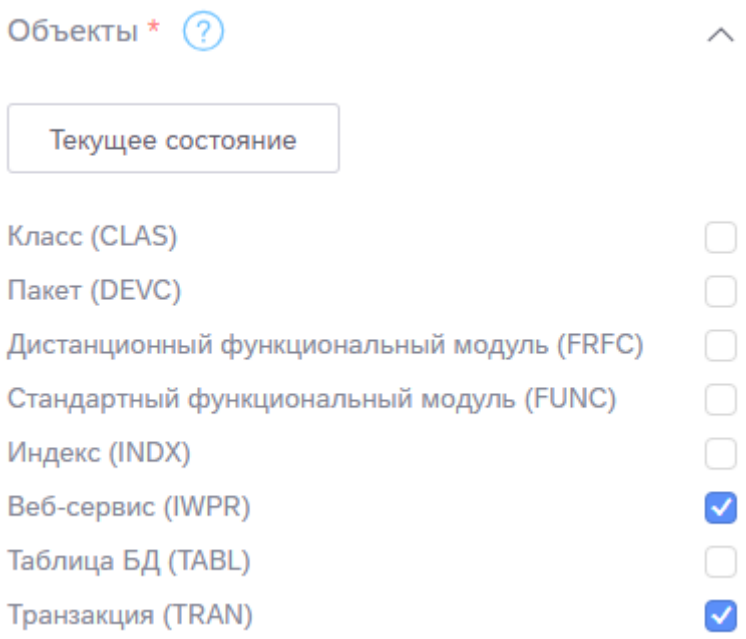


Рисунок 217 – Вкладка «Объекты» для проектов типа СО

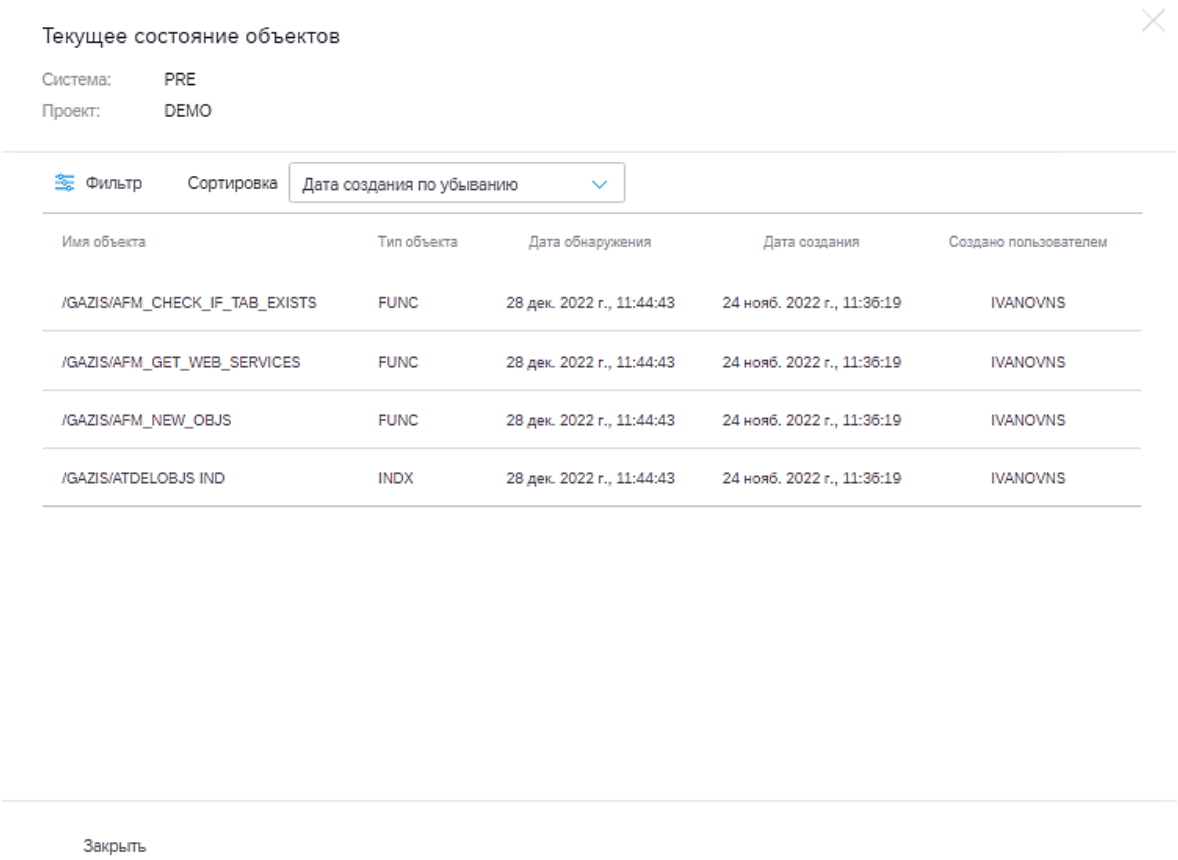


Рисунок 218 – Окно «Текущее состояние объектов» для проектов типа СО

7.1.2.1.5 Индикация проектов

Значения цветов индикаторов на иконке (см. рис. 137) в столбце «Тип» проекта приведены в таблице 11.

Таблица 11 – Значения цветов индикаторов в столбце «Тип» проекта

	Цвет индикатора			
	Тип проекта			
События индикации	КН	– ошибка RFC - соединения (ошибки получения данных с агента); – выявлены уязвимости с высокой степенью критичности; – невозможно определить статус анализа (ошибки фоновых заданий); – ошибка лицензии	Средняя степень критичности полученных результатов	Критичных результатов нет (данные в наличии, анализ проведен)
	КЦ	– ошибка RFC - соединения (ошибки получения данных с агента); – ошибка лицензий; – невозможно определить статус анализа (ошибки фоновых заданий); – выявлено изменение контрольных сумм объектов	Данная индикация не применяется	Отсутствуют изменения контрольных сумм (данные в наличии, анализ проведен)
	ОД	– ошибка RFC - соединения (ошибки получения данных с агента); – ошибка лицензии	Обнаружены события доступа к объектам ограниченного доступа	События отсутствуют (фоновое задание отработало)
	АВ	– ошибка RFC – соединения (ошибки получения данных с агента); – ошибка лицензии	Обнаружены события обращений к авторизациям	События отсутствуют (фоновое задание отработало)

	СО	– ошибка RFC – соединения (ошибки получения данных с агента); – ошибка лицензии	Обнаружены новые объекты	События отсутствуют (фоновое задание отработало)

7.1.2.1.6 Полномочия доступа к функциям модуля

Полномочия доступа администратора ПК «SafeERP Security Suite» к функциям модуля «Сканер» согласно типу проекта:

1) Для проектов типа КН:
— создание проекта (контроль параметров безопасности);
— изменение проекта (контроль параметров безопасности);
— удаление проекта (контроль параметров безопасности);
— принудительный запуск проекта (контроль параметров безопасности);
— просмотр истории итераций (контроль параметров безопасности);
— просмотр текущего состояния в отчете;
— сохранение отчета по итерации в файл;
— активация «Передача данных в SIEM»;
— активация метки ознакомления;
— изменение профиля сканирования для КН.
2) Для проектов типа КЦ:
— создание проекта;
— изменение проекта;
— удаление проекта;
— принудительный запуск проекта;
— просмотр истории итераций;
— просмотр текущего состояния;
— просмотр объектов контроля;
— сохранение отчета по объектам в файл;
— снятие объектов с контроля;
— просмотр изменений объекта с помощью метки «Спец. контроль»;
— выравнивание объектов;
— загрузка объектов из шаблона.
3) Для проектов типа ОД:
— создание проекта;
— изменение проекта;
— удаление проекта;
— принудительный запуск проекта (если он не по расписанию);
— просмотр истории итераций;
— просмотр текущего состояния объектов;
— просмотр объектов контроля;

— сохранение отчета по объектам в файл;
— снятие объектов с контроля;
— возврат объектов на контроль;
— сохранение шаблона с данными (CSV);
— загрузка объектов из шаблона.
— загрузка объектов из шаблона;
— активация «Передача данных в SIEM».

4) Для проектов типа AB:

— создание проекта;
— изменение проекта;
— удаление проекта;
— принудительный запуск проекта (если он не по расписанию);
— просмотр истории итераций.

5) Для проектов типа CO:

— создание проекта;
— изменение проекта;
— удаление проекта;
— принудительный запуск проекта (если он не по расписанию);
— активация «Передача данных в SIEM».

7.1.2.2 Модуль «Анализ кода»

Веб-интерфейс модуля «Анализ кода» (программный модуль SafeERP Code Security) предназначен для настройки параметров запуска проверки программных объектов на языке ABAP в настроенных для анализа системах, активации самой операции анализа и получения отчетов. Элементы основной рабочей области «Анализ кода» представлены на рис. 127.

Основные типы процедур анализа, которые могут быть применены для проверки систем в данном модуле:

— АК – анализ кода ABAP на наличие небезопасного кода;
— ИК – анализа кода на подсчет количественных характеристик (состав пакета, пакеты, объекты, количество строк кода, частота транспортных запросов, количество комментариев в коде, процент комментариев, динамику изменения количества кода).

В основной рабочей области «Анализ кода» доступны следующие действия:

1) Поиск проекта в списке проектов.
2) Добавление проекта.
3) Просмотр/редактирование/запуск/прерывание/удаление проекта.
4) Просмотр отчетов.
5) Просмотр метрик безопасности программного кода.

7.1.2.2.1 Поиск проекта

Поиск проекта выполняют через формы поиска (фильтры) в основной рабочей области «Анализ кода». Доступные варианты поиска проекта (рис. 219):

- по названию агента (поле «Агент»);
- по названию проекта (поле «Название»).

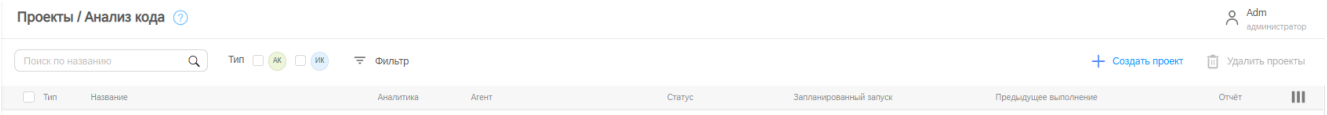


Рисунок 219 – Область поиска проекта

Чтобы начать процедуру поиска проекта через форму поиска по названию агента, необходимо нажать кнопку *«Фильтр»*, поставить ☑ флаг напротив агента, нажать кнопку *«Применить»* (рис. 220).

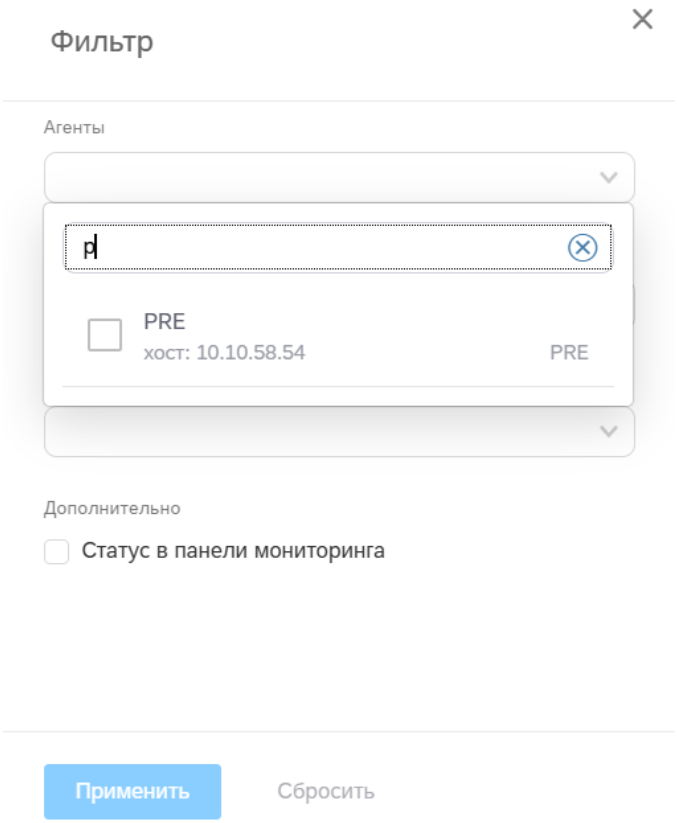


Рисунок 220 – Поиск проекта по названию агента

Результат поиска проекта по названию агента представлен на рис. 221.

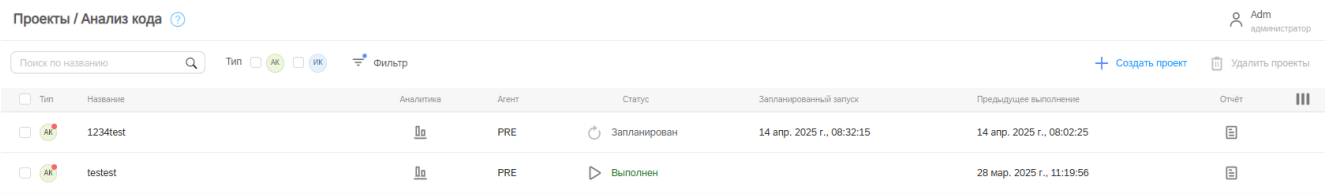


Рисунок 221 – Результат поиска проекта по названию агента

Чтобы начать процедуру поиска проекта по его названию (рис. 222), необходимо задать символьную маску в соответствующей форме поиска.

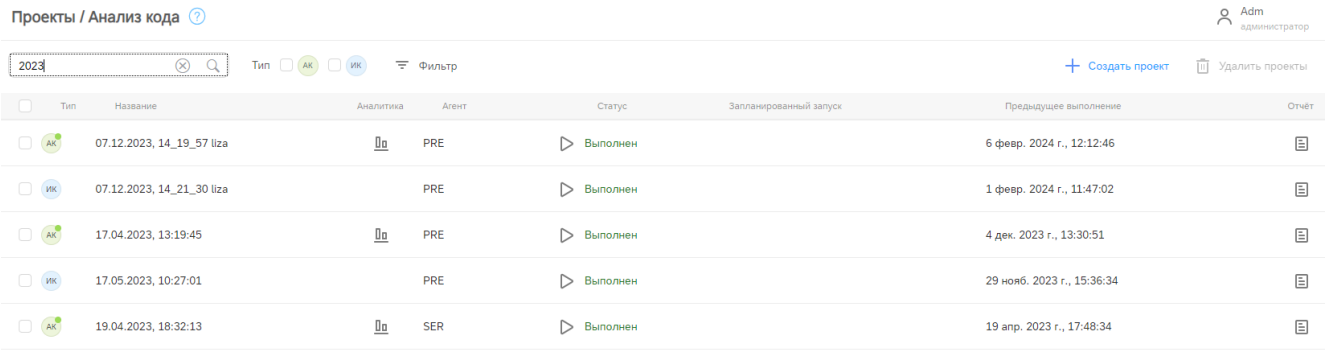


Рисунок 222 – Результат поиска проекта по его названию

При вводе маски агента или проекта в соответствующем поле поиска необходимо нажать кнопку *«Поиск»*. Для сброса введенных данных предусмотрена кнопка *«Сбросить»*.

Для сброса выбранных значений сразу во всех формах поиска предусмотрена кнопка *«Отменить»*.

7.1.2.2.2 Создание проекта

Чтобы создать проект, необходимо нажать кнопку *«+Создать проект»* в основной рабочей области «Анализ кода» (см. рис. 127) Функция добавления проекта предоставляется только пользователям с полномочиями на администрирование ПК «SafeERP Security Suite».

При нажатии кнопки добавления проекта необходимо выбрать тип проекта и разворачивается окно выбора параметров проекта (рис. 223).

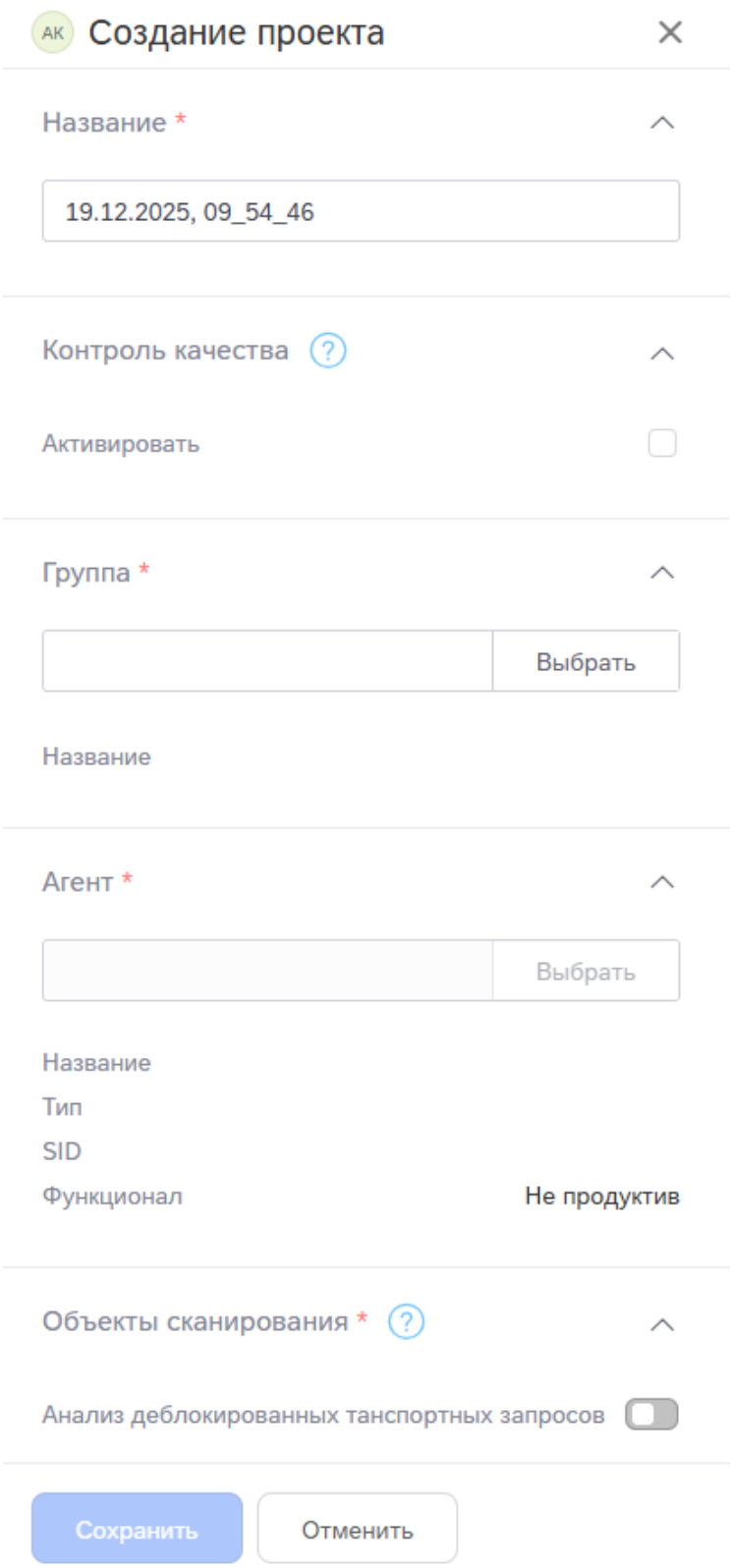


Рисунок 223 – Окно выбора параметров проекта

После выбора параметров проекта необходимо нажать кнопку сохранения проекта *«Сохранить»*. Кнопка сохранения проекта станет активной только в случае определения всех параметров проекта.

Обязательные для определения параметры проекта приведены в таблице 12.

Таблица 12 – Обязательные для определения параметры проекта

Тип проекта	Название	Группа	Агент	Объекты	Профили	Параметры запуска
АК	+	+	+	+	+	+
ИК	+	+	+	+	+	+

7.1.2.2.2.1 Выбор названия проекта

Для выбора названия проекта необходимо выполнить действия согласно подпункту 7.1.2.1.2.1 Выбор

7.1.2.2.2.2 Выбор группы агента

Для выбора группы агента необходимо выполнить действия согласно подпункту 7.1.2.1.2.2 Выбор

7.1.2.2.2.3 Выбор агента

Для выбора агента необходимо выполнить действия согласно подпункту 7.1.2.1.2.3

Примечание. В модуле «Анализ кода» используются агенты типа ABAP.

7.1.2.2.2.4 Сравнение итераций

Поле «Сравнение итераций» доступно для проектов типа АК с 2-мя и более количеством итераций.

Примечание. Для сравнения итерации необходимо соблюдать временные промежутки. В качестве первой итерации необходимо выбрать более раннюю итерацию.

Для сравнения итераций необходимо выполнить следующие действия:

1) Раскрыть вкладку «Сравнение итераций» (рис. 224).

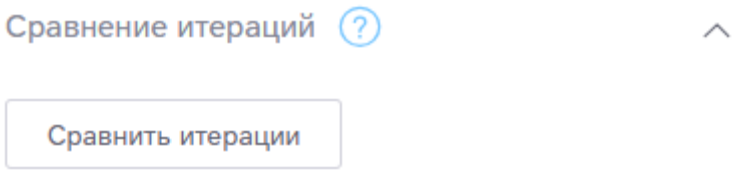


Рисунок 224 – Поле «Сравнение итераций»

2) Нажать кнопку *«Сравнить итерации»* (рис. 224).
3) Нажать кнопку *«Сравнить»* в окне «Сравнение итераций» (рис. 225).

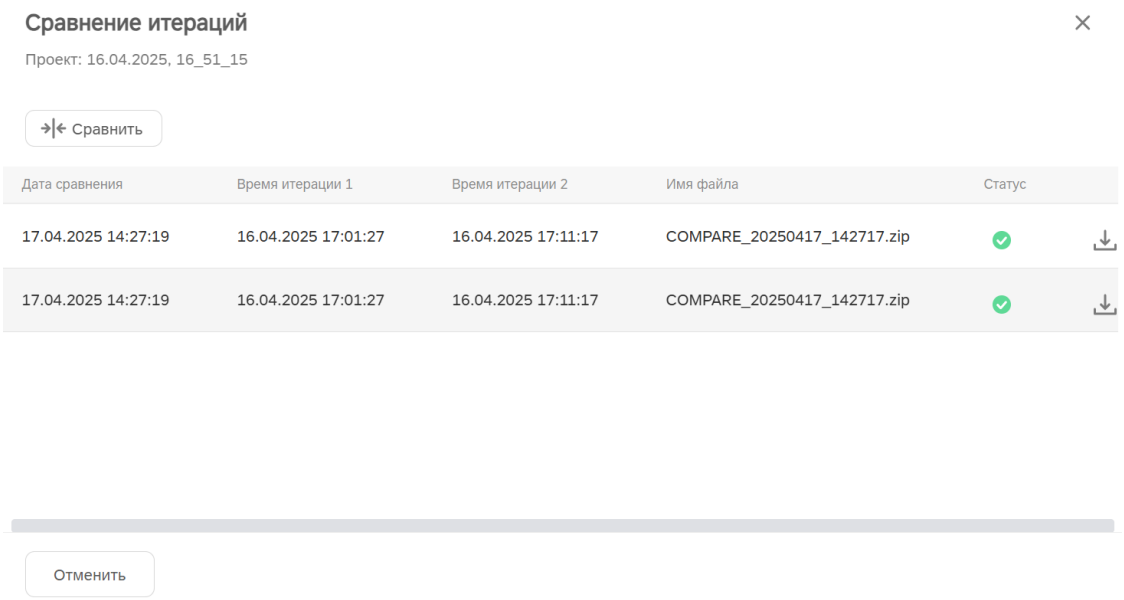


Рисунок 225 – Окно «Сравнение итераций»

4) Выбрать 2 итерации в окне «Сравнить итерации» (рис. 226).

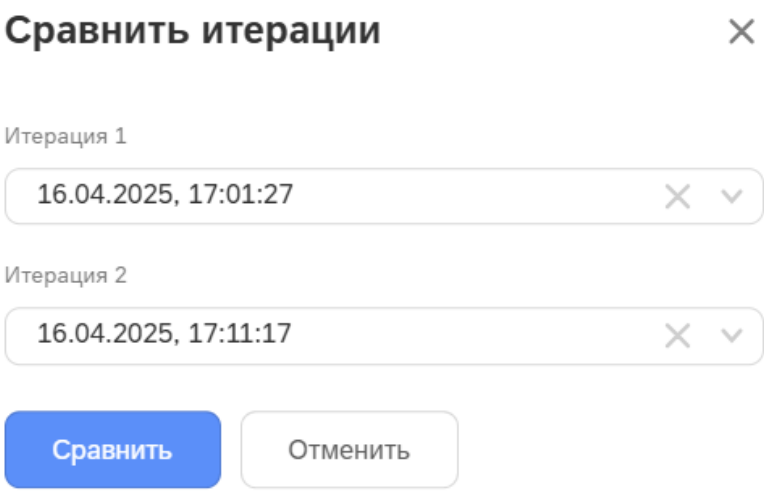


Рисунок 226 – Окно «Сравнить итерации»

5) Нажать кнопку *«Сравнить»*.

Для загрузки результатов итераций в формате *zip на локальную ЭВМ необходимо нажать кнопку .

В архиве формата *zip содержатся следующие файлы:

- OBJECT.XLSX – изменение количества и качества объектов;
- ITERATION.XLSX – общие изменения в настройках запуска проекта;
- FLAW.XLSX – изменения найденных уязвимостей (обнаружены, изменены);
- CHECKS.XLSX – изменения по проверкам.

7.1.2.2.2.5 Учет импортированных запросов

Поле «Учет импортированных запросов» доступно для проектов типа ИК. Используется для считывания количества импортированных запросов.

Для активации учета импортированных запросов необходимо уставить флаг напротив активировать во вкладке «Учет импортированных запросов» и выбрать начало и конец периода, нажать кнопку *«Сохранить».*

7.1.2.2.2.6 Контроль качества

Поле «Контроль качества» доступно для проектов типа АК. Предназначено для анализа кода заданными характеристика.

Для активации контроля качества необходимо поставить флаг напротив активировать, выбрать шаблон из списка, нажать кнопку *«Сохранить».*

После прохождения анализа предоставляется возможность просмотр результата. Для просмотра результатов анализа необходимо выбрать метрику в поле «Контроль качества».

Примечание. Уязвимости со статусом «Закрыто» не учитываются при подсчете метрик в поле «Контроль качества».

Статусы метрик

В поле «Контроль качества» доступны следующие статусы метрик:

- «Пройден» – проект соответствует заданным метрикам;
- «Не пройден» – проект не соответствует заданным метрикам;
- невозможно рассчитать метрику.

Для метрик «Безопасность», «Производительность», «Удобство сопровождения» доступны следующие статусы:

- A – уязвимости отсутствуют;
- B – обнаружены уязвимости с категорией критичности «Информация»;
- C – обнаружены уязвимости со степенью критичности «Низкая»;
- D – обнаружены уязвимости со степенью критичности «Средняя»;
- E – обнаружены уязвимости со степенью критичности «Высокая».
- Для метрики «Чистота кода» доступен процент чистоты кода.

Примечания:

1. Метрика «Чистота кода» вычисляется по следующей формуле:

$$100 - \frac{N}{M} \times 100$$

где N – количество найденных недостатков;

M – количество просканированных строк кода

2. Для метрики «Чистота кода» доступен ввод целочисленного значения от 0 до 100.

Статусы контроля качества

В поле «Контроль качества» доступны следующие статусы контроля качества:

- «Пройден» – проект соответствует заданным метрикам;
- «Не пройден» – проект не соответствует заданным метрикам.

7.1.2.2.2.7 Критические объекты

Поле «Критические объекты» доступно для проектов типа ИК. Используется для просмотра, утверждения объектов со степенью критичности «Высокая».

Для анализа критических объектов необходимо выполнить следующие действия:

1) Нажать кнопку «Выбор профиля».
2) Выбрать профиль в открывшемся окне.
3) Уставить флаг ☑ напротив активировать и выбрать.
4) Нажать кнопку *«Сохранить»*.

Для того, чтобы объекты повторно не попадали в результаты анализа, их необходимо утвердить. Для утверждения объектов необходимо выполнить следующие действия:

1) Нажать кнопку «Текущее состояние» в поле «Критические объекты».
2) В окне «Текущее состояние» выбрать тип объектов «Не утвержденные» (рис. 227).

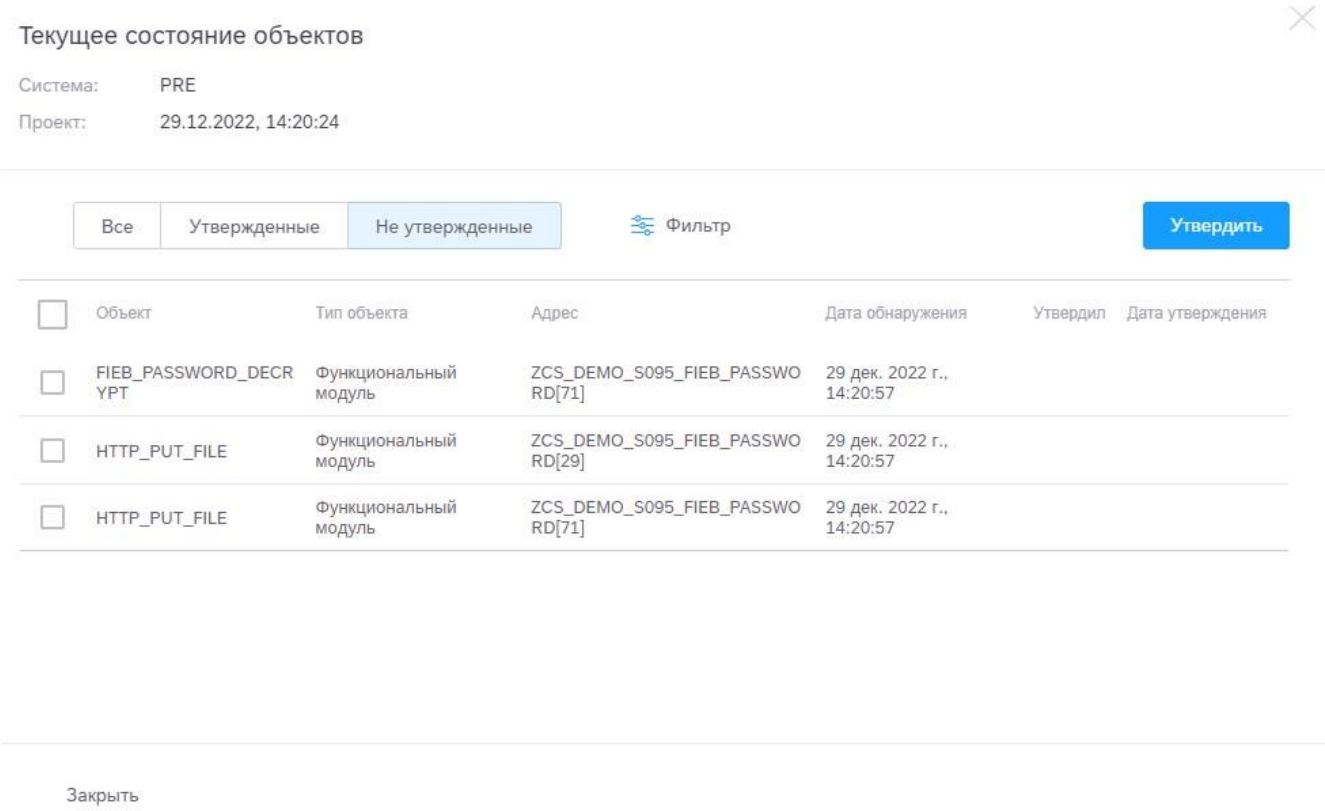


Рисунок 227 – Вкладка «Не утвержденные объекты»

3) Уставить флаг ☑ напротив объекта.
4) Нажать кнопку «Утвердить».

7.1.2.2.2.8 Выбор объектов

Для проектов типа АК объектами анализа могут быть только программные объекты ABAP-агента:

— пакет;
— программа;
— класс;

— метод;
— группа функций;
— функциональный модуль;
— pdf-интерфейс (включая pdf-формуляр);
— SAP-query (запрос);
— SAP-query (группа пользователей);
— проект LSMW;
— подпроект LSMW;
— объект LSMW;
— транспортный запрос;
— точки расширения (Реализация).

Для проекта типа ИК объектами анализа могут быть только программные объекты ABAP-агента:

— пакет.

Процедура выбора объектов анализа доступна только после определения группы для агента и самого агента. Работа с объектами анализа осуществляется в поле «Объекты сканирования» (рис. 228).

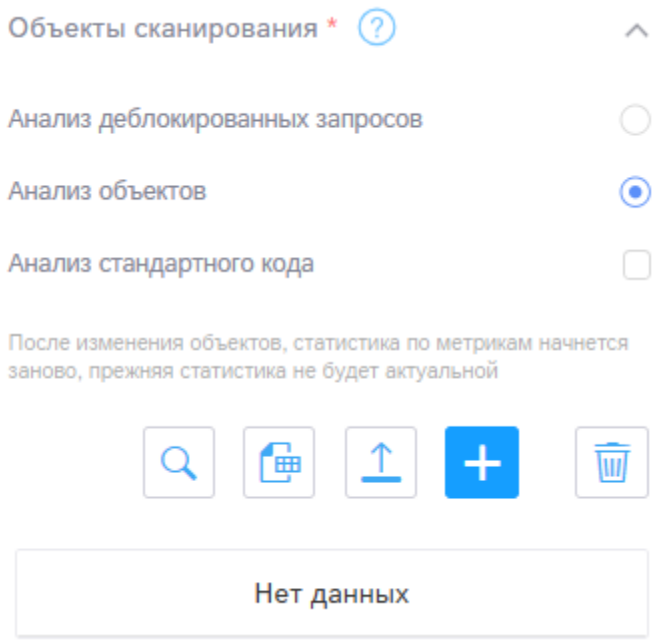


Рисунок 228 – Поле выбора объектов анализа

Для работы с объектами анализа доступны следующие действия:

1) Поиск объектов. Для активации поиска объектов необходимо нажать кнопку . В открывшемся окне (рис. 229) ввести название пакета или выбрать тип объекта. Для добавления объектов в проект, необходимо уставить флаг напротив объекта, нажать кнопку *«Добавить в проект»*.
   Примечание. При выборе типа объектов «Транспортный запрос» анализируются

все объекты, которые входят в транспортный запрос. Список проанализированные объектов находится в файле «OBJECT.XLSX».

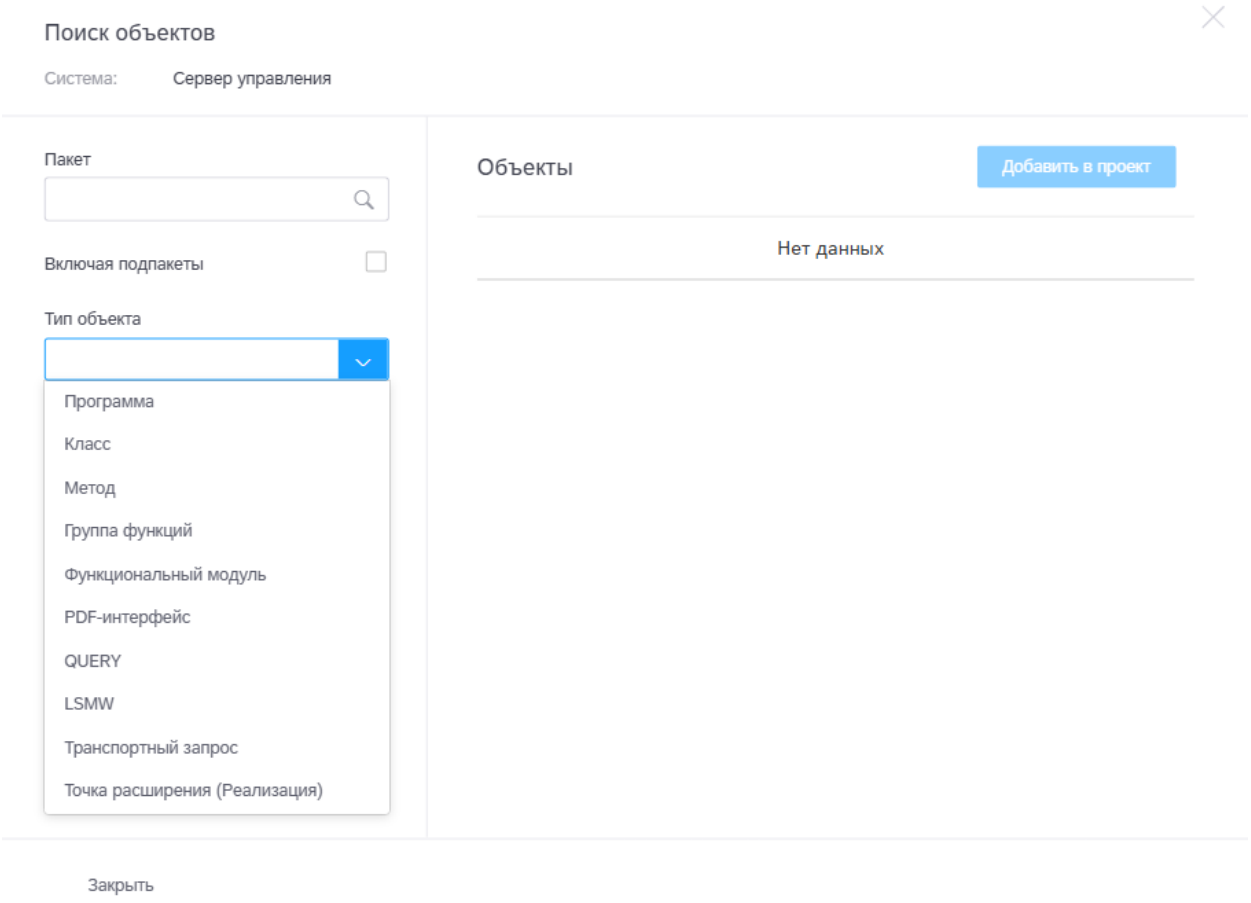


Рисунок 229 – Окно «Поиск объектов»

2) Получить шаблон. Чтобы получить форму для внесения данных по объектам анализа, необходимо нажать соответствующую кнопку *«Получить шаблон».* Шаблон создан в Excel-формате с набором вкладок согласно списку объектов. В первом столбце шаблона (в каждой вкладке) необходимо указать маски для проверяемых в проекте объектов. Шаблон для указания масок объектов представлен на рис. 230 и 231.

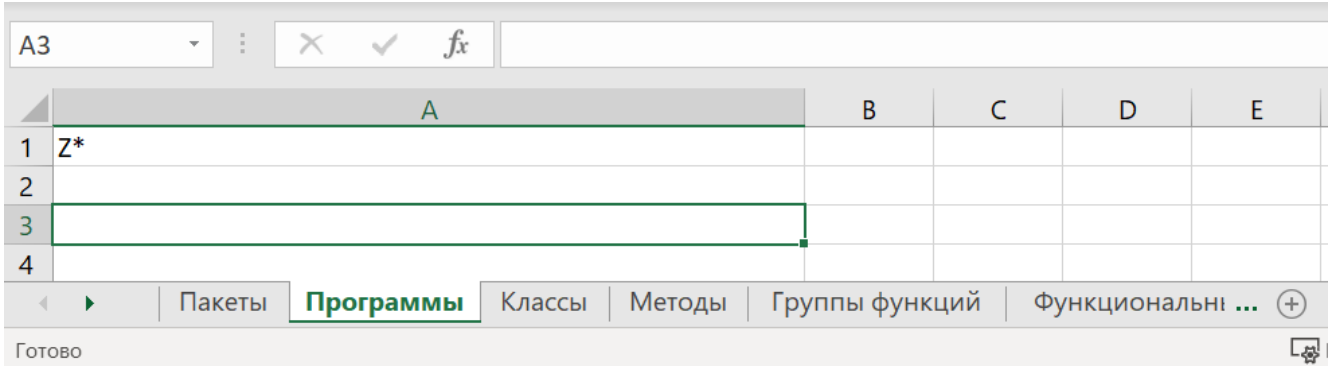


Рисунок 230 – Шаблон для масок объектов проекта типа АК

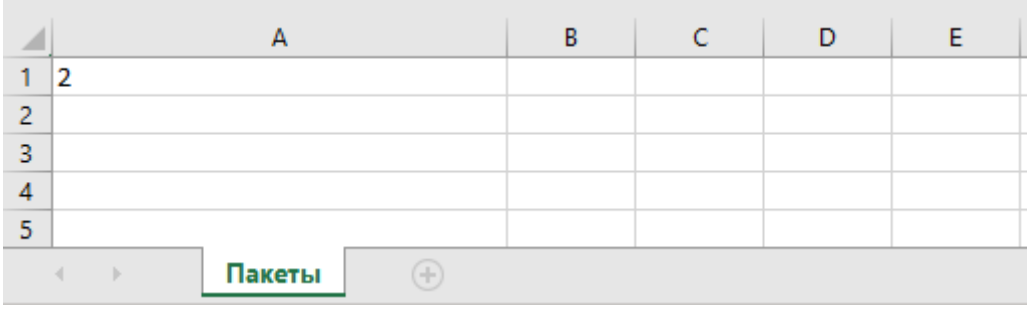


Рисунок 231 – Шаблон для масок объектов проекта типа ИК

3) Загрузить шаблон. Чтобы загрузить подготовленный шаблон с масками объектов, необходимо нажать соответствующую кнопку *«Загрузить шаблон»* (рис. 232).

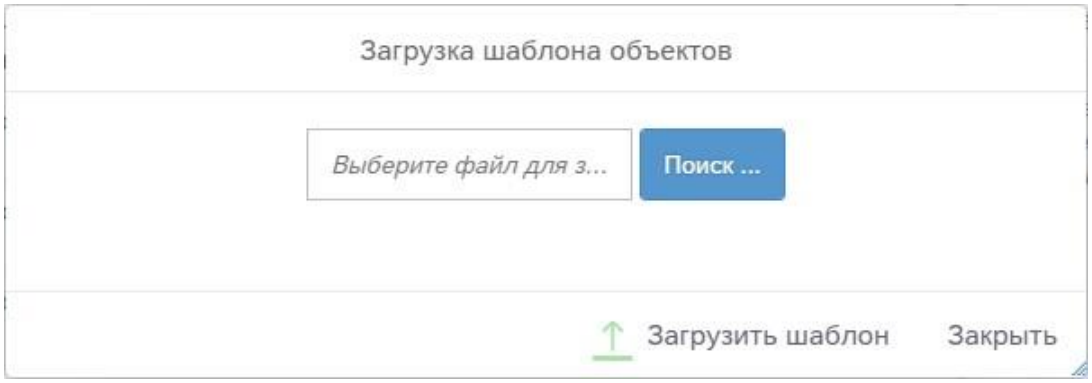


Рисунок 232 – Загрузка шаблона с масками объектов

4) Добавить маску объекта. Чтобы добавить маску объекта, необходимо нажать соответствующую кнопку *«Добавить маску объекта»*. Для выбора объекта из списка необходимо нажать на его название левой кнопкой мыши. Появится поле для указания маски объекта в области «Маска объекта» (рис. 233).

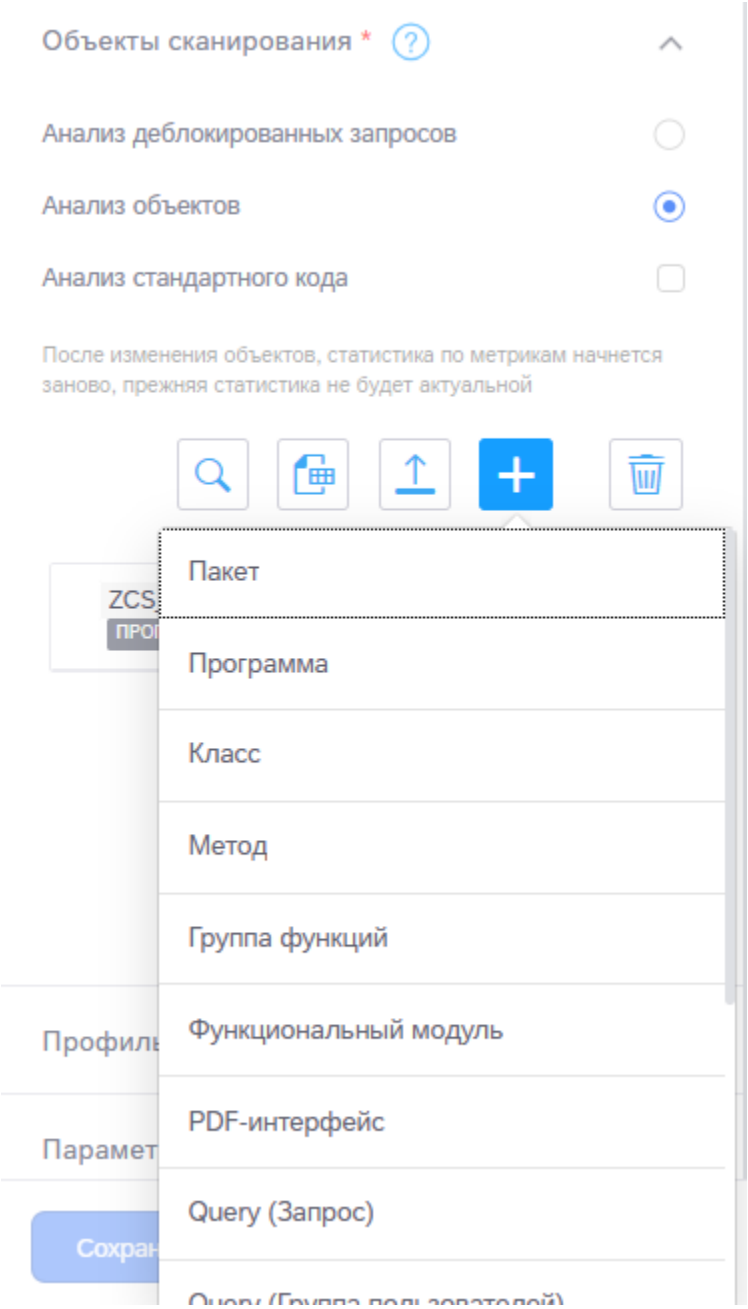


Рисунок 233 – Определение перечня и маски объектов

5) Очистить маски объектов.

Чтобы отредактировать данные и полностью очистить поля с масками объектов, необходимо нажать кнопку *«Очистить маски объектов»*.

В случае просмотра параметров уже созданного проекта, в поле «Объекты» будет доступен для просмотра и редактирования список объектов для анализа, установленный для данного проекта. Чтобы выполнить просмотр или отредактировать список объектов проекта, необходимо нажать левой кнопкой мыши на строчку «Объекты» соответствующего проекта в окне выбора параметров проекта (рис. 234).

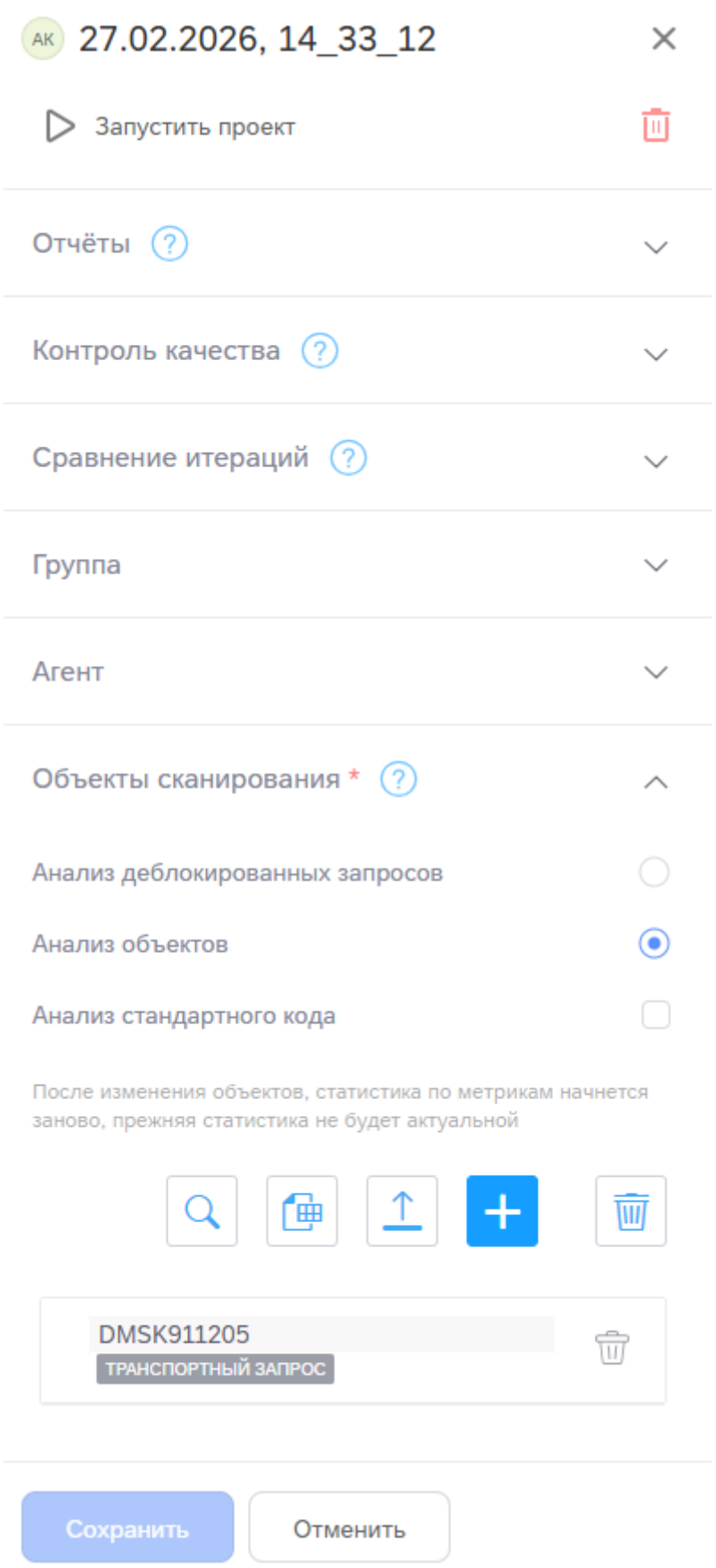


Рисунок 234 – Просмотр и редактирование объектов анализа в созданном проекте типа АК

Анализ транспортных запросов

В ПК «SafeERP Security Suite» реализована функциональность по анализу транспортных запросов.

Для анализа транспортных запросов необходимо выполнить следующие действия:

1) Нажать кнопку «Поиск объектов» в поле «Объекты сканирования» (см. рис. 233).
2) Выбрать тип объекта «Транспортный запрос» в окне «Поиск объектов» (рис. 235).

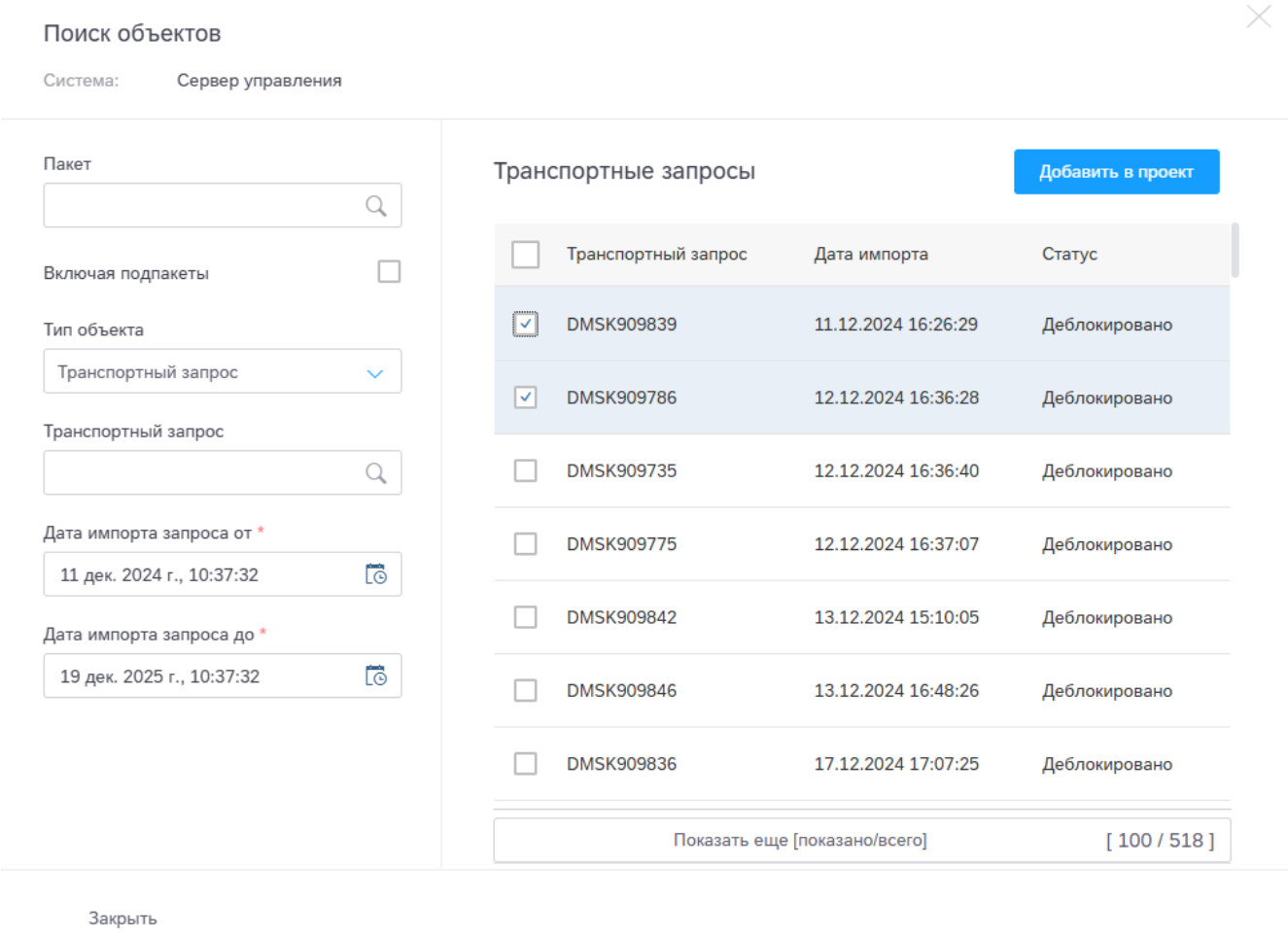


Рисунок 235 – Окно «Поиск объектов»

3) Ввести данные в поля «Дата импорта запроса от» и «Дата импорта запроса до» (см. рис. 235).
4) Нажать кнопку «Поиск» в поле «Транспортный запрос» (см. рис. 235).
5) Установить флаг напротив транспортных запросов (см. рис. 235).
6) Нажать кнопку «Добавить в проект» в окне «Поиск объектов» (см. рис. 235).
7) Нажать кнопку «Сохранить».

Примечания:

1. Доступно сканирование транспортных запросов со следующими статусами:

— «Деблокировано»;
— «Изменяемо».

2. При выборе типа объектов «Транспортный запрос» анализируются все объекты, которые входят в транспортный запрос. Список проанализированные объектов находится в файле «OBJECT.XLSX».

Анализ деблокированных транспортных запросов

Для активации анализа транспортных запросов необходимо установить переключатель «Анализ деблокированных транспортных запросов».
После активации область «Анализ стандартного кода» и область выбора объектов скрываются.
Функциональность используется для:

— выявления небезопасного ABAP-кода, предназначенного для переноса по ландшафту системы;
— анализа деблокированных транспортных запросов.

Примечания:

1. Транспортные запросы, прошедшие анализ, учитываются во всех проектах, где активирована данная настройка.
2. Каждый транспортный запрос анализируется только один раз.
3. Во вкладке «Анализ деблокированных транспортных запросов» выполняется анализ всех деблокированных запросов в системе.
4. При первом запуске анализируются запросы за последние 24 часа. При повторных запусках анализируются только запросы, деблокированные после предыдущей итерации.

Анализ стандартного кода

Стандартный код — это код, поставляемый компанией SAP и написанный на языке ABAP.
Стандартный код не подлежит изменению.
Функциональность «Анализ стандартного кода» позволяет сканировать объекты, предоставленные вендором.
Для активации анализа необходимо установить флаг напротив параметра «Активировать».

7.1.2.2.2.9 Выбор профиля проекта

Профиль проекта предназначен для определения набора проверок (сценариев), которые будут применены к выбранной агент-системе для анализа программного кода.
Чтобы выбрать профиль из предварительно настроенного списка, необходимо нажать кнопку *«Выбор профиля»* (рис. 236).

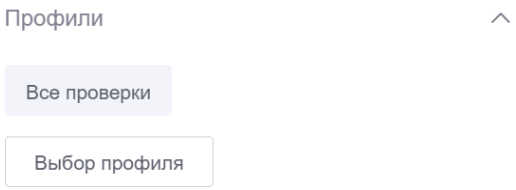


Рисунок 236 – Настройка профилей проектов типа АК

В поле выбора доступна функция поиска по названию профиля. Для добавления профиля в проект необходимо выделить профили (нажать на наименование профиля). Для отмены выбора профиля необходимо нажать кнопку *«Отменить»* (рис. 237).

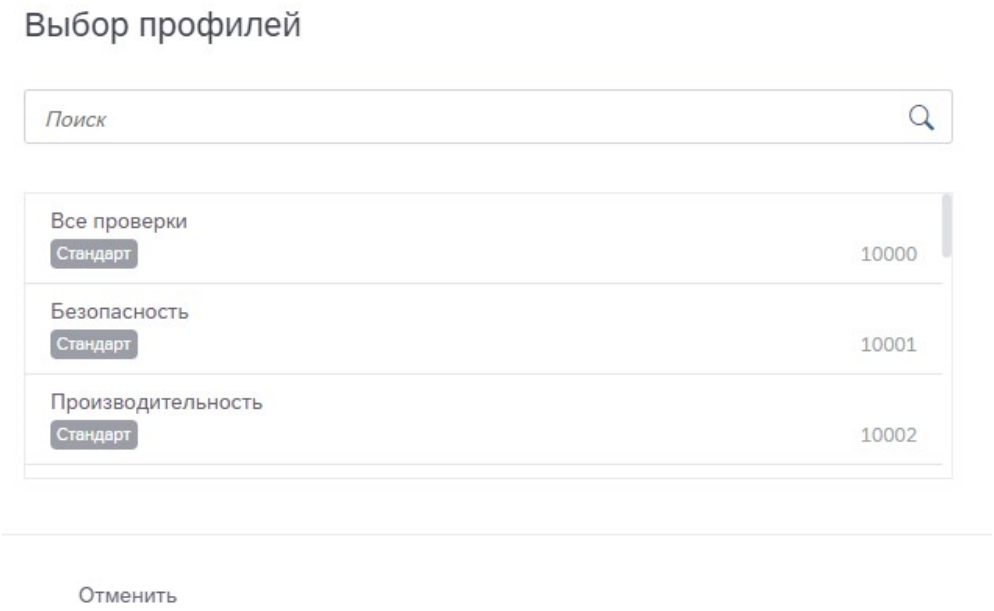


Рисунок 237 – Выбор профиля из списка

7.1.2.2.2.10 Выбор параметров запуска

Для выбора параметров запуска проекта необходимо выполнить действия согласно подпункту 7.1.2.1.2.7 Выбор

7.1.2.2.3 Просмотр/редактирование/запуск/прерывание/удаление проекта

Для просмотра, редактирования, запуска или удаления проекта необходимо выполнить действия согласно подпункту 7.1.2.1.3

Для прерывания проекта, при проведении процедуры анализа, в области содержания проекта предусмотрена кнопка *«Прервать проект»* (рис. 238).

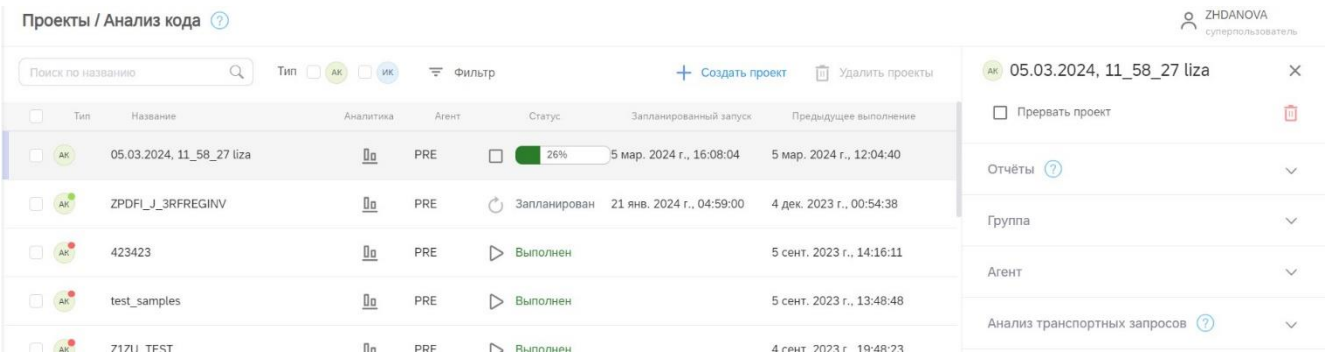


Рисунок 238 – Кнопка прерывания процедуры анализа проекта

Функция прерывания проекта становится активной после запуска проекта, если процедура анализа выполняется длительное время.

7.1.2.2.4 Просмотр отчетов по проектам типа АК

Процедуру просмотра отчетов по проектам АК осуществляют двумя способами:

1) По последней итерации проекта.

Чтобы просмотреть отчет по последней итерации проекта, необходимо нажать кнопку в соответствующей строке с названием проекта в поле «Отчет». Выгрузка отчетных документов осуществляется на локальный компьютер в виде архива в формате *.tar (рис. 239).

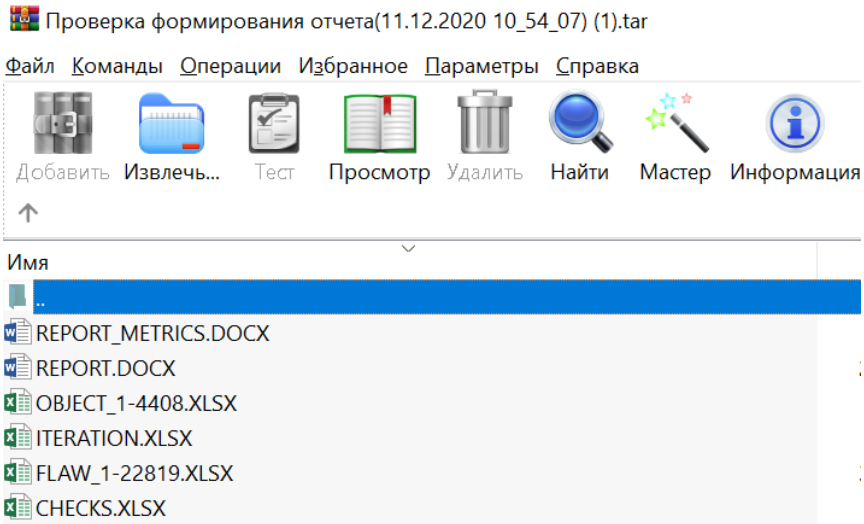


Рисунок 239 – Выгрузка отчета по итерации проекта

2) Из списка отчетов по всем итерациям проекта.

Чтобы просмотреть список отчетов по всем итерациям проекта, необходимо развернуть поле «Отчеты» в области параметров проекта (рис. 240).

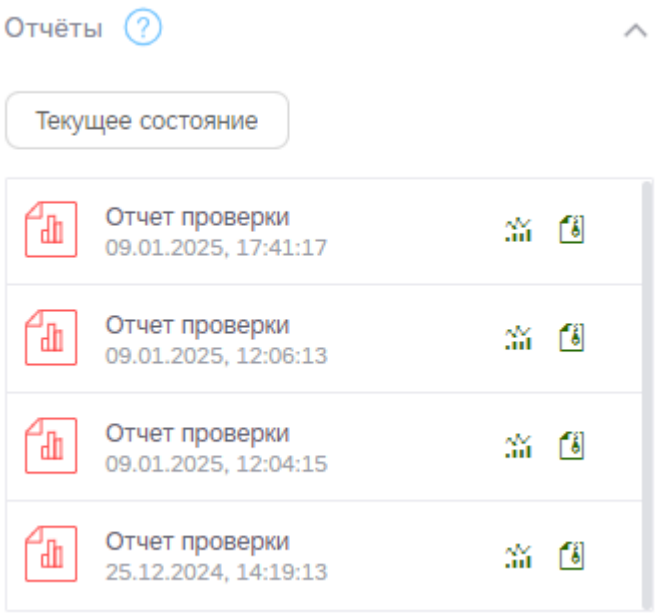


Рисунок 240 – Список отчетов по итерациям проекта

Для выгрузки отчетов необходимо нажать кнопку *«Скачать отчет»* в соответствующей строке итерации проекта. Выгрузка отчетных документов осуществляется на локальный компьютер в виде архива в формате *.tar (см. рис. 239). Назначение отчетов в архиве *.tar:

- CHECKS.XLSX – сводный список всех сработавших проверок по итерации проекта с указанием их степеней критичности;
- FLAW.XLSX – сводный список всех сработавших проверок по итерации проекта с указанием адреса найденного недостатка кода: пакета, типа объекта, участка кода;
- ITERATION.XLSX – сводная таблица по метрикам итерации проекта;
- OBJECT.XLSX – сводный список всех проверяемых программных пакетов и их объектов;
- REPORT.DOCX – подробное описание всех сработавших проверок по итерации проекта (назначение проверки, угрозы, рекомендации);
- REPORT-METRICS.DOCX – отчет в форме презентации по метрикам итерации проекта в категории «Безопасность» (формируется только при установке стандартного проверочного профиля «Безопасность» для итерации проекта). Данный файл доступен при наличии иконки в строке итерации;
- REQUESTS.XLSX – список по деблокированным транспортным запросам с указанием даты деблокирования и с указанием наличия уязвимости у объекта.

3) Просмотр отчетов в отдельном окне.

Для просмотра необходимо отчета необходимо выбрать итерацию проекта во вкладке «Отчеты» (см. рис. 240). В открывшемся окне выбрать степень критичности проверки, раскрыть проверку, выбрать программный объект.

В открывшемся окне доступен просмотр по степени критичности проверок:

— высокая;
— средняя;
— низкая;
— информация.

Для просмотра подробной информации необходимо выбрать критичность проверки, раскрыть группу проверок в области «Уязвимости», выбрать уязвимость из списка.

Примечание. Доступен просмотр уязвимостей по категории проверки и номеру проверки. Для просмотра необходимо нажать кнопку *«Фильтр»* (рис. 241).

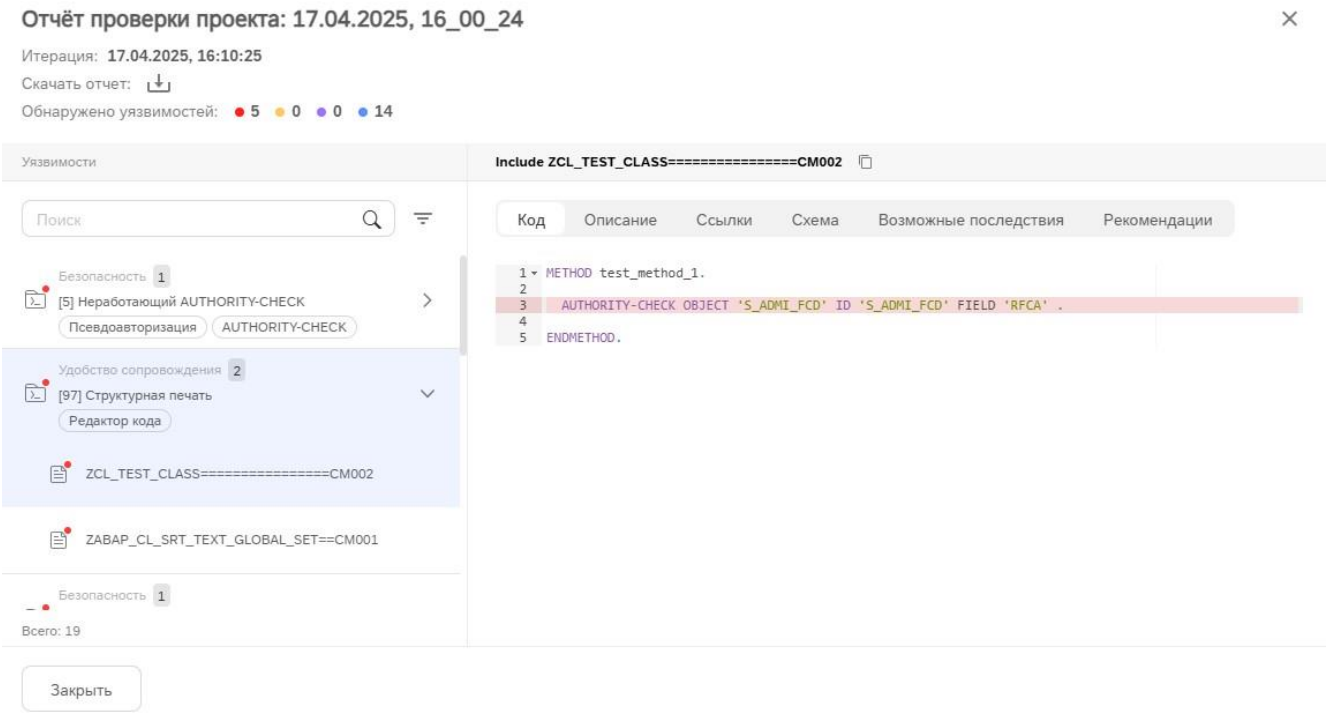


Рисунок 241 – Окно «Отчет проверки проекта» (для проекта типа АК)

Примечания:

1. Для изменения типа архива (с *.tar на *.zip или с *.zip на *.tar) необходимо обратиться к транзакции /n/gazis/sega (см. подраздел 4.2) или к подпункту 7.1.10.
2. В окне «Отчет проверки проекта» пользователю доступна кнопка «Фильтр». Доступна фильтрация по следующим параметрам:

— проверка;
— категория проверки;
— критичность;
— теги.

3. В окне «Отчет проверки проекта» пользователю доступен просмотр тегов проверки. Добавление проверок осуществляется в модуле «Профили». Список стандартных тегов представлен в приложении 3. Список тегов проверки представлен на рис. 242.

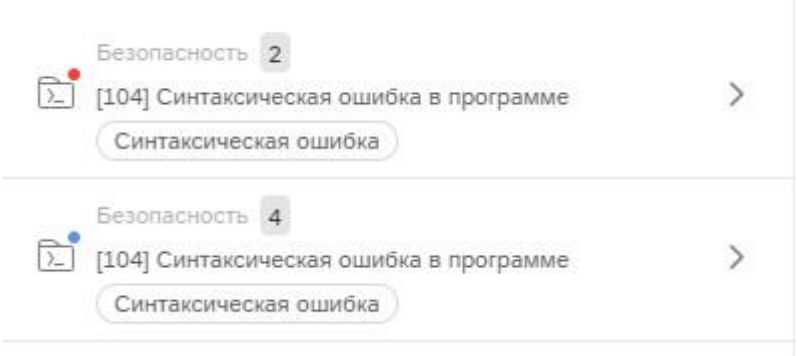


Рисунок 242 – Список тегов в проверках

7.1.2.2.4.1 Текущее состояние

Для проектов типа АК доступен просмотр текущего состояния и изменение статуса найденных уязвимостей.

Для просмотра необходимо нажать кнопку *«Текущее состояние»* в области «Отчеты» (см. рис. 240).

Окно текущее состояние состоит из следующих областей (рис. 243):

- основная – содержит информацию о системе, профиле, количестве и критичности уязвимостей, дата и время сканирования. Доступен просмотр всех и новых уязвимостей;
- меню – содержит поисковую строку, кнопку «Фильтр», сплит-кнопку «Все/Новые», а также кнопки «Скачать отчет» и «Управление уязвимостями»;
- уязвимости – содержит фильтр и поисковую строку, а также список уязвимостей.

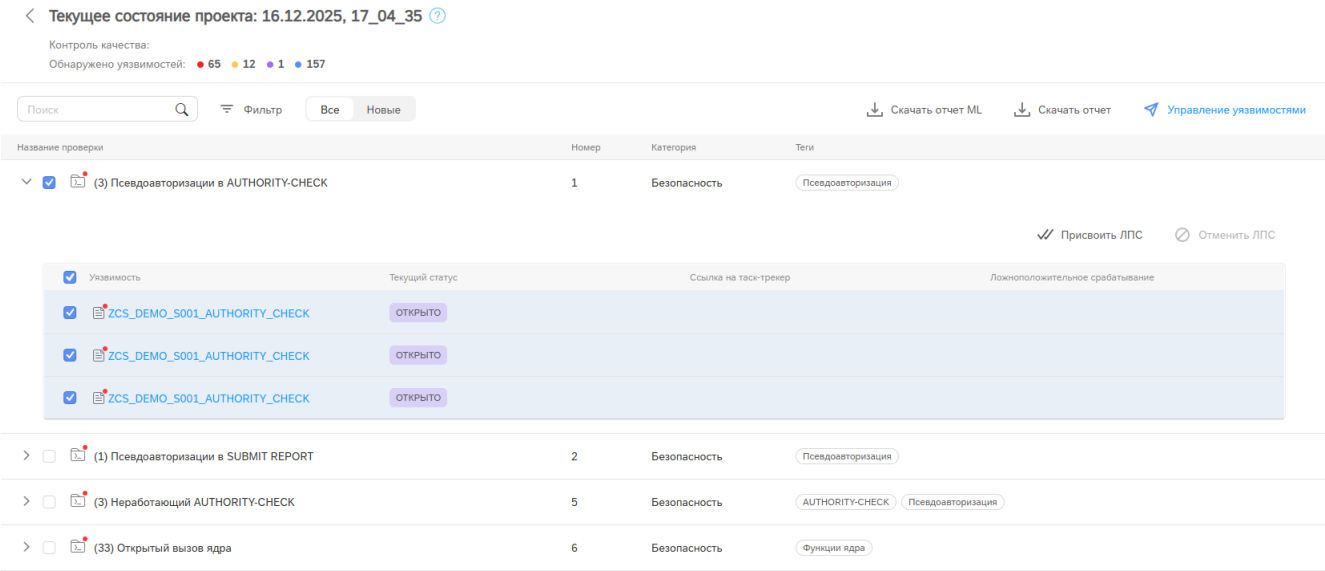


Рисунок 243 – Окно «Текущее состояние»

Примечания:

1. В окне «Текущее состояние» доступен просмотр уязвимости в отдельном окне. В окне доступен просмотр строки с уязвимостью (рис. 244), просмотр истории изменений и добавление комментария во вкладке «История изменений» (рис. 245).

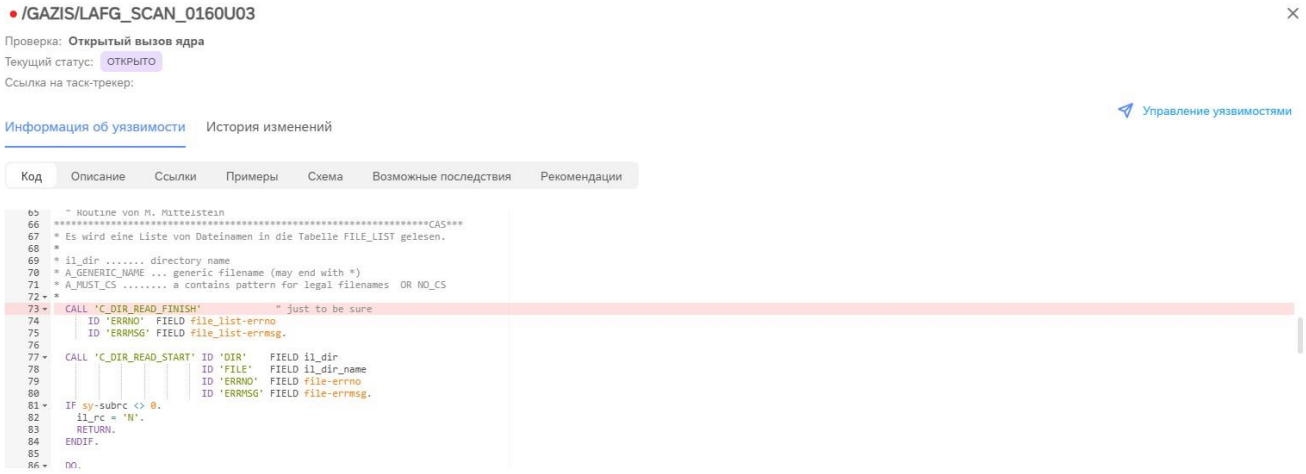


Рисунок 244 – Окно с указанием строки с уязвимостью

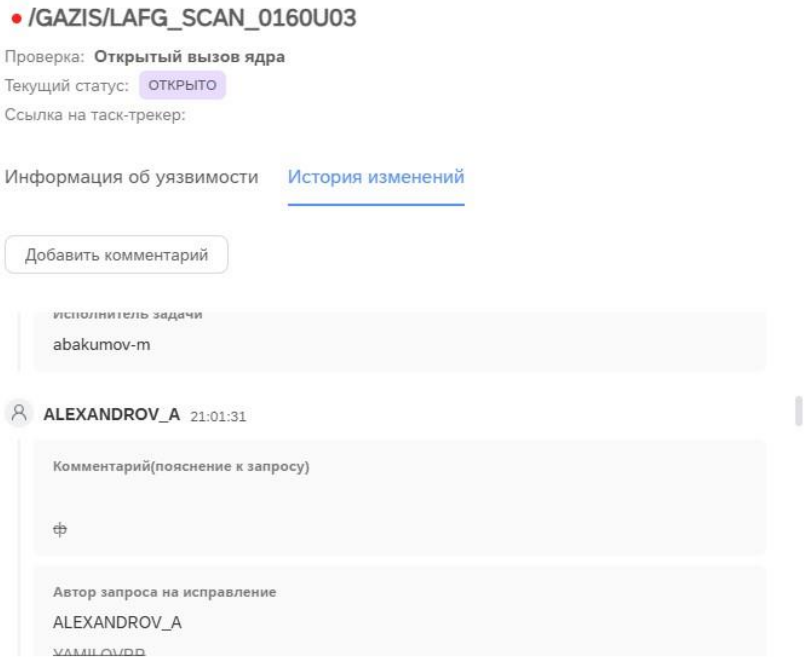


Рисунок 245 – Вкладка «История изменений»

2. Ссылка на таск-трекер (см. рис. 244) формируется после активации переключателя «Добавить задачу в таск-трекер» в окне «Управление уязвимостями» (см. рис. 247).
3. В окне «Текущее состояние» доступна выгрузка пользовательского отчета. Для выгрузки пользовательского отчета необходимо нажать кнопку *«Скачать*

отчет», выбрать параметры отчета в окне «Настройка отчета», нажать кнопку «Скачать». После выгрузки отчета параметры, установленные в окне «Настройка отчета», сохраняются. Пользователю предоставляется возможность настройки местоположения столбцов в окне «Настройка отчета» (см. рис. 243, 246).

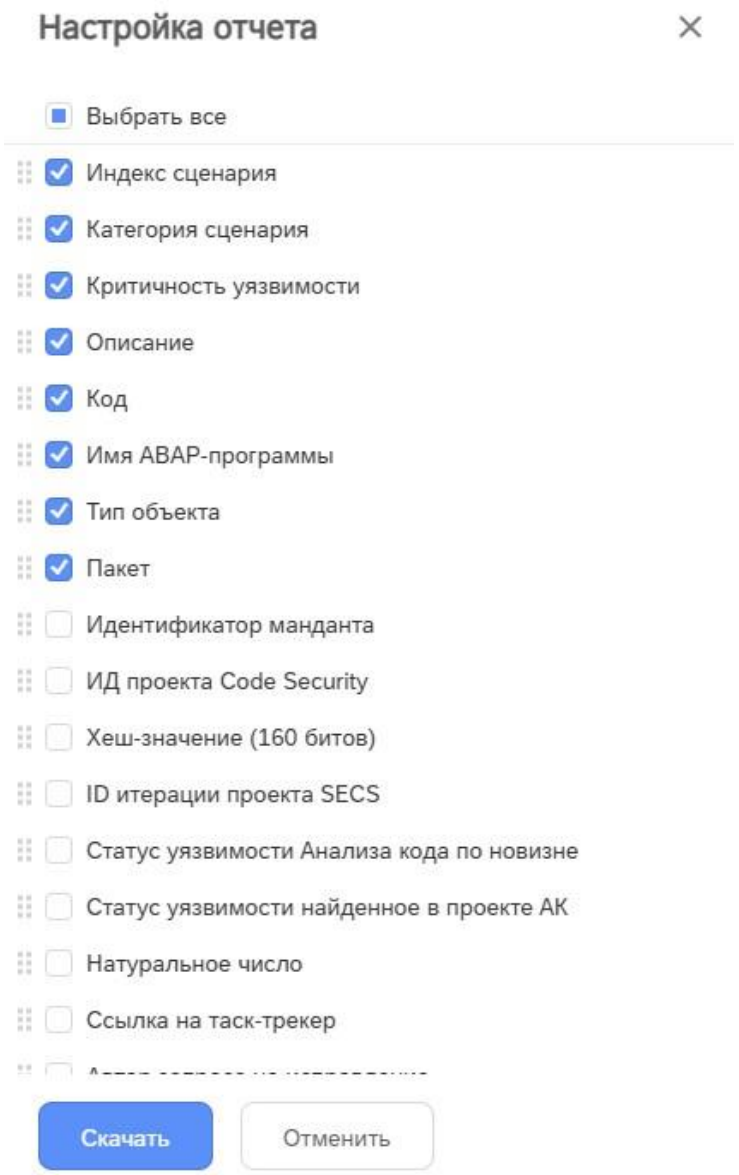


Рисунок 246 – Окно «Настройка отчета» (для проектов типа АК)

4. В окне «Текущее состояние» доступна выгрузка ML отчета. Для выгрузки пользовательского отчета необходимо нажать кнопку «Скачать отчет ML» (см. рис. 243).
5. В окне «Текущее состояние» доступна кнопка «Фильтр». Доступна фильтрация по следующим параметрам:

— проверка;
— категория проверки;
— критичность;

- статус уязвимости;
- наличие ссылки на таск-трекер;
- ID задачи;
- ложноположительное срабатывание;
- теги.

Найденные уязвимости принимают следующие степени критичности:

- красный цвет – высокая;
- оранжевый цвет – средняя;
- фиолетовый цвет – низкая;
- синий цвет – информация.

Функциональность «Управление уязвимостями»

Окно «Управление уязвимостями» предназначена для ведения и управления параметрами уязвимостей.

В окно «Управление уязвимостями» входят следующие поля:

- «Статус» - статус исправляемой уязвимости;
- «Таск-трекер» – тип таск-трекера. Доступна система отслеживания задач «Jira»;
- «Автор исправления в Jira» – список пользователей, подключенного таск-трекера;
- «Приоритет задачи» – список приоритетов задач согласно выбранному таск-трекеру;
- «Автор запроса на исправление» – пользователь, от которого поступила уязвимость на устранение;
- «Комментарий отправляющего» – комментарий отправляющего к уязвимости;
- «Система исправления» – система, в которой будет исправлена уязвимость;
- «Автор исправления» – пользователь, которому необходимо устранить обнаруженную уязвимость;
- «До какой даты исправить» – дата и время, до которого необходимо устранить обнаруженную уязвимость.

Доступны следующие статусы:

- «Открыто» – уязвимость найдена после сканирования.
- «В работе» – находится в процессе исправления у назначенного лица.
- «На проверке» – находится на рассмотрении у запрашивающего или на согласовании.
- «Исправлено» – уязвимость исправлена.

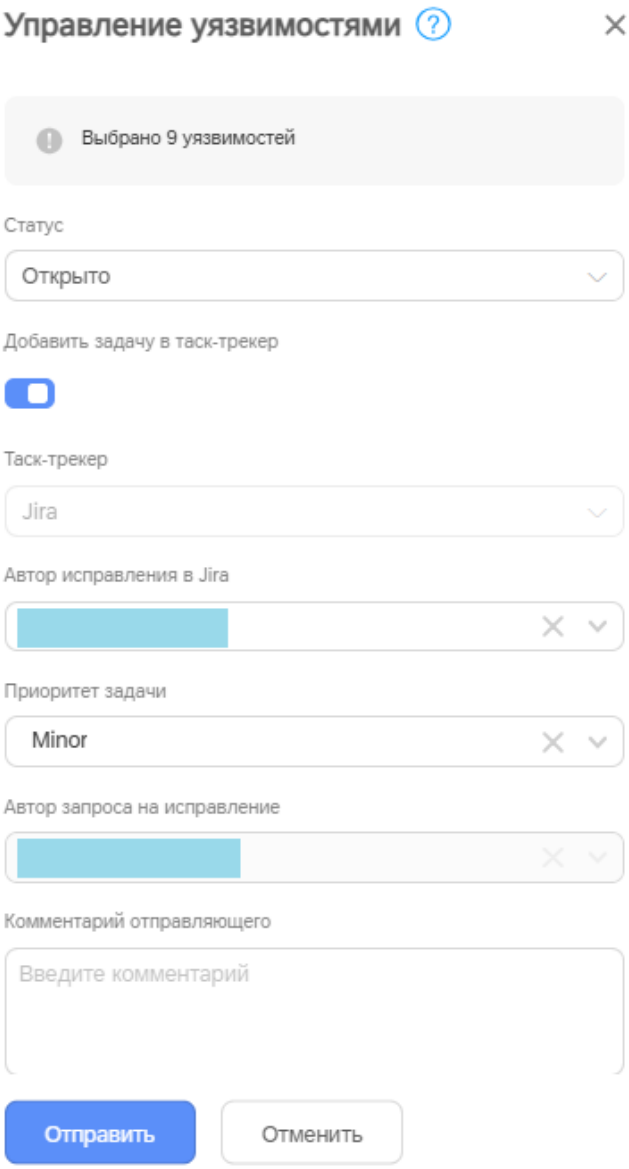


Рисунок 247 – Окно «Управление уязвимостями»

В окне «Управление уязвимостями» доступно изменение статуса найденных уязвимостей.

Вызов окна «Управление уязвимостями» осуществляется следующими способами:

- при просмотре уязвимости;
- в основной рабочей области окна «Текущее состояние».

Для изменения статуса уязвимостей необходимо выбрать проверку или уязвимости в области «Уязвимости», нажать кнопку *«Управление уязвимостями»*, ввести необходимые данные в окне «Управление уязвимостями» (рис. 247), нажать кнопку *«Отправить»*.

Примечания:

1. При выборе двух и более уязвимостей поле «Автор запроса на исправления» заполняется автоматически.
2. Список пользователей в поле «Автор исправления в Jira» появляется автоматически после выбора системы отслеживания задач «Jira» в поле «Таск-трекер».
3. В окне «Текущее состояние» доступен просмотр пользователю доступен просмотр тегов проверки. Добавление проверок осуществляется в модуле «Профили». Список тегов проверки представлен на рис. 248.

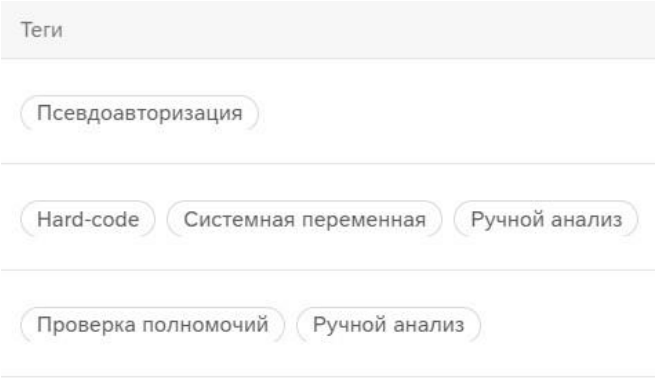


Рисунок 248 – Список тегов в проверке (окно «Текущее состояние»)

4. При редактировании полей в окне «Управление уязвимостями» сохраняются изменения в тех полях, в которые были внесены изменения. Поля без изменений не меняются. Количество измененных уязвимостей выводится в информационное сообщение.

Почтовые уведомления

Администратору ПК «SafeERP Security Suite» поступают почтовые уведомления по проектам типа АК в случаях, которые указаны в таблице 13.

Таблица 13 – События для проектов типа АК

Источник изменений	Событие	Отправитель	Получатель
Сервер управления(FIORI)	Добавлен комментарий	Тех.пользователь	Автор запроса
	Изменены данные	Тех.пользователь	Автор исправления
Агент (транзакция /n/gazis/secs_vulners)	Добавлен комментарий	Тех.пользователь	Автор запроса
	Изменен статус	Тех.пользователь	Автор запроса

Примечания:

1. Предварительно должна быть отключена настройка в разделе «Сканер». Для настройки необходимо обратиться к модулю «Администрирование» или к транзакции /N/GAZIS/SEGA.
2. Адрес электронной почты пользователя находится в разделе «Коммуникация». Для просмотра раздела «Коммуникация» необходимо обратиться к транзакции SU01.
3. Необходимо настроить интеграцию с почтовым сервером компании.

Функциональность «ЛПС»

Ложноположительное срабатывание (ЛПС) – это результат, когда система некорректно выявила уязвимость.

Функциональность помогает сформировать массив неверно выявленных уязвимостей, которые можно определить, как ЛПС, и в будущих итерациях они не будут попадать в отчет.

Параметры выявленных ЛПС помогут исключать уязвимости по атрибутам и не допускать их срабатывания для систем.

Окно «Ложноположительное срабатывание» (ЛПС) предназначено для изменения ложноположительного срабатывания у найденной уязвимости. Окно «Ложноположительное срабатывание» доступно для проверок категории «Безопасность».

Пользователям доступны следующие действия:

- присвоение ЛПС;
- редактирование ЛПС;
- отмена ЛПС.

Присвоение «Ложноположительного срабатывания»

Присвоение «ЛПС» доступно в следующих окнах:

- при просмотре списка уязвимостей;
- при подробном просмотре уязвимости.

Окно «Присвоить ЛПС» состоит из следующего (рис. 249):

- поле «Причина» – необходимо выбрать причину из выпадающего списка, по которой произошло ложноположительное срабатывание. Является обязательным для заполнения.

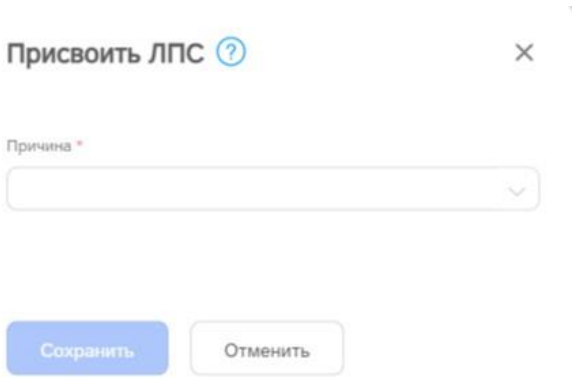


Рисунок 249 – Окно «Присвоить ЛПС»

Примечание. После выбора причины ложноположительного срабатывания в поле «Причина» (для некоторых проверок) доступно следующее:

- поле «Команда» – необходимо выбрать команду из выпадающего списка. Данное поле доступно после выбора причины в соответствующем поле. Является обязательным для заполнения;
- поле «Постпроверка» – наименование постпроверки. Поле заполняется автоматически после выбора причины и команды в соответствующих полях;
- поле «Имя системной переменной» – имя системной переменной. Поле заполняется автоматически после выбора причины и команды в соответствующих полях;
- поле «Значение системной переменной» – значение системной переменной. Поле заполняется автоматически после выбора причины, команды и имени системной переменной в соответствующих полях;
- поле «Имя параметра команды» – имя системной переменной. Поле заполняется автоматически после выбора причины и команды в соответствующих полях;
- поле «Значение параметра команды» –значение параметра команды. Поле заполняется автоматически после выбора причины и команды в соответствующих полях, а также пользователю предоставляется возможность добавление и удаление переменной. Разрешено добавление латинских букв, цифр и символов (разрешенные символы: -,_, «, », ", ");
- поле «Имя атрибута команды» – имя атрибута команды. Поле заполняется автоматически после выбора причины и команды в соответствующих полях;
- поле «Значение параметра команды» – значение параметра команды. Поле заполняется автоматически после выбора причины, команды и значения параметра команды в соответствующих полях;
- поле «Имя атрибута команды» – имя атрибута команды. Поле заполняется автоматически после выбора причины и команды в соответствующих полях;
- поле «Значение атрибута команды» - значение атрибута команды. Поле заполняется автоматически после выбора причины, команды и имени атрибута команды в соответствующих полях, а также пользователю предоставляется

возможность добавление и удаление значений. Разрешено добавление латинских букв, цифр и символов (разрешенные символы: -,_, «, », ", ");

- поле «Список активностей проверки» – список активностей проверки. Поле заполняется автоматически после выбора причины и команды в соответствующих полях;
- поле «Список разрешенных программ» – список разрешенных программ. Поле заполняется автоматически после выбора причины и команды в соответствующих полях, а также пользователю предоставляется возможность добавления и удаления наименований программ. Разрешено добавление латинских букв, цифр и символов (разрешенные символы: -,_, «, », ", ");
- поле «Комментарий» – комментарий отправляющего. Данное поле является необязательным для заполнения.

Для присвоения ЛПС необходимо выполнить следующие действия:

1) Выбрать уязвимость, не имеющую ЛПС, из списка.
2) Нажать кнопку «Присвоить ЛПС».
3) Заполнить необходимые поля в окне «Присвоить ЛПС».
4) Нажать кнопку *«Сохранить».*

Примечание. При выборе 2-х и более уязвимостей из списка в окне «Ложноположительное срабатывание» отображается количество уязвимостей, которым не присвоен признак ЛПС.

Редактирование ЛПС

Редактирование ЛПС после присвоение признака ЛПС у уязвимости. Кнопка «Редактировать ЛПС» доступно в окне просмотра уязвимости или при просмотре списка уязвимостей.

Доступно редактирование следующего (рис. 250):

- поле «Причина»;
- поле «Значение параметра команды»;
- поле «Значение атрибута команды»;
- поле «Список разрешенных программ»;
- поле «Комментарий».

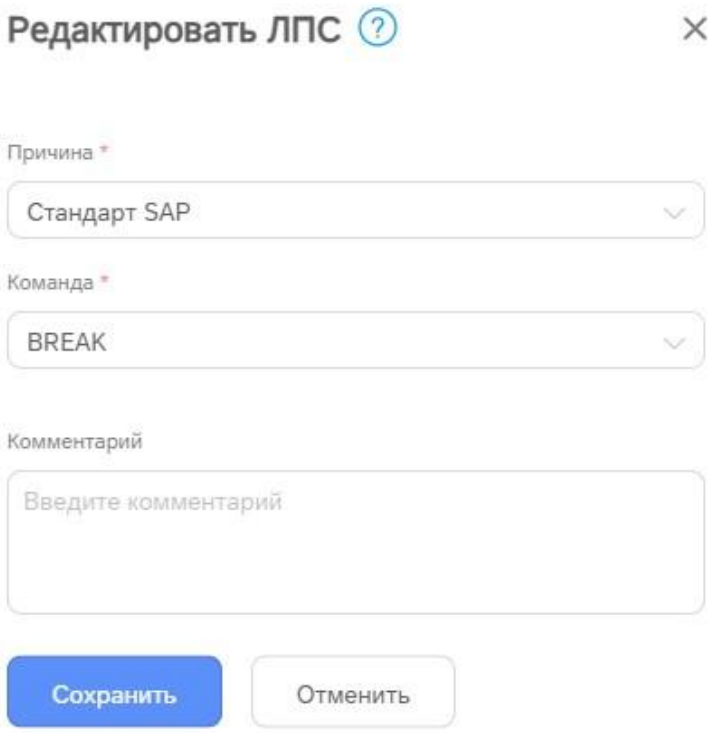


Рисунок 250 – Окно «Редактировать ЛПС»

Для редактирования ЛПС необходимо выполнить следующие действия:

1) Выбрать уязвимость из списка. Нажать кнопку «Редактировать ЛПС».
2) Внести изменения в окне «Редактировать ЛПС» (см. рис. 250).
3) Нажать кнопку «Сохранить» (см. рис. 250).

Отмена ЛПС

Отмена ЛПС доступно после присвоение признака ЛПС уязвимости.

Для отмены признака ЛПС необходимо выполнить следующие действия:

1) Выбрать уязвимость, имеющую ЛПС, из списка.
2) Нажать кнопку *«Отменить ЛПС».*

7.1.2.2.5 Просмотр отчетов по проектам типа ИК

Для просмотра отчетов типа необходимо выполнить действия согласно пп. 7.1.2.2.4 Просмотр

Назначение отчетов в архиве *.tar:

- REPORT.DOCX – подробное описание результата сканирования по итерации проекта (информация о проекте, подробные результаты сканирования, анализ пакетов).
- CRITICAL_OBJECTS.XLSX − подробное описание результата сканирования критических объектов по итерации проекта.

Примечание. Для изменения типа архива необходимо обратиться к пункту 4.2.3 или 7.1.9.

7.1.2.2.6. Просмотр метрик безопасности программного кода

Просмотр метрик безопасности кода доступен для проектов типа АК.

Для просмотра метрик безопасности программного кода необходимо нажать кнопку в соответствующей строке проекта в столбце «Аналитика» таблицы со списком проектов (см. рис. 127).

Окно с результатами анализа по метрикам безопасности программного кода представлено на рис. 251.

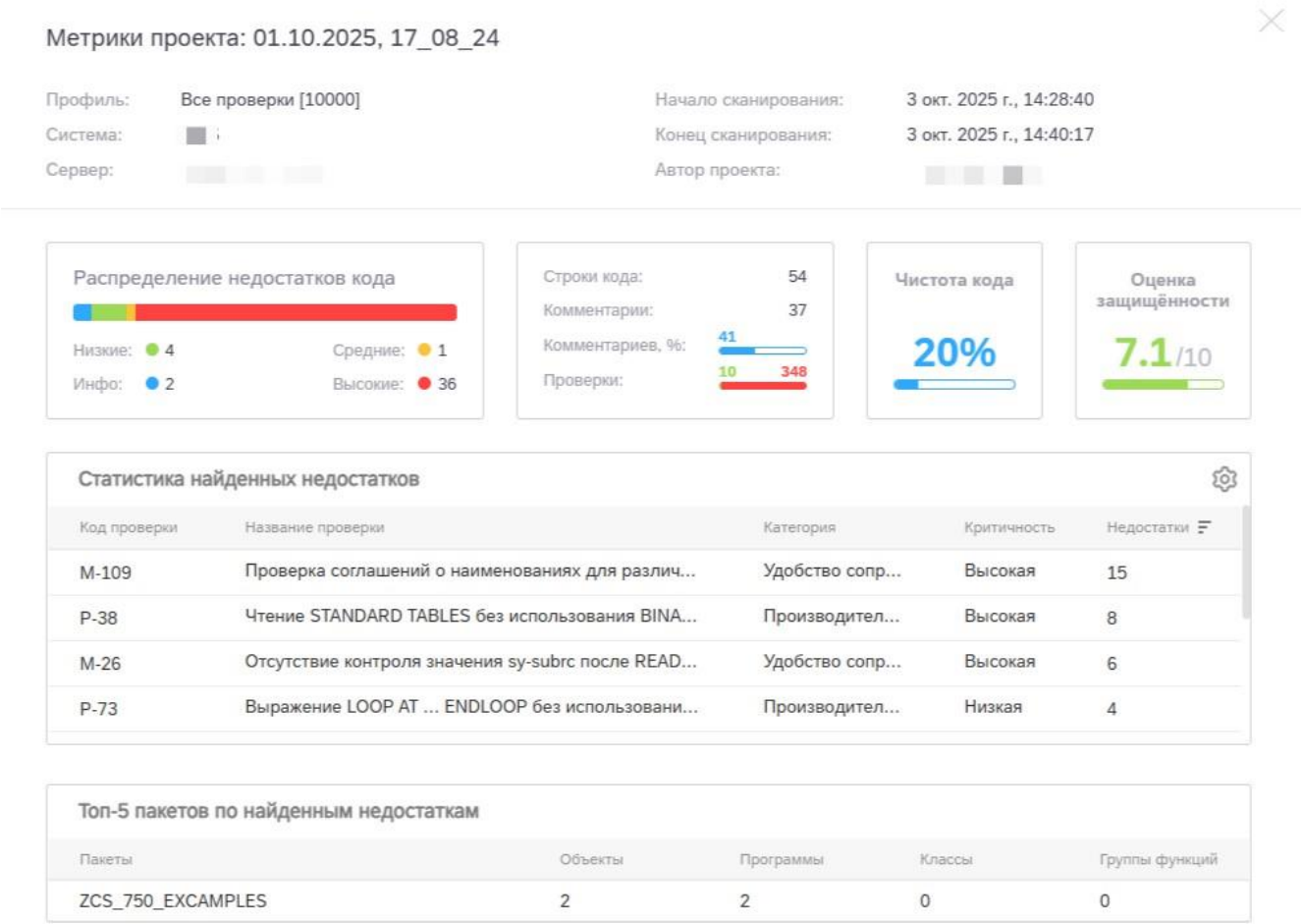


Рисунок 251 – Результаты анализа по метрикам безопасности

В окне «Метрики проекта» доступны следующие области:

- «Распределение недостатков кода» – распределение недостатков по степени критичности и количеству;
- основные данные кода – приведена информация о количестве строк кода, количестве комментарий в коде, процентное содержание комментариев в коде, количество сработанных проверок;
- «Чистота кода» – процентное содержание кода
- «Оценка защищенности» – оценка защищенности кода;

- «Статистика найденных уязвимостей» – приведены данные о сработанных проверках (код проверки, наименование проверки, категория, критичность, недостатки);
- «Топ-5 пакетов по найденным недостатков» – приведены 5 пакетов с наибольшим количеством недостатков;
- «Сравнение итераций» – сравнение количества и критичности недостатков текущей и предыдущих итераций;
- «Динамика оценки защищенности» – изменение динамики;
- «Динамика уязвимостей» – динамика изменений уязвимостей в виде гистограмм;
- «Динамика количества строк кода» – изменение количества строк кода в виде гистограмм.

Примечание. В области «Статистика найденных недостатков» доступны следующие действия:

- сортировка недостатков – сортировка количества недостатков по возрастанию или убыванию;
- настройка виджета – настройка виджета по следующим параметрам: проверка, категория проверки, критичность (рис. 252). Для настройки виджета необходимо нажать на всплывающую кнопку в области «Статистика найденных недостатков».

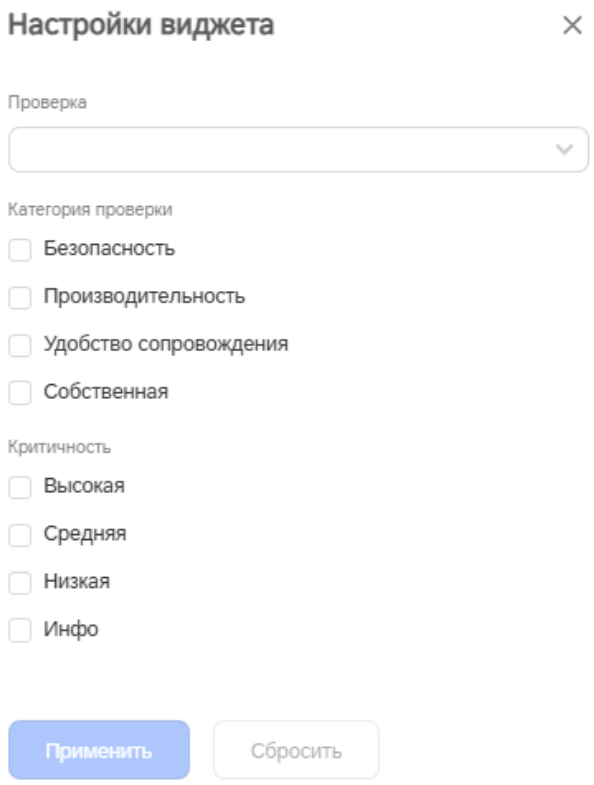


Рисунок 252 – Окно «Фильтр» (для окна «Метрики проекта»)

7.1.2.2.7 Индикация проектов

Индикация используется для проектов типа АК.

Значения цветов индикаторов на иконке в столбце «Тип» проектов приведены в таблице 14.

Таблица 14 – Значения цветов индикаторов в столбце «Тип» проектов

Цвет индикатора	События индикации
	– ошибка RFC -соединения (ошибки получения данных с агента); – выявлены проверки с высокой степенью критичности; – невозможно определить статус анализа (ошибки фоновых заданий); – ошибка лицензии.
	Выявлены проверки со средней степенью критичности
	Критичных результатов нет (данные в наличии, анализ проведен)

7.1.2.2.8 Полномочия доступа к функциям модуля

Полномочия доступа оператора ПК «SafeERP Security Suite» к функциям модуля «Анализ кода» для проектов типа АК:

- принудительный запуск проекта;
- просмотр истории итераций;
- поиск объектов;
- просмотр истории итераций;
- сохранение отчета по итерации в файл;
- выгрузка шаблона с объектами.

Полномочия доступа оператора ПК «SafeERP Security Suite» к функциям модуля «Анализ кода» для проектов типа ИК:

- принудительный запуск проекта;
- просмотр истории итераций;
- просмотр текущего состояния критических объектов;
- использование функций фильтра для текущего состояния объектов;
- сохранение отчет по итерации в файл;
- выгрузка шаблона с объектами.

7.1.3 Модуль «Агенты»

Веб-интерфейс модуля «Агенты» (программный модуль SafeERP Platform Security) предназначен для ведения агентов в ПК «SafeERP Security Suite». В модуль «Агенты» входит раздел «Агенты». Элементы основной рабочей области модуля «Агенты» представлены на рис. 128.

В основной рабочей области «Агенты» доступны следующие действия:

1) Просмотр агента.
2) Добавление агентов.
3) Присвоение лицензии агенту.
4) Редактирование агентов.

5) Удаление агентов
6) Просмотр группы.
7) Добавление группы.
8) Редактирование группы.
9) Удаление группы.

В рабочую область «Агенты» входят следующие столбцы:

- название – название агента в системе;
- тип агента – тип агента в системе. Агенты подразделяются на следующие типы: ABAP, JAVA, HANA, BO;
- основанная лицензия – статус основной лицензии. – лицензия действительна, – лицензия недействительна;
- лицензия поддержки – статус лицензии поддержки. – лицензия действительна, – лицензия недействительна;
- RFC статус – статус RFC-соединения. – агента доступен, – ошибка соединения;
- RFC-соединение – имя RFC-соединения агента с сервером управления;
- Версия агента – номер версии агента;
- SID – идентификатор агента в системе;
- функционал – статус агента в системе. Доступные статусы: продуктив и пустой;
- хост – IP-адрес агента в системе;
- сканер – статус подключения агента к модулю «SafeERP Platform Security». – агента подключен к модулю соответствующему, – агент не подключен к соответствующему модулю;
- анализ кода ABAP – статус подключения агента к модулю «SafeERP Code Security». – агента подключен к модулю соответствующему, – агент не подключен к соответствующему модулю;
- RFC статус с агента – RFC-соединение с агента к серверу;
- тенант – наименование тенанта, к которому подключен агент.

7.1.3.1 Агенты

Агенты используются во всех типах проектов в модулях «Сканер» и «Анализ кода».

7.1.3.1.1 Просмотр агента

Для просмотра агента необходимо проекта необходимо группу «Все системы» или другую группу, нажать кнопку , нажать левой кнопкой мыши на наименование агента.

7.1.3.1.2 Добавление агента

Для добавления агента необходимо нажать кнопку Добавить , выбрать Агент , в открывшемся окне вести название агента, выбрать RFC-соединение, группу и основную лицензию, нажать кнопку *«Добавить»* (рис. 253).

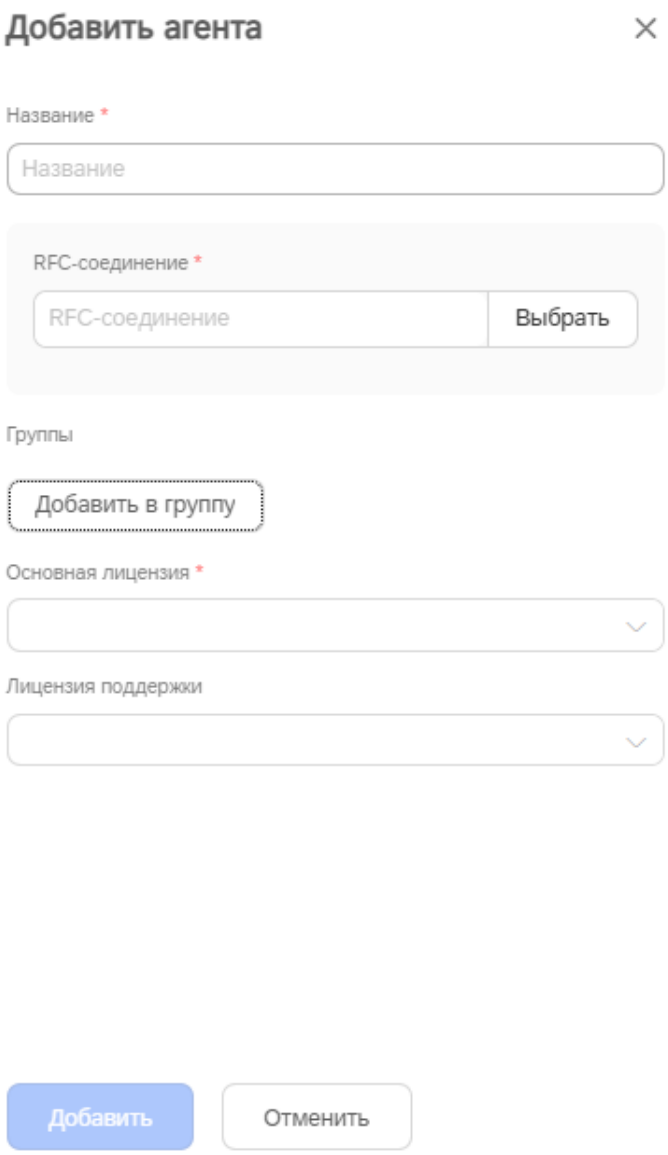


Рисунок 253 – Окно «Добавить агента»

Примечание. Активировать настройку «Учет прагм» необходимо в следующих случаях: для корректной работы проверок по поиску прагм или версия netweaver агента содержит прагмы.

7.1.3.1.3 Присвоение лицензии агенту

Для присвоения лицензии агенту необходимо выбрать агента из группы «Все системы», нажать кнопку *«Редактировать агента»* в выпадающем окне, в области «Основная лицензия» или «Основная лицензия» нажать кнопку , выбрать лицензию, нажать кнопку *«Сохранить»*.

Примечание. Для корректной работы проекта необходимо присвоить основную лицензию агенту.

7.1.3.1.4 Редактирование агента

Редактирование агента осуществляется в следующих полях:

- название;
- RFC соединение;
- учет прагм;
- RFC соединение с агента (для агента типа ABAP);
- группы;
- основная лицензия;
- лицензия поддержки.

Для редактирования агента необходимо выбрать агент из списка, нажать кнопку *«Редактировать агент»*, внести изменения, нажать кнопку *«Сохранить»* (рис. 254).

Примечание. При редактировании агента или группы устанавливается блокировка на запись для редактируемого объекта. Время блокировки ограничено настройкой в параметрах «Профиля инстанций», при истечении этого времени блокировка снимается. Для изменения времени блокировки необходимо обратиться к группе SAP базис.

При закрытии окна, вкладки, браузера или переходу на другую страницу блокировка снимается.

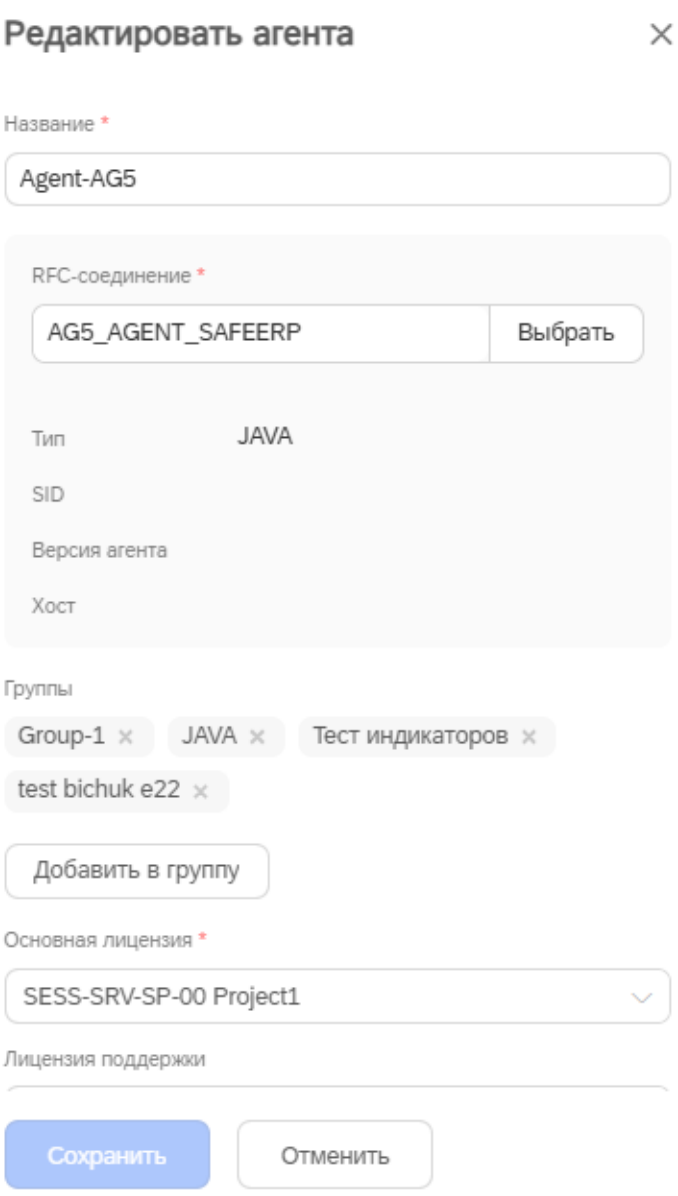


Рисунок 254 – Окно «Редактировать агента»

7.1.3.1.5 Удаление агента

Для удаления агента необходимо выбрать агента из списка, нажать кнопку , подтвердить действие.

7.1.3.2 Группа агентов

Группа агентов – это агенты, объединённые по определенному признаку (тип агента, тип RFC соединения и другие признаки).

7.1.3.2.1 Просмотр группы агентов

Для просмотра группы агента необходимо нажать кнопку > напротив названия группы агентов.

7.1.3.2.2 Добавление группы агентов

Для добавления агента необходимо нажать кнопку *«+ Добавить»*, выбрать «Группа» , в открывшемся окне вести название группы агентов, нажать кнопку «Добавить агентов»

(рис. 255), в отрывшемся окне уставить флаг ☑ напротив агента, нажать кнопку *«Выбрать»* (рис. 256), нажать кнопку *«Добавить»* (рис. 255).

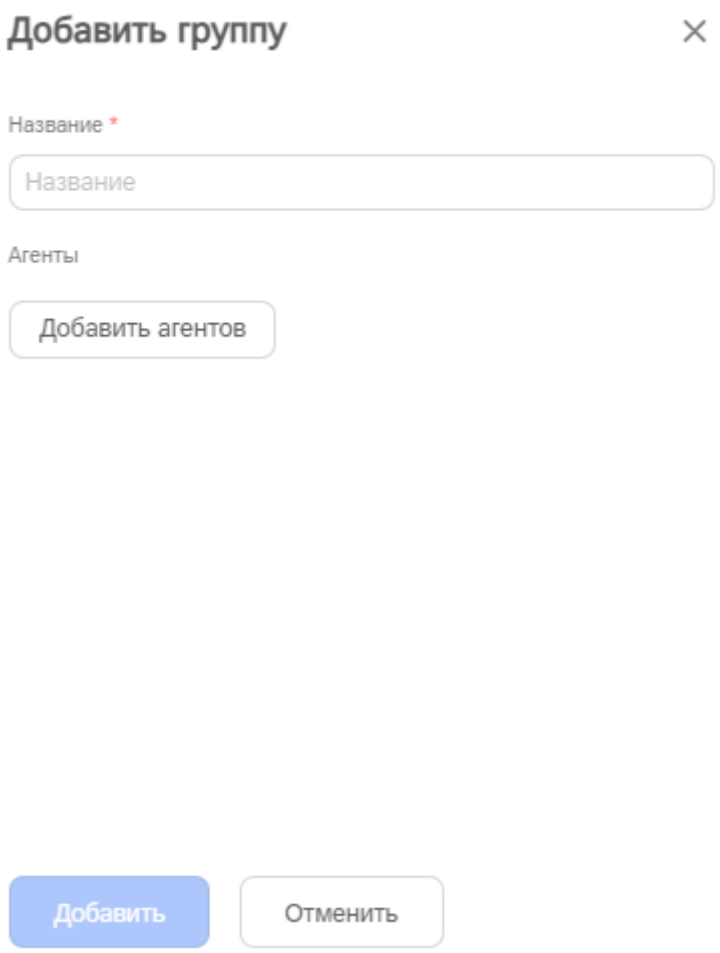


Рисунок 255 – Добавление группы агентов

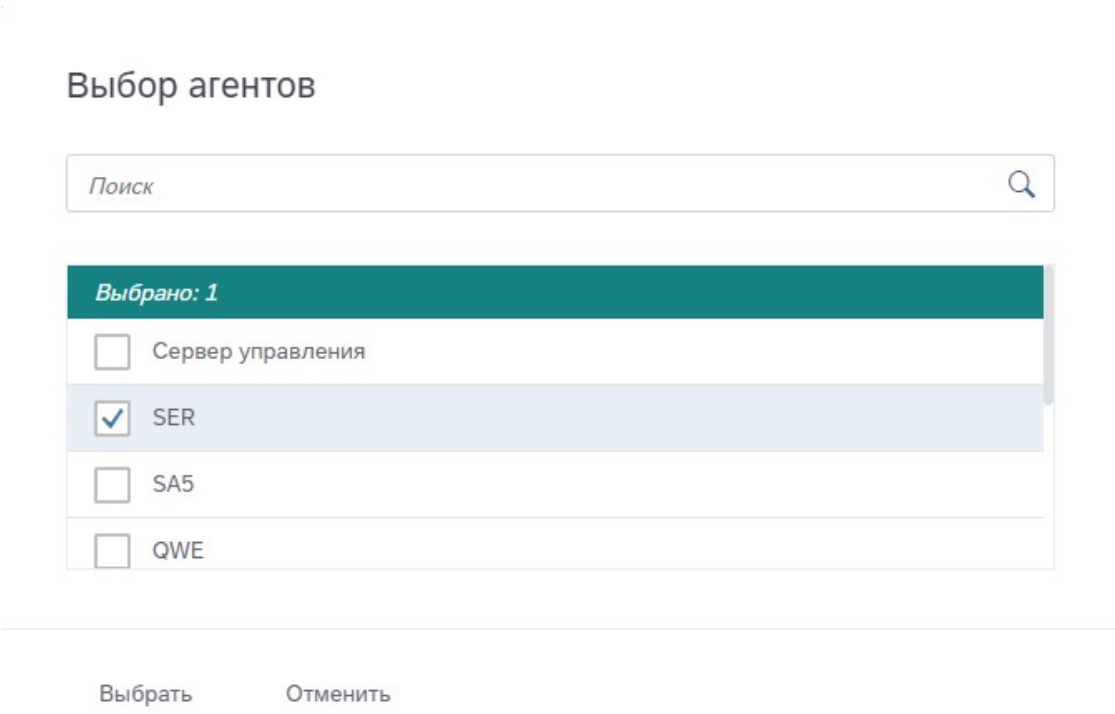


Рисунок 256 – Окно «Выбор агентов»

7.1.3.2.3 Редактирование группы агентов

Для редактирования группы агентов необходимо выбрать группу из списка, нажать кнопку *«Редактировать группу»* (см. рис. 128), внести изменения, нажать кнопку *«Сохранить»* (рис. 257).

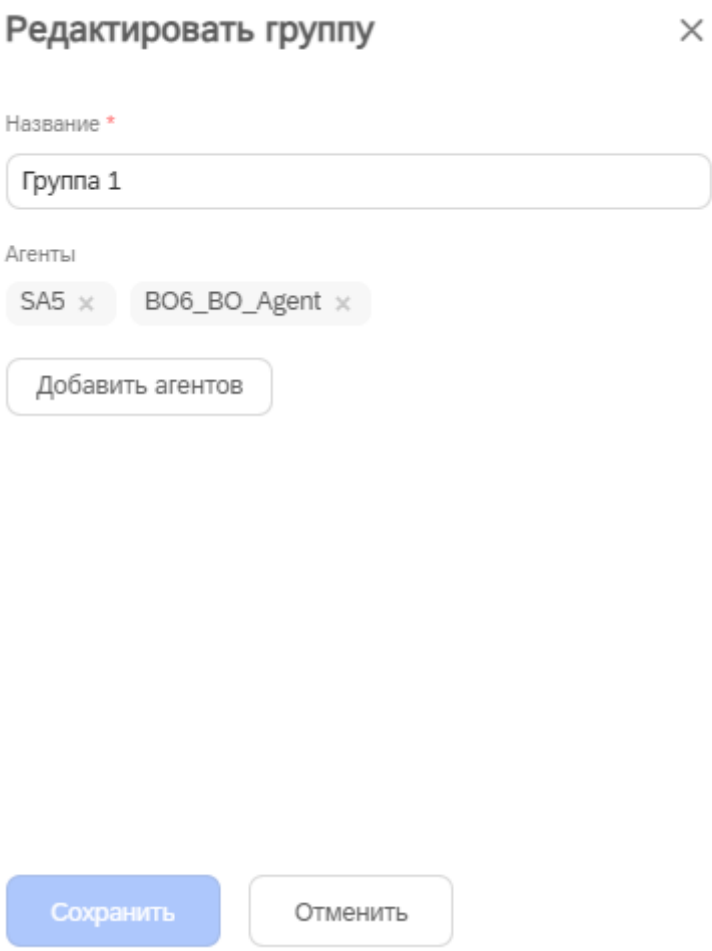


Рисунок 257 – Окно «Редактировать группу»

7.1.3.2.4 Удаление группы агентов

Для удаления группы агентов необходимо выбрать группу агентов, нажать кнопку *«Удалить»* (см. рис. 128), в открывшемся окне нажать кнопку *«Удалить»* (рис. 258).

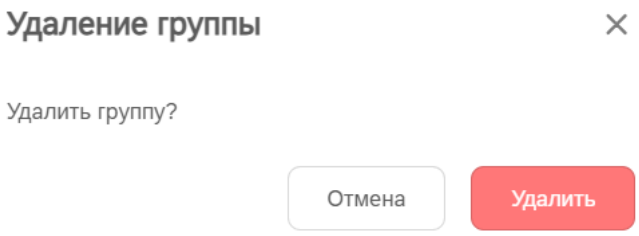


Рисунок 258 – Окно подтверждения «Удаление группы»

7.1.4 Модуль «Ландшафт»

Веб-интерфейс модуля «Ландшафт» предназначен для просмотра схемы взаимодействия, подключенных к ПК «SafeERP Security Suite» агентов и маршрутов их взаимодействия. Основная рабочая область «Ландшафт» представлена на рис. 259 и 260.

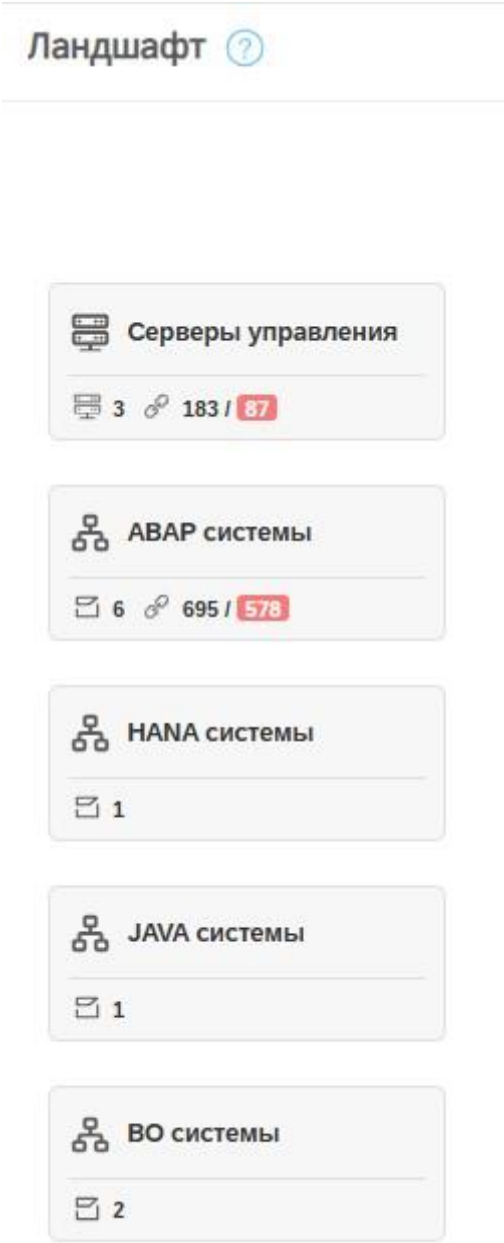


Рисунок 259 – Модуль «Ландшафт» (группы систем)

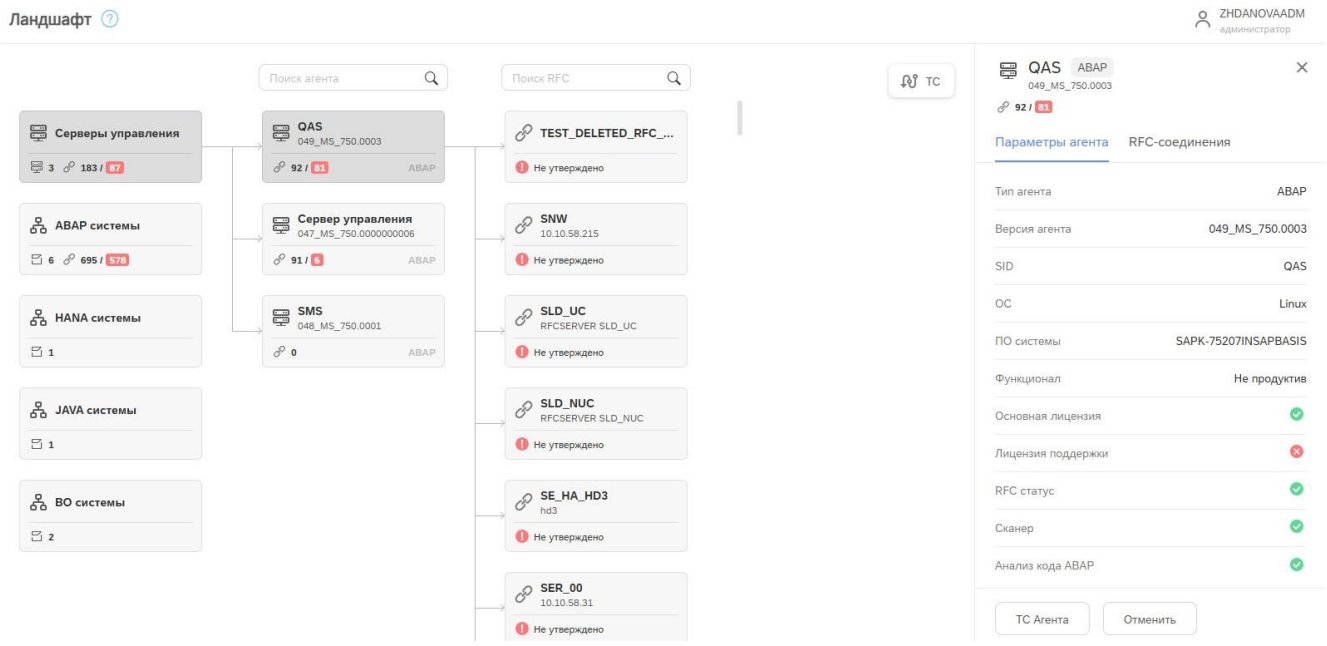


Рисунок 260 – Модуль «Ландшафт» (агенты и RFC-соединения)

В основной рабочей области «Ландшафт» доступны следующие действия:

1) Обзор ландшафта.
2) Поиск агента.
3) Просмотр транспортной системы (ТС) агента.
4) Просмотр RFC соединений.
5) Утверждение RFC соединений.

Примечания:

1. Для корректного отображения ландшафта необходимо повторно запустить фоновое задание в соответствующем разделе модуля «Администрирование».
2. Для корректного отображения RFC-соединений необходимо запустить фоновое задание в разделе «Управление RFC» модуля «Администрирование».

В модуле «Ландшафт» доступны следующие элементы:

— системы (рис. 261);
— RFC-соединение (рис. 262).

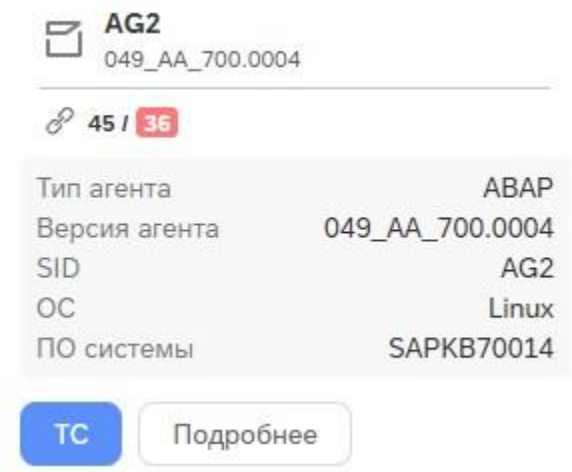


Рисунок 261 – Элемент «Система»

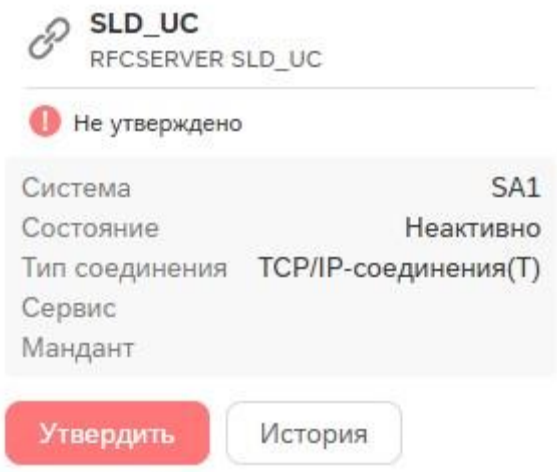


Рисунок 262 – Элемент «RFC-соединение»

Для поиска узла необходимо выбрать группу систем, ввести название системы в строке «Поиск агента».

Элемент «Система» (рис. 263) содержит следующие данные:

- название системы;
- наименование и тип агента;
- версия агента;
- системный идентификатор;
- версия ОС;
- версия ПО системы;
- количество RFC-соединений/ утвержденных RFC-соединений.

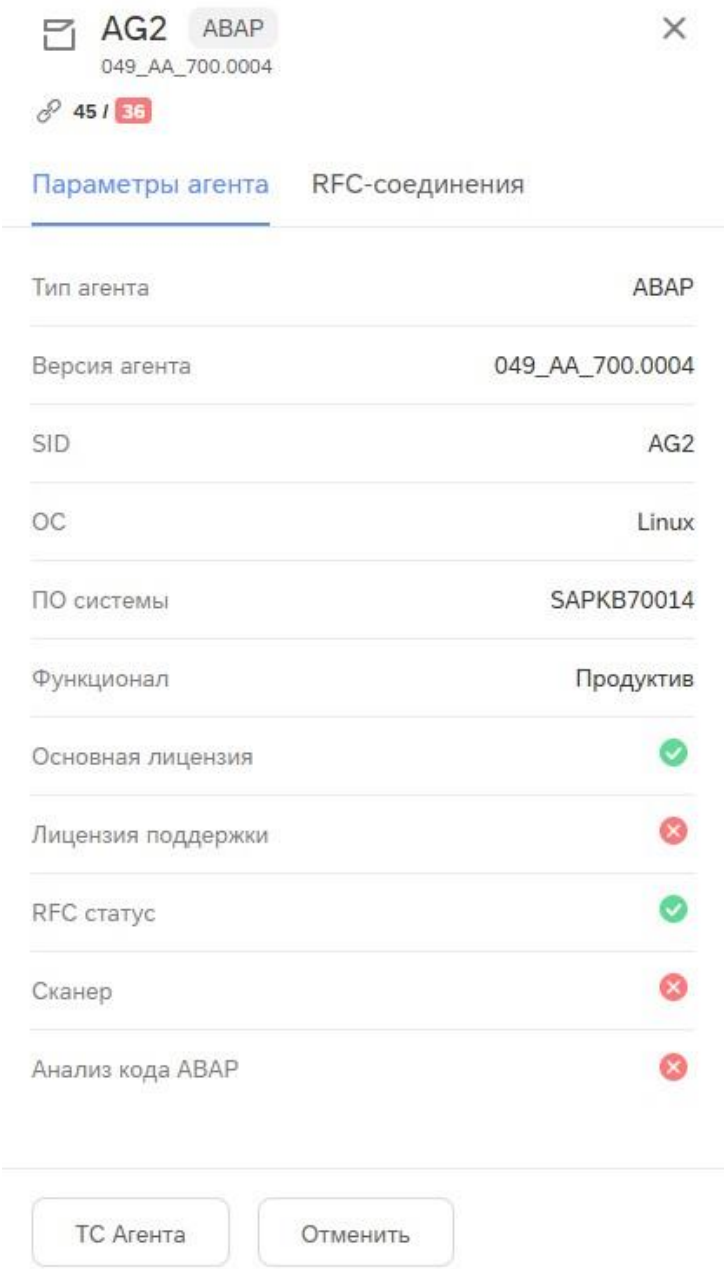


Рисунок 263 – Подробное описание элемента «Агент»

Примечание. При просмотре данных агента доступны следующие действия:

- Утверждение RFC-соединения. Для утверждения RFC-соединения необходимо выбрать вкладку соответствующую вкладку (рис. 263), выбрать соединение из списка, нажать кнопку *«Утвердить».*
- Просмотр истории RFC-соединения. Для просмотра истории RFC-соединения необходимо выбрать вкладку соответствующую вкладку (рис. 263), выбрать соединение из списка, нажать кнопку *«История».*

Для поиска RFC-соединения необходимо выбрать группу систем, выбрать агента, ввести название RFC-соединения в строке «Поиск RFC».

Элемент «RFC-соединение» (рис. 264) содержит следующие данные:

- IP-адрес;

- система;
- состояние;
- тип соединения;
- сервис;
- мандант;
- тип изменения;
- автор изменения;
- статус;
- утвердил;
- дата утверждения.

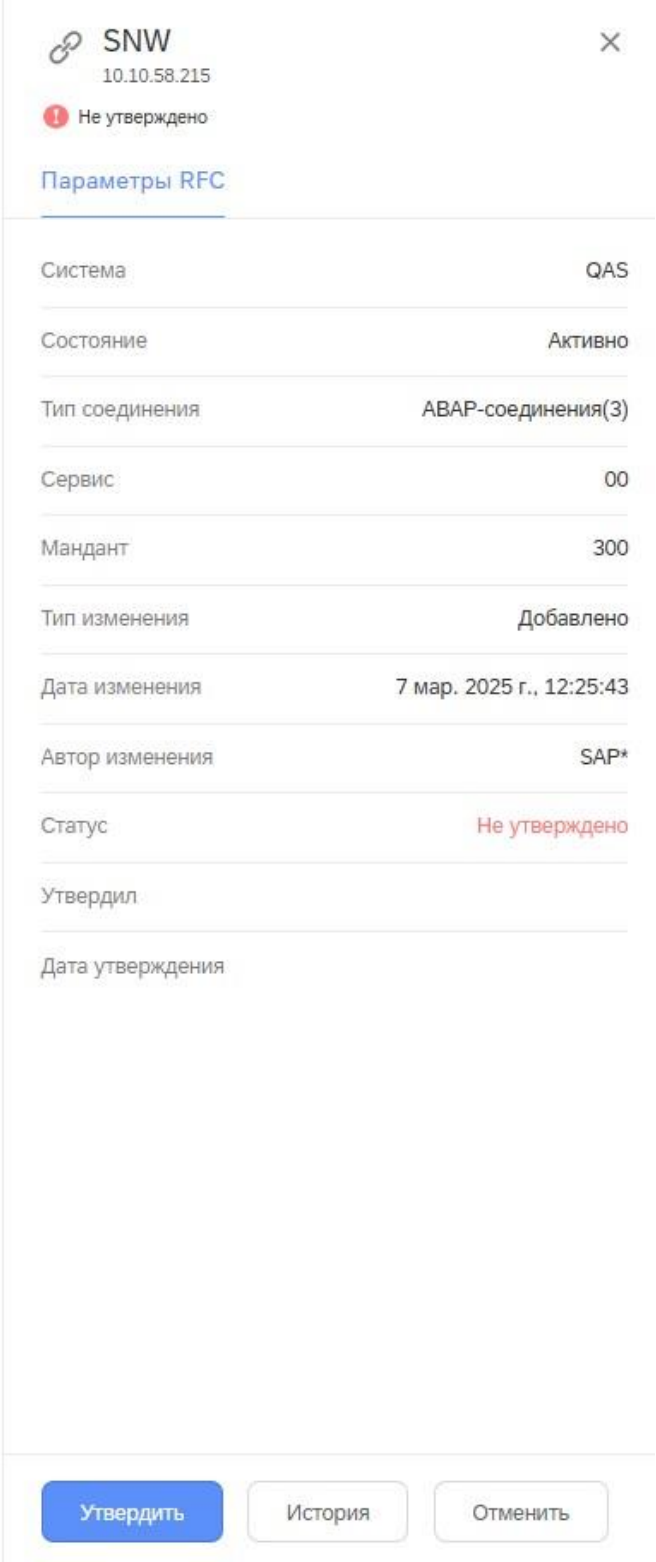


Рисунок 264 – Подробные данные RFC-соединения

7.1.4.1 Утверждение RFC-соединений

Утверждение RFC-соединения – это процедура утверждения, что выбранное RFC-соединение является безопасным.

В модуле «Ландшафт» доступно утверждение и просмотр истории RFC-соединений.

Для утверждения RFC-соединения необходимо выбрать группу агентов, выбрать агента из списка, выбрать RFC-соединение из списка, нажать кнопку *«Утвердить»* (рис. 264).
Примечание. Утверждение RFC-соединения доступно при наведении курсора (рис. 262).
Утверждение RFC-соединений происходит следующим способами:

- во всплывающем окне при просмотре списка RFC-соединений в основной рабочей области модуля «Ландшафт»;
- в подробном описанием RFC-соединения. Для утверждения необходимо выбрать агент из списка, нажать кнопку «Подробнее» в всплывающем окне, выбрать вкладку «RFC-соединения», развернуть RFC-соединение из списка, нажать кнопку «Утвердить»;
- через модальное окно «Агенты». Для утверждения необходимо выбрать агент из списка, нажать кнопку «Подробнее» в всплывающем окне, выбрать вкладку «RFC-соединения», установить флаг напротив RFC-соединения из списка, нажать кнопку «Утвердить»;
- через модальное окно «RFC соединения». Для утверждения необходимо выбрать агент из списка, выбрать RFC-соединение из списка, нажать кнопку «Подробнее», нажать кнопку «Утвердить».

Для просмотра истории RFC-соединения необходимо выбрать группу агентов, выбрать агента из списка, выбрать вкладку «RFC-соединения», выбрать RFC-соединение из списка, нажать кнопку «История».

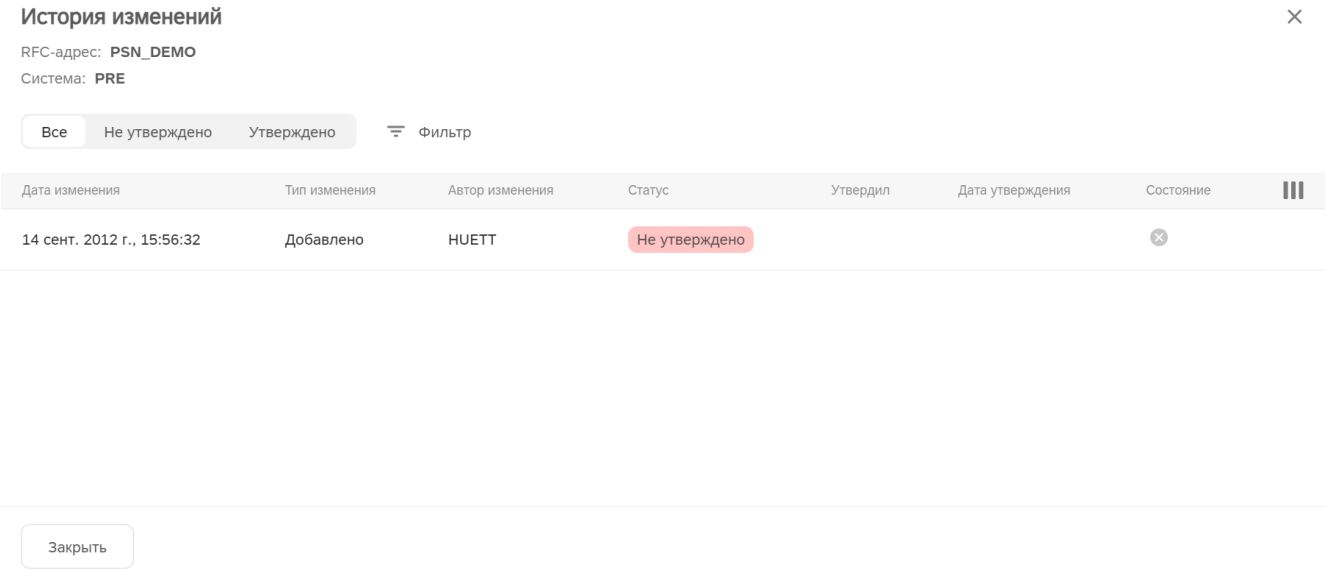


Рисунок 265 – История изменения RFC-соединения

Примечание. Просмотр истории RFC-соединения доступно при наведении курсора (рис. 262).

7.1.4.2 ТС агента

В модуле «Ландшафт» доступен просмотр транспортной системы агента. Транспортная система необходима для графического представления подключенных агентов и RFC-соединений в соответствии с выбранной системой. Схема транспортной системы

состоит из узлов и маршрутов их взаимодействия. Расположение узлов и направления линий маршрутов слева направо от систем разработки к продуктивным системам.
Просмотр ТС агента доступен для следующих версий ПК SafeERP: 4.8.7 и выше.
Просмотр ТС агента осуществляется следующими способами:

- при активации кнопки «ТС» в основной рабочей области модуля «Ландшафт». После активации кнопки «ТС» необходимо выбрать агент в поле «Агент» в окне «Транспортная система»;
- в модальном окне при просмотре подробной информации об агенте;
- в модальном окне при просмотре RFC-соединения;
- во всплывающем окне при просмотре списка агентов в основном рабочей области модуля «Ландшафт». Для просмотра ТС агента необходимо выбрать группу агентов или групп сервера управления, выбрать агента из списка, нажать кнопку «ТС» во всплывающем окне (см. рис. 263). ТС агента представлена на рис. 266.

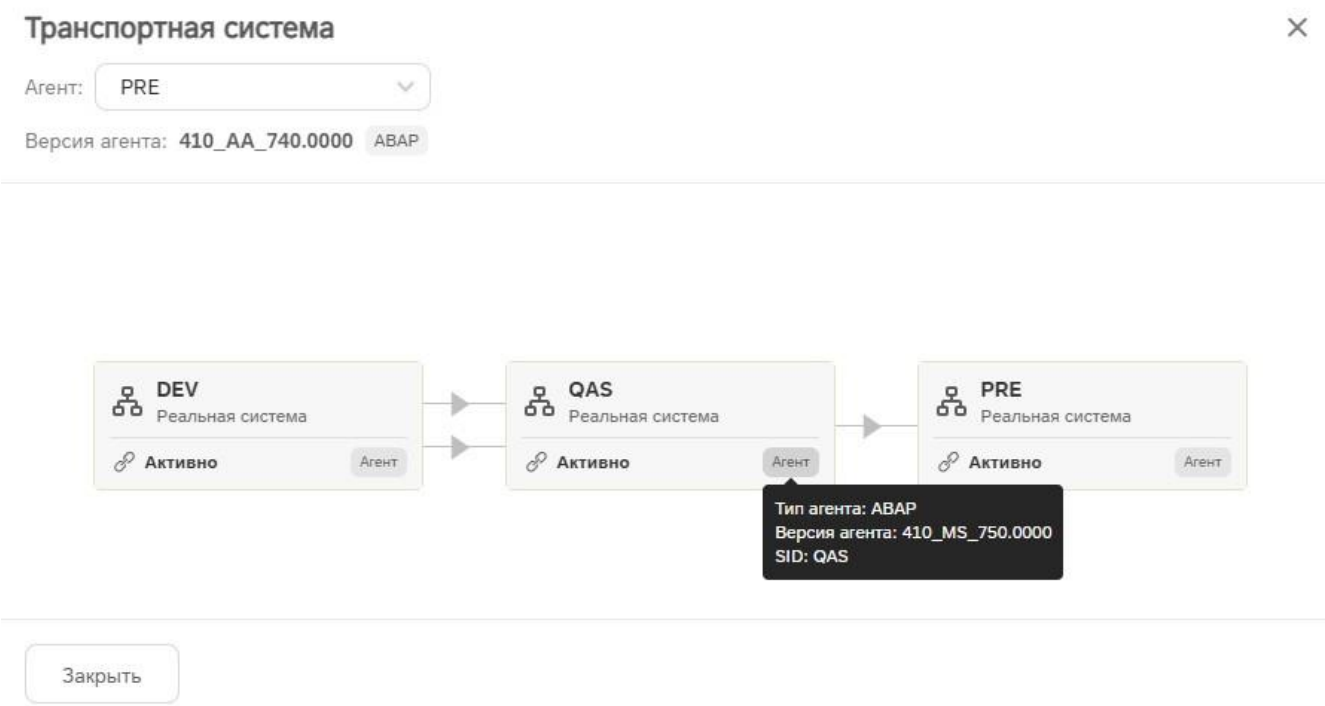


Рисунок 266 – ТС агента

7.1.5 Модуль «Контроль RFC»

Веб-интерфейс модуля «Контроль RFC» предназначен для контроля состояния RFC-соединений в ПК «SafeERP Security Suite», а также для просмотра истории изменения RFC-соединения.
Примечание. Для корректной работы модуля «Контроль RFC» и получения актуальной

информации необходимо ручное обновление данных или настроить периодический запуск фонового задания. Ручное обновление возможно выполнить в транзакции /N/GAZIS/SEGA (см. п. 4.2.3) или в модуле «Администрирование» (см. подпункт 7.1.9.7).

Модуль «Контроль RFC» состоит из следующего (см.рис. 130):

- дерева групп и систем;
- основной рабочей области.

Примечание. Настройка дерева групп и систем доступно в модуле «Агенты» или в транзакции /n/gazis/sega.

В основной рабочей области модуля «Контроль RFC» доступна фильтрация по следующим параметрам:

- RFC-адрес;
- система;
- состояние;
- тип изменения;
- автор изменения;
- дата изменения с;
- дата изменения по;
- утвердил;
- дата утверждения с;
- дата утверждения по;
- тип соединения;
- пароль;
- достоверная система;
- RFC SNC;
- дата создания с;
- дата создания по.

Доступны следующие типы изменений RFC соединений:

- добавлено – RFC соединения были добавлены в систему;
- изменено – RFC соединения были изменены;
- удалено – RFC соединения были удалены из системы.

Доступные статусы для RFC соединений:

- утверждено – RFC-соединение было утверждено;
- не утверждено – RFC-соединение не было утверждено

Для утверждения RFC-соединения необходимо выбрать, поставить флаг напротив RFC-соединения, нажать кнопку *«Утвердить»* (см. рис. 130).

Для просмотра истории RFC-соединения необходимо выбрать соединение из списка.

Окно «История изменений» представлено на рис. 267.

В данном окне доступен просмотр утвержденных, не утвержденных и всех событий, а также кнопка *«Фильтр»*.

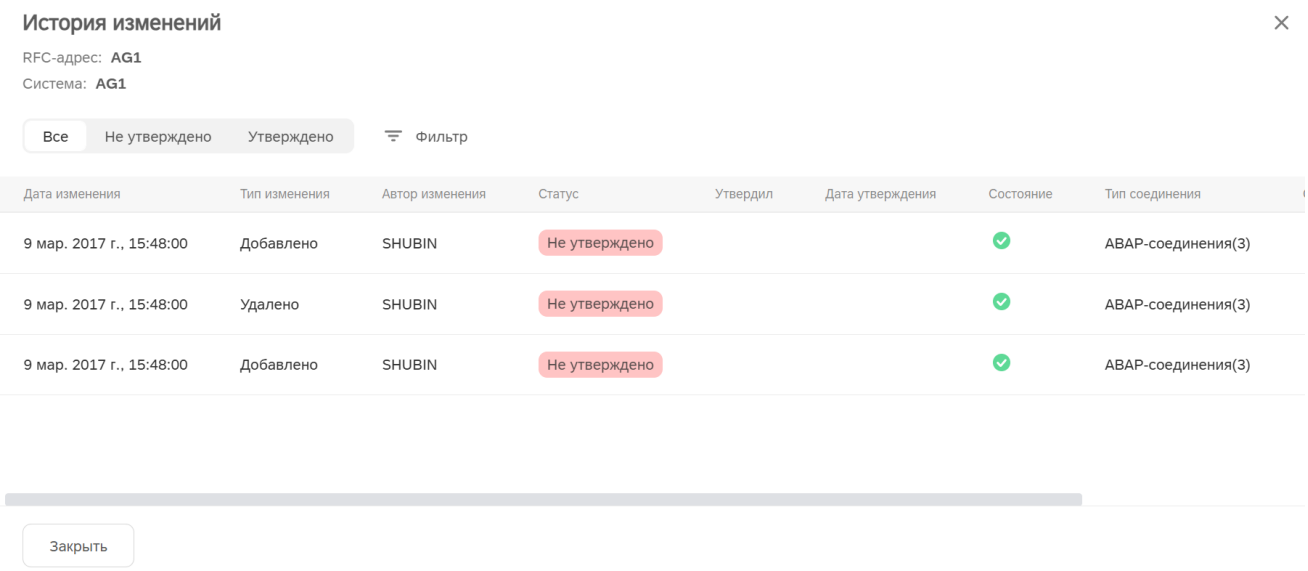


Рисунок 267 – Окно «История изменений» для RFC соединения

В окне «История изменений доступен просмотр следующих полей:

- «Статус»;
- «Система»;
- «Тип соединения»;
- «RFC-адрес»;
- «Описание»;
- «Целевой пост»;
- «Автор изменения»;
- «Дата изменения»;
- «Сервис»;
- «Мандант»;
- «Текущий пользователь»;
- «Пользователь»;
- «Язык»;
- «Пароль»;
- «Экран RFC-хода»;
- «Достоверная система»;
- «RFC SNC»;
- «Полномочия»;
- «Создал»;
- «Дата создания».

В окне «История изменений» доступна фильтрация по следующим параметрам:

- «Состояние»;
- «Тип изменения»;
- «Автор изменения»;
- «Дата изменения с»;

— «Дата изменения по»;
— «Утвердил»;
— «Дата утверждения с»;
— «Дата утверждения по»;
— «Тип соединения»;
— «Пароль»;
— «Достоверная система»;
— «RFC SNC».

7.1.6 Модуль «Профили»

Веб-интерфейс модуля «Профили» предназначен для ведения профилей в веб-интерфейсе ПК «SafeERP Security Suite». Элементы основной рабочей области модуля «Профили» представлены на рис. 131.

Функция ведения профилей предоставляется только пользователям с полномочиями на администрирование ПК «SafeERP Security Suite».

В данном модуле используется профили для сканера и анализа кода ABAP.

Профили бывают двух типов:

— стандартные – входят при поставке комплекса «SafeERP Security Suite»;
— собственные – создаются администратором комплекса «SafeERP Security Suite».

В основной рабочей области «Профили» доступны следующие действия:

1) Поиск профиля в списке профилей.
2) Просмотр профилей.
3) Создание собственного профиля.
4) Редактирование собственного профиля.
5) Экспорт профиля.
6) Импорт профиля.
7) Удаление собственного профиля.
8) Просмотр проверок.
9) Создание собственных проверок.
10) Добавление проверок в собственные профили.
11) Редактирование проверок.
12) Удаление проверок.

7.1.6.1 Профили для модуля «Сканер»

Для работы с профилями необходимо выбрать раздел «Сканер» в боковом меню. В профили для сканера входят проекты типа «КН».

7.1.6.1.1 Поиск профиля

Поиск профиля выполняют через форму поиска (фильтр) в основной рабочей области «Профили» (рис. 131).

Чтобы начать поиск профиля по его названию, необходимо ввести название (символьную маску) в форме поиска (рис. 268).

Рисунок 268 – Область поиска профиля

Откроется окно с результатами поиска профиля по названию, представленное на рис. 269.

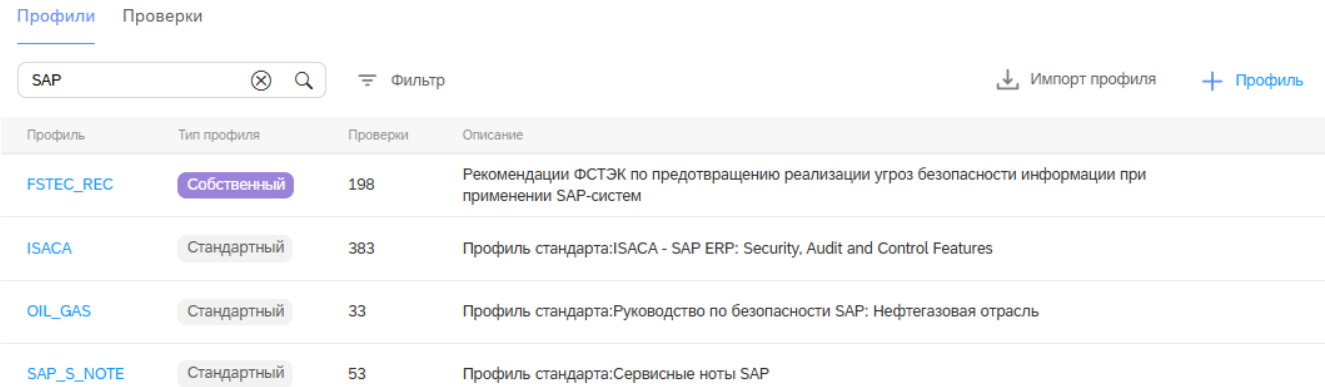


Рисунок 269 – Результат поиска профиля по названию

Для сброса введенных данных предусмотрена кнопка *«Сбросить».*

Примечание. Доступен поиск профиля по типу. Для поиска профиля по типу необходимо нажать на кнопку *«Фильтр»*, выбрать тип профиля (рис. 270).

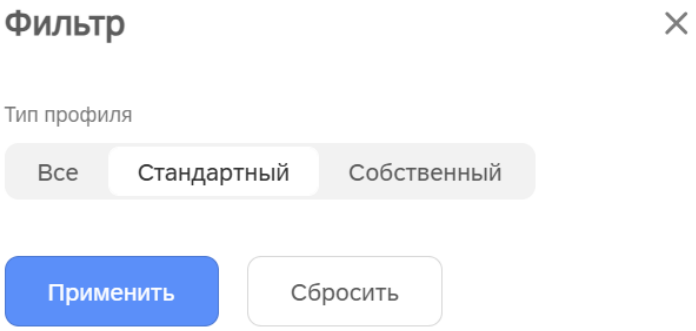


Рисунок 270 – Окно «Фильтр» во вкладке «Профили»

7.1.6.1.2 Просмотр профилей

Просмотр стандартных или собственных профилей выполняют с помощи кнопки *«Фильтр»* переключения в основной рабочей области модуля «Профили» (рис. 268).

Для просмотра профилей необходимо выбрать соответствующую вкладку (рис. 271).

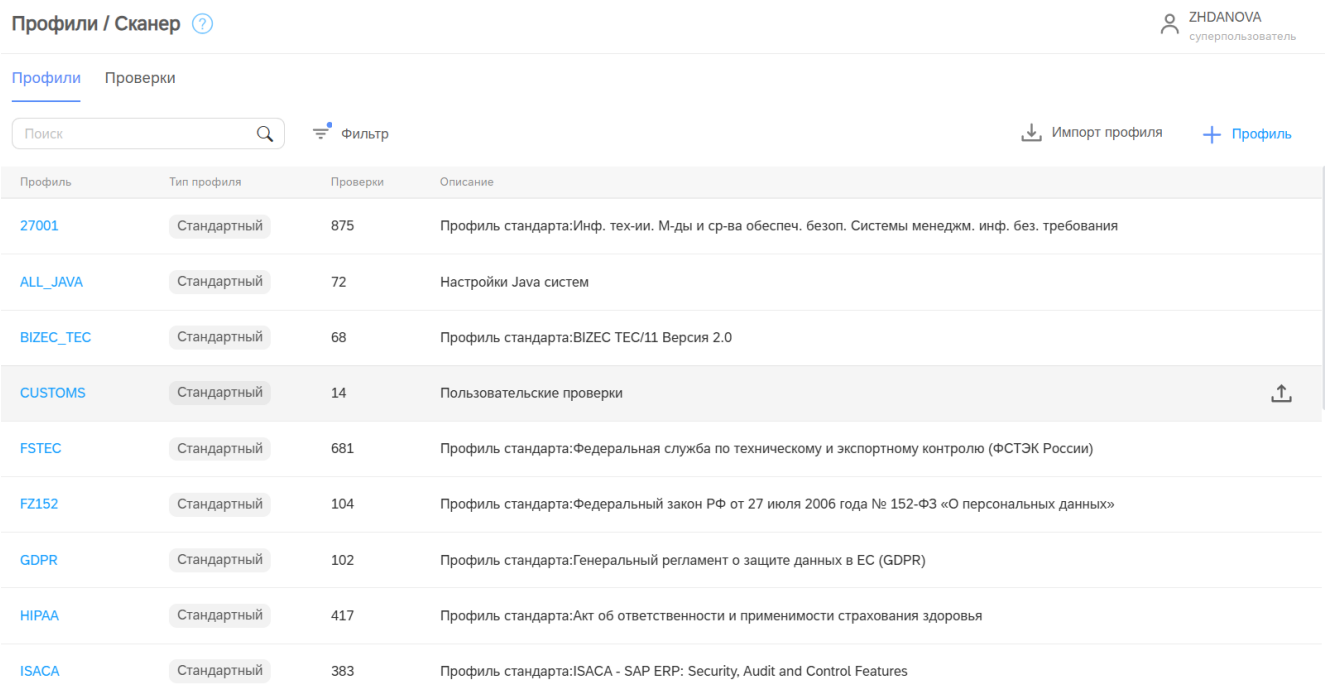


Рисунок 271 – Результат отображения определенного типа профиля

7.1.6.1.2.1 Просмотр проверок в профиле

Просмотр проверок доступен для всех типов проверок (собственных и стандартных). В описании проверок представлены следующие поля:

- «Параметры»;
- «Профили»;
- «Описание»;
- «Ссылки»;
- «Схема»;
- «Возможные последствия»;
- «Рекомендации».

Для просмотра проверок в профиле необходимо выполнить следующие действия:

1) Выполнить действия согласно подпункту 7.1.6.1.2
2) Выбрать проверку из списка.

Примечание. При просмотре профиля доступна кнопка «Фильтр». Доступен фильтрация проверок по следующим параметрам:

- категория (категория проверки. Доступны следующие категории проверок: все, стандартная, собственная);
- группы проверок;
- подгруппы проверок;
- мандатозависимость;
- тип инстации (для каких типов агентов, применяются проверки);
- ключевые параметры проверки.

7.1.6.1.3 Создание собственного профиля

Чтобы создать собственный профиль, необходимо нажать кнопку *«+ Профиль»* в основной рабочей области «Профили» (рис. 131).

При нажатии кнопки добавления профиля разворачивается окно «Добавить профиль» (рис. 272).

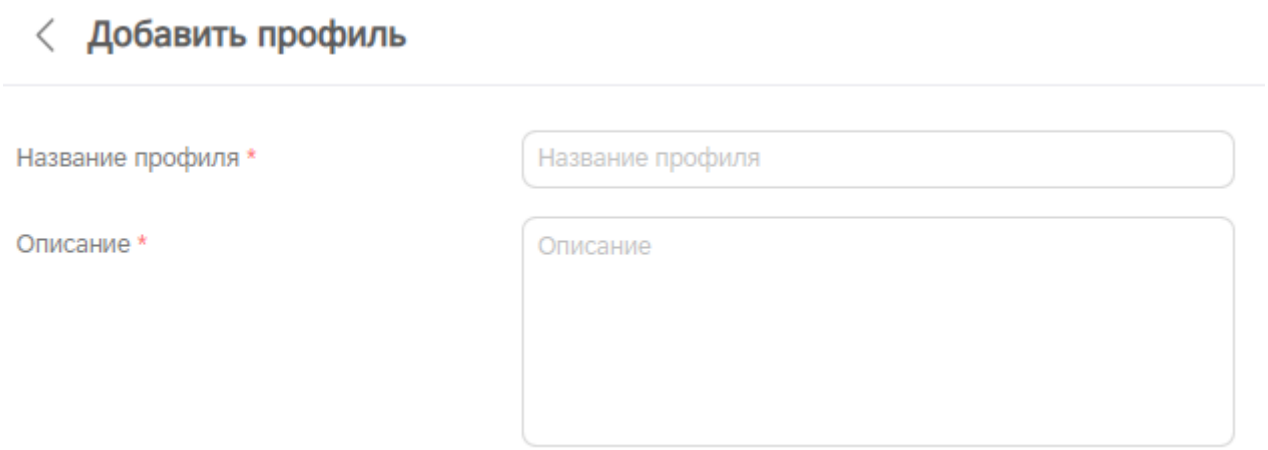


Рисунок 272 – Окно «Добавить профиль» для модуля «Сканер»

После ввода названия и описания профиля в окне «Создание профиля» необходимо нажать кнопку *«Сохранить»*. Кнопка создания профиля станет активной только в случае определения всех параметров.

Примечание. При создании профиля доступно добавление проверок из списка или создание собственной проверки. Подробное описание редактирования профиля см. в подпункте 7.1.6.1.4

7.1.6.1.4 Редактирование собственного профиля

Редактирование осуществляется в следующих полях:

- «Описание»;
- «Критичности проверок»;
- Добавление или удаление проверок.

Для редактирования описания собственного профиля необходимо в основной рабочей области «Профили» (см. рис. 131) выбрать профиль из списка или ввести название, внести изменения, нажать кнопку *«Сохранить».*

Для добавления проверок из существующих в собственный профиль необходимо нажать кнопку *«+ Проверка»*, выбрать вкладку «Выбрать из существующих» (рис. 273), поставить флаг ☑ напротив проверки, нажать кнопку *«Добавить в профиль»*.

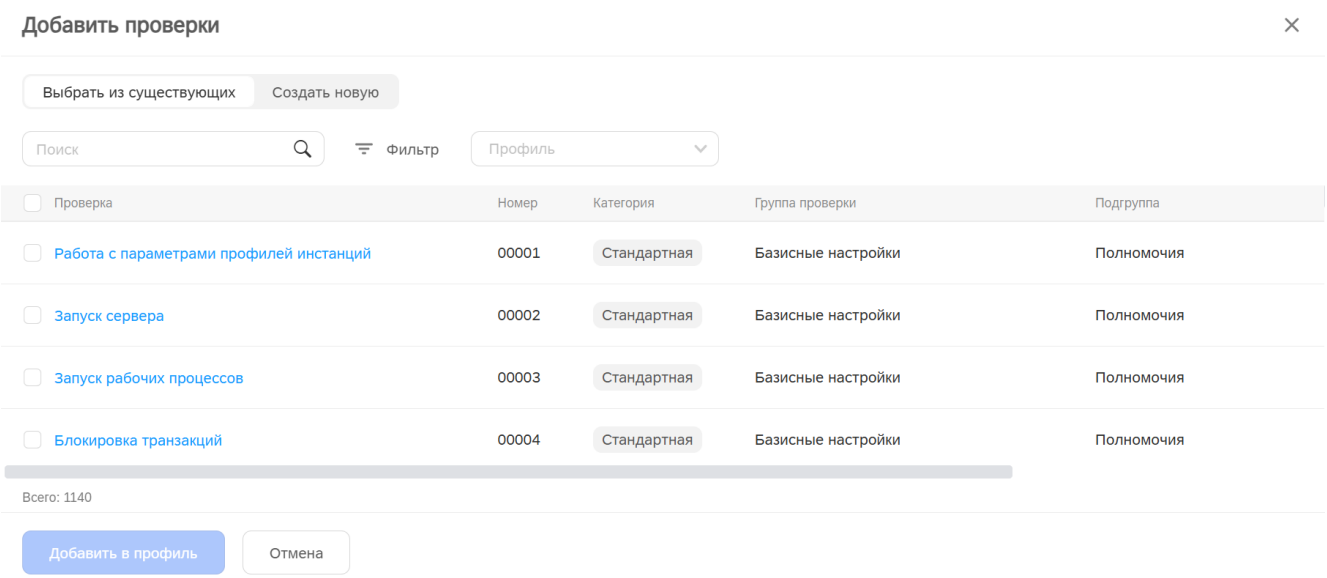


Рисунок 273 – Окно «Добавить проверки»

В окне «Добавить проверки» предоставляется возможность создать новую проверку. Для создания новой проверки необходимо нажать кнопку *«+ Проверка»*, выбрать вкладку «Создать новую», выполнить действия согласно подпункту 7.1.6.1.8.2

Примечание. При добавлении проверок в профиль доступна кнопка «Фильтр». Доступна фильтрация проверок по следующим параметрам:

- категория (категория проверки. Доступны следующие категории проверок: все, стандартная, собственная);
- группы проверок;
- подгруппы проверок;
- мандатозависимость;
- тип инстации (для каких типов агентов, применяются проверки);
- ключевые параметры проверки.

Редактирование проверок осуществляется в следующих областях:

- название проверки;
- уровень критичности.

Для редактирования проверки необходимо выбрать собственный профиль из списка или ввести название, выбрать вкладку «Выбрать из существующих», внести изменения, нажать кнопку *«Сохранить».*

Примечание. Изменения проверок сохраняются в выбранном профиле.

Для удаления проверок из собственного профиля необходимо выбрать профиль, поставить флаг напротив ☑ проверок, нажать кнопку *«Удалить из профиля»*, подтвердить действие.

7.1.6.1.5 Экспорт профилей

Экспорт профилей осуществляется следующего формата *.prf. Доступен экспорт стандартных и собственных профилей.

Экспорт профилей осуществляется следующими способами:

— при просмотре профиля;
— при просмотре списка профилей.

Для экспорта профиля со страницы просмотра профиля необходимо нажать кнопку «Экспорт профиля».

Для экспорта профиля со страницы просмотра списка профилей необходимо нажать кнопку «Экспорт профиля» в строке профиля проекта.

7.1.6.1.6 Импорт профилей

Импорт профилей осуществляется следующего формата *.prf. Доступен импорт стандартных и собственных профилей.

Импорт профилей осуществляется со страницы списка профилей.

Для импорта профиля необходимо нажать кнопку *«Импорт профиля»*, выбрать профиль файл профиля в открывшемся окне, нажать кнопку *«Открыть»* (рис. 274).

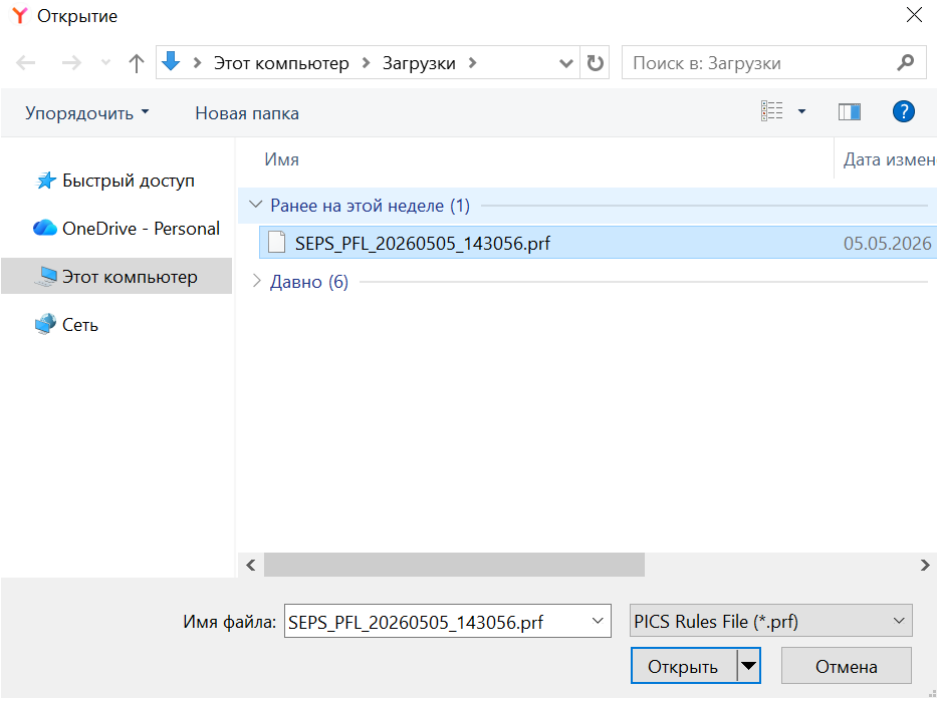


Рисунок 274 – Выбор профиля для импорта

7.1.6.1.7 Удаление собственного профиля

Для удаления собственного профиля необходимо в основной рабочей области «Профили» (см. рис. 131) нажать кнопку *«Удалить»*.

Примечание. Невозможно удалить стандартные профили. После активации кнопки *«Удалить»* откроется окно подтверждения действия. После подтверждения действия выбранный профиль будет удален.

7.1.6.1.8 Проверки

Для анализа системы используют два типа проверок: стандартные (входят в пакет при поставке) и собственные (создает администратор).

Для создания собственных проверок необходимо учесть следующие параметры: тип проверки и условия.

Примечания:

1. Для каждого типа проверок используют два критерия: первый – для удачного

прохождения, второй – для неудачного. В каждом поле вводится любой тип данных.

2. При изменении типа проверок не изменяются ранее внесенные данные в условиях уровней критичности.
3. При введении недостаточного количества данных для проверок будет показано сообщение «Не хватает данных для создания записи».

В условия проверки входят следующие данные:

- критичность (высокая, средняя, низкая, информация, неприменимо, корректно);
- опция (равно, не равно, больше, меньше, больше или равно, меньше или равно, между … и … , не между … и …);
- значение, минимальное для уровня критичности;
- значение, максимальное для уровня критичности.

Описание настроек собственных проверок представлено в подпунктах 7.1.6.1.8.2 – 7.1.6.1.8.2.9.

7.1.6.1.8.1 Просмотр проверок

Для просмотра проверок во соответствующей необходимо выбрать проверку из списка или ввести наименование или номер проверки в поисковую строку (рис. 275).

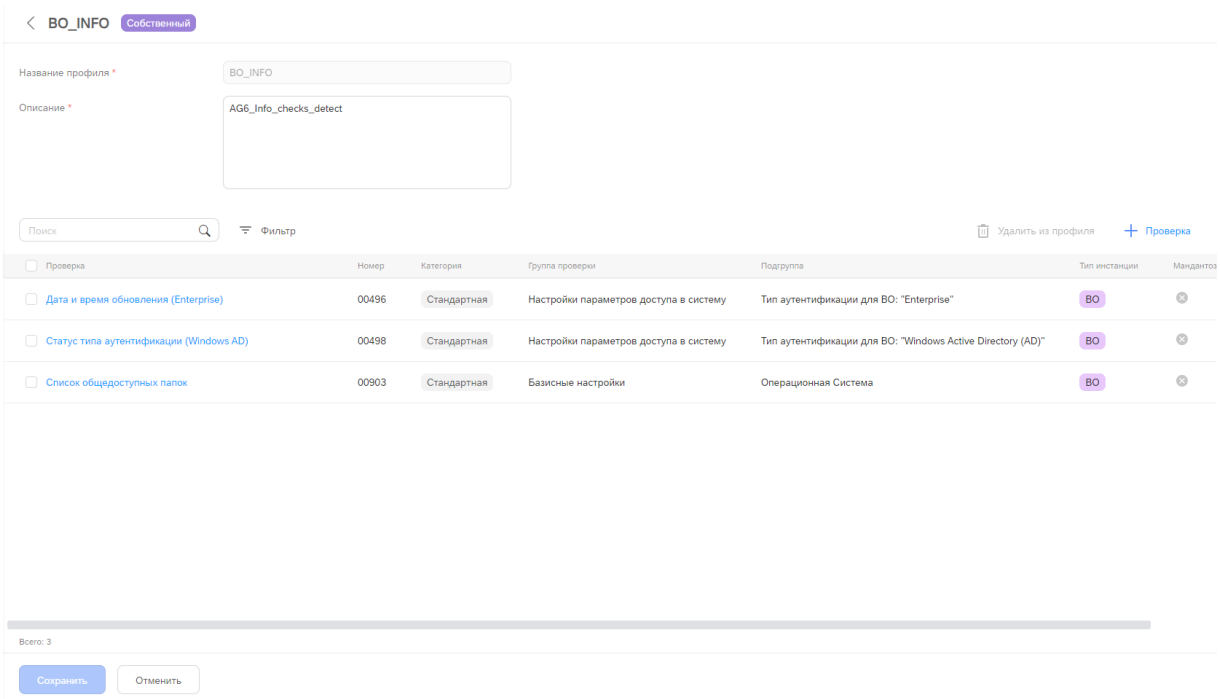


Рисунок 275 – Собственный профиль для проектов типа КН

Подробное описание проверки представлено на рис. 276.

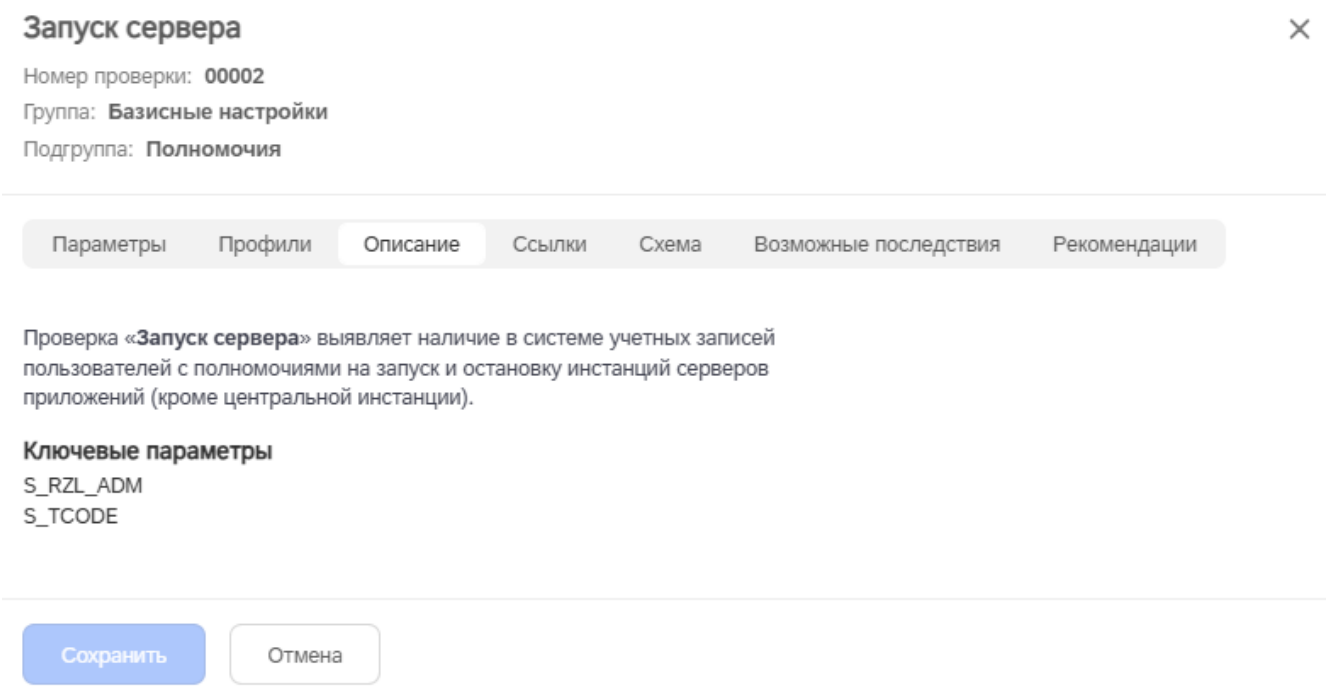


Рисунок 276 – Подробное написание проверки

Примечание. При просмотре списка проверок доступна кнопка «Фильтр». Доступен фильтрация проверок по следующим параметрам:

- категория (категория проверки. Доступны следующие категории проверок: все, стандартная, собственная);
- группы проверок;
- подгруппы проверок;
- мандатозависимость;
- тип инстации (для каких типов агентов, применяются проверки);
- ключевые параметры проверки.

7.1.6.1.8.2 Создание собственных проверок

Создание собственных проверок доступно пользователю с ролью «Администратор».

Примечание. Подробное описание собственных проверок представлено в таблице 15.

Таблица 15 – Подробное описание собственных проверок для модуля «Сканер»

Наименование	Описание
Проверка параметров профилей инстанции [PPI_CUST]	Создается проверка, в которой можно ввести имя ППИ и его граничные значения
Проверка полномочий на уровне авторизационных объектов [AUTHO_CUST]	Проверка пользователей, которые обладают данными авторизаций, поставленных на учёт
Авторизационная группа таблицы [TABU_CUST]	Проверяют наличие группы полномочий у таблицы. Группа полномочий на таблицы позволяет проверять разрешение на работу с таблицей только тем, кому это

	разрешено. Присвоение возможно каждой таблице, включая стандартные.
Активность сервиса [ICF_CUST]	Проверяет активность/неактивность определенного сервиса в системе
Проверка блокировок транзакций [BLOCK_CUST]	Любая транзакция в системе может быть заблокирована для работы пользователей. Проверка проверяет блокировки
Наличие указанных записей в таблицах/Значение в поле таблицы [LINE_CUST]	Возможны проверки значений определенных полей в таблицах БД. Условие пишет пользователь. Свободное описание проверок, но надо знать, какие поля есть в таблице и чему должны быть равны значения полей
Проверка пользователей с присвоенной ролью [ROLE_CUST]	В проверке задается определённая роль. Выявляются пользователи, которым присвоена роль
Проверка пользователей с присвоенным профилем [PROF_CUST]	В проверке задается определённый профиль. Выявляются пользователи, которым присвоен профиль
Уровень доступа к директории/Привилегии доступа к директории [FILE_CUST]	В проверке указывается папка на сервере приложений SAP. Проверяется доступ к папке, если есть возможность для этого. Папки должны выбираться из разрешённого списка для сервера приложений

Для создания проверок необходимо выполнить следующие действия:

1) Нажать кнопку *«+ Проверка»* (см. рис. 269). Откроется окно, в котором необходимо ввести название, описание проверки (см. рис. 277), выбрать тип проверок и задать условия для уровней критичности (см. рис. 278).

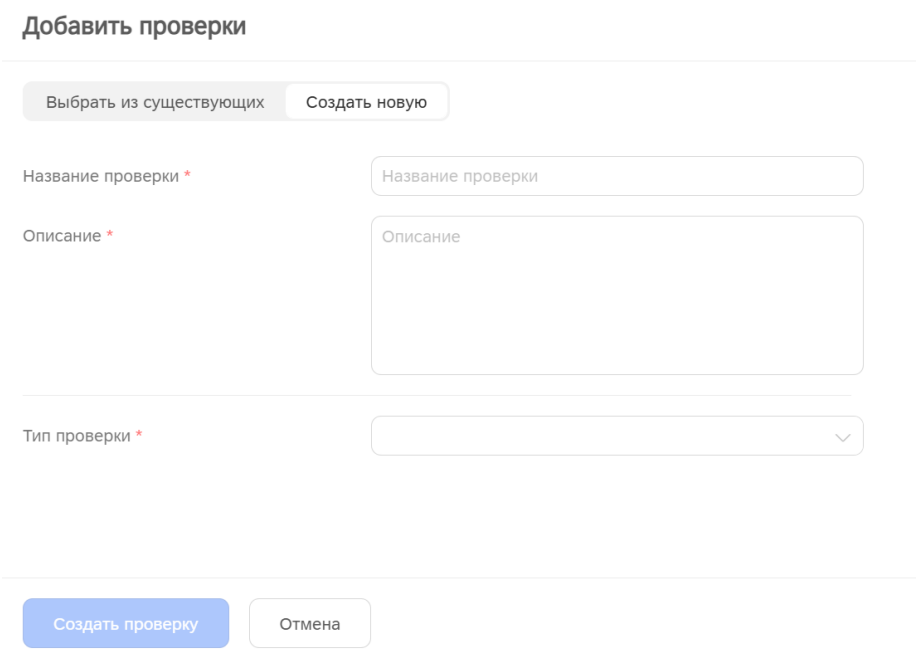


Рисунок 277 – Поле для задания типа проверки

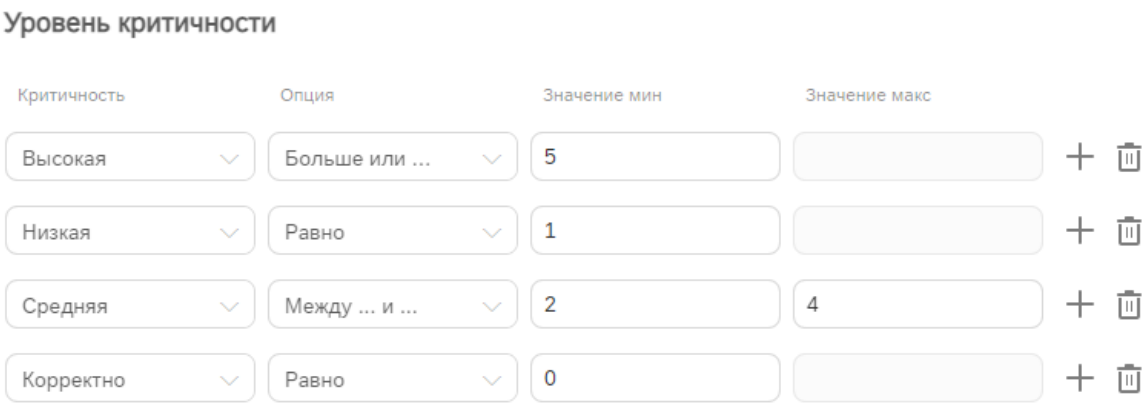


Рисунок 278 – Поля для задания условий для уровней критичности

2) После создания проверки в открывшемся окне будет указано: номер собственной проверки, название профиля, группа и подгруппа (рис. 279). Необходимо нажать кнопку *«ОК»*.

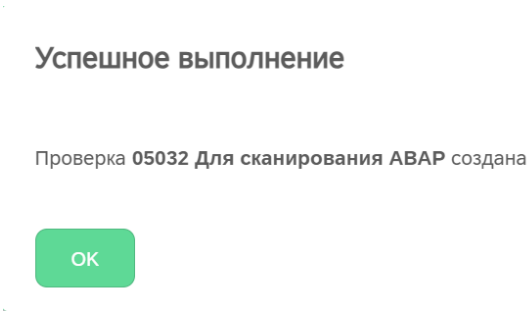


Рисунок 279 – Окно о создании собственной проверки

7.1.6.1.8.2.1 Проверка полномочий на уровне авторизированных объектов [AUTHO_CUST]

Для настройки проверки на уровне авторизированных объектов, необходимо задать название и описание проверки (см. рис. 277), условия для уровней критичности проверки (см. рис. 278) и заполнить данные в окне «Добавить шаблон проверки» (рис. 280, 281).

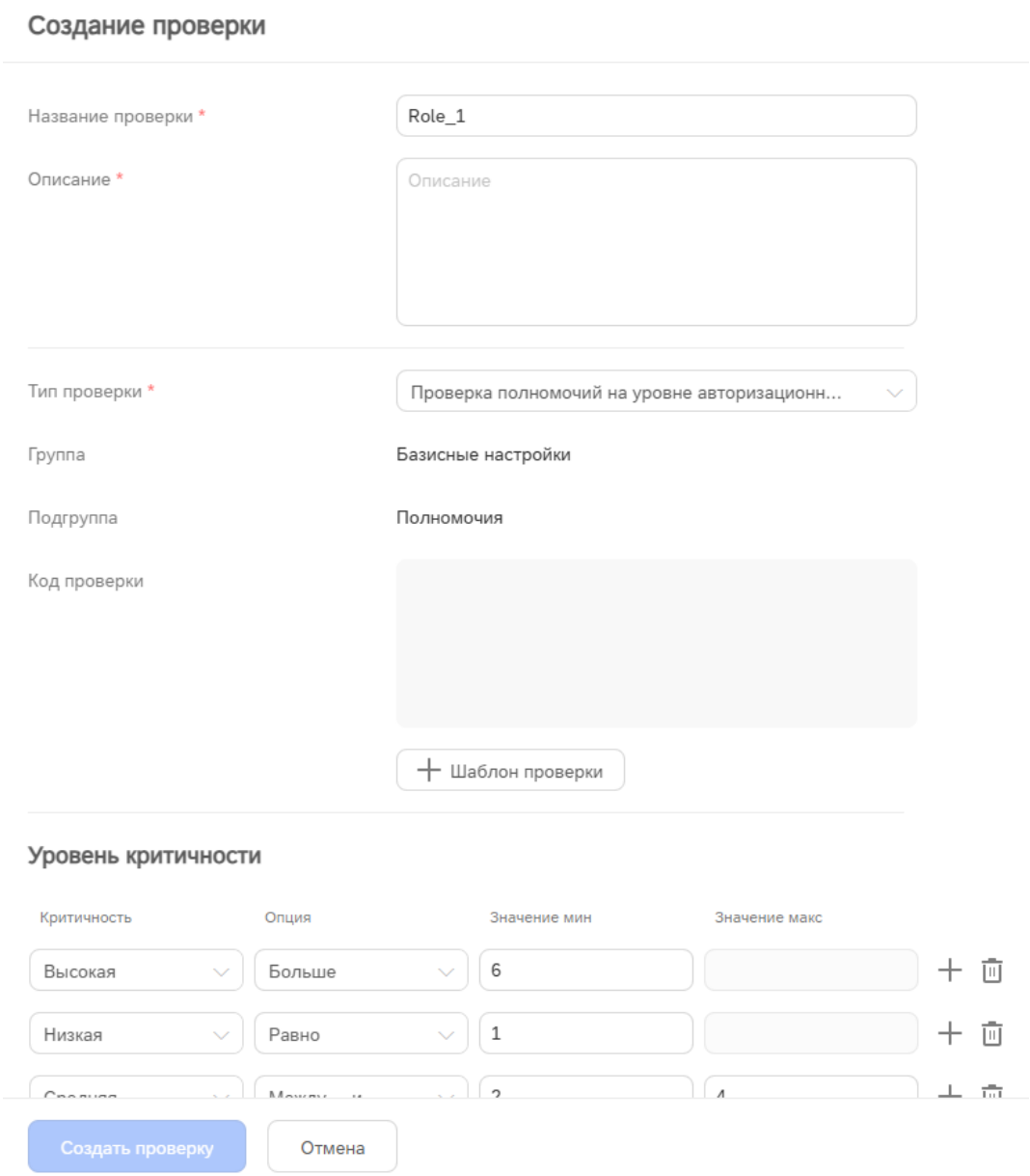


Рисунок 280 – Параметры для проверки на уровне авторизированных объектов

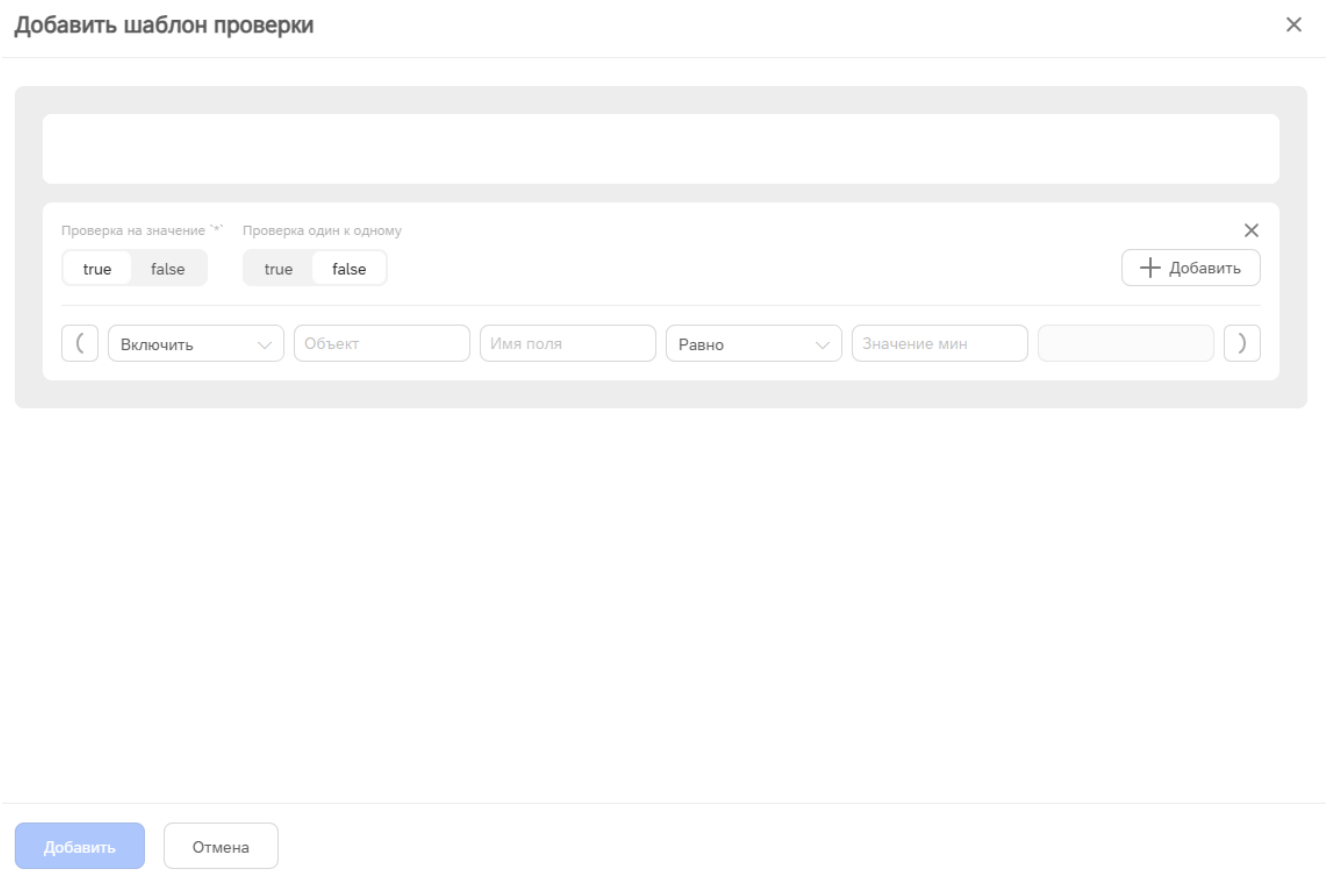


Рисунок 281 – Окно «Добавить шаблон проверки»

7.1.6.1.8.2.2 Проверка блокировок транзакций [BLOCK_CUST]

Для настройки проверки на блокировку транзакций, необходимо ввести название и описание проверки (см. рис. 277), условия для уровней критичности проверки (см. рис. 278) и имя транзакции (рис. 282).

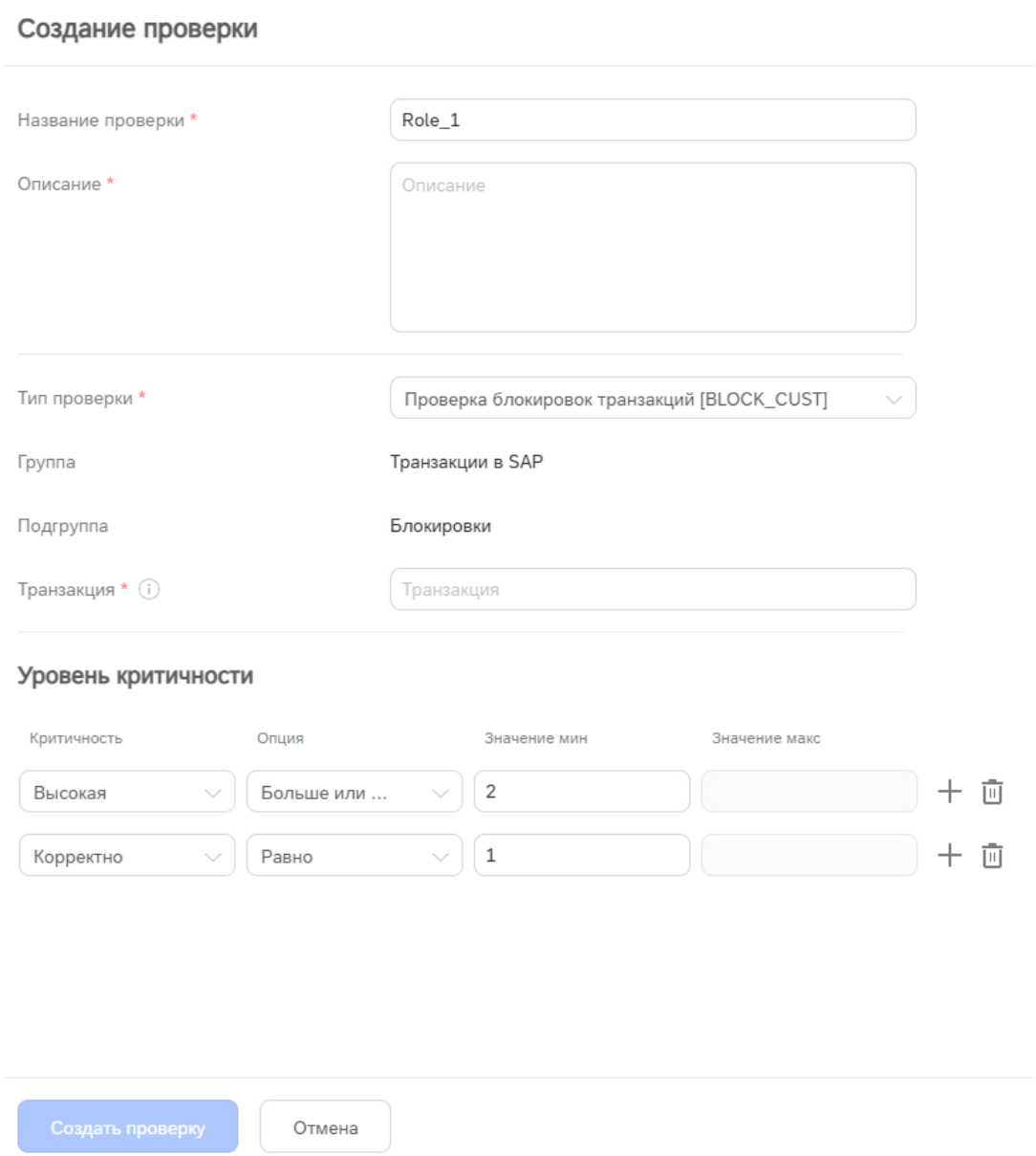


Рисунок 282 – Параметры для проверки на блокировку транзакций

7.1.6.1.8.2.3 Уровень доступа к директории/Привилегии доступа к директории [FILES_CUST]

Для настройки уровня доступа к директории необходимо ввести название и описание проверки (см. рис. 277), условия для уровней критичности проверки (см. рис. 278) и указать следующие параметры (рис. 283):

- директорию;
- тип объекта;
- вариант проверки (уровень доступа, уровень привилегий).

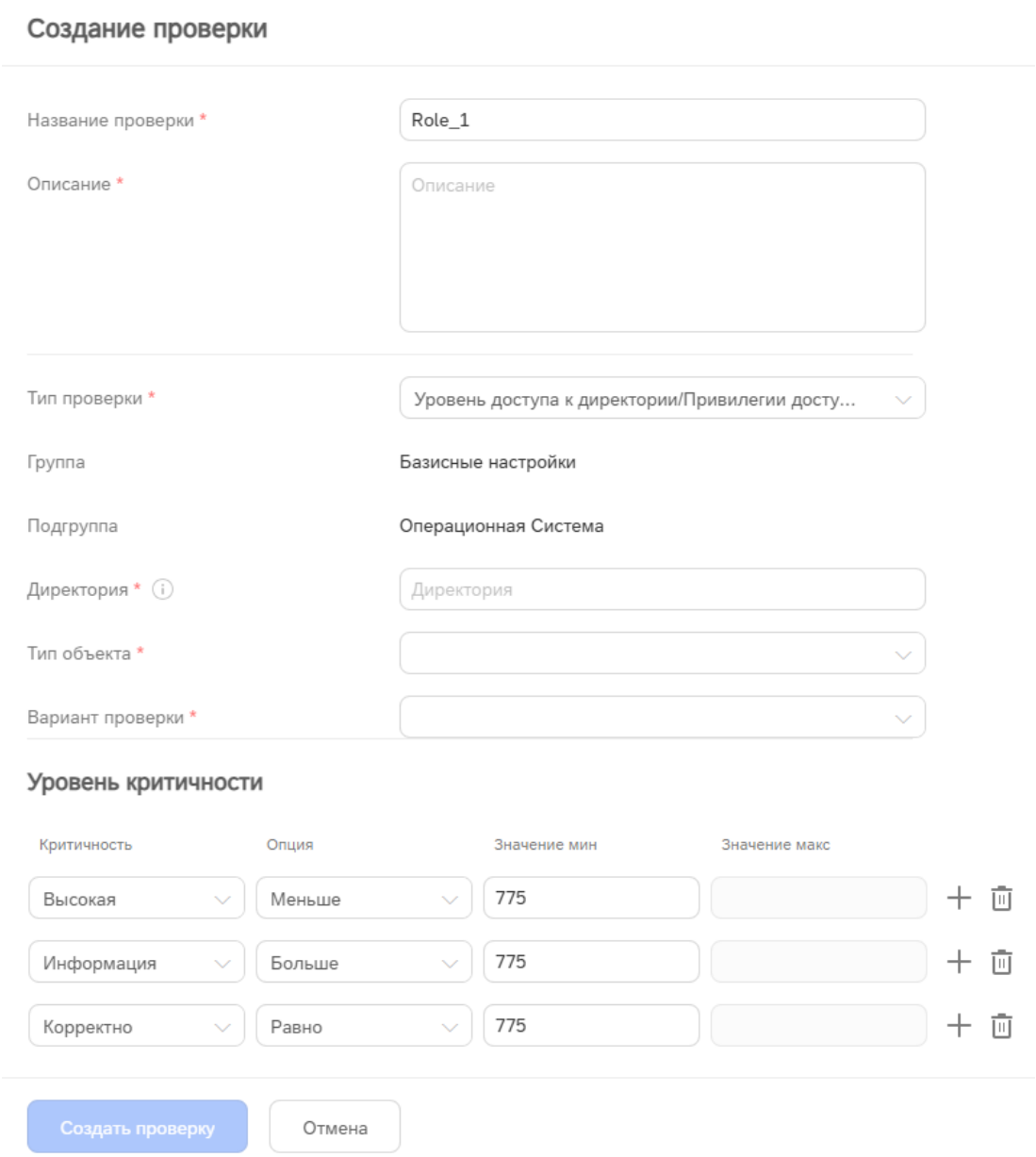


Рисунок 283 – Параметры для проверки уровня доступа директории/привилегии к доступу директории

7.1.6.1.8.2.4 Активность сервиса [ICF_CUST]

Для настройки активности сервиса необходимо ввести название и описание проверки (см. рис. 277), условия для уровней критичности проверки (см. рис. 278) и имя сервиса (рис. 284).

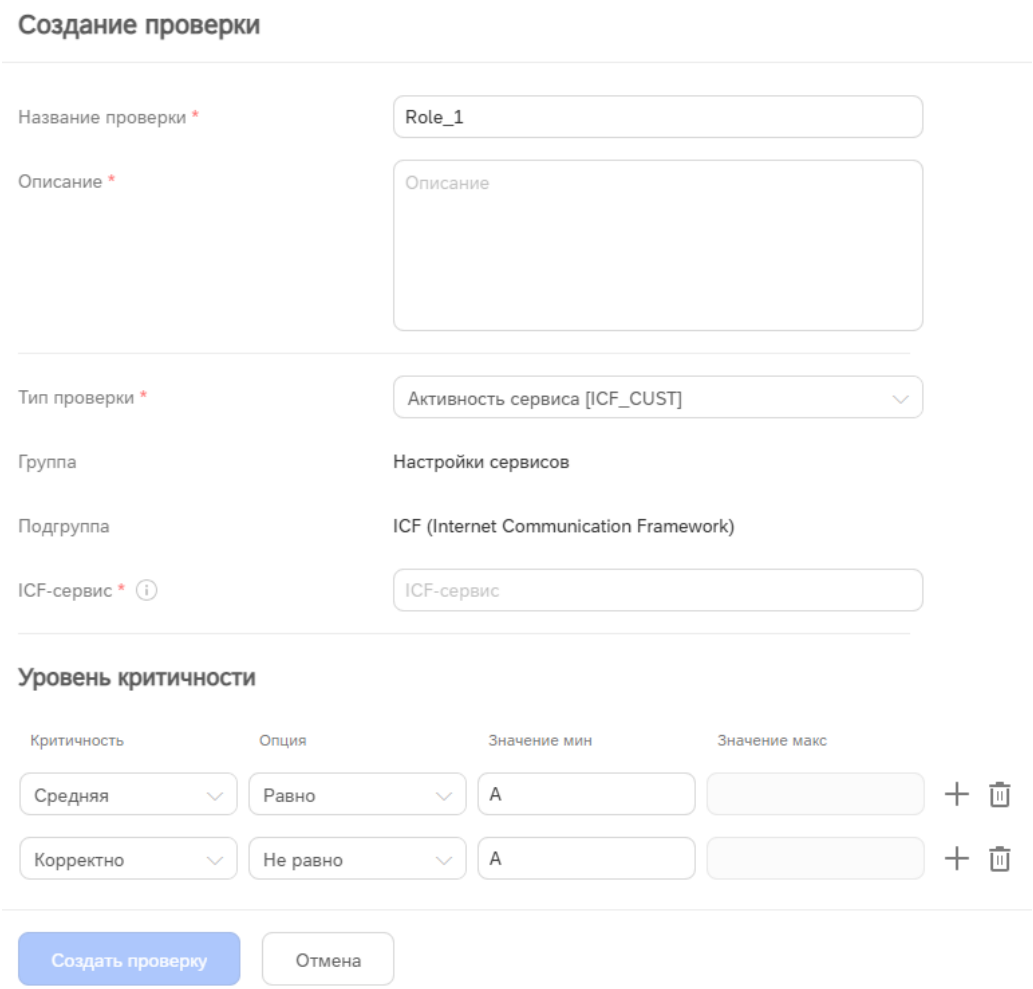


Рисунок 284 – Параметры для проверки активность сервиса

7.1.6.1.8.2.5 Наличие указанных записей в таблице/ Значение в поле таблицы [LINES_CUST]

Для настройки наличия указанных записей в таблице необходимо ввести название и описание проверки (см. рис. 277), условия для уровней критичности проверки (см. рис. 278) и указать следующие параметры (рис. 285):

- имя таблицы;
- вариант проверки (количество записей/значение в поле таблицы);
- условие выборки;
- поля таблицы для вывода в отчет (требуется вводить символьные значения. Настраивается так же, как и критичность).

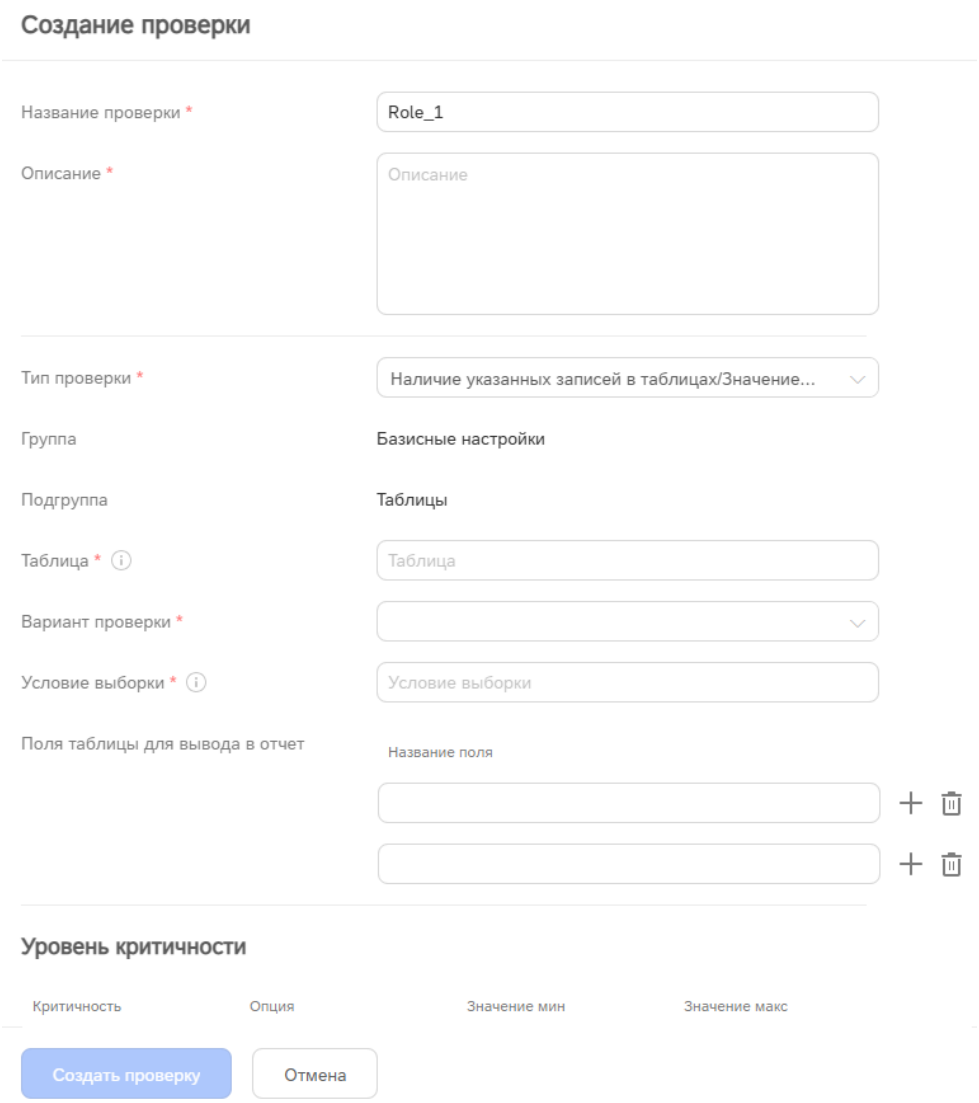


Рисунок 285 – Параметры для проверки наличия указанных записей в таблице/ значение в поле таблицы

7.1.6.1.8.2.6 Проверка параметров профиля инстанции [PPI_CUST]

Для настройки проверки параметров профиля инстанции необходимо ввести название и описание проверки (см. рис. 277), условия для уровней критичности проверки (см. рис. 278) и имя параметра профиля инстанции (рис. 286).

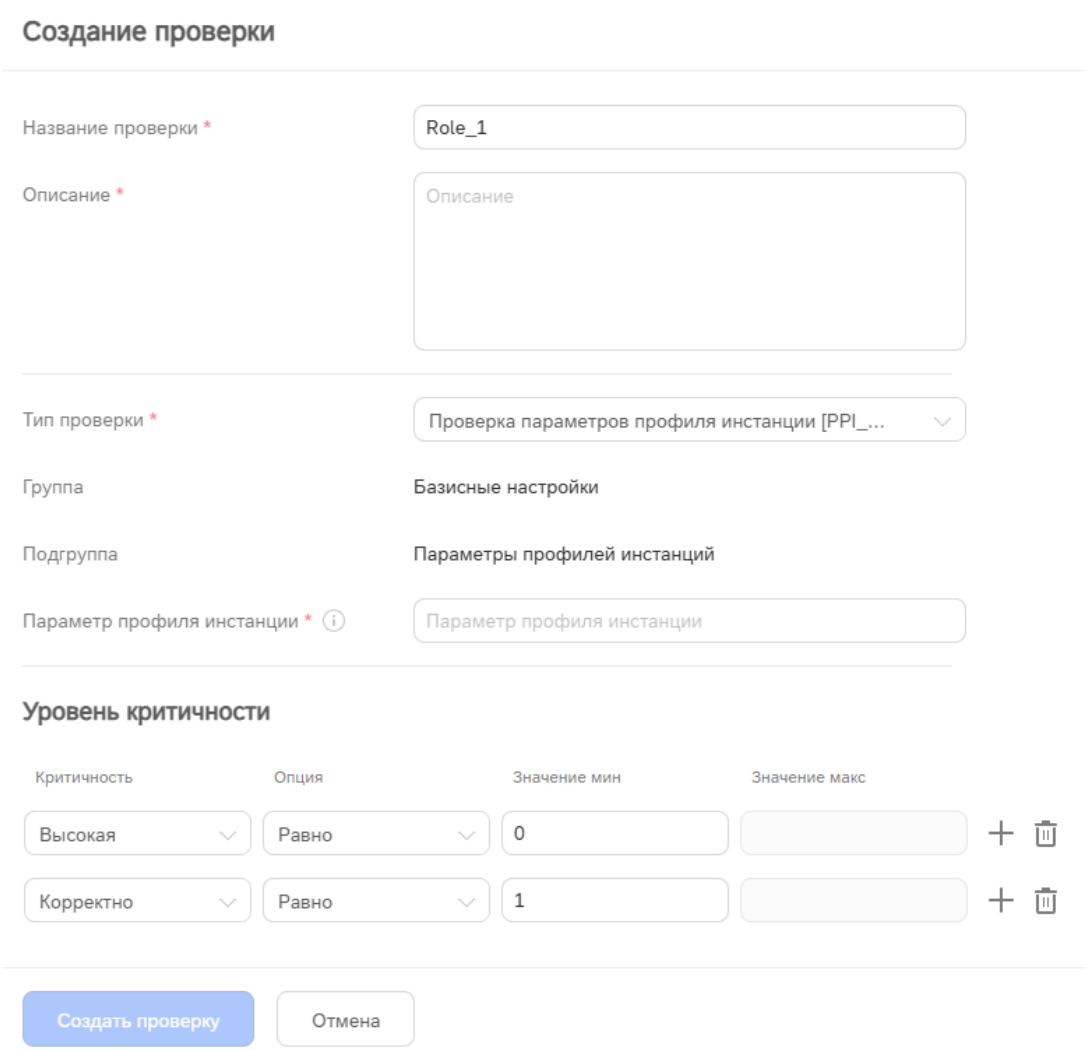


Рисунок 286 – Параметры для проверки параметров профиля инстанции

7.1.6.1.8.2.7 Проверка пользователей с присвоенным профилем [PROF_CUST]

Для настройки проверки пользователей с присвоенным профилем необходимо ввести название и описание проверки (см. рис. 277), условия для уровней критичности проверки (см. рис. 278) и имя профиля (рис. 287).

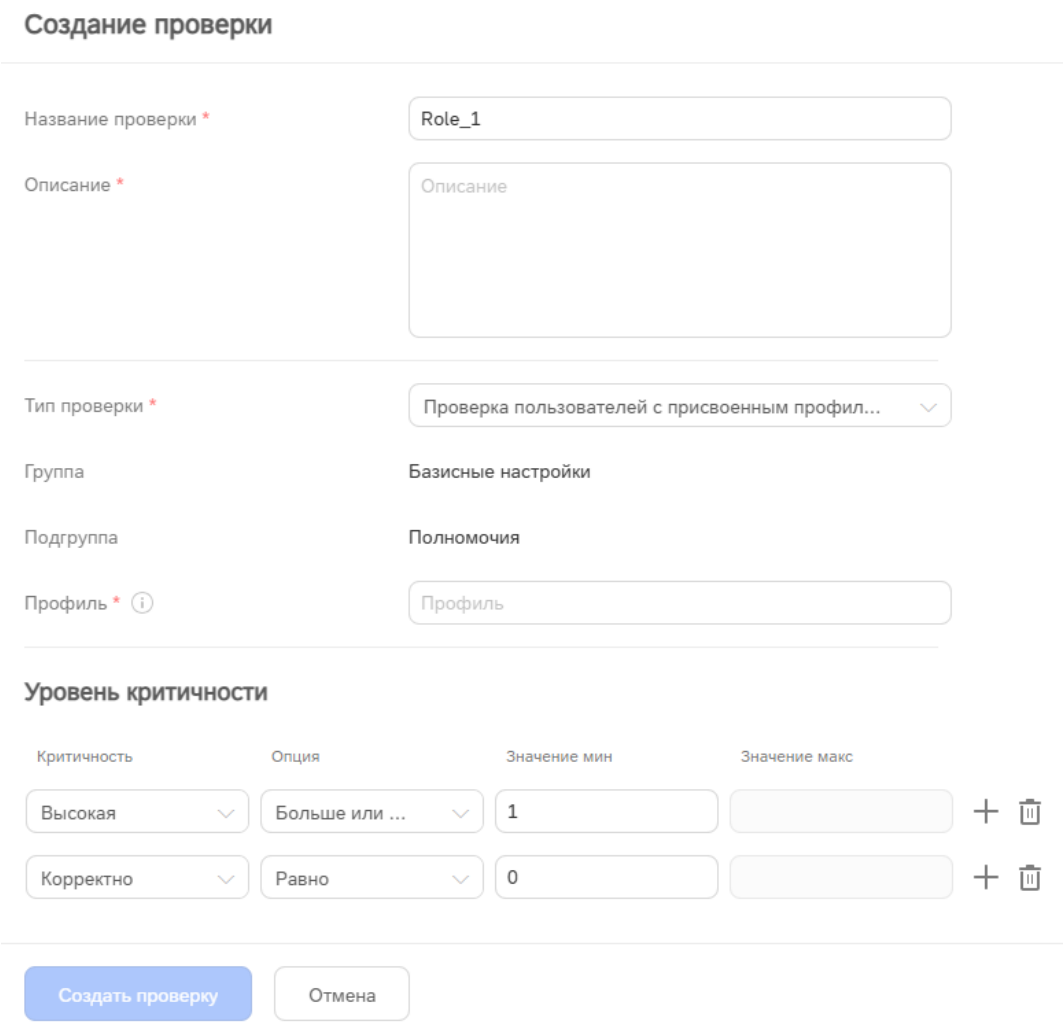


Рисунок 287 – Параметры для проверки пользователей с присвоенным профилем

7.1.6.1.8.2.8 Проверка пользователей с присвоенной ролью [ROLE_CUST]

Для настройки проверки пользователей с присвоенной ролью необходимо ввести название и описание проверки (см. рис. 277), условия для уровней критичности проверки (см. рис. 278) и роль пользователя (рис. 288).

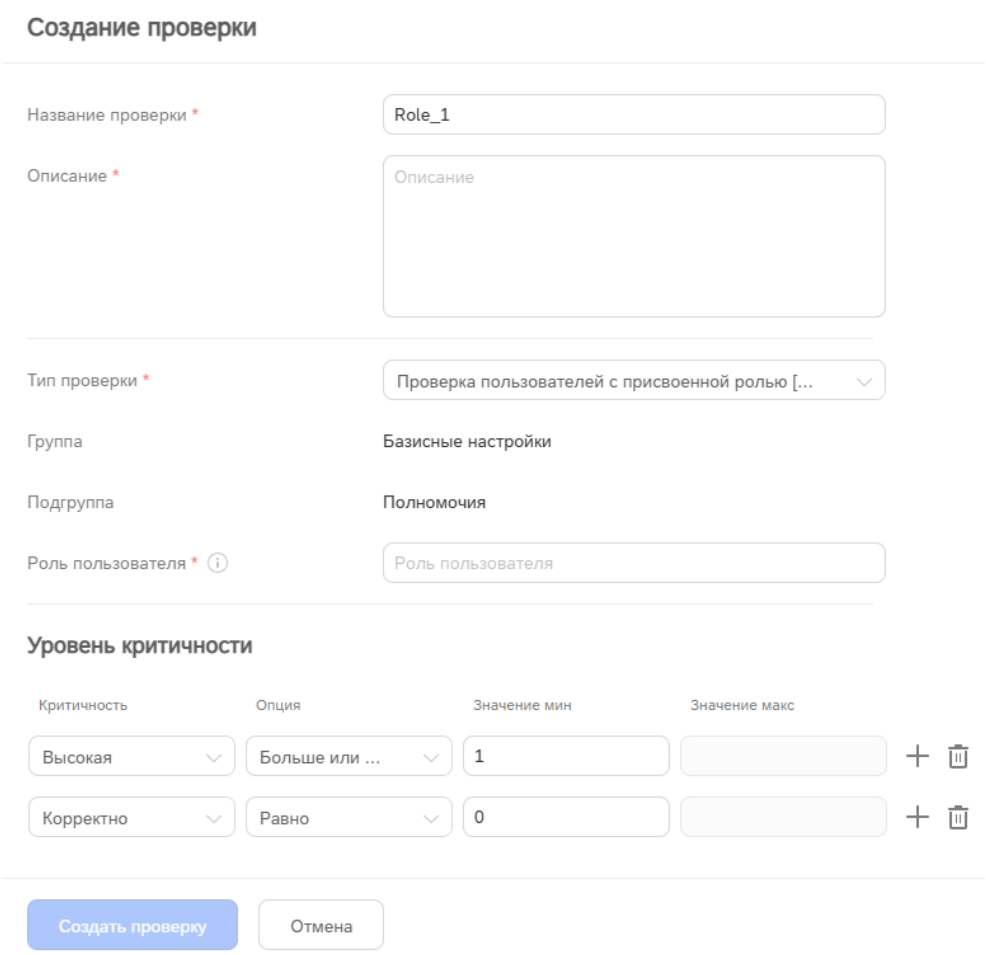


Рисунок 288 – Параметры для проверки пользователей с присвоенной ролью

7.1.6.1.8.2.9 Авторизационная группа таблицы [TABU_CUST]

Для настройки авторизационной группы таблицы необходимо ввести название и описание проверки (см. рис. 277), условия для уровней критичности проверки (см. рис. 278) и имя таблицы (рис. 289).

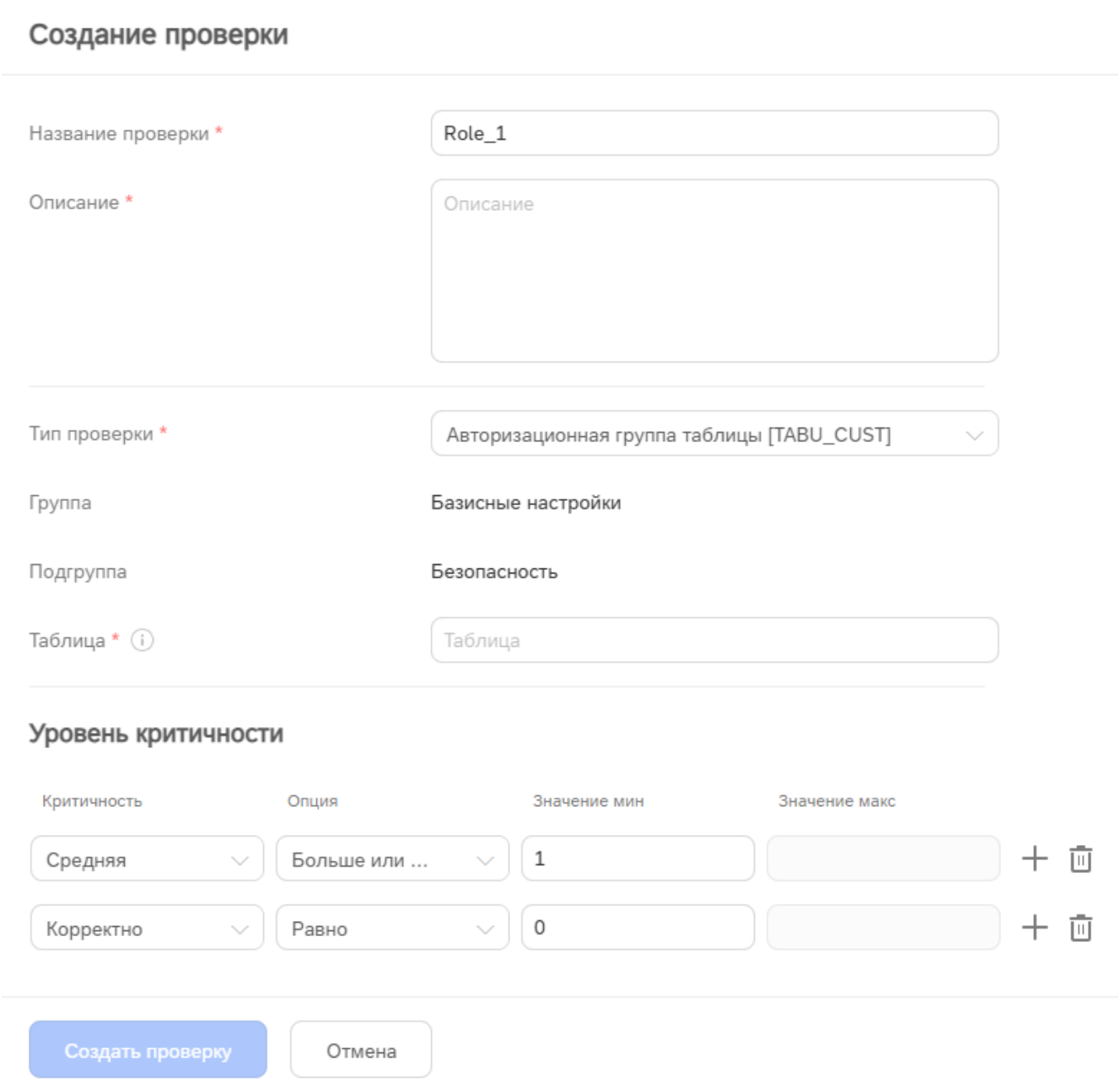


Рисунок 289 – Параметры для проверки авторизационная группа таблицы

7.1.6.1.8.3 Добавление проверок в собственный профиль

В собственный профиль предоставляется возможность добавления нот, собственных и пользовательских проверок.

Для добавления проверок в собственный профиль необходимо выполнить следующие действия:

1) Поставить флаг напротив проверок.
2) Нажать кнопку «Добавить в профиль».
3) Выбрать профиль в окне «Добавить в профиль» (рис. 290).

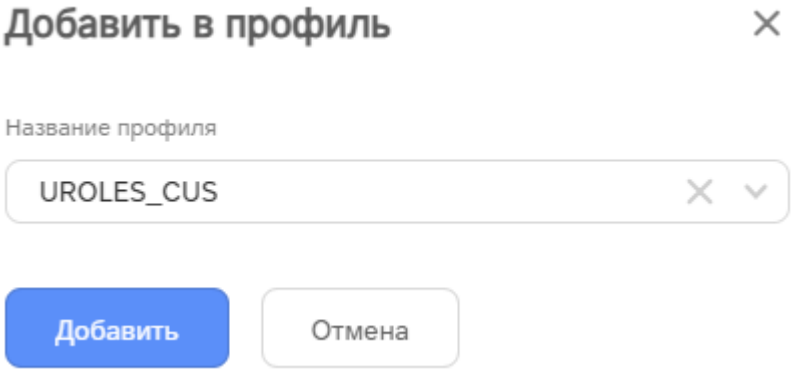
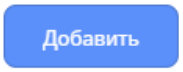


Рисунок 290 – Окно «Добавить в профиль»

4) Нажать кнопку 

.

7.1.6.1.8.4 Редактирование собственной проверки

Редактирование собственной проверки осуществляется в следующих полях:

- «Название проверки»;
- «ICF-сервис»;
- «Уровень критичности».

Для редактирования проверок необходимо выполнить следующие действия:

1) Выбрать проверку из списка.
2) Внести изменения.
3) Нажать кнопку *«Сохранить»*.

Примечания:

1. Для стандартных проверок доступно изменение уровня критичности. Изменения сохраняются в профиле SESS_PRD.
2. Изменения собственных проверок сохраняются в профиле CUSTOMS.

7.1.6.1.8.5 Удаление проверок из собственного профиля

Для удаления проверок необходимо выполнить следующие действия:

1) Поставить флаг напротив проверки.
2) Нажать кнопку «Удалить».
3) Нажать кнопку *«Удалить»* в окне «Удаление проверок» (рис. 291).

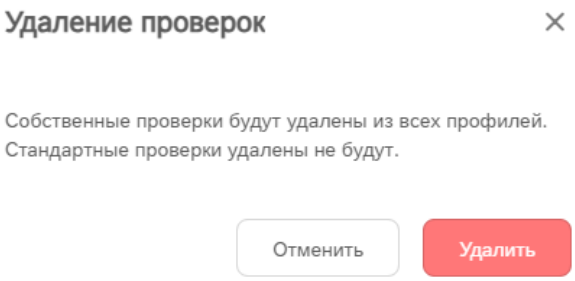


Рисунок 291 – Окно «Удаление проверок»

Примечание. Удаление проверок осуществляется в собственных профилях.

7.1.6.2 Профили для модуля «Анализ кода»

Для работы с профилями необходимо выбрать тип профилей «Анализ кода» в боковом меню (рис. 292).

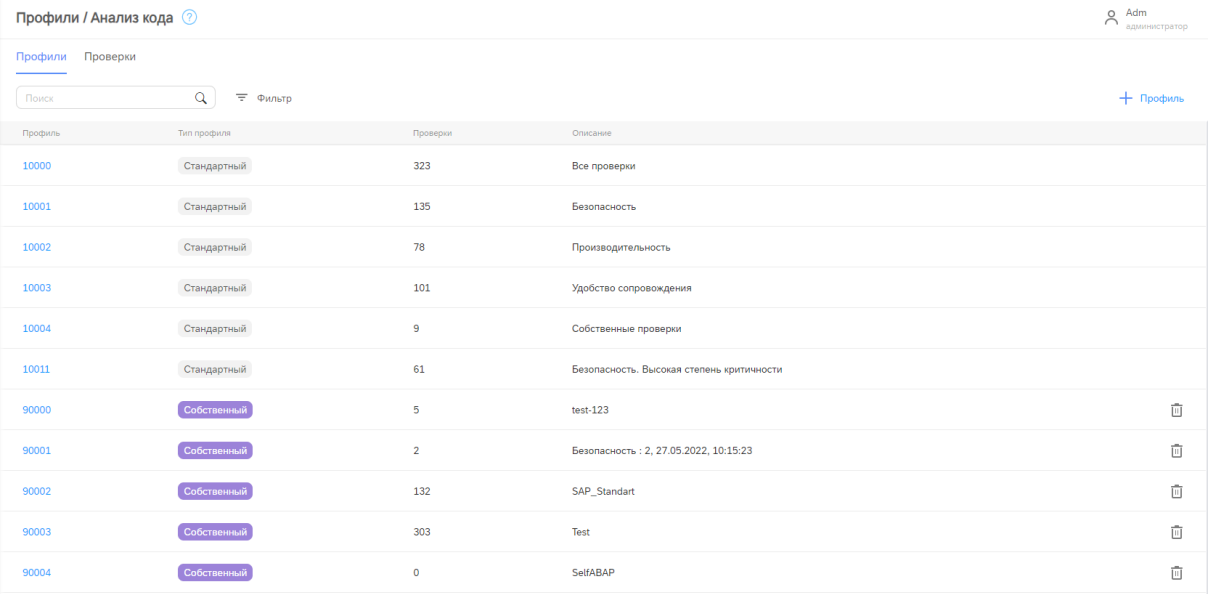


Рисунок 292 – Профили для модуля «Анализ кода»

7.1.6.2.1 Поиск профиля

Для поиска профиля необходимо ввести наименование профиля в поисковую строку в основной области (рис. 292).

7.1.6.2.2 Просмотр профилей

Для просмотра профилей необходимо выбрать профиль в основной области (рис. 292).

Примечание. При просмотре профиля доступна кнопка «Фильтр» в области с проверками. Доступна фильтрация по следующим проверкам:

- категория;
- теги.

7.1.6.2.3 Добавление собственного профиля

Чтобы добавить собственный профиль, необходимо нажать кнопку *«+Профиль»* в основной рабочей области «Профили» (см. рис. 292). После нажатия кнопки добавления профиля разворачивается окно «Создание профиля» для модуля «Анализ кода» (рис. 293).

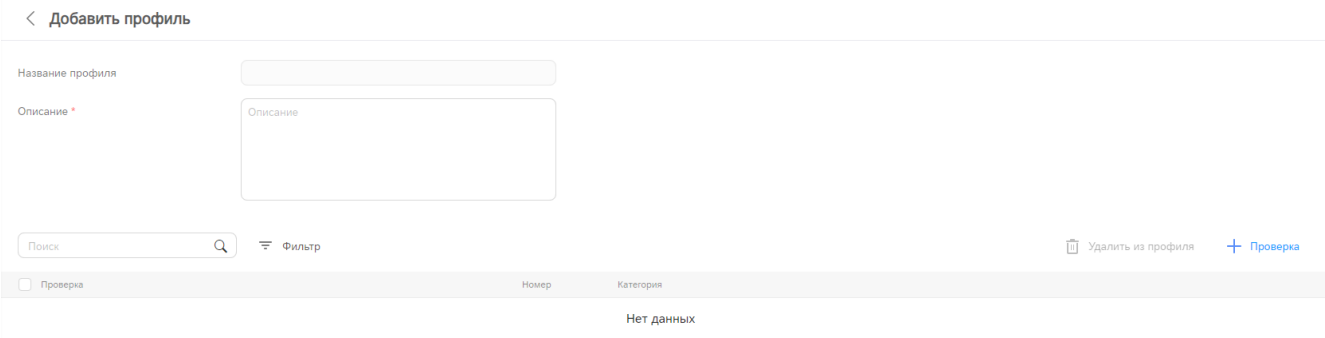


Рисунок 293 – Окно «Создание профиля» для модуля «Анализа кода»

После ввода описания профиля в окне «Создание профиля» для модуля «Анализ кода» необходимо нажать кнопку *«Сохранить».*

Примечания:

1. В качестве названия для собственных профилей для проверок типов «Анализа кода» используют номера с 90000 включительно.
2. Во время создания профиля пользователю предоставляется возможность добавления проверок. Для добавления проверок в профиль необходимо нажать кнопку *«+ Проверка»* (рис. 293).
3. При добавлении нового собственного профиля доступна кнопка «Фильтр» в области со списком проверок (см. рис. 293). Доступна фильтрация по следующим параметрам:

— категория;
— теги.

7.1.6.2.4 Редактирование собственного профиля

В собственных профилях доступно добавление и удаление проверок. В собственных профилях доступно добавление стандартных проверок, а также изменение критичности собственной проверки.

Для редактирования профиля необходимо в основной рабочей области «Профили» (см. рис. 292), выбрать профиль из списка, внести изменения, нажать кнопку *«Сохранить».*

7.1.6.2.5 Экспорт профилей

Экспорт профилей осуществляется следующего формата *.prf. Доступен экспорт стандартных и собственных профилей.

Экспорт профилей осуществляется следующими способами:

— при просмотре стандартных собственных профилей;
— при просмотре списка профилей.

Для экспорта профиля со страницы просмотра стандартных собственных профилей необходимо нажать кнопку «Экспорт профиля».

Для экспорта профиля со страницы просмотра списка профилей необходимо нажать кнопку «Экспорт профиля» в строке профиля проекта.

7.1.6.2.6 Импорт профилей

Импорт профилей осуществляется следующего формата *.prf. Доступен импорт

стандартных и собственных профилей.
Импорт профилей осуществляется со страницы списка профилей.
Для импорта профиля необходимо нажать кнопку *«Импорт профиля»*, выбрать профиль файл профиля в открывшемся окне, нажать кнопку *«Открыть»* (рис. 274).

7.1.6.2.7 Удаление собственного профиля

Для удаления собственного профиля необходимо нажать кнопку *«Удалить»* напротив профиля.
Существует ограничение: невозможно удалить стандартные профили. После активации кнопки *«Удалить из профиля»* откроется окно подтверждения действия. После подтверждения действия выбранный профиль будет удален.

7.1.6.2.8 Проверки

В модуле «Профили» существует 2 категории проверок:

- стандартные (входят при поставке в комплекс);
- собственные (проверки, которые создает Администратор ПК «SafeERP Security Suite»).

7.1.6.2.8.1 Собственные проверки

7.1.6.2.8.1.1 Просмотр собственных проверок

Для просмотра собственных проверок необходимо выбрать собственный профиль из списка (рис. 292), выбрать проверку из списка.

7.1.6.2.8.1.2 Создание собственных проверок

Для модуля «Анализ кода» доступно создание собственных проверок.
Подробное описание собственных проверок представлено в таблице 16.
Таблица 16 – Подробное описание собственных проверок для модуля «Анализ кода»

Наименование	Описание
Проверка наличия ФМ в тексте программы [FUNC_CUST]	Выявляет наличие вызова заданного функционального модуля в тексте программы
Проверка «наличия класса и/или метода в тексте программы [CLAS_CUST]	Выявляет создание инстанции заданного класса либо вызовы преднастроенных методов в тексте программы
Проверка «наличия любой команды в тексте программ [COMM_CUST]	Выявляет использование в тексте программы заданного оператора из зарезервированных операторов, используемых в языке ABAP (SELECT, REPORT, DELETE...)
Проверка параметров авторизации. Удаление команды [AUTH_CUST]	Выявляет места в исходном коде, где проверяемое значение параметров авторизации в коде не соответствует заданному в проверке, отслеживает изменения (в том числе удаление) в команде проверки объектов полномочий AUTHORITY-CHECK

Создание проверки осуществляется следующими способами:

— через вкладку «Профили». Для создания проверки необходимо выбрать собственный профиль, нажать кнопку *«+ Проверка»*, выбрать вкладку «Добавить новую» в открывшемся окне, заполнить необходимые поля, добавить теги, нажать кнопку *«Создать проверку»*;

— через вкладку «Проверки». Для создания проверки необходимо нажать кнопку *«+ Проверка»*, заполнить необходимые поля (рис. 295), добавить теги, нажать кнопку *«Создать проверку».*

Примечания:

1. При создании проверки доступно добавление тегов в проверки. Максимальное количество тегов в проверке – 5. Максимальная длина тега – 25 символов.
2. Доступно добавление тегов в стандартную проверку.
3. При добавлении тегов пользователю доступен выбор тегов из выпадающего списка (рис. 294).

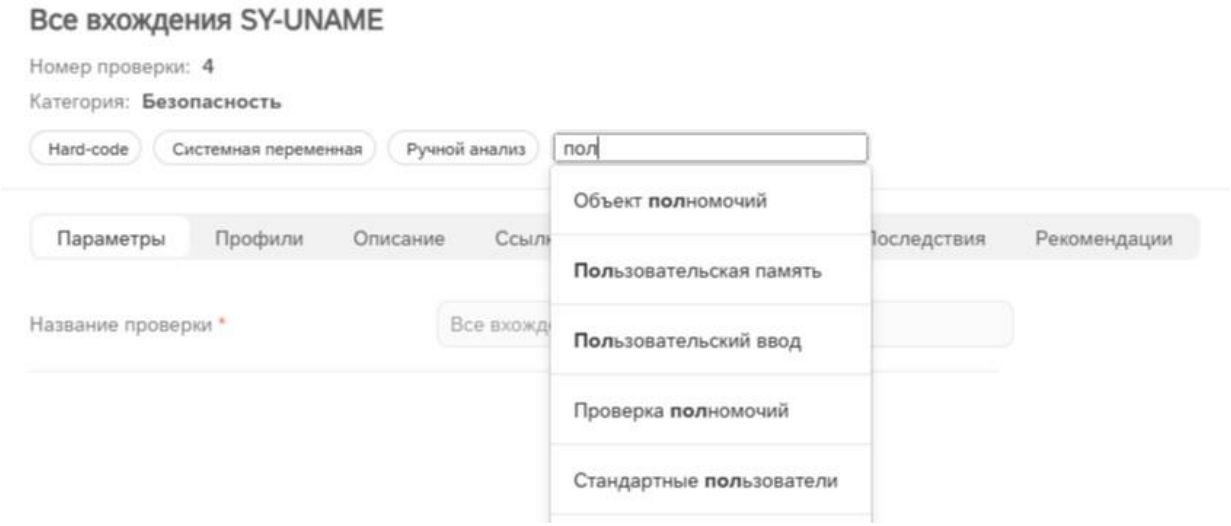


Рисунок 294 – Выбор тегов

4. При добавлении тегов нельзя использовать «пробел» как имя тега.
5. Стандартные теги приведены в приложении 3.

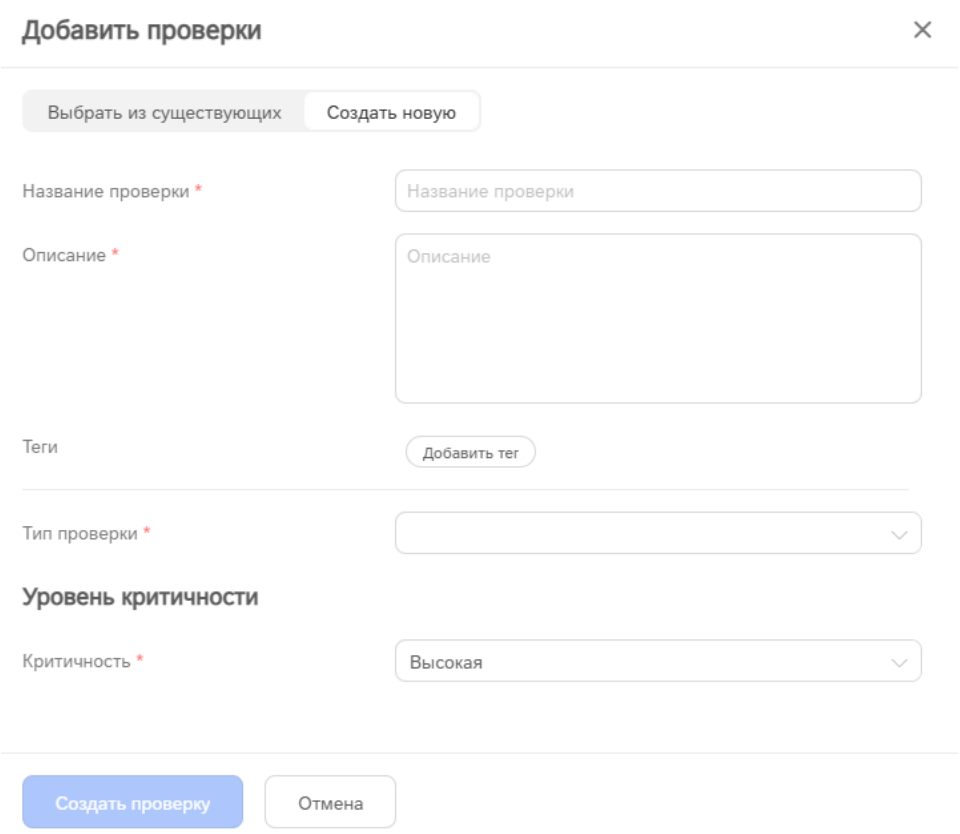


Рисунок 295 – Окно «Создание проверки»

7.1.6.2.8.1.3 Редактирование собственной проверки

Редактирование собственной проверки осуществляется в следующих полях:

- «Название»;
- «Описание»;
- «Критичность»;
- «Класс»;
- «Функциональный модуль»;
- «Модуль»;
- «Код проверки»;
- «Команда»;
- «Теги».

Редактирование проверки осуществляется следующими способами:

- через вкладку «Профили». Для редактирования собственных проверок необходимо выбрать собственный профиль из списка (рис. 292), выбрать проверку, внести изменения в окне проверки (рис. 296), нажать кнопку *«Сохранить»*;
- через вкладку «Проверки». Для редактирования собственных проверок необходимо выбрать собственную проверку из списка, внести изменения, нажать кнопку *«Сохранить».*

Примечания:

1. При редактировании проверки доступно добавление тегов в проверки. Максимальное количество тегов в проверке – 5. Максимальная длина тега – 25 символов.
2. Доступно добавление тегов в проверку в стандартных профилях.

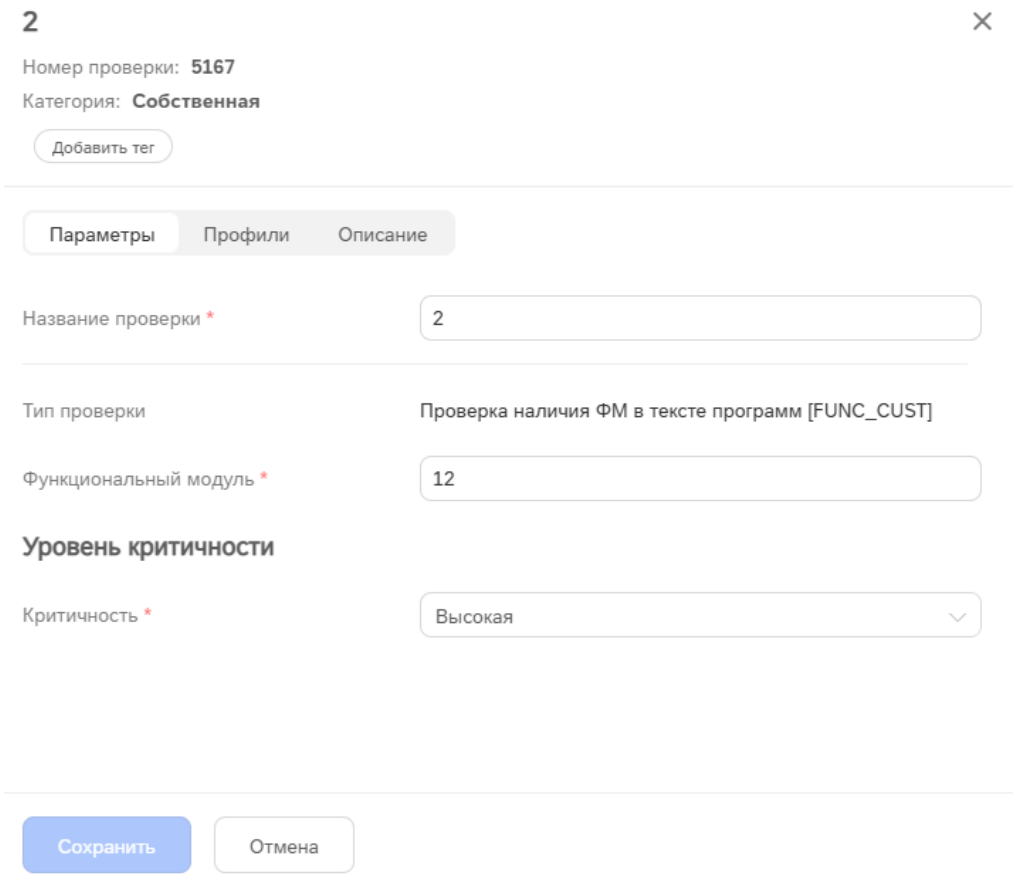


Рисунок 296 – Окно редактирование параметров проверки

7.1.6.2.8.1.4 Добавление проверок в профиль

Добавление проверок осуществляется в собственные профили. В собственных профиль предоставляется возможность добавления стандартных и собственных проверок.

Добавление проверок осуществляется следующими способами:

- через вкладку «Профили». Для добавления проверок в профиль необходимо выбрать профиль, выбрать вкладку «Выбрать из существующих», установить флаг напротив проверок ☑, нажать кнопку *«Добавить в профиль»*;
- через вкладку «Проверки». Для добавления проверок в профиль необходимо поставить флаг ☑ напротив проверок, нажать кнопку *«Добавить в профиль»*, выбрать профиль в открывшемся окне, нажать кнопку *«Добавить».*

7.1.6.2.8.1.5 Удаление проверок

Удаление проверок осуществляется во вкладке «Проверки».

Для удаления собственных проверок необходимо поставить флаг ☑ напротив проверок, нажать кнопку «Удалить», нажать кнопку *«Удалить»* в окне подтверждения (рис. 297).

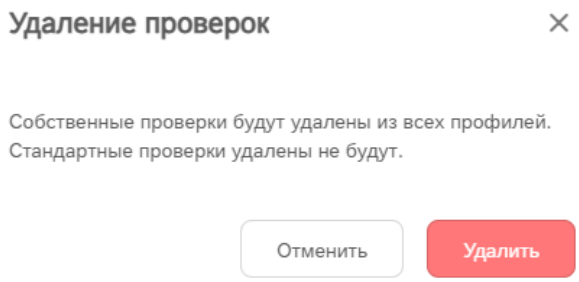


Рисунок 297 – Окно подтверждения удаления проверок

7.1.7 Модуль «Авторизации»

Модуль «Авторизации» предназначен для отслеживания изменений полномочий в ролях.

Модуль «Авторизации» состоит из следующих разделов:

- «История полномочий»;
- «Иерархия полномочий»;
- «Сравнение ролей».

7.1.7.1 История полномочий

В ПК «SafeERP Security Suite» существует функциональность, позволяющая получить историю полномочий.

История полномочий формируется на результатах сработанных проверок авторизации, которые относятся к профилям модуля «Сканер».

Раздел «История полномочий» предназначен для обнаружения новых или удаленных полномочий у пользователей согласно заданному запросу.

Является аналогом транзакции /n/gazis/history.

Раздел «История полномочий» состоит из следующих областей:

- «Основная рабочая» – предназначена для составления запросов;
- «Список истории полномочий» – предназначена для отображения списка запросов.

Основная рабочая область из следующих полей (рис. 298):

- «Агент» – выбор агент-системы для анализа. В данном поле доступны агенты типа ABAP.
- «Мандант» – выбор манданта для анализа. В данном поле доступны манданты согласно выбранному агенту.
- «Дата с» – дата начала периода поиска.
- «Дата по» – дата конца периода поиска.
- «Авторизации» – выбор алгоритма.

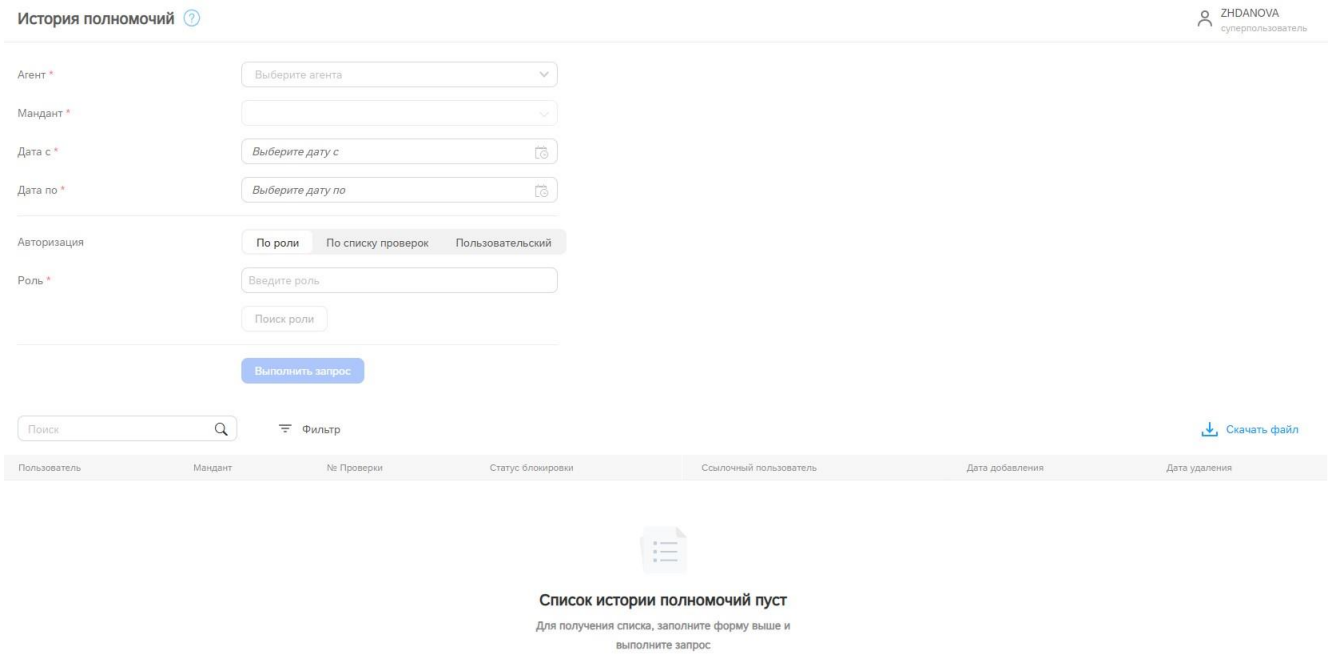


Рисунок 298 – Раздел «История полномочий»

В поле «Авторизации» доступны следующие сплит-кнопки:

— «По роли» – при выборе данного типа анализа происходит поиск новых или удаленных полномочий в ролях.
— «По списку проверок» – при выборе данного типа анализа происходит поиск новых или удаленных полномочий согласно выбранным проверкам.
— «Пользовательский» – при выборе данного типа анализа происходит поиск новых или удаленных полномочий согласно заданному шаблону. При выборе шаблона доступно следующее:
  А) выбор шаблона из существующих;
  Б) создание нового шаблона – для создания нового шаблона необходимо нажать кнопку «+Создать», ввести данные в окне «Добавить новый шаблон», нажать кнопку «Сохранить шаблон» (рис. 301).

Примечания:

1. В поле «Авторизации» будут доступны роли согласно выбранному агенту и манданту.
2. При выборе сплит-кнопки *«По роли»* будет доступен список ролей согласно выбранному агенту, а также доступен поиск ролей. Для поиска роли необходимо нажать кнопку *«Поиск роли»*, ввести название роли в поисковую строку окна «Поиск роли», нажать кнопку *«Поиск».*
3. В окне «Поиск» роли доступен поиск ролей (рис. 299). При вводе данных в поисковую строку необходимо учитывать следующее:

— при вводе «Z*» происходит поиск ролей, которые начинаются с Z;
— при вводе «*Z» происходит поиск ролей, которые заканчиваются на Z;
— при вводе «*Z*» происходит поиск ролей, которые содержат в названии «Z»;
— при вводе «Z» происходит поиск ролей, которые содержат в названии «Z».

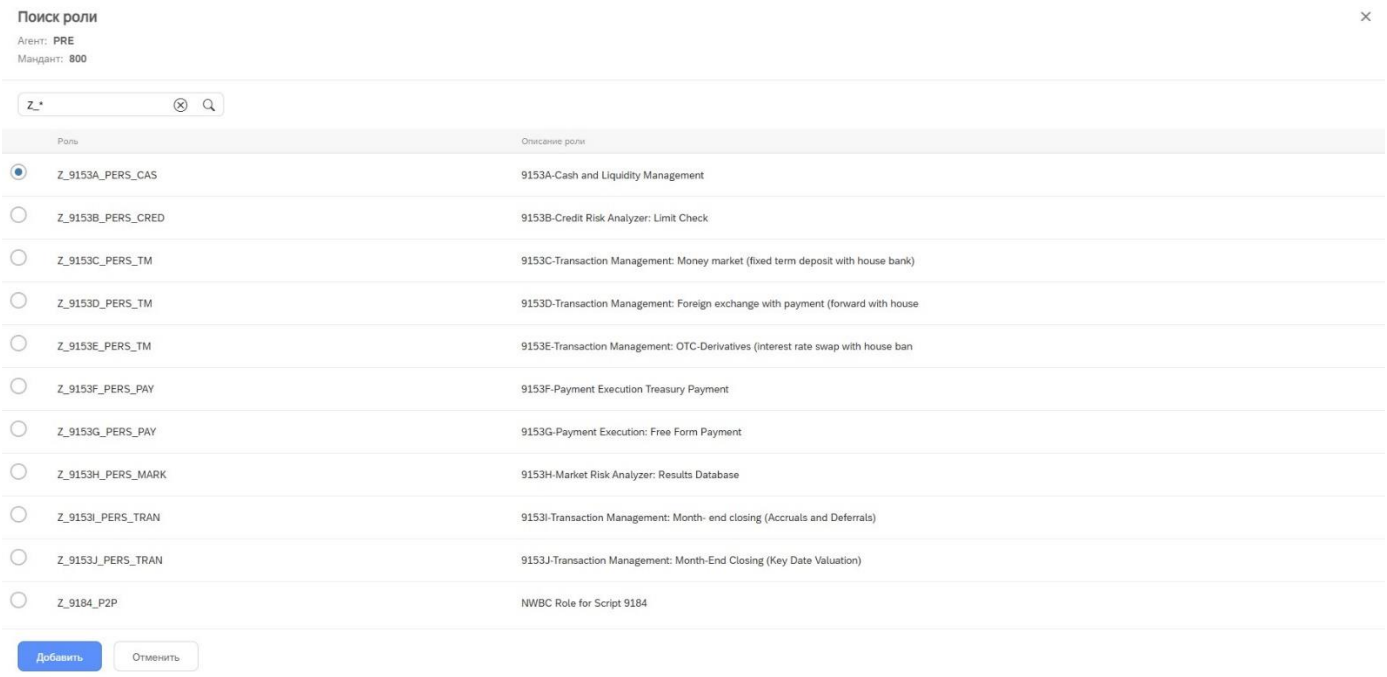


Рисунок 299 – Окно «Поиск роли»

Для выполнения запроса необходимо выполнить следующие действия:

1) Выбрать агента, мандант, дату начала и конца периода поиска.
2) Выбрать тип авторизации в соответствующем поле.
3) Нажать кнопку *«Выполнить запрос».*

В области «Список истории полномочий» доступен просмотр выполненных запросов.
В области «Список истории полномочий» доступны следующие действия:

1) Выгрузка отчета. Выгрузка отчета доступна после выполнения запроса. Для выгрузки отчета необходимо нажать кнопку *«Скачать файл»*. Скачанный файл применяется для дальнейшей настройки полномочий у пользователей.
2) Просмотр запросов.
3) Фильтрация запросов согласно выбранному пользователю в области «Список истории полномочий». Для фильтрации запросов необходимо ввести имя пользователя в поисковую строку, нажать кнопку *«Поиск»*. При сбросе данных в поле «Поиск» возвращается список пользователей согласно запросу.
4) Фильтрация запросов с помощью кнопки *«Фильтр».* Доступна фильтрация по следующим параметрам:
   - ссылочный пользователь;
   - дата добавления с;
   - дата добавления по;
   - дата удаления с;
   - дата удаления по;
   - статус блокировки.

Примечание. При переключении на другой раздел или модуль данные запроса и список истории полномочий не сохраняются.

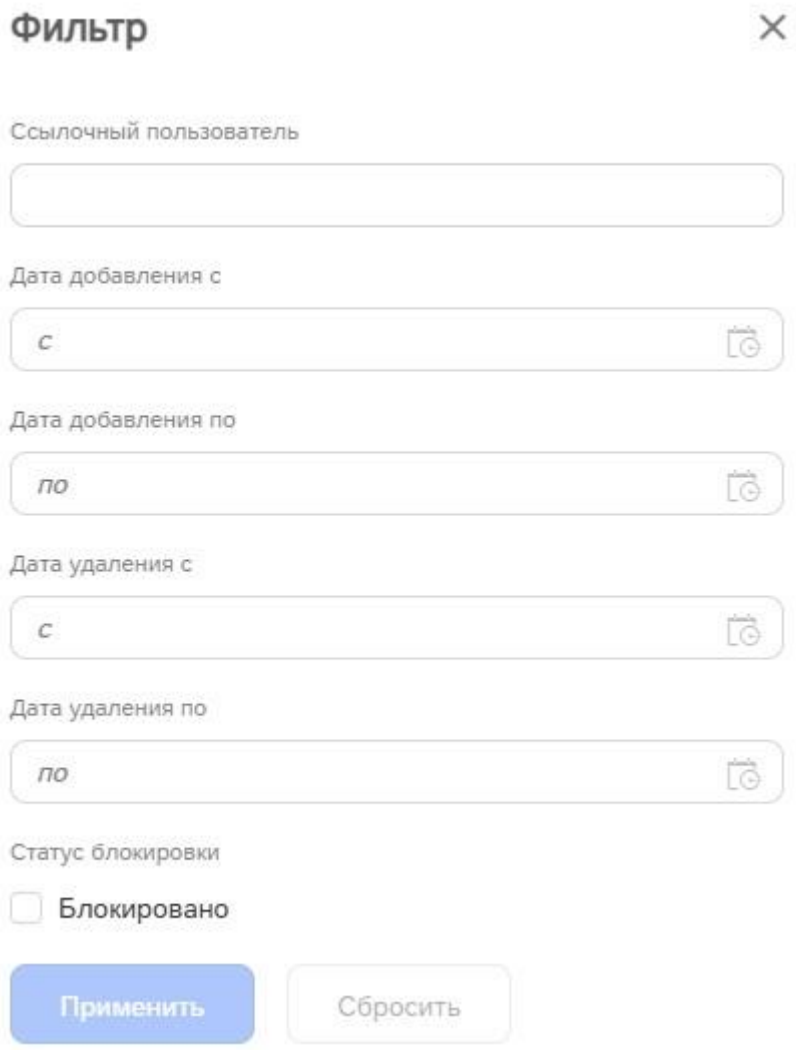


Рисунок 300 – Окно «Фильтр» в разделе «История полномочий»

7.1.7.1.1 Ведение шаблонов

При выборе сплит-кнопки «Пользовательский» в поле «Авторизации» пользователю доступна работа с шаблонами.

Пользователю доступны следующие действия:

- выбор шаблона из существующих. Для выбора шаблона необходимо нажать кнопку *«Существующий шаблон»*, ввести название шаблона в поисковую строку или выбрать из выпадающего списка в поле «Шаблон»;
- создание шаблона;
- редактирование шаблона.

Создание шаблона

Для создания шаблона необходимо выполнить следующие действия:

1) Нажать кнопку *«+ Создать».*
2) Заполнить необходимые данные в окне «Добавить шаблон проверки» (рис. 301).

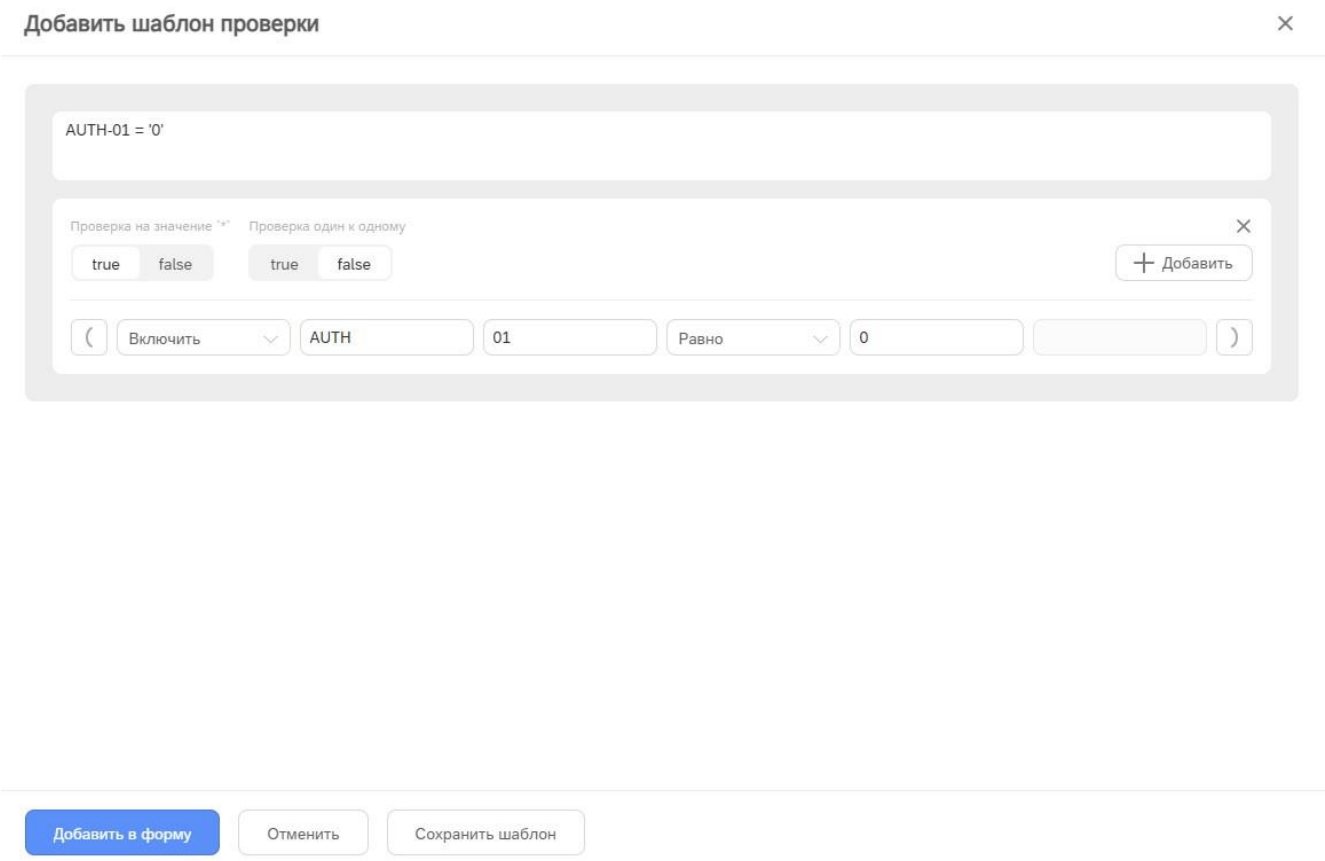


Рисунок 301 – Создание шаблона в разделе «История полномочий»

3) Нажать кнопку *«Сохранить шаблон»* (см. рис. 300).
4) Ввести имя шаблона в окне «Сохранить шаблон» (рис. 302). Нажать кнопку *«Сохранить».*

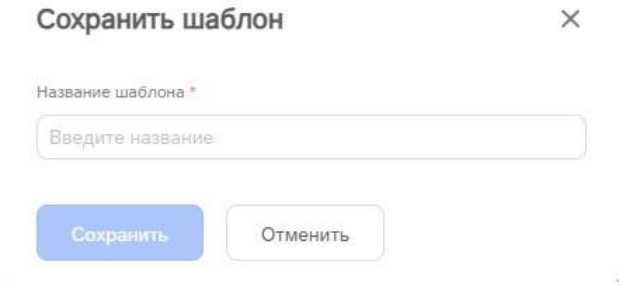


Рисунок 302 – Окно сохранения шаблона

Примечания:

1. После активации кнопки *«Сохранить шаблон»* внесенные данные добавятся в поле «Код проверки».
2. Созданные шаблоны не подлежат удалению.

Редактирование шаблона

Редактирование шаблона доступно после активации кнопки «Добавить в форму» в окне «Добавить шаблон проверки».

Для редактирования шаблона необходимо выполнить следующие действия:

1) Нажать кнопку *«Редактировать шаблон»*.
2) Внести изменения в окне «Добавить шаблон проверки». Нажать кнопку *«Добавить в форму»*.

Примечание. После активации кнопки *«Добавить в форму»* изменения добавятся в поле «Код проверки».

Удаление шаблона

Удаление шаблона осуществляется в поле «Шаблон».

Для удаления шаблона необходимо выполнить следующие действия:

1) Выбрать «Пользовательский» и «Существующий шаблон» в поле «Авторизация».
2) Нажать кнопку «Удалить» в строке шаблона. Подтвердить действие.

7.1.7.2 Раздел «Иерархия полномочий»

В ПК «SafeERP Security Suite» существует функциональность, позволяющая получить иерархию полномочий.

Иерархия полномочий формируется на результатах сработанных проверок авторизации, которые относятся к профилям модуля «Сканер».

Раздел «Иерархия полномочий» предназначен для выявления списка пользователей, которые обладают излишними полномочиями согласно запросу.

Данный раздел является аналогом транзакции /n/gazis/hierarchy.

Раздел «Иерархия полномочий» состоит из следующих областей:

- «Основная рабочая» – предназначена для составления запросов;
- «Список иерархии полномочий» – предназначена для отображения списка запросов.

Основная рабочая область из следующих полей (рис. 298):

- «Агент» – выбор агент-системы для анализа. В данном поле доступны агенты типа ABAP.
- «Мандант» – выбор манданта для анализа. В данном поле доступны манданты согласно выбранному агенту.
- «Авторизации» – выбор алгоритма.

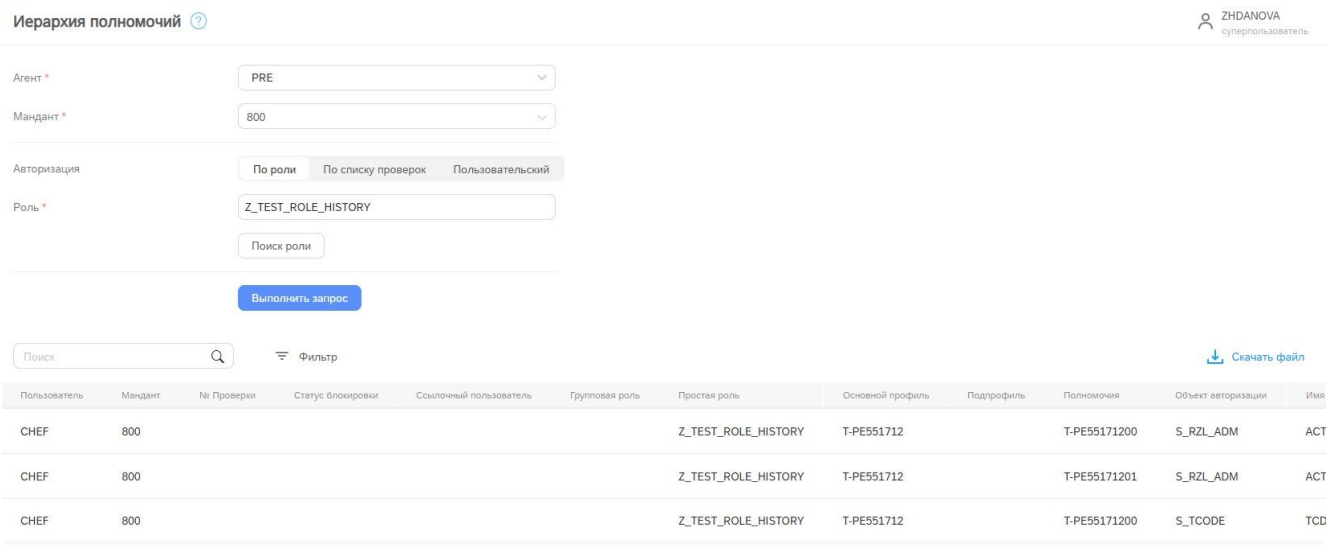


Рисунок 303 – Раздел «Иерархия полномочий»

В поле «Авторизации» доступны следующие сплит-кнопки:

- «По роли» – при выборе данной сплит-кнопки происходит поиск полномочий согласно выбранной роли.
- «По списку проверок» – при выборе данной сплит-кнопки происходит поиск полномочий согласно выбранным проверок.
- «Пользовательский» – при выборе данной сплит-кнопки происходит поиск полномочий согласно заданному шаблону. При выборе шаблона доступно следующее:

  А) выбор шаблона из существующих;

  Б) создание нового шаблона – для создания нового шаблона необходимо нажать кнопку «+Создать», ввести данные в окне «Добавить новый шаблон», нажать кнопку «Сохранить шаблон» (рис. 301).

Примечания:

1. В поле «Авторизации» будут доступны роли согласно выбранному агенту и манданту.
2. При выборе сплит-кнопки *«По роли»* будет доступен список ролей согласно выбранному агенту, а также доступен поиск ролей. Для поиска роли необходимо нажать кнопку *«Поиск роли»*, ввести название роли в поисковую строку окна «Поиск роли», нажать кнопку *«Поиск».*
3. В окне «Поиск» роли доступен поиск ролей (см. рис. 299). При вводе данных в поисковую строку необходимо учитывать следующее:

- при вводе «Z*» происходит поиск ролей, которые начинаются с Z;
- при вводе «*Z» происходит поиск ролей, которые заканчиваются на Z;
- при вводе «*Z*» происходит поиск ролей, которые содержат в названии «Z»;
- при вводе «Z» происходит поиск ролей, которые содержат в названии «Z».

Для выполнения запроса необходимо выполнить следующие действия:

1) Выбрать агент, мандант в соответствующих полях.
2) Выбрать тип авторизации в соответствующем поле.
3) Нажать кнопку *«Выполнить запрос».*

В области «Список иерархии полномочий» доступен просмотр выполненных запросов.

В области «Список иерархии полномочий» доступны следующие действия:

1) Выгрузка отчета. Выгрузка отчета доступна после выполнения запроса. Для выгрузки отчета необходимо нажать кнопку *«Скачать файл»*. Скачанный файл применяется для дальнейшей настройки полномочий у пользователей.
2) Просмотр запросов.
3) Фильтрация запросов согласно выбранному пользователю в области «Список иерархии полномочий». Для фильтрации запросов необходимо ввести имя пользователя в поисковую строку, нажать кнопку *«Поиск»*. При сбросе данных в поле «Поиск» возвращается список пользователей согласно запросу.
4) Фильтрация запросов с помощью кнопки *«Фильтр».* Доступна фильтрация по следующим параметрам (рис. 304):

— Ссылочный пользователь;
— статус блокировки;
— простая роль;
— объект полномочий.

Примечание. При переключении на другой раздел или модуль данные запроса и список истории полномочий не сохраняются.

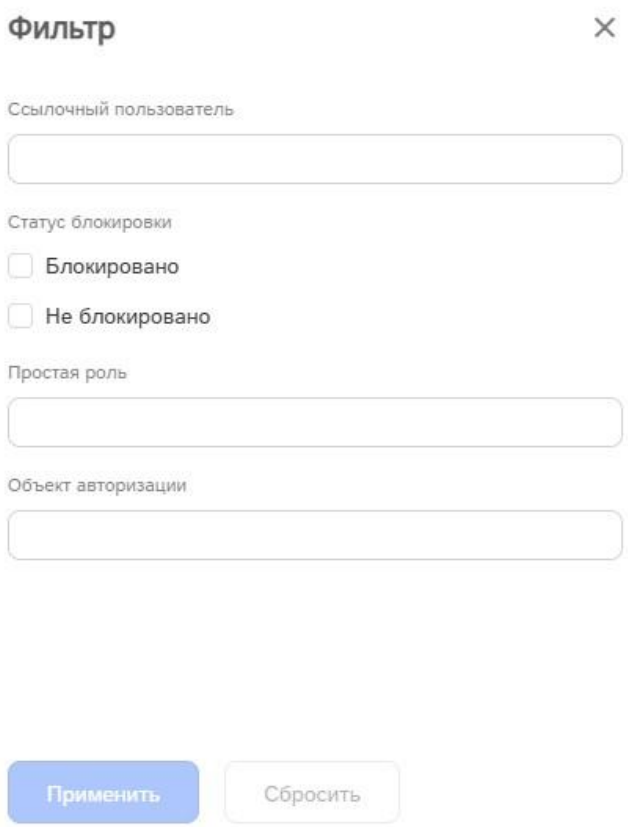


Рисунок 304 – Окно «Фильтр» в разделе «Иерархия полномочий»

7.1.7.2.1 Ведение шаблонов

При выборе сплит-кнопки «Пользовательский» в поле «Авторизации» пользователю доступна работа с шаблонами.

Пользователю доступны следующие действия:

- выбор существующего шаблона из существующих. Для выбора шаблона необходимо нажать кнопку «Существующий шаблон», ввести название шаблона в поисковую строку или выбрать из выпадающего списка в поле «Шаблон»;
- создание шаблона;
- редактирование шаблона.

Создание шаблона

Для создания шаблона необходимо выполнить следующие действия:

1) Нажать кнопку *«+ Создать».*
2) Заполнить необходимые данные в окне «Добавить шаблон проверки» (рис. 305).

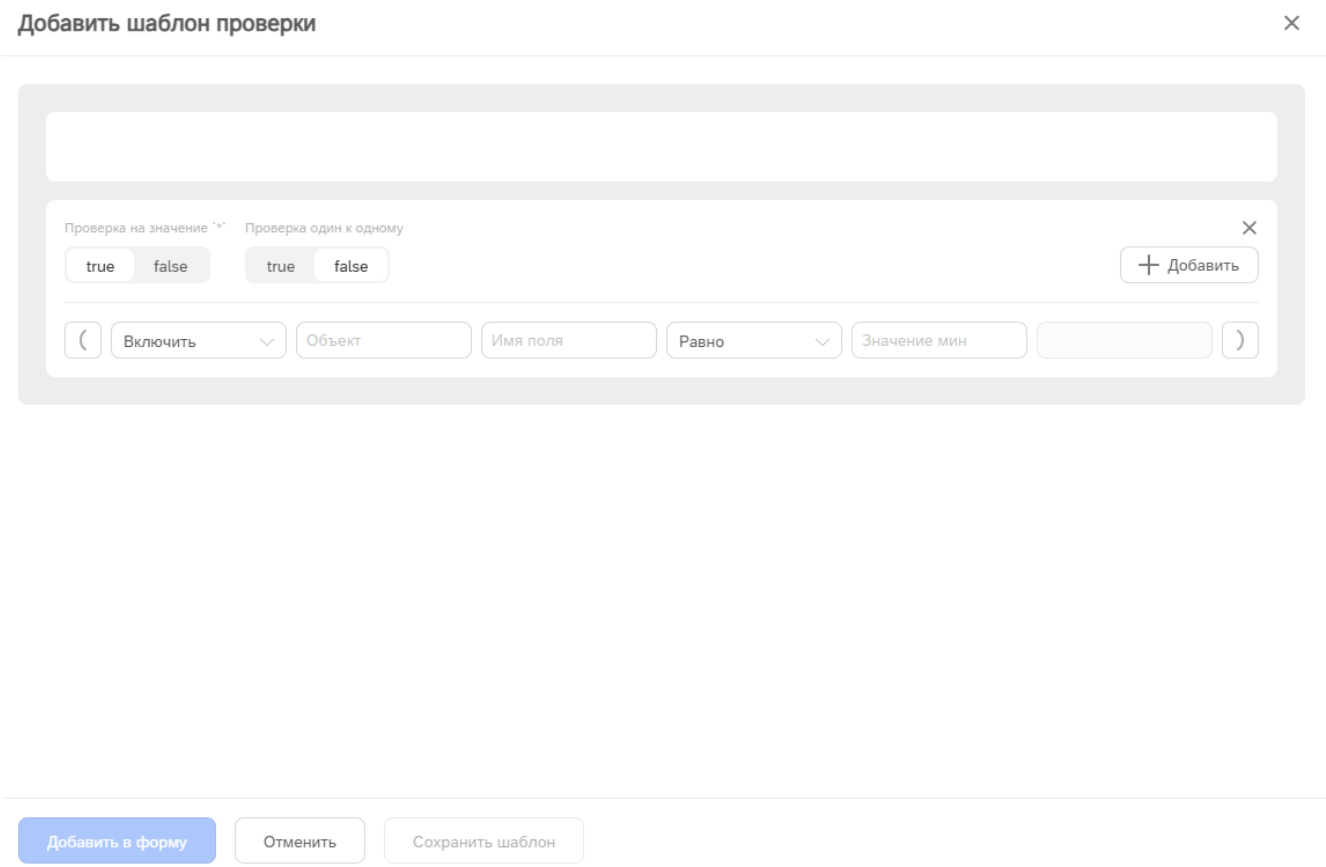


Рисунок 305 – Создание шаблона в разделе «Иерархия полномочий»

3) Нажать кнопку *«Сохранить шаблон».*
4) Ввести имя шаблона в окне «Сохранить шаблон». Нажать кнопку *«Сохранить»* (см. рис. 302).

Примечания:

1. После активации кнопки *«Сохранить»* внесенные данные добавятся в поле «Код проверки».
2. Созданные шаблоны не подлежат удалению.

Редактирование шаблона

Редактирование шаблона доступно после активации кнопки «Добавить в форму» в окне «Добавить шаблон проверки».

Для редактирования шаблона необходимо выполнить следующие действия:

1) Нажать кнопку *«Редактировать шаблон»*.
2) Внести изменения в окне «Добавить шаблон проверки». Нажать кнопку *«Добавить в форму»*.

Примечание. После активации кнопки *«Добавить в форму»* внесенные данные добавятся в поле «Код проверки».

Удаление шаблона

Удаление шаблона осуществляется в поле «Шаблон».

Для удаления шаблона необходимо выполнить следующие действия:

1) Выбрать «Пользовательский» и «Существующий шаблон» в поле «Авторизация».
2) Нажать кнопку «Удалить» в строке шаблона. Подтвердить действие.

7.1.7.3 Раздел «Сравнение ролей»

В ПК «SafeERP Security Suite» существует функциональность, позволяющая сравнить две роли, которые находятся в разных системах и мандантах.

Примечание. Сравниваемые роли могут находится в одной системе или в одном манданте.

Сравнение ролей формируется на основе сравнения соответствующих параметров ролей (объект полномочий, поле полномочий, со значения, по значения). Индикация параметров сравнения доступна в столбце «Результат сравнения». После процедуры сравнения ролей пользователю доступна выгрузка отчета в формате *csv. Отчет по сравнению ролей используют для дальнейшей настройки ролей в ПК «SafeERP Security Suite».

Раздел «Сравнение ролей» предназначен для выявления отличий между ролями согласно запросу.

Данный раздел является аналогом транзакции /n/gazis/compare_role.

Раздел «Сравнение ролей» состоит из следующих областей (рис. 306):

— «Основная рабочая» – предназначена для составления запросов;
— «Список сравнения ролей» – предназначена для отображения результата запроса.

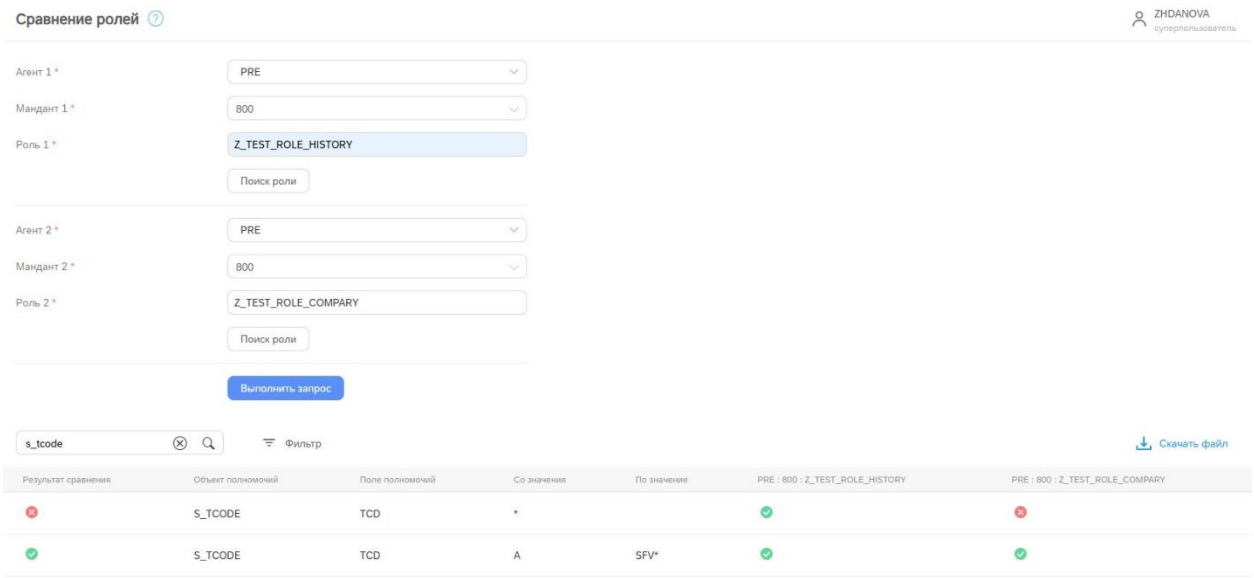


Рисунок 306 – Основная рабочая область раздела «Сравнение ролей»

Основная рабочая область (см. рис. 306) состоит из следующих полей:

— «Агент 1» – выбор агент-системы для анализа. В данном поле доступны агенты типа ABAP.

— «Мандант 1» – выбор манданта для анализа. В данном поле доступны манданты согласно выбранному агенту.
— «Роль 1» – выбор роли согласно выбранным агенту и манданту.
— «Агент 2» – выбор агент-системы для анализа. В данном поле доступны агенты типа ABAP.
— «Мандант 2» – выбор манданта для анализа. В данном поле доступны манданты согласно выбранному агенту.
— «Роль 2» – выбор роли согласно выбранным агенту и манданту.

Примечания:

1. После выбора агента и манданта в соответствующих полях будет доступен список ролей, а также доступен поиск ролей. Для поиска роли необходимо нажать кнопку «Поиск роли», ввести название роли в поисковую строку окна «Поиск роли», нажать кнопку «Поиск».
2. В окне «Поиск» роли доступен поиск ролей. При вводе данных в поисковую строку необходимо учитывать следующее:

— при вводе «Z*» происходит поиск ролей, которые начинаются с Z;
— при вводе «*Z» происходит поиск ролей, которые заканчиваются на Z;
— при вводе «*Z*» происходит поиск ролей, которые содержат в названии Z;
— при вводе «Z» происходит поиск ролей, которые содержат в названии Z.

Для сравнения ролей необходимо выполнить следующие действия:

1) Выбрать агента в поле «Агент 1», мандант в поле «Мандант 1», роль в поле «Роль 1» (см. рис. 306).
2) Выбрать агента в поле «Агент 2», мандант в поле «Мандант 2», роль в поле «Роль 2» (см. рис. 306).
3) Нажать кнопку *«Выполнить запрос»* (см. рис. 306).

В области «Список сравнения ролей» пользователю доступен просмотр сравниваемых ролей (см. рис. 306).
В области «Список сравнения ролей» пользователю доступны следующие действия:

— Выгрузка отчета. Выгрузка отчета доступна после выполнения запроса. Для выгрузки отчета необходимо нажать кнопку «Скачать файл».
— Просмотр запроса.
— Фильтрация запросов согласно введённому объекту полномочий в области «Список сравнения ролей». Для фильтрации запросов необходимо ввести наименование объекта полномочий в поисковую строку, нажать кнопку «Поиск». При сбросе данных в поле «Поиск» возвращается список объектов полномочий согласно запросу.
— Фильтрация запросов с помощью кнопки «Фильтр». Доступна фильтрация по следующим параметрам:

А) результат сравнения;
Б) поле полномочий.

Примечание. При переключении на другой раздел или модуль данные запроса и список сравнения ролей не сохраняются.

7.1.8 Модуль «Контроль качества»

Веб-интерфейс модуля «Контроль качества» представлен на рис. 133.

Модуль «Контроль качества» предназначен для ведения шаблонов, а также для добавления шаблонов в проекты.

Контроль качества доступен для следующих типов проекта:

- «КН» – для активации необходимо обратиться к модулю «Сканер»;
- «АК» – для активации необходимо обратиться к модулю «Анализ кода».

7.1.8.1 Метрики

Метрики для проектов типа КН

Доступен выбор следующих метрик:

- «Требования ФСТЭК России» – при расчете данной метрики применяются уязвимости, у которых есть ссылка на требования ФСТЭК России. У метрики «Требования ФСТЭК России» по умолчанию задано значение 100;
- «Уязвимости в базисных настройках» – при расчете данной метрики применяются уязвимости, которые относятся к группе «Базисные настройки»;
- «Уязвимости в настройках параметров доступа в систему» – при расчете данной метрики применяются уязвимости, которые относятся к группе «Настройки параметров доступа в систему»;
- «Уязвимости в статусе «Открыто» – при расчете данной метрики применяются все уязвимости со статусом «Открыто». Метрика «Уязвимости в статусе «Открыто» задается при добавлении или редактировании шаблона;
- «Рейтинг безопасности» – при расчете данной метрики применяются критичности всех уязвимостей, выявленных в проекте КН, независимо от группы или подгруппы проверок;
- «Уязвимости в полномочиях» – при расчете данной метрики применяются уязвимости, которые относятся ка к подгруппе «Полномочия»;
- «Уязвимости в параметрах профилей инстанции» – при расчете данной метрики применяются уязвимости, которые относятся к подгруппе «Параметры профилей инстанций».

Расчет метрики «Требования ФСТЭК России»

Для метрики «Требования ФСТЭК России» применяется следующий метод расчета:

$$\frac{M_{\text{КИ}}+M_{\text{ВЗ}}+M_{\text{СЗ}}+M_{\text{НЗ}}}{N} \times 100\% \quad (1)$$

где

$M_{КИ}$ – количество уязвимостей с критичностью «Информация» и «Корректно»;

$M_{ВЗ}$ – количество уязвимостей с критичностью «Высокая» и в статусе «Закрыто»;
$M_{СЗ}$ – количество уязвимостей с критичностью «Средняя» и в статусе «Закрыто»;
$M_{НЗ}$ – количество уязвимостей с критичностью «Низкая» и в статусе «Закрыто».
N – количество уязвимостей с критичностью «Информация» и «Корректно»
Примечание. У метрики «Требования ФСТЭК России» по умолчанию задано значение 100.

Расчет метрики «Настройки параметров доступа в систему»

При расчете метрики «Настройки параметров доступа в систему» критичностям соответствует числовая оценка:

- «Высокая» – 4;
- «Средняя» – 3;
- «Низкая» – 2;
- «Информация» – 1;
- «Корректно» – 1;
- «Не определено» – в расчете не применяется;
- «Уязвимости в статусе «Закрыто» соответствуют оценке – 1.

Для метрики «Настройки параметров доступа в систему» применяется следующий метод расчета:

$$\frac{4\times(n_{\text{В}}-n_{\text{ВЗ}})+3\times(n_{\text{С}}-n_{\text{СЗ}})+2\times(n_{\text{Н}}-n_{\text{НЗ}})+1\times(n_{\text{И}}+n_{\text{К}}+n_{\text{ВЗ}}+n_{\text{СЗ}}+n_{\text{НЗ}})}{n} \quad (2)$$

где
$n_{В}$ – количество уязвимостей с критичностью «Высокая»;
$n_{ВЗ}$ – количество уязвимостей с критичностью «Высокая» и со статусом «Закрыто»;
$n_{С}$ – количество уязвимостей с критичностью «Средняя»;
$n_{СЗ}$ – количество уязвимостей с критичностью «Средняя» и со статусом «Закрыто»;
$n_{Н}$ – количество уязвимостей с критичностью «Низкая»;
$n_{НЗ}$ – количество уязвимостей с критичностью «Низкая» и со статусом «Закрыто»;
$n_{И}$ – количество уязвимостей с критичностью «Информация»;
$n_{К}$ – количество уязвимостей с критичностью «Корректно»;
n – общее количество уязвимостей, кроме уязвимостей с критичностью «Не определено».

Расчет метрики «Уязвимости в базисных настройках»

Метрика «Уязвимости в базисных настройках» рассчитывается таким же образом, как и метрика «Настройки параметров доступа в систему» согласно формуле (2).

Расчет метрики «Уязвимости в статусе «Открыто»

Метрика «Уязвимости в статусе «Открыто» задается при создании или редактировании шаблона. Метрика «Уязвимости в статусе «Открыто» считается пройденной, когда

рассчитанное значение не превышает заданное.

Расчет метрики «Рейтинг безопасности»

Метрика «Рейтинг безопасности» рассчитывается таким же образом, как и метрика «Настройки параметров доступа в систему» согласно формуле (2).

Расчет метрики «Уязвимости в полномочиях»

Метрика «Уязвимости в полномочиях» рассчитывается таким же образом, как и метрика «Настройки параметров доступа в систему» согласно формуле (2).

Расчет метрики «Уязвимости в параметрах профилей инстанции»

Метрика «Уязвимости в параметрах профилей инстанции» рассчитывается таким же образом, как и метрика «Настройки параметров доступа в систему» согласно формуле (2).

Значения рассчитанных метрик приведено в таблице 17.

Таблица 17 - Значение рассчитанных метрик

Значение	Числовой интервал
A	(0;1]
B	(1;2]
C	(2;3]
D	(3;4]

Условия прохождения метрик проектов типа КН

Метрика «Требования ФСТЭК России» считается пройденной, если критичность всех уязвимостей равна «Информация» или «Корректно».

Метрика «Уязвимости в базисных настройках» считается пройденной, когда результат метрики равен A.

Метрика «Уязвимости в настройках параметров доступа в систему» считается пройденной, когда результат метрики равен A.

Метрика «Уязвимости в статусе «Открыто» считается пройденной, если количество уязвимостей в статусе «Открыто» меньше или равно значению в поле «Условие» из шаблона контроля качества.

Метрика «Рейтинг безопасности» считается пройденной, когда результат метрики равен A.

Метрика «Уязвимости в полномочиях» считается пройденной, когда результат метрики равен A.

Метрика «Уязвимости в параметрах профилей инстанции» считается пройденной, когда результат метрики равен A.

Метрики для проектов типа АК

Доступен выбор следующих метрик:

- «Чистота кода»;
- «Рейтинг удобства сопровождения»;

— «Рейтинг производительности»;
— «Рейтинг безопасности».

Для метрик «Рейтинг удобства сопровождения», «Рейтинг производительности», «Рейтинг безопасности» доступны следующие статусы:

— «A» – уязвимости отсутствуют;
— «B» – найдены уязвимости с категорией критичности «Информация»;
— «C» – найдены уязвимости со степенью критичности «Низкая»;
— «D» – найдены уязвимости со степенью критичности «Средняя»;
— «E» – найдены уязвимости со степенью критичности «Высокая.

Примечания:

1. Метрика «Чистота кода» вычисляется по следующей формуле:

$$100 - \frac{N}{M} \times 100 \quad (3)$$

где *N* – количество найденных недостатков;
M – количество просканированных строк кода

2. Для метрики «Чистота кода» доступен ввод целочисленного значения от 0 до 100.

7.1.8.2 Создание шаблона

Для создания шаблона необходимо нажать кнопку *«+Шаблон качества»* (см. рис. 133.), заполнить поле «Название шаблона» (рис. 307), нажать кнопку *«+Добавить метрику»*, выбрать необходимые метрики, задать необходимые параметры в области «Список метрик», нажать кнопку *«Сохранить».*

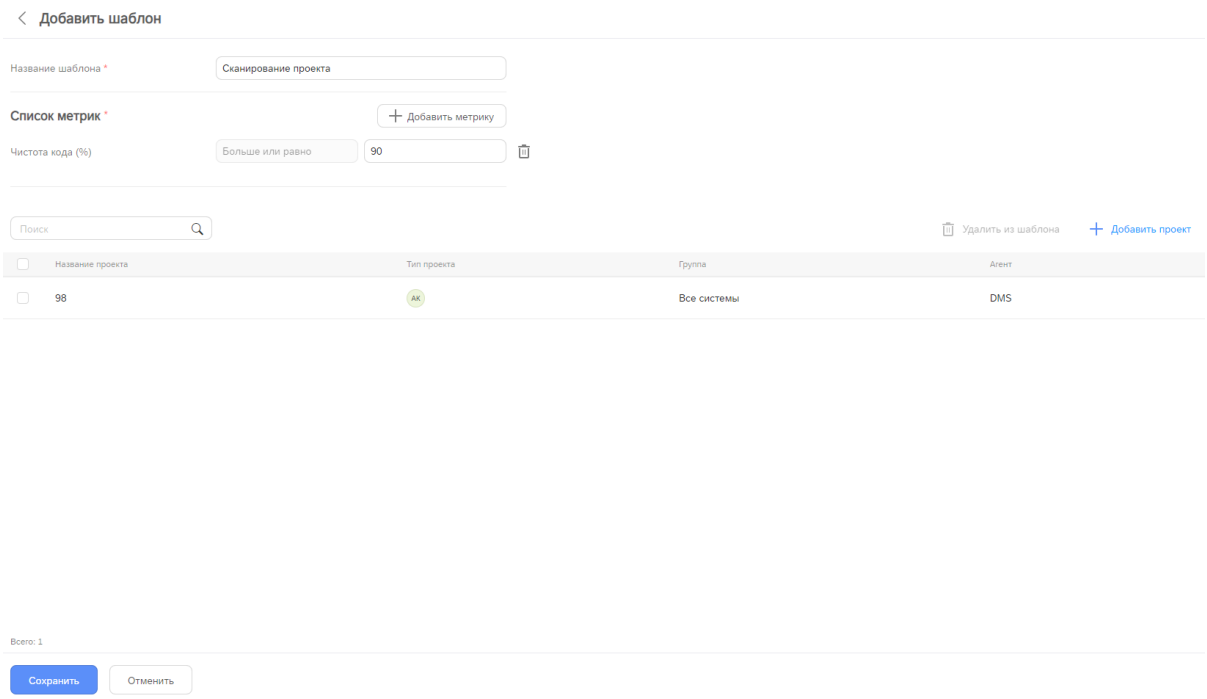


Рисунок 307 – Добавление шаблона

7.1.8.3 Редактирование шаблона

Для редактирования шаблона необходимо ввести название в поисковую строку или выбрать из списка в поисковую строку, внести изменения (добавить, изменить или удалить метрику, добавить или удалить проект, изменение название проекта), нажать кнопку *«Сохранить»* (рис. 308).

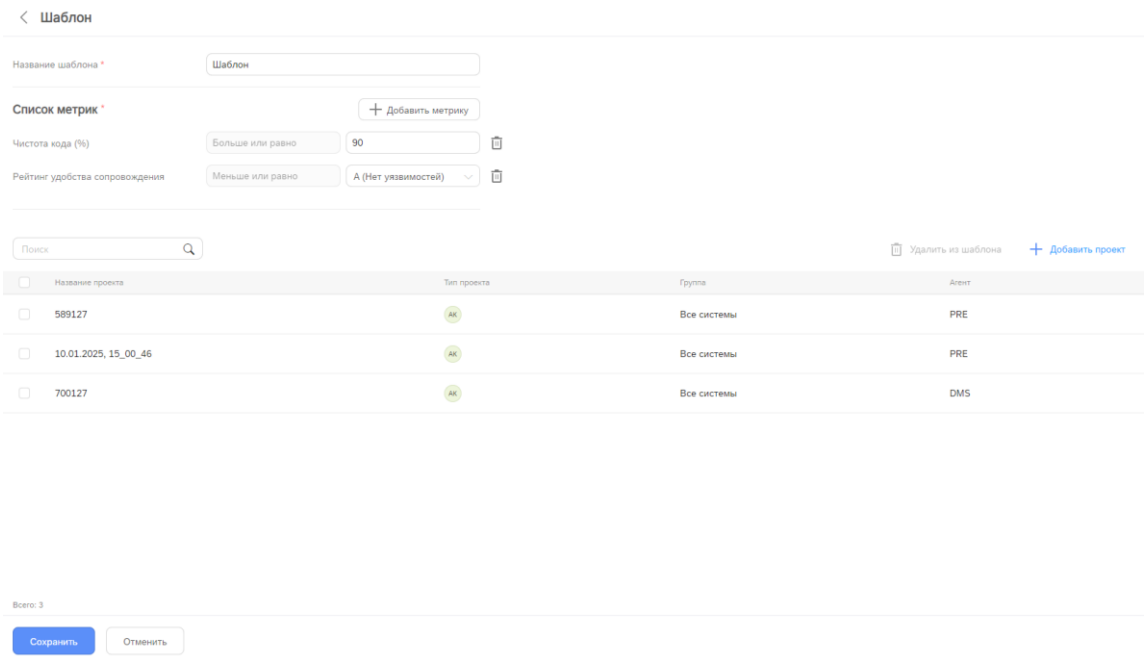


Рисунок 308 – Редактирование шаблона

7.1.8.4 Копирование шаблона

Для копирования шаблона необходимо нажать кнопку *«Копировать»* в строке шаблона (см. рис. 133), внести изменения (добавить, изменить или удалить метрику; изменить название; добавить или удалить проект), нажать кнопку *«Сохранить».*

7.1.8.5 Удаление шаблона

Для удаления шаблона необходимо нажать кнопку «Удалить» в строке проекта (см. рис. 133).

7.1.9 Модуль «Администрирование»

Веб-интерфейс модуля «Администрирование» предназначен для настройки параметров ПК «SafeERP Security Suite». В модуль «Администрирование» входят следующие разделы:

- «Лицензии»;
- «Общие настройки»;
- «Сервисное задание»;
- «Сканер»;
- «Анализ кода»;
- «Панель мониторинга»;
- «Ландшафт»;

— «Ankey IDM»;
— «Управление RFC».

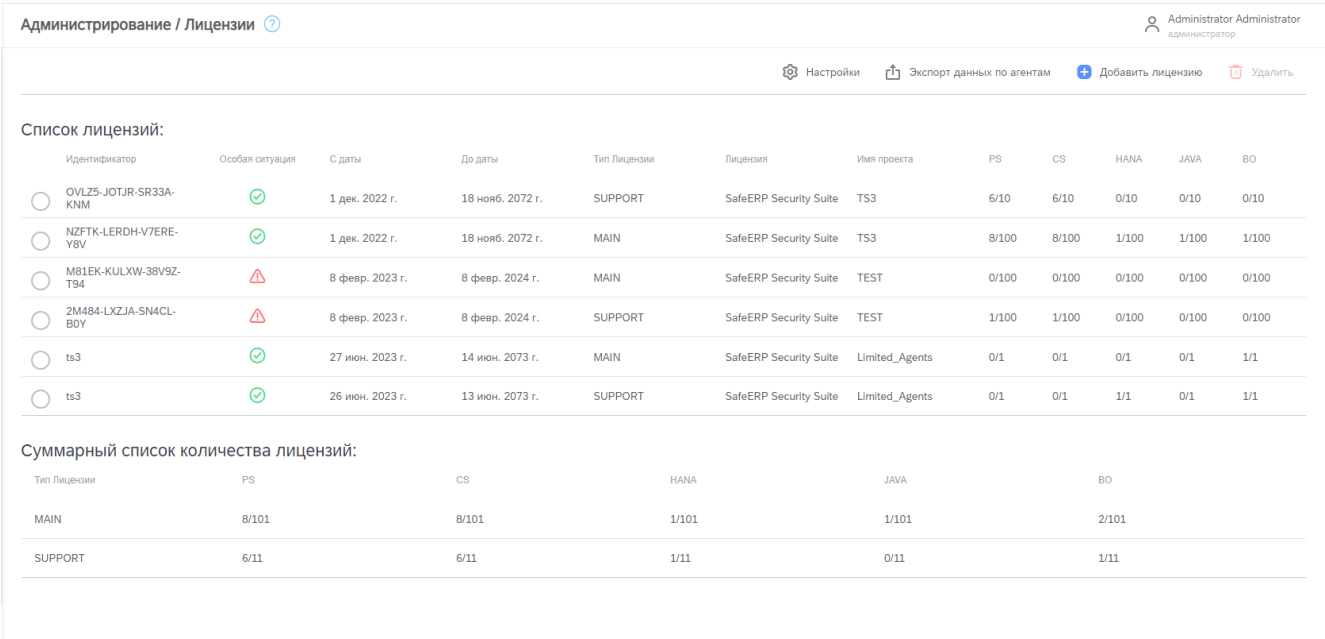
Элементы основной рабочей области модуля «Администрирование» представлены на рис. 134.

В основной рабочей области «Администрирование» доступны следующие действия:

1) Настройка раздела «Лицензии» (генерация запроса на активацию лицензии, папка для лицензии, загрузка активированной лицензии, сайт активации, предупреждение об истечении срока лицензии, просмотр количества подключений, удаление лицензии).
2) Настройка модуля «Общие настройки».
3) Настройка модуля «Сканер» (настройка проектов, настройка путей хранения данных).
4) Настройка модуля «Анализ кода» (настройка проектов, типа архива отчета).
5) Настройка модуля «Панель мониторинга» (настройка архивации проекта).
6) Настройка модуля «Ландшафт» (отображение модуля, сбор данных).
7) Настройка раздела «Ankey IDM».
8) Настройка RFC соединений.

7.1.9.1 Лицензии

Раздел «Лицензии» предназначен работы с лицензиями (рис. 309).



Идентификатор	Особая ситуация	С даты	До даты	Тип Лицензии	Лицензия	Имя проекта	PS	CS	HANA	JAVA	BO
OVLZ5-JOTJR-SR33A-KNM		1 дек. 2022 г.	18 нояб. 2072 г.	SUPPORT	SafeERP Security Suite	TS3	6/10	6/10	0/10	0/10	0/10
NZFTK-LERDH-V7ERE-Y8V		1 дек. 2022 г.	18 нояб. 2072 г.	MAIN	SafeERP Security Suite	TS3	8/100	8/100	1/100	1/100	1/100
M81EK-KULXW-38V9Z-T94		8 февр. 2023 г.	8 февр. 2024 г.	MAIN	SafeERP Security Suite	TEST	0/100	0/100	0/100	0/100	0/100
2M484-LXZJA-SN4CL-B0Y		8 февр. 2023 г.	8 февр. 2024 г.	SUPPORT	SafeERP Security Suite	TEST	1/100	1/100	0/100	0/100	0/100
ts3		27 июн. 2023 г.	14 июн. 2073 г.	MAIN	SafeERP Security Suite	Limited_Agents	0/1	0/1	0/1	0/1	1/1
ts3		26 июн. 2023 г.	13 июн. 2073 г.	SUPPORT	SafeERP Security Suite	Limited_Agents	0/1	0/1	1/1	0/1	1/1

Тип Лицензии	PS	CS	HANA	JAVA	BO
MAIN	8/101	8/101	1/101	1/101	2/101
SUPPORT	6/11	6/11	1/11	0/11	1/11

Рисунок 309 – Раздел «Лицензии»

В окно «Информация о лицензии» входят следующие поля (рис. 310):

— «Путь к папке DLL лицензии» – папка, в которой находятся файлы для активации лицензии. Папки необходимо настроить через интерфейс SAP GUI. Подробное описание настроек в пункте 4.2.1;
— «Сайт активации лицензии» – сайт, на котором необходимо активировать

лицензию. Сайт для активации лицензий необходимо уточнить у поставщиков услуг;

— «Предупреждать за (день)» – за какое количество дней предупреждать об истекающей лицензии;
— «Версия сервера управления» – информация о номере последней установленной версии (релиза) сервера управления ПК «SafeERP Security Suite»;
— «HwKey system» – информация о параметре «HwKey system», содержащем хэш-сумму ключа оборудования.

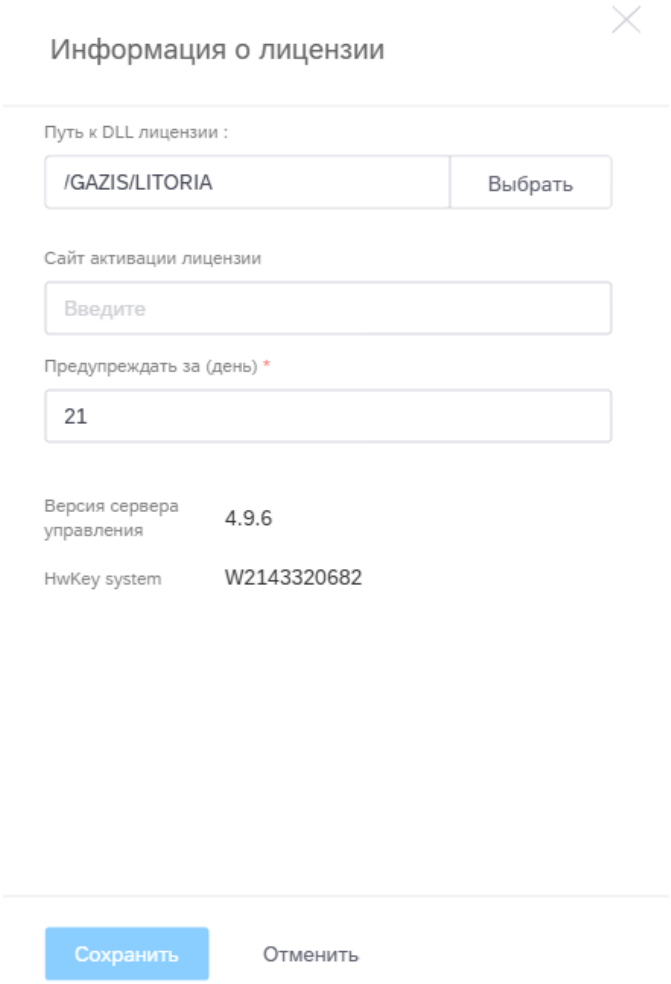


Рисунок 310 – Окно «Информация о лицензии» в разделе «Лицензии»

В рабочую область «Список лицензий» входят следующие поля (рис. 309):

— «Идентификатор лицензии» – индивидуальный идентификатор лицензии;
— «Особая ситуация» – статус лицензии. «Успешно» – лицензия действительна, «Ошибка» – лицензия недействительна, – лицензия с истекающим сроком действия;
— «С даты» – дата начала действия лицензии;
— «До даты» – дата окончания действия лицензии;

- «Тип лицензии» – тип лицензий, используемый в ПК «SafeERP Security Suite». Лицензии бывают следующих типов: MAIN (основная лицензия на подключение агентов) и SUPPORT (лицензия на техническую поддержку выбранного программного продукта);
- «Лицензия» – тип продукта, для которого приобретена лицензия. По умолчанию установлено – SafeERP Security Suite;
- «Имя проекта» – название проекта компании-заказчика, для которого приобретены лицензии на программные продукты SafeERP;
- «PS» – количество подключенных агентов и общее количество агентов на ABAP-системы для проверки программным модулем SafeERP Platform Security;
- «CS» – количество подключенных агентов и общее количество агентов на ABAP-системы для проверки программным модулем SafeERP Platform Security;
- «HANA» – количество подключенных агентов и общее количество агентов на HANA-системы для проверки программным модулем SafeERP Platform Security;
- «JAVA» – количество подключенных агентов и общее количество агентов на JAVA-системы для проверки программным модулем SafeERP Platform Security;
- «BO» – количество подключенных агентов и общее количество агентов на BO-системы для проверки программным модулем SafeERP Platform Security.

7.1.9.1.1 Генерация офлайн запроса на активацию лицензии

Для офлайн активации лицензии необходимо настроить следующие параметры:

- «Путь к папке DLL лицензии» – папка, в которой находятся файлы для активации лицензии. Папки необходимо настроить через интерфейс SAP GUI;
- «Сайт активации лицензии» – сайт, на котором необходимо активировать лицензию. Сайт для активации лицензии необходимо уточнить у поставщиков услуг.

Для офлайн активации лицензии необходимо выполнить следующие действия:

1) Нажать кнопку *«Добавить лицензию»* (рис. 309), выбрать «Сгенерировать запрос на лицензию», заполнить поля «Ключ лицензии» и «E-mail адрес», выбрать имя лицензии в окне «Генерация запроса на получение лицензии» для отправки ключа (рис. 311). Нажать кнопку *«Сгенерировать запрос»*. После генерации запроса автоматически загрузиться файл с расширением .json .

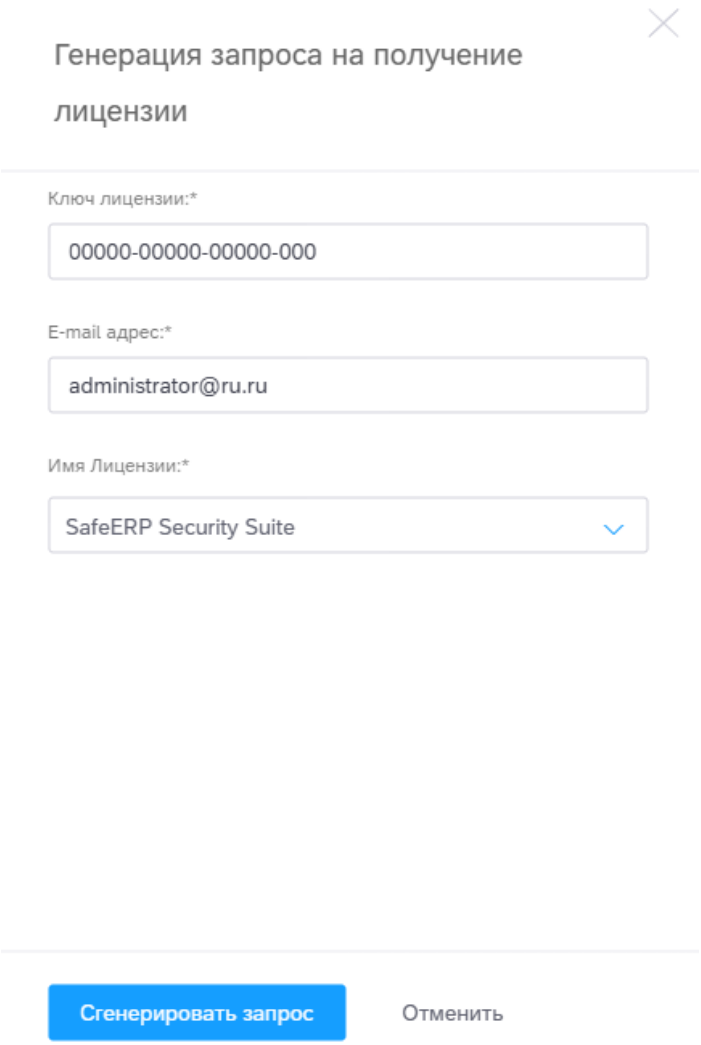


Рисунок 311 – Окно «Генерация запроса на получение лицензии»

2) Открыть в браузере новую вкладку. Ввести адрес сайта по активации лицензии. Нажать кнопку *«Выберите файл»*. В открывшемся окне выбрать файл с расширением .json. (рис. 312).

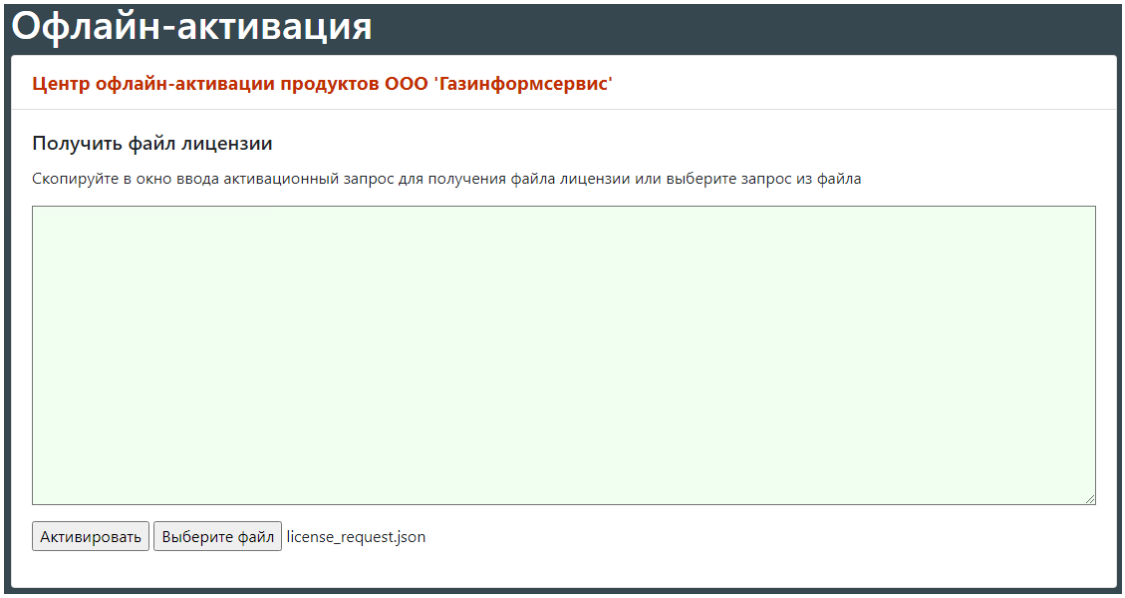


Рисунок 312 – Окно активации лицензии

3) Нажать кнопку *«Активировать»* (рис. 312). После успешной активации необходимо обратиться к электронной почте, указанной при активации ключа. На почту поступит архив, содержащий файл лицензии с расширением bin.
   Примечание. После активации лицензии пользователю доступна выгрузка активированного файла лицензии. Для выгрузки необходимо нажать кнопку *«Сохранить в файл»*.
4) Загрузить файл с расширение bin (см. подпункте 7.1.9.1.2).

7.1.9.1.2 Загрузка активированной лицензии

Примечание. Осуществляется загрузка только активированных лицензий.

Для загрузки активированной лицензии необходимо нажать кнопку «*Добавить лицензию»* (рис. 309), выбрать «Загрузить лицензию» (рис. 313).

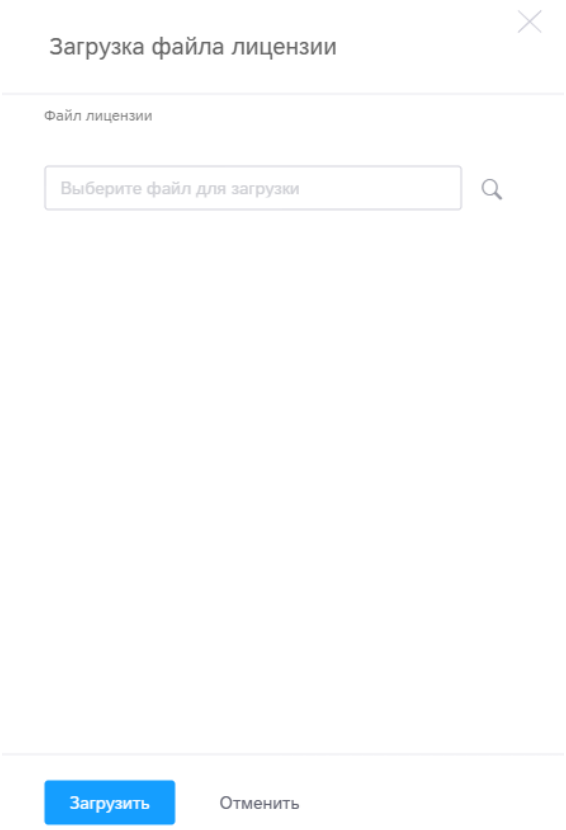


Рисунок 313 – Окно «Загрузка файла лицензии»

7.1.9.1.3 Экспорт данных по агентам

Для экспорта данных по агентам необходимо нажать соответствующую кнопку (рис. 309) в основной рабочей области раздела «Лицензии».

Файл по экспорту данных по агентам содержит следующее:

- SID – трехзначный идентификатор агента;
- описание – краткое описание агента;
- тип – тип агента, который используется в системе;
- версия – версия агента, который подключен в системе;
- группа – группа, в которую входит агент;
- ID основной лицензии – ключ основной лицензии;
- проект основной лицензии – информационно-управляющая система, к которой подключен агент;
- активность основной лицензии от – дата начала срока действия основной лицензии;
- активность основной лицензии до – дата конца действия основной лицензии;
- ID лицензии поддержки – ключ лицензии поддержки;
- проект лицензии поддержки – информационно-управляющая система, к которой подключен агент;
- активность лицензии поддержки от – дата начала срока действия лицензии поддержки;

— активность лицензии поддержки до – дата конца срока действия лицензии поддержки.

7.1.9.1.4 Удаление лицензии

Для удаления лицензии необходимо выбрать лицензию в списке, нажать кнопку *«Удалить»* (рис. 309) в основной рабочей области раздела «Лицензии», подтвердить действие.

7.1.9.2 Общие настройки

Раздел «Общие настройки» содержит следующие области:

— «Параметры запуска»;
— «Архивирование удаленных проектов»;
— «Временная папка»;
— «Настройка цвета».

В раздел «Параметры запуска» входят следующие поля (рис. 314):

— «Тип пользователя» – тип пользователя для запуска фонового задания. Существуют 2 типа пользователя: текущий пользователь (учетная запись пользователя, используемая для входа в систему сервера приложения ПК «SafeERP Security Suite») и технический пользователь (специальная техническая учетная запись для операций администрирования);
— «Учетная запись» – имя учетной записи пользователя при установке в поле «Тип пользователя» значения «Технический пользователь».

В область «Архивирование удаленных проектов» входит следующее поле (рис. 314):

— «Время архивации (дней)» – количество дней для хранения удаленных отчетов о проверках. При превышении заданного времени отчеты о проверках удаляются.

В область «Удаление итераций активных проектов» входят следующее:

— тумблер «Удаление итераций у проектов» – предназначен для активации процедуры удаления итераций у проекта.
— поле «Удалять итерации через (дней)» – количество дней, через которое будут удалены итерации. Минимальное значение – 1, максимальное значение – 1825. Поле становится доступным после перемещения тумблера в активное положение.

В область «Временная папка» входит следующее поле (рис. 314):

— «Логический путь для временных файлов» – путь к папке для временного хранения файлов на сервере приложений.

Примечание. При выборе папки /tmp/ очищение происходит раз в 10 дней. В других случаях необходимо очищать самостоятельно.

В область «Настройка цветов» входит следующий поле (рис. 314):

— «Цвет диаграммы» – цвет диаграммы на стартовой странице в ПК «SafeERP Security Suite». Доступные цвета: красный и синий.

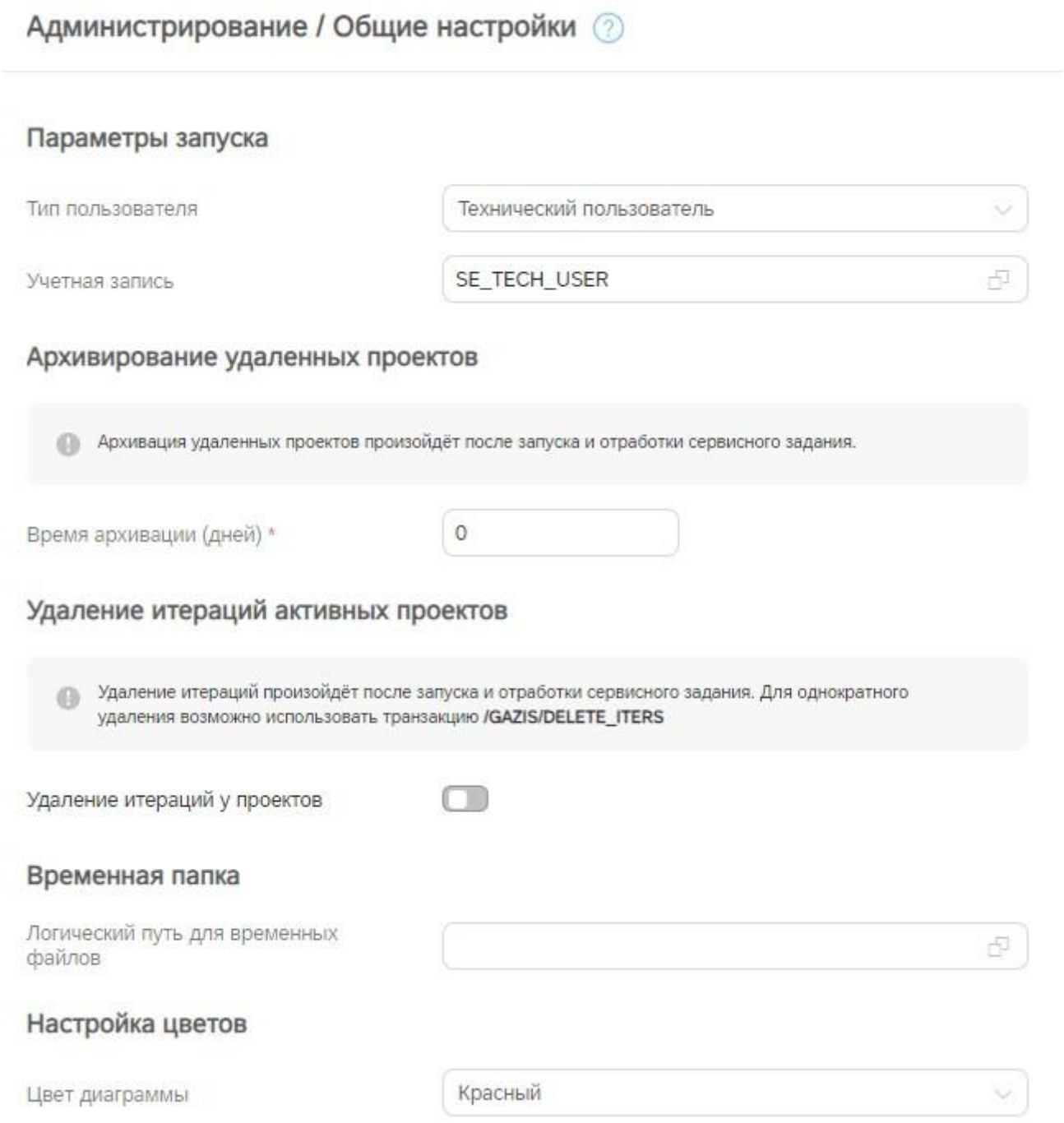


Рисунок 314 – Раздел «Общие настройки»

7.1.9.3 Сервисное задание

В область «Параметры запуска» входят следующие поля (рис. 315):

- «Имя программы» – имя программы, которая используется в качестве фонового задания;
- «Имя фонового задания» – имя задания, которое используется в качестве фонового задания;
- «Периодичность запуска» – период запуска фонового задания. Доступно для типа «по расписанию»;

— «Дата и время запуска» – дата и время запуска фонового задания;
— «Период» – периодичность запуска фонового. Доступно для типа запуска «по расписанию»;
— «Сервер»;
— «Следующий запуск» – дата и время следующего запуска фонового задания.

В область «Последнее выполненное задание» входят следующие поля (рис. 315):

— «Дата выполнения» – дата и время выполнения фонового задания;
— «Статус» – статус выполнения последнего фонового задания.

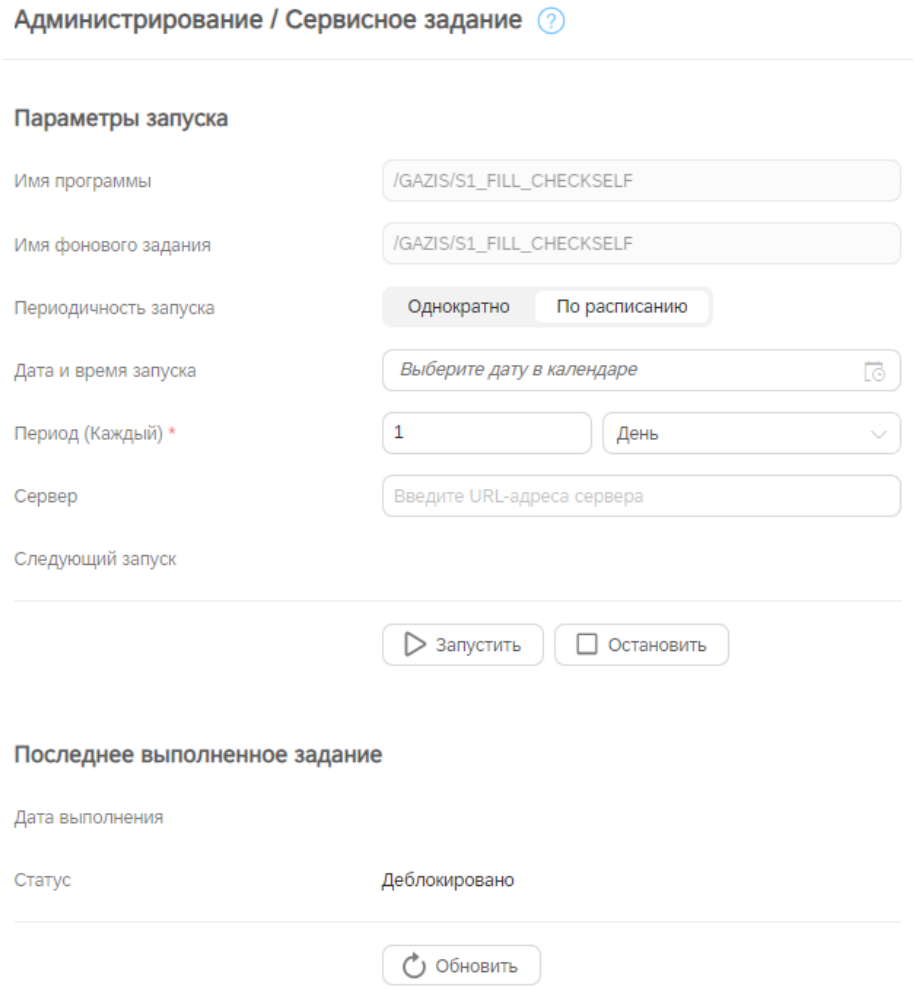


Рисунок 315 – Раздел «Сервисное задание»

7.1.9.4 Сканер

Раздел «Сканер» предназначен для настройки проектов соответствующего модуля.

Раздел «Сканер» состоит из двух вкладок:

— «Основные настройки» – общие настройки для модуля «Сканер»;
— «Настройки проектов» – настройки для типов проектов, которые применяются в модуле «Сканер».

Во вкладку «Основные настройки» входят следующие поля (рис. 316):

— «Логический путь данных» – выбор папки на дисковом пространстве АРМ для выгрузки и хранения отчетов с результатами анализа;

- «Логический путь хранения журналов» – выбор папки на дисковом пространстве для выгрузки и хранения журналов логирования;
- «Логический путь для файлов SIEM» – выбор места (названия папки) на дисковом пространстве для выгрузки и хранения журналов систем;
- «Время отклика RFC-соединения (сек.)» – ввод максимального времени ожидания проверки отклика от RFC-соединения;
- «Период анализа журнала (Дн.)» – выбор периода чтения лог-файлов из таблиц транзакции SE16 (с момента запуска анализа);
- «Лимит между СУ и агентами (мин)» – установка допустимой разницы во времени, установленном на сервере управления и агентах;
- «Количество недостатков в файле» – количество недостатков, которое войдет в отчет Excel.

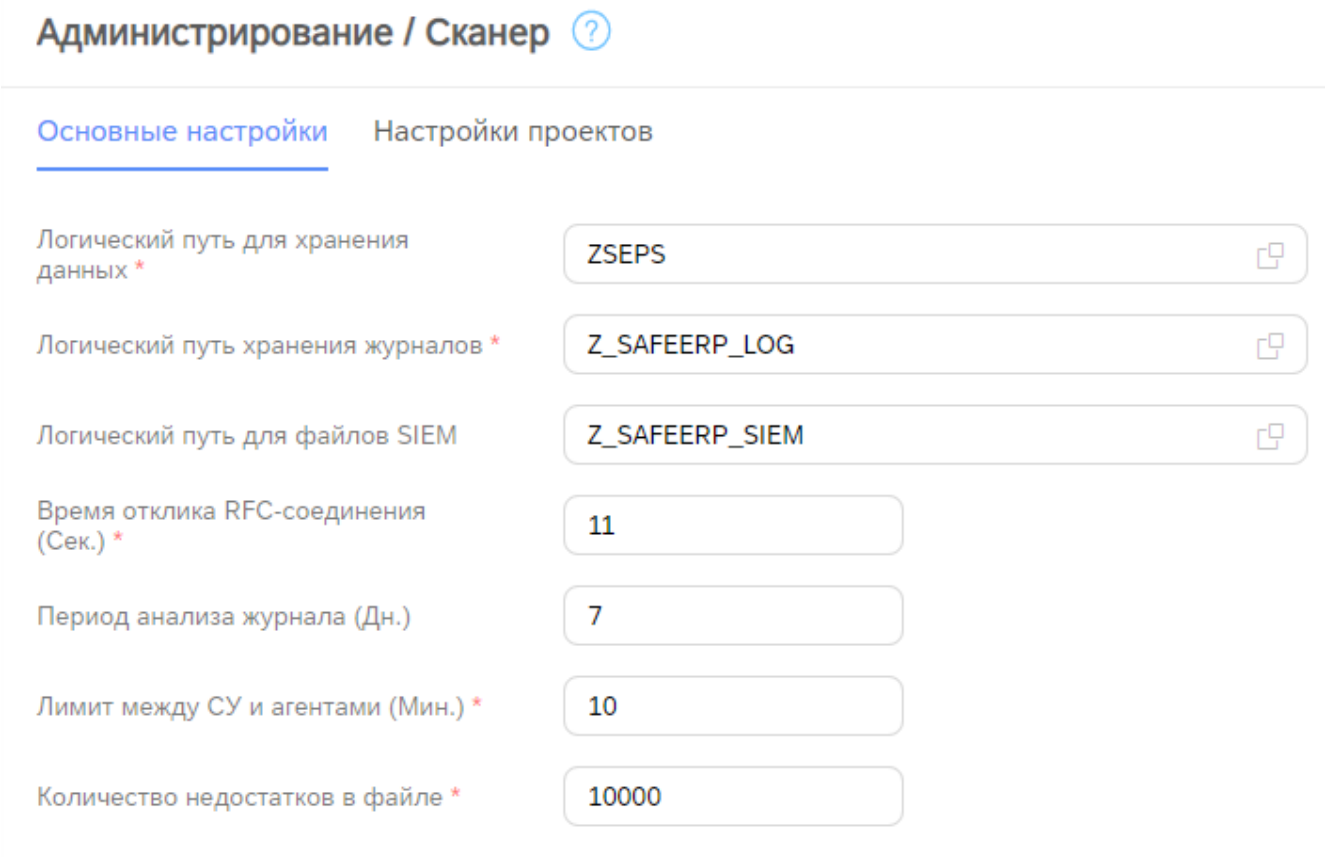


Рисунок 316 – Вкладка «Основные настройки» раздела «Сканер»

Во вкладку «Настройки проектов» входят следующие поля (рис. 317):

- «Рабочий отчёт(.xlsx)» – активация процедуры сохранения в архив рабочего отчета (в формате .xlsx) для всех итераций анализа;
- «Подробный отчет(.docx)» – активация процедуры сохранения в архив подробного отчета (в формате .docx) для всех итераций анализа;
- «Отключить уведомления для инструмента фиксации результатов КН» – отключение почтовых уведомлений для инструмента фиксации результатов;

— «Алгоритм вычисления контрольных сумм на агентах» – выбор алгоритма хэширования (вычисления контрольных сумм) для агентов типа ABAP и JAVA, HANA, BO. Для агента типа ABAP используются следующие алгоритмы: «ГОСТ Р 34.11-2012», «ГОСТ Р 34.11-94», «СТБ 34.101-2011», «Secure Hash Algorithm 1», «Message Digest 5». Для агентов типа JAVA, HANA, BO используются следующие алгоритмы: «Secure Hash Algorithm 1» и «Message Digest 5»;
— «Тип получения данных ИОД (тип T/E/P)» – тип получения данных для транзакций, EP Java и программ;
— «Тип получения данных ИОД (тип W)» – тип получения исходных данных для рабочей книги.

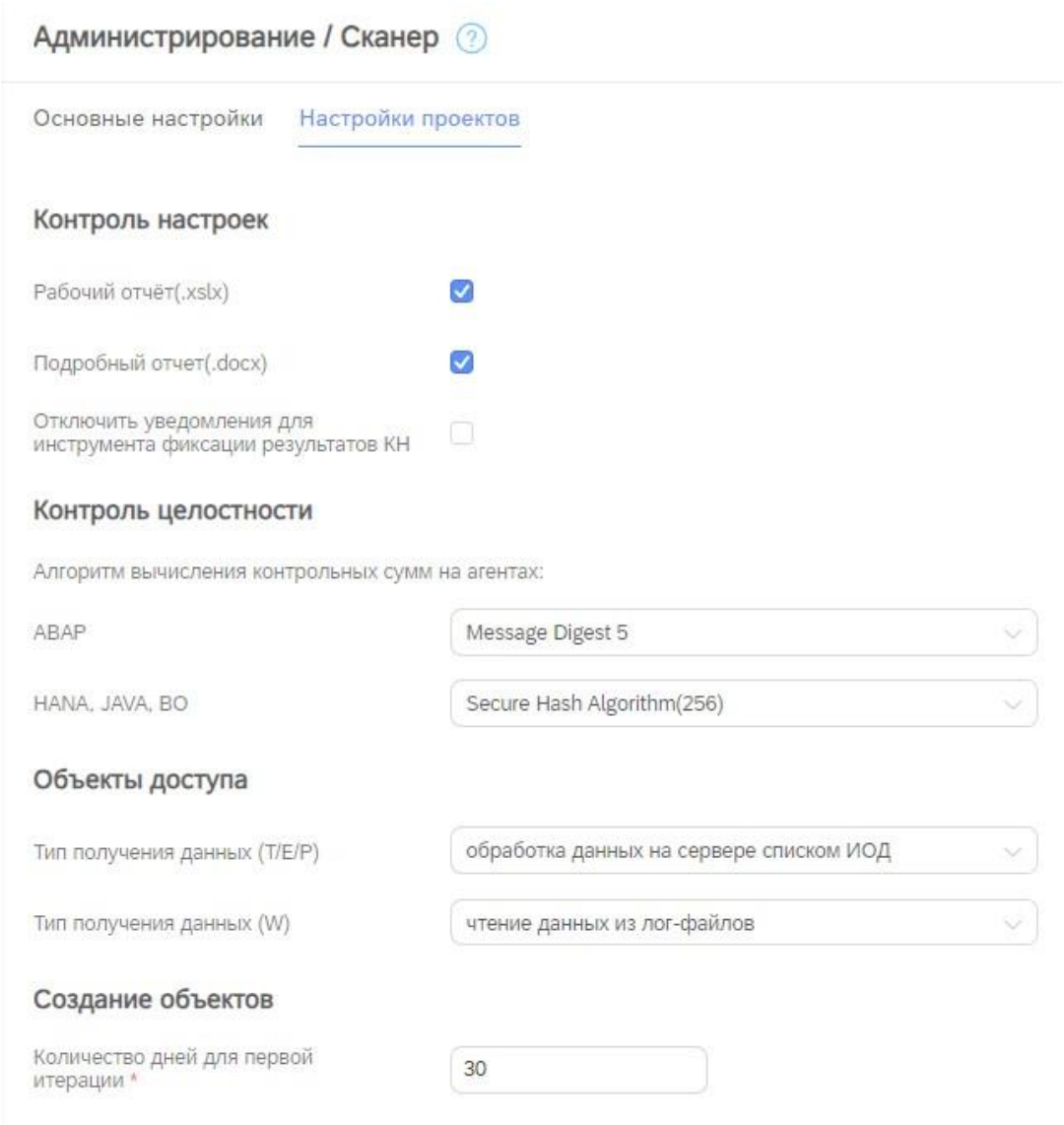


Рисунок 317 – Вкладка «Настройка проектов» раздела «Сканер»

Подробное описание алгоритмов работы представлено в таблице 18.

Таблица 18 – Описание алгоритмов для поля «Тип получения данных (тип T/E/P)»

Наименование	Описание
Обработка данных на сервере списком ИОД	Алгоритм работы с данными подразумевает чтение лог-файлов с агента на сервер управления и запись их на сервере управления для дальнейшей обработки. После чтения и обработки данные логов удаляются на сервере управления. Это устаревший тип обработки, не рекомендуется к использованию
Обработка данных на агенте списком ИОД	С сервера управления посылается список с перечнем объектов: транзакций, программ, BI книг. На агенте собираются данные, которые затем пересылаются на сервер управления. Вариант хорошо работает, когда список ИОД небольшой
Обработка данных на агенте по каждому ИОД на сервере	С сервера управления на агент посылается запрос на получение данных по событиям ИОД. На агенте собираются данные, которые затем пересылаются на сервер. Данные обрабатываются по одному значению
Обработка данных на агенте по каждому ИОД на агенте	С сервера управления посылается список с перечнем объектов: транзакций, программ, BI книг. На агенте собираются данные, которые затем пересылаются на сервер управления. Данные собираются по каждому объекту, объединяются и пересылаются на сервер управления
Анализ журнала проверки безопасности, новая версия	Рекомендуется использовать для новых версий SAP-систем. В работе транзакции SM20 произошли изменения: SAP разработал новое ПО, в котором для HANA-систем учитывается также возможность записи событий аудита в БД. Чтение данных в новой версии ПО не совместимы с предыдущими версиями. Рекомендуется использовать только данный тип получения данных ИОД

Подробное описание алгоритмов чтения представлено в таблице 19.

Таблица 19 – Описание алгоритмов для поля «Тип получения данных ИОД (тип W)»

Наименование	Описание
Чтение данных из таблиц статистики	Данные событий получают из таблиц БД
Данные событий получают из лог-файлов	Данные событий получают из лог-файлов

7.1.9.5 Анализ кода

Раздел «Анализ кода» предназначен для настройки проектов соответствующего модуля. Раздел «Анализ кода» содержит следующие вкладки (рис. 318):

- «Основные настройки»;
- «Интеграция с АТС»;
- «Интеграция с ТС SAP»;
- «Отчёты».

Во вкладку «Основные настройки» входят следующие поля (рис. 318):

- «Логический путь для хранения данных» – папка для выгрузки и хранения отчетов с результатами анализа;
- «Глубина анализа» – выбор количества проверяемых цепочек вызовов подпрограмм;
- «Потоки» – последовательность инструкций, которые выполняются параллельно с другими потоками;
- «Количество недостатков программ в файле» – максимального количества строк с перечнем результатов анализа, которое может содержать отчет в формате Excel;
- «Количество строк кода в оценке защищенности» – максимальное количества строк в программе для анализа кода;
- «Кэширование данных программных объектов» – сохранения данных о проверяемых программных объектах в базу данных;
- «Выбор варианта проверок для обратного вызова» – варианта проверки (профиля), который должен использоваться для анализа кода при деблокировании транспортного запроса на агенте;
- «Кэширование данных о программных объектах» – сохранения данных о проверяемых программных объектах в базу данных;
- «Почтовые уведомления при управлении уязвимостями «Анализ кода» – активация почтовых уведомлений для инструмента фиксации.

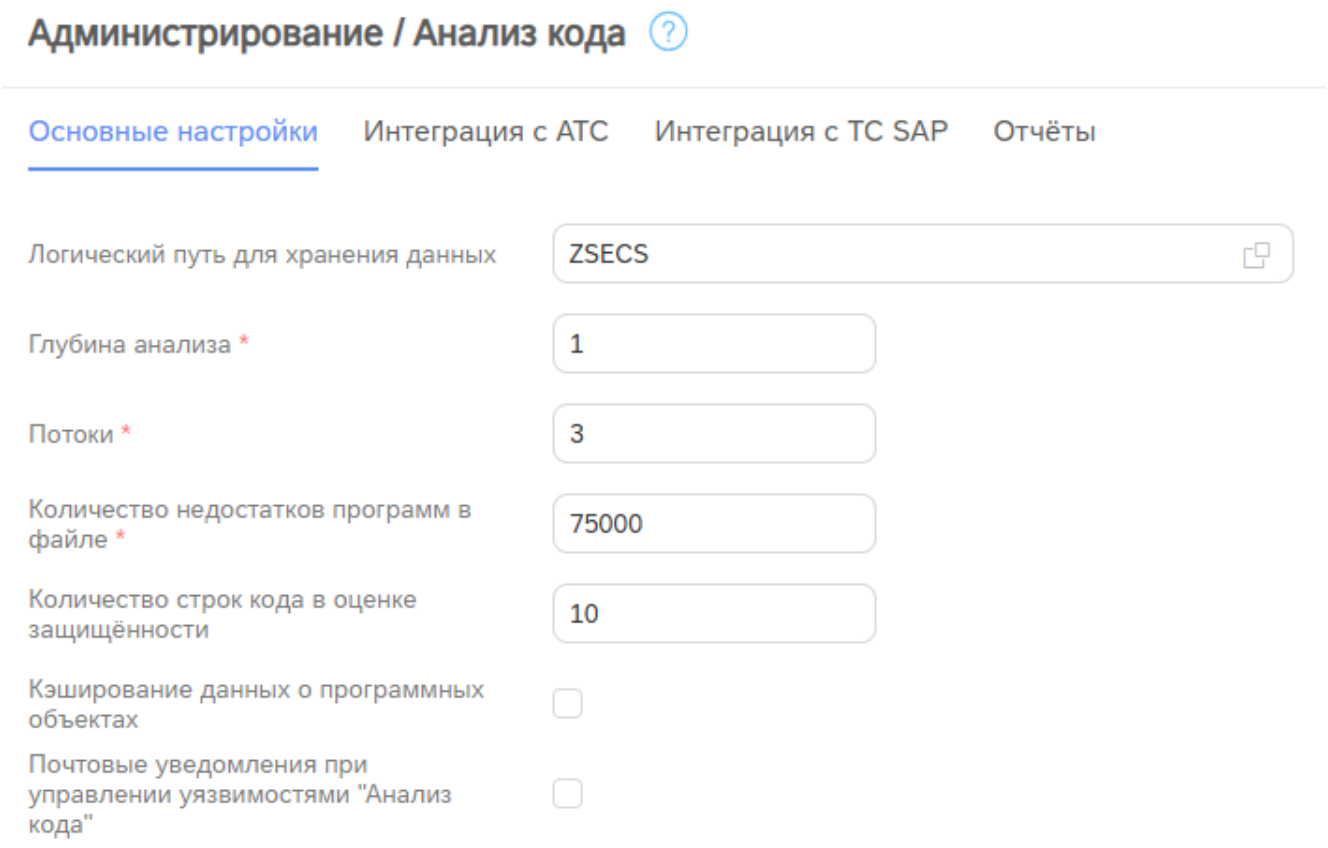


Рисунок 318 – Вкладка «Основные настройки»

Во вкладку «Интеграция с АТС» входят следующие поля (рис. 319):

- «Автоматический экспорт в АТС» – активация процедуры экспорта в АТС;
- RFC-соединение к АТС-серверу – имя RFC-соединения, которое используется для подключения к центральной системе проверки АТС;
- «Тип запрашиваемого пользователя» – тип пользователя, по действиям которого необходимо формировать уведомления о запросе на утверждение освобождения уязвимости от ложного срабатывания: автор объекта (учетная запись пользователя, под которой создавался программный объект, требующий утверждения), последний изменивший объект (учетная запись пользователя, под которой изменялся программный объект, требующий утверждения), указанный пользователь (выбираемая учетная запись пользователя, от которой разрешается принимать запросы на утверждение освобождений по программным объектам);
- «Тип учетной записи утверждающего» – выбор типа пользователя для получения уведомлений и согласовании запросов на утверждение освобождения уязвимости от ложного срабатывания: текущий пользователь (учетная запись пользователя, используемая для входа в систему сервера приложения ПК «SafeERP Security Suite»), указанный пользователь (выбираемая учетная запись пользователя для согласования запросов на утверждение освобождения);

— «Учетная запись» – учетной записи пользователя при установке в полях «Тип запрашивающего пользователя» и «Тип утверждающего пользователя» значения «Указанный пользователь»;
— «Описание разработчика» – записи описания разработчика для автоматического заполнения соответствующего поля при утверждении освобождения;
— «Заключение» – записи заключения для автоматического заполнения соответствующего поля при утверждении освобождения.

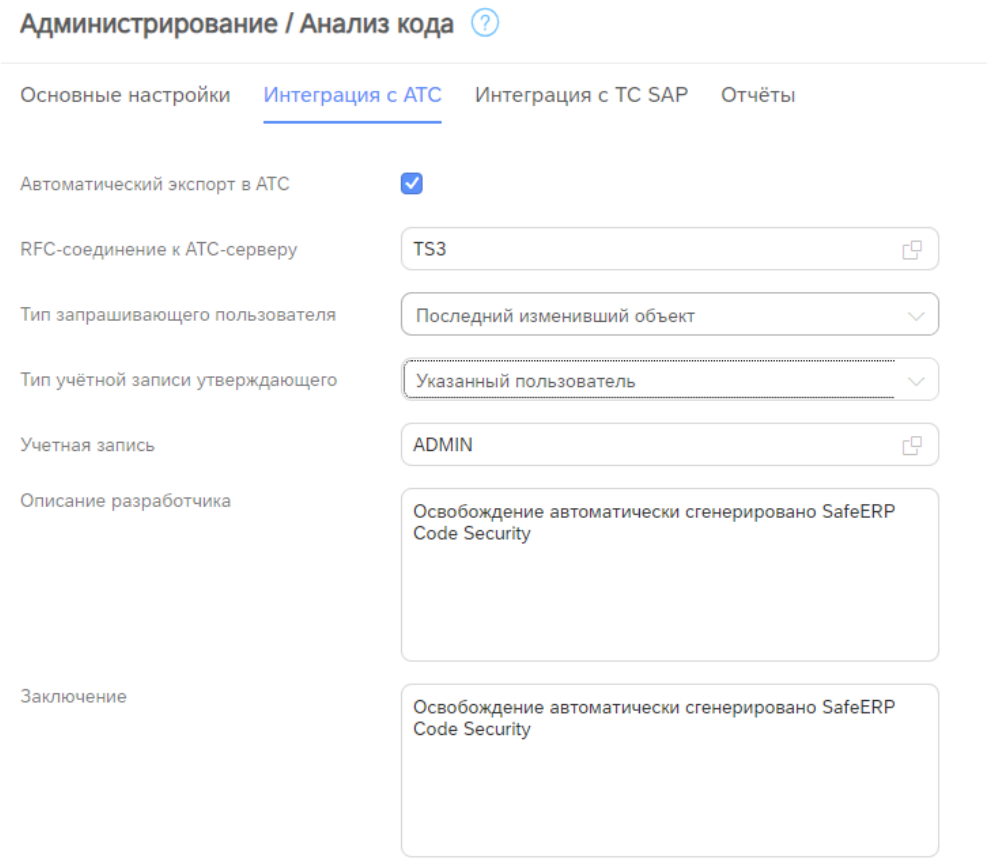


Рисунок 319 – Вкладка «Интеграция с АТС»

Вкладка «Интеграция с ТС SAP» (рис. 320) предназначена для проверки количества проверок на агенте и сервере управления.

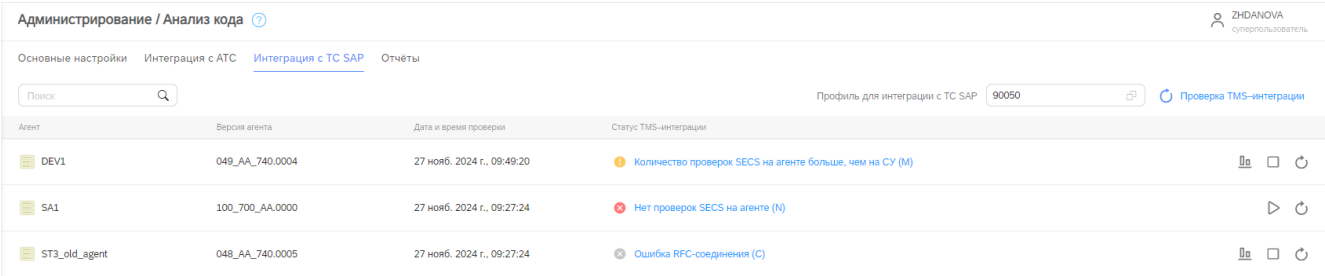


Рисунок 320 – Вкладка «Интеграция с ТС SAP

Запуск проверки осуществляется следующим способами:

— через кнопку Проверка TMS–интеграции «Проверка TMS-интеграций» – проверяются все агенты, которые подключены к системе;

— через кнопку «Проверка TMS-интеграций» – проверяется выбранный агент.

Статусы агента после процедуры проверки бывают следующими:

— A – количество сценариев на агенте = 0 или количество сценариев на агенте = количеству сценариев на сервере;
— C – ошибка RFC-соединения
— E – несуществующий профиль для варианта проверок обратного вызова
— I – количество сценариев на сервере и на агенте одинаково, но есть различия в самих сценариях;
— L – количество сценариев на сервере, больше чем на агенте;
— M – количество сценариев на агенте, больше чем на сервере;
— N – сценарии на агенте отсутствуют;
— R – список активных сценариев не соответствует эталонному.

Примечание. Для выравнивания количества проверок на агенте необходимо нажать кнопку *«Выровнять».*

Во вкладку «Отчеты» входят следующие поля (рис. 321):

— «Рабочий отчет (.xlsx)» – активация процедуры сохранения в архив рабочего отчета (в формате .xlsx) для всех итераций анализа. Список документов, формирующихся при активации данной формы отчета, – CHECKS.XLSX, FLAW.XLSX, ITERATION.XLSX, OBJECT.XLSX;
— «Основной отчет (.docx)» – активация процедуры сохранения в архив подробного отчета (в формате .docx) для всех итераций анализа. Документ, формирующийся при активации данной формы отчета, – REPORT.DOCX;
— «Отчет-презентация» – активация процедуры сохранения в архив отчета с метриками результата анализа по категории «Безопасность» (в формате .docx) для всех итераций анализа. Документ, формирующийся при активации данной формы отчета, – REPORT-METRICS.DOCX;
— «Тип архива» – тип архива отчета. В модуле используются следующие типы архивов: tar и zip.

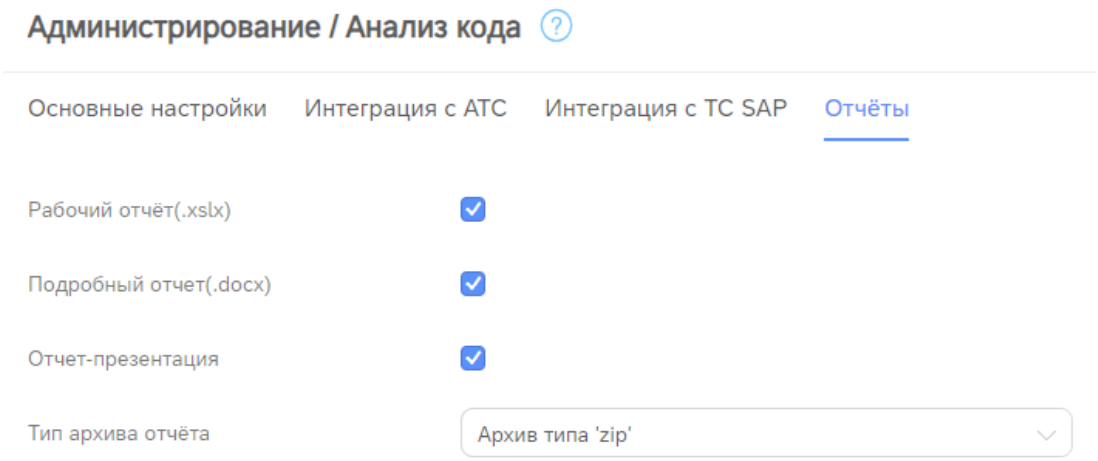


Рисунок 321 – Вкладка «Отчеты» раздела «Анализ кода»

7.1.9.6 Панель мониторинга

Раздел «Панель мониторинга» предназначен для настройки соответствующего модуля. В раздел «Панель мониторинга» входят следующие области (рис. 322):

- «Анализ данных»;
- «Данные по агентам»;
- «Архивирование проекта»;
- «Временная папка»;
- «Настройка цвета».

В область «Анализ данных» входят следующие поля (рис. 322):

- «Период анализа (дней)» – установка периода для сбора и учета данных по результатам анализа систем (по итерациям проектов) для формирования соответствующих аналитик и статистики в панели мониторинга;
- «Период анализ динамических ошибок DUMPs (дней)» – установка периода для сбора и учета данных по результатам анализа систем (по итерациям проектов) для формирования соответствующих аналитик и статистики в панели мониторинга.

В область «Данные по агентам» входят следующие поля (рис. 322):

- «Количество продуктивных ABAP-агентов» – количество продуктивных агентов типа ABAP в системе;
- «Количество непродуктивных ABAP-агентов» – количество непродуктивных агентов типа ABAP в системе;
- «Количество ABAP-агентов» – количество продуктивных и непродуктивных агентов типа ABAP в системе;
- «Количество JAVA-агентов» – количество агентов типа JAVA в системе;
- «Количество HANA-агентов» – количество агентов типа HANA в системе;
- «Количество BO-агентов» – количество агентов типа BO в системе.

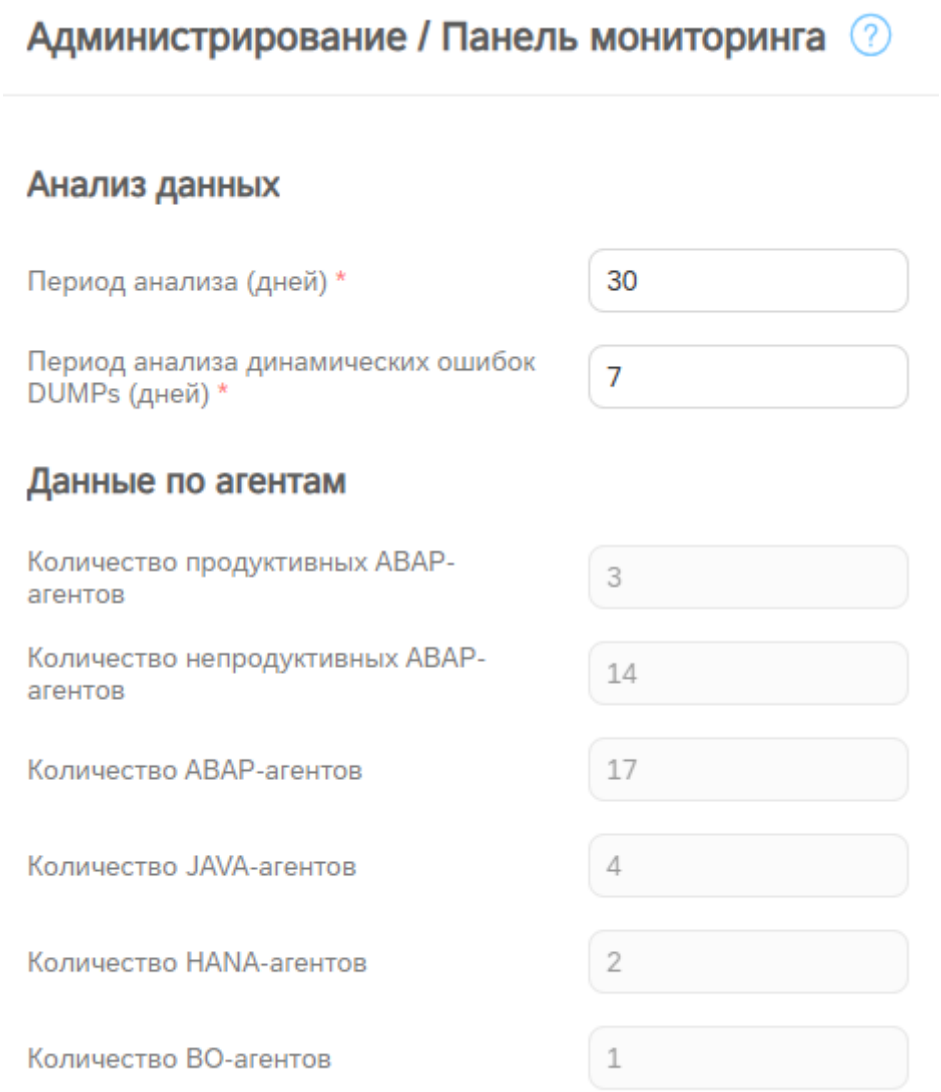


Рисунок 322 – Раздел «Панель мониторинга»

7.1.9.7 Ландшафт

Раздел «Ландшафт» предназначен для настройки проектов соответствующего модуля.

Раздел «Ландшафт» состоит из следующих областей:

- «Параметры запуска сбора данных»;
- «Последнее выполненное задание».

Для включения отображения модуля «Ландшафт» необходимо переместить переключатель в активное положение.

В раздел «Ландшафта» входят следующие поля (рис. 323):

- «Имя фонового задания» – название программы с фоновым заданием, которая выполняет сбор данных для карты сети. По умолчанию стоит программа: /GAZIS/S1_MAP.
- «Периодичность запуска» – временный промежуток для сбора данных карты соединений. Доступны следующие варианты периодичности: однократно (фоновое задание выполняется немедленно) и по расписанию.
- «Дата и время запуска» – дата и время следующего запуска фонового задания).

— «Период (каждый)» – временный промежуток для сбора данных карты соединений. Доступны следующие варианты периода: минуты, часы, день, неделя, месяц).
— «Сервер» – адрес сервера, через который запускается фоновое задание. Для просмотра необходимо обратиться к транзакции SM36 в SAP GUI.
— «Следующий запуск» – дата и время следующего выполнения фонового задания.

В область «Последнее фоновое задание» входят следующие поля:

— «Дата выполнения» – дата и время выполнения последнего фонового задания.
— «Статус» – статус последнего фонового задания.

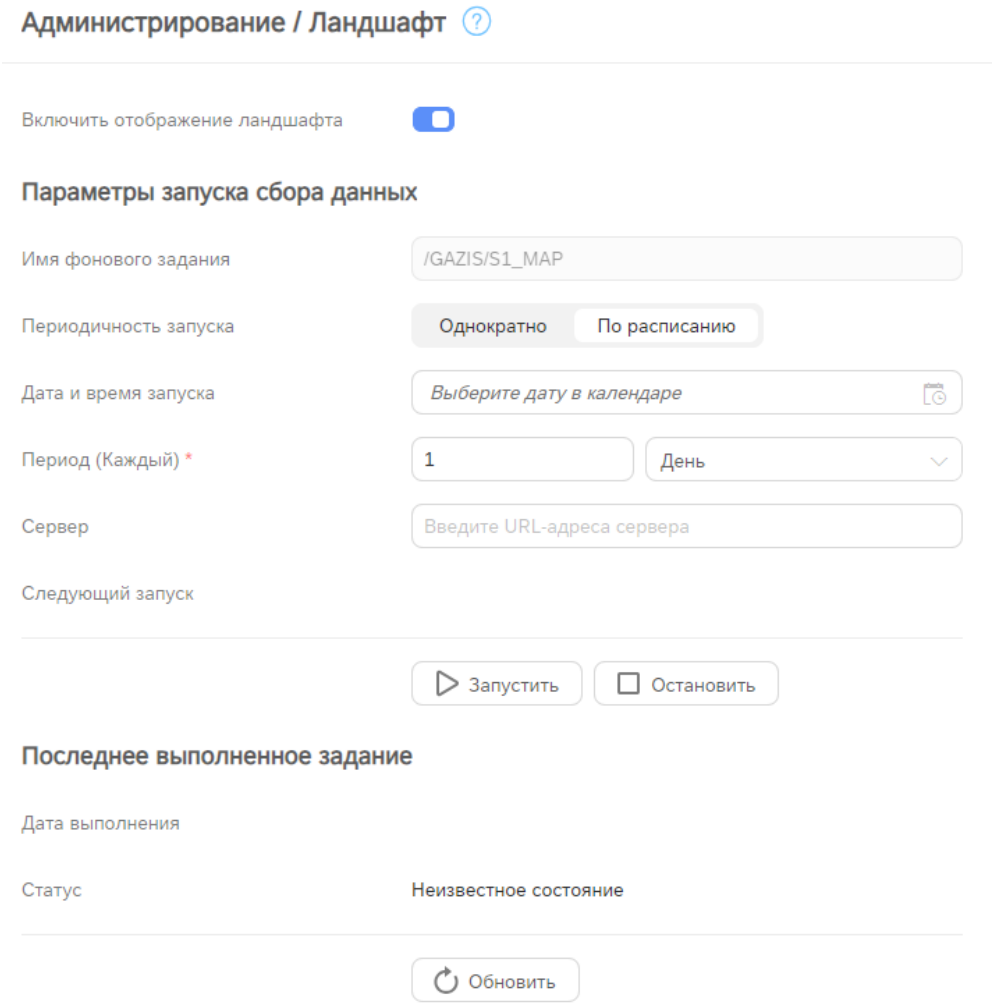


Рисунок 323 – Раздел «Ландшафт»

7.1.9.8 Ankey IDM

Раздел «Ankey IDM» предназначен для настройки проектов соответствующего модуля.

В раздел «Ankey IDM» входят следующие поля (рис. 324):

— «Профиль» – профиль, в котором содержатся проверки для анализа пользователя;
— «Алгоритм расчета» – алгоритм проверок IDM. Алгоритмы подразделяются на следующие типы: общий алгоритм и организационные уровни;
— «URL доступа ANKEY IDM» – url-адрес, для передачи https post-запроса из Ankey

IDM;

— «RFC-адрес» – RFC-адрес, по которому передаются данные для SAP. Для настройки RFC-соединения необходимо выбирать тип соединения G.

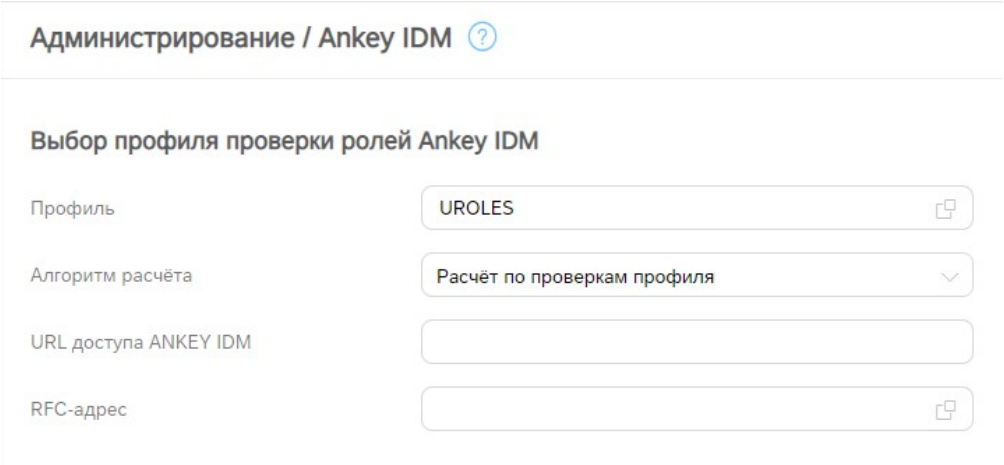


Рисунок 324 – Раздел «Ankey IDM»

7.1.9.9 Управление RFC

Раздел «Управление RFC» предназначено для ведения настроек RFC соединений. Является аналогом транзакции /N/GAZIS/CONTROL_RFC.

В раздел входят следующие вкладки (рис. 325):

— «Общие настройки»;

— «Фоновое задание».

В области «Общие настройки» доступен выбор агентов и атрибутов RFC соединений.

В область «Общие настройки» входят следующие поля (рис. 325):

— «Сканируемые агенты» – список агентов, которые входят в проверку.

— «Проверка активности RFC» – проверка RFC-соединений агентов. По умолчанию проверка активна.

В области «Атрибуты на контроле» доступен выбор следующего (рис. 325):

— целевой хост;

— мандант;

— текущий пользователь;

— пользователь;

— пароль;

— экран RFC входа;

— достоверная система;

— RFC SNC;

— полномочия на адрес;

— язык.

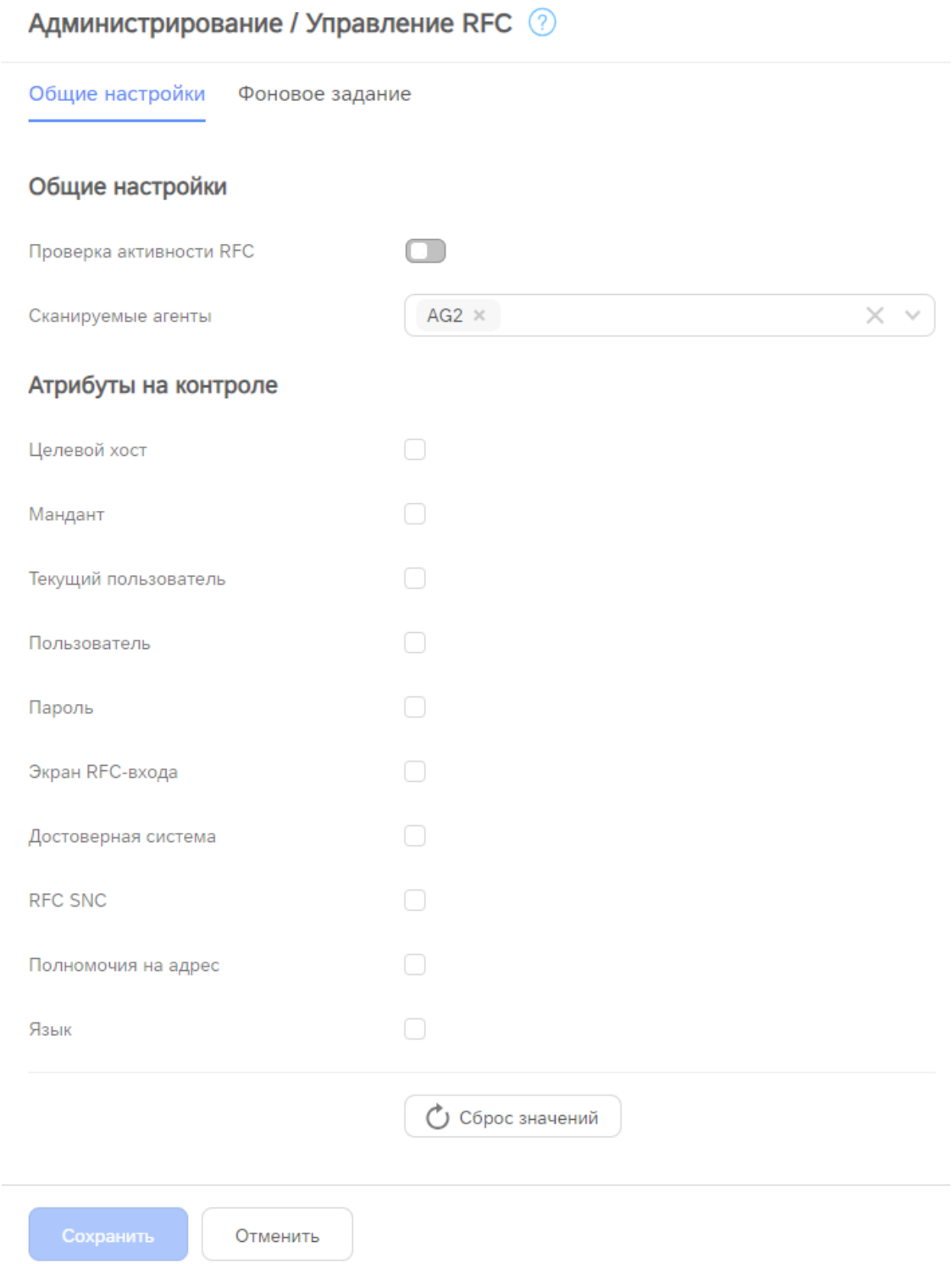


Рисунок 325 – Раздел «Управление RFC»

Во вкладке «Фоновое задание» предоставляется возможность настройки фонового задания.

Во вкладку «Фоновое задание» входят следующие области (рис. 326):

- «Параметры запуска»;
- «Последнее выполненное задание».

В область «Параметры запуска» входят следующие поля (рис. 326):

- «Имя фонового задания» – название программы, которое используется в качестве фонового задания. По умолчанию задана программа /GAZIS/S1_MAP_RFC_SCAN;
- «Периодичность запуска» – выбор периода запуска фонового задания;
- «Дата и время запуска» – дата и время следующего запуска фонового задания;
- «Период (каждый)» – период повтора фонового задания;
- «Сервер» – адрес сервера, через который запускается фоновое задание. Для просмотра необходимо обратиться к транзакции SM36 в SAP GUI;
- «Следующие запуск» – дата и время следующего запуска фонового задания.

В область «Последнее выполненное задание» входят следующие поля (рис. 326):

- «Дата выполнения» – дата и время выполнения фонового задания;
- «Статус» – статус выполнения фонового задания.

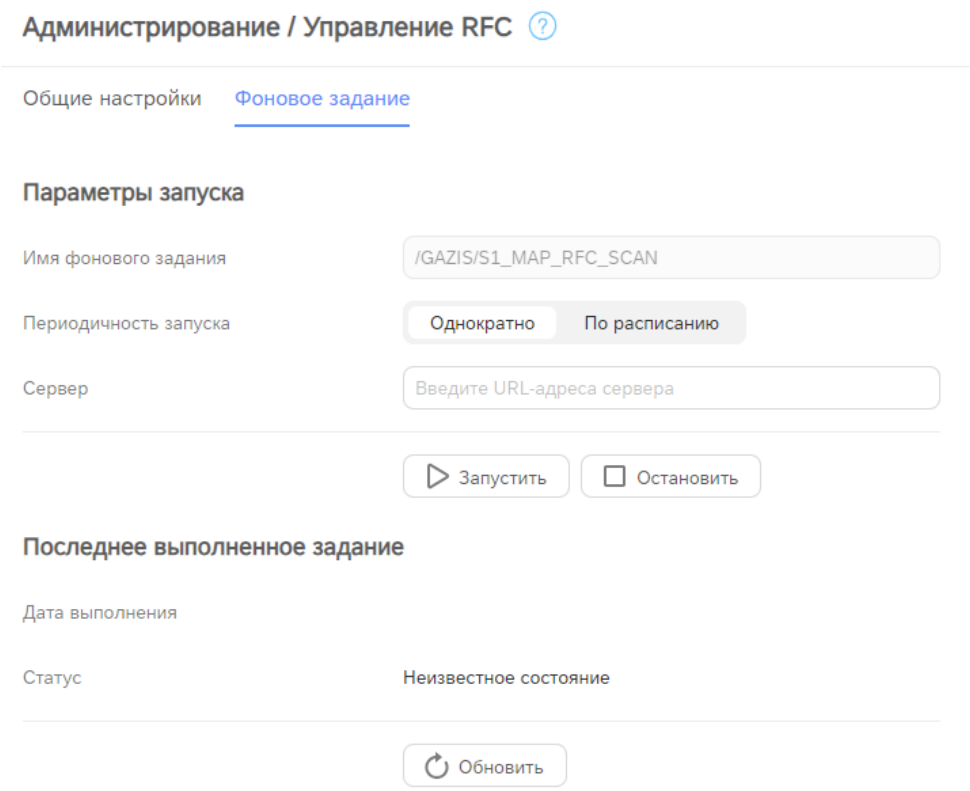


Рисунок 326 – Вкладка «Фоновое задание»

7.1.10 Модуль «Аудит»

Модуль «Аудит» предназначен для просмотра логов по событиям системы SAP ABAP NetWeaver.

Модуль «Аудит» состоит из следующего раздела:

- «Аудит логов».

Раздел «Аудит логов»

Раздел «Аудит логов» предназначен для просмотра логов по событиям системы SAP ABAP (NetWeaver).

Данный раздел является аналогом стандартной транзакции SM20.

Раздел «Аудит логов» состоит из следующих областей:

- «Основная рабочая» – предназначена для составления и выполнения запросов;
- «Результат запроса» – предназначена для отображения логов после выполнения запроса.

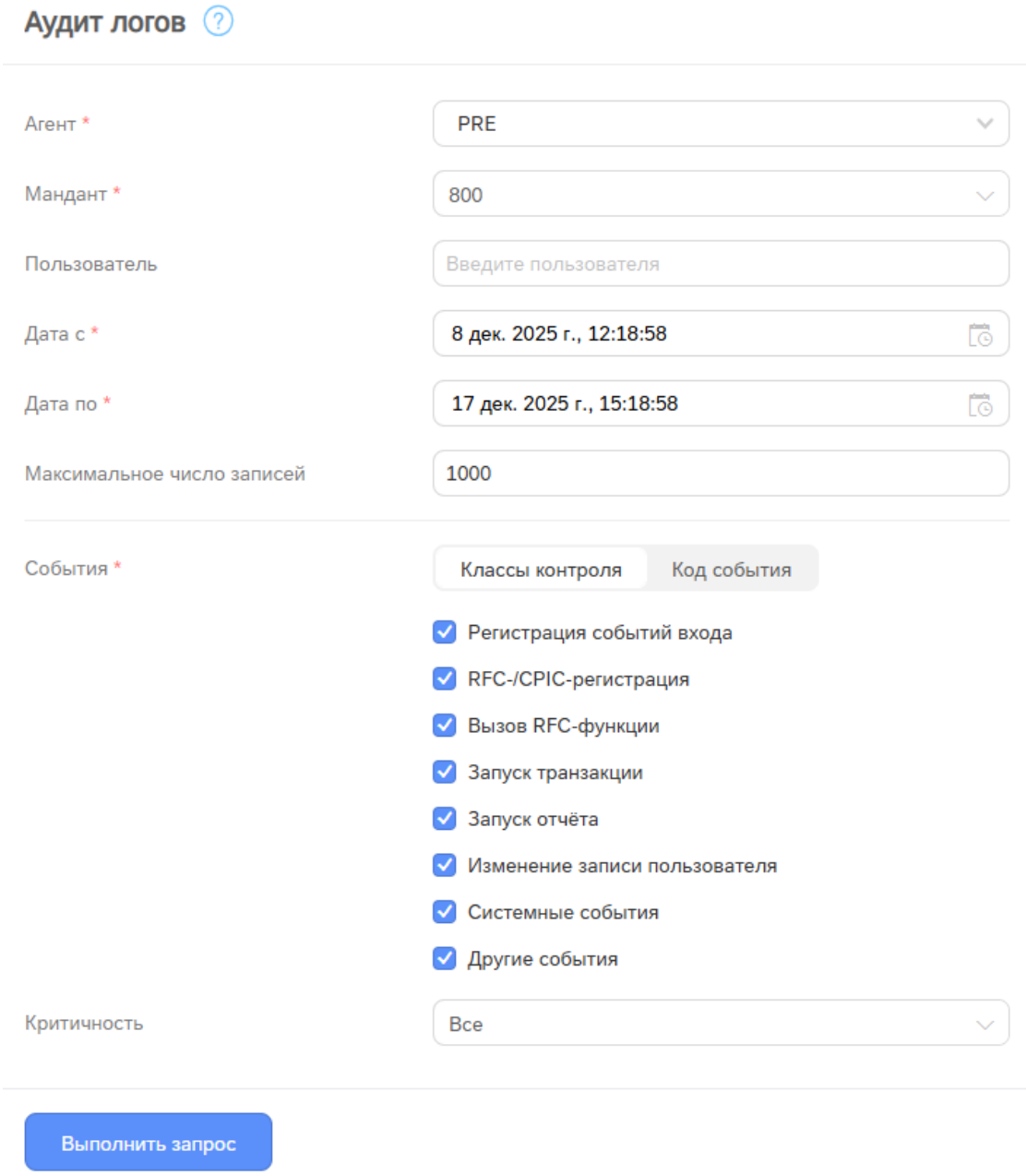


Рисунок 327 – Основная рабочая область раздела «Аудит логов»

Основная рабочая область состоит из следующих полей:

— «Агент» – выбор агент-системы для анализа. В данном поле доступны агенты ABAP;
— «Мандант» – выбор манданта для анализа. Список мандантов формируется в соответствии с выбранным агентом. По умолчанию установлено значение «Все»;
— «Пользователь» – выбор пользователя для поиска событий;
— «Дата с» – дата начала периода поиска. По умолчанию установлено значение «Текущее время - 3 ч»;
— «Дата по» – дата окончания периода поиска. По умолчанию установлено значение «Текущее время»;
— «Максимальное число записей» – количество строк, отображаемых в результатах. По умолчанию задано значение 1000;
— «События» – сплит-кнопка, содержащая два режима выбора событий:
  А) «Классы контроля» – по умолчанию активный режим. При выборе отображается список доступных классов контроля (чекбоксы), а также поле «Критичность» для дополнительной фильтрации.
  Б) «Код события» – при выборе отображается кнопка «Выбор событий», которая открывает модальное окно. В окне можно выбрать одно или несколько конкретных событий для выполнения запроса. После выбора выбранные события выводятся под сплит-кнопкой;
— «Критичность» – выбор критичности событий. Доступны следующие степени критичности: все, высокая и средняя, высокая;
— «Выполнить запрос» – кнопка, выполняет поиск по заданным параметрам. Доступна после заполнения всех обязательных полей.

Примечания:

1. В поле «Пользователи» можно ввести только одно значение.
2. Если поле «Пользователи» пустое, то поиск выполняется по всем пользователям.
3. При вводе данных в поле «Пользователи» действуют следующие правила:

— «А*» – поиск пользователей, начинающихся на А;
— «*А» – поиск пользователей, заканчивающихся на А;
— «*А*» – поиск пользователей, содержащих А;
— «А» – поиск пользователей, имеющих полное совпадение;
— «*» – поиск всех пользователей.

Модальное окно «Выбор событий»

Модальное окно «Выбор событий» используется для выбора одного или нескольких событий, которые будут включены в запрос.

В окне отображаются и доступны следующие элементы управления (рис. 328):

— поле «Агент»;
— поле «Мандант»;
— поле «Выбранные события (максимум 30)»;

— поле «Поиск»;
— кнопка «Фильтр»;
— таблица событий.

Таблица событий содержит следующие столбцы:

— «Класс контроля»;
— «Критичность»;
— «Код события»;
— «Сообщение».

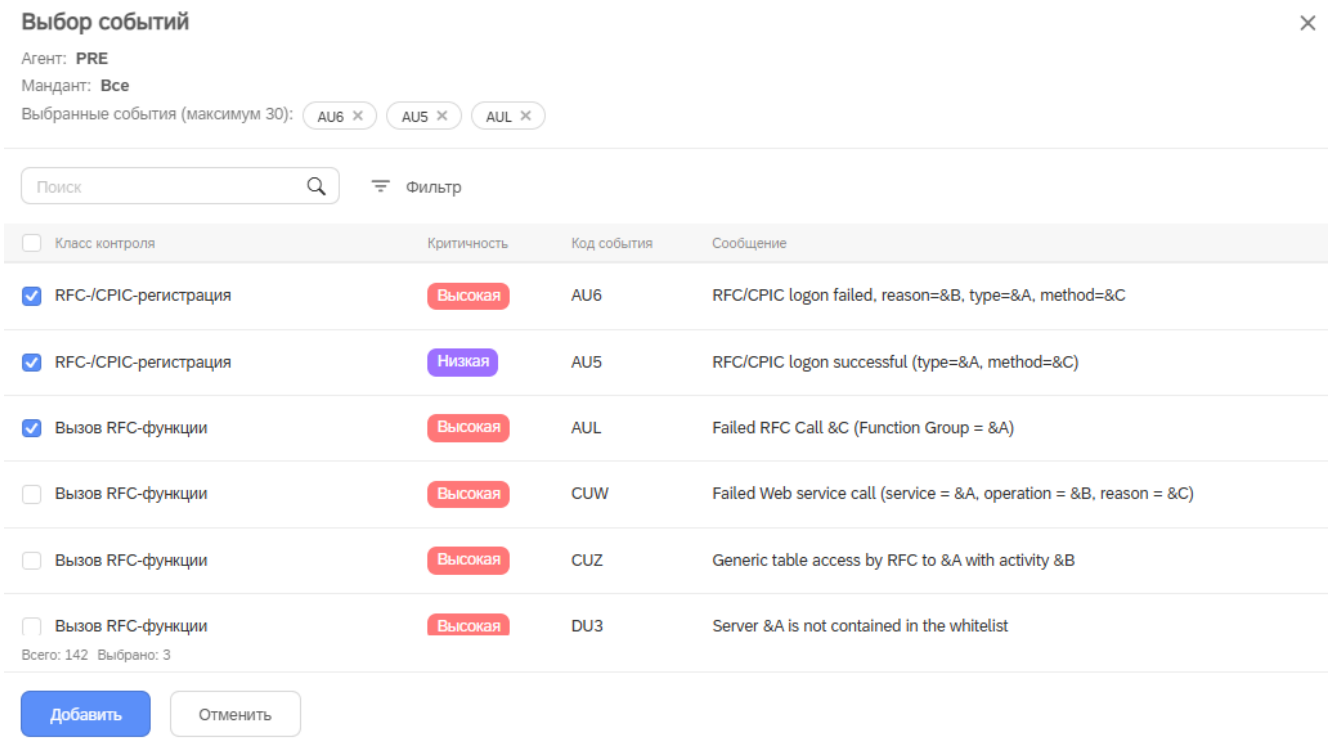


Рисунок 328 – Модальное окно «Выбор событий»

Пользователю доступен выбор одно или несколько событий с помощью чекбоксов.
Пользователю доступен выбор одного или нескольких событий. В поле «Выбранные события» отображаются коды выбранных событий.
Под таблицей отображается счётчик общего количества событий и количества выбранных.
Примечание. Максимальное количество выбранных событий в окне «Выбор событий» - 30.
В нижней части окна расположены кнопки:

— «Добавить» – сохраняет выбранные события и закрывает окно;
— «Отменить» – закрывает окно без сохранения.

Для выполнения запроса необходимо выполнить следующие действия:

1) Выбрать агент и мандант.
2) Указать диапазон дат («Дата с» и «Дата по»).

3) Выбрать режим «Классы контроля» или «Код события».
4) Нажать кнопку *«Выполнить запрос»*.

Модальное окно «Результат запроса»

Модальное окно «Результат запроса» предназначено для просмотра результатов выполнения запроса по событиям аудита.

В окне «Результат запроса» отображаются и доступны следующие элементы управления (рис. 329):

- выбранный агент;
- поле «Поиск» – предназначено для поиска записей по пользователю;
- кнопка «Фильтр» – используется для фильтрации результатов запроса по доступным параметрам;
- таблица результатов.

Таблица результатов содержит следующие столбцы:

- «Дата создания»;
- «Мандант»;
- «Пользователь»;
- «Код события»;
- «Класс контроля»;
- «Критичность»;
- «Сообщение»;
- «Терминал»;
- «Сервер»;
- «Инстанция»;
- «Код транзакции»;
- «Программа».

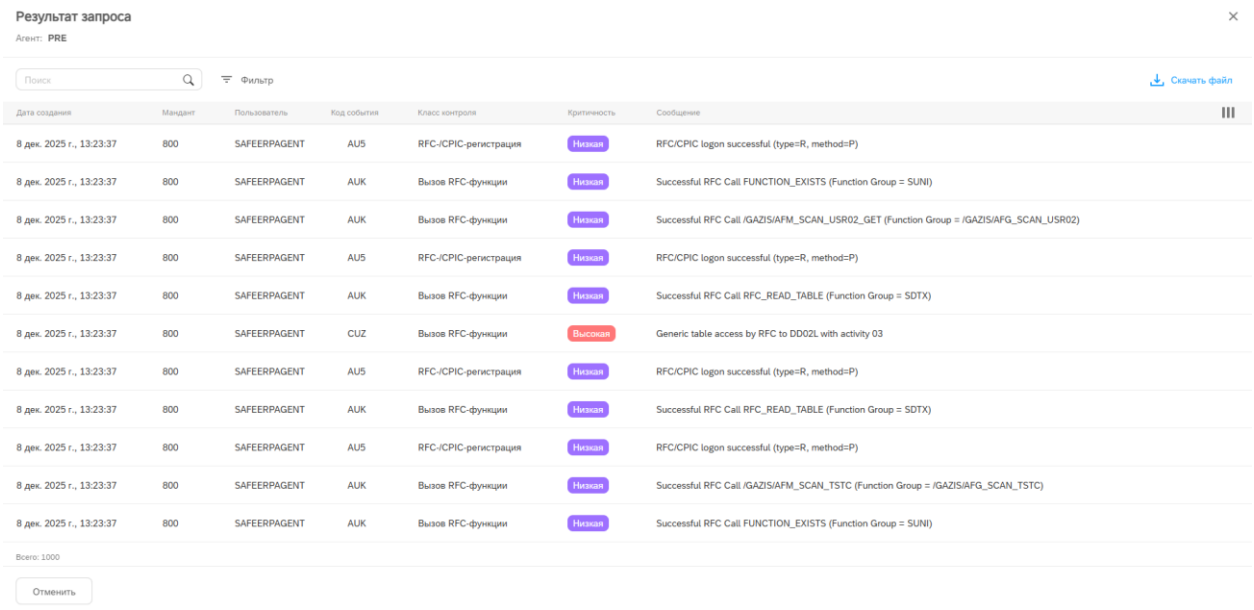


Рисунок 329 – Модальное окно «Результат запроса»

Под таблицей отображается счётчик количества найденных записей.
В окне «Результат запроса» доступна выгрузка отчета. Для выгрузки отчета необходимо нажать кнопку «Скачать файл».
В нижней части окна находится кнопка «Отменить», которая закрывает окно.
Примечание. При переключении на другой раздел или модуль параметры запроса и полученные результаты не сохраняются.

7.1.11 Модуль «Уведомления»

Модуль «Уведомление» предназначен для просмотра и событий, зарегистрированных в ПК «SafeERP Security Suite», а также для просмотра изменений стандартных профилей. Для функциональности ПК «SafeERP Security Suite» предусмотрена система уведомлений, состоящая из двух разделов:

- «Журнал событий» – информация о действиях пользователей в ПК «SafeERP Security Suite»;
- «Обновление профилей» – информация об изменениях проверочных профилей проектов.

Для просмотра информации системы уведомлений необходимо в верхнем правом углу основной рабочей области функциональности ПК «SafeERP Security Suite» нажать кнопку *«Уведомления»* (рис. 330).

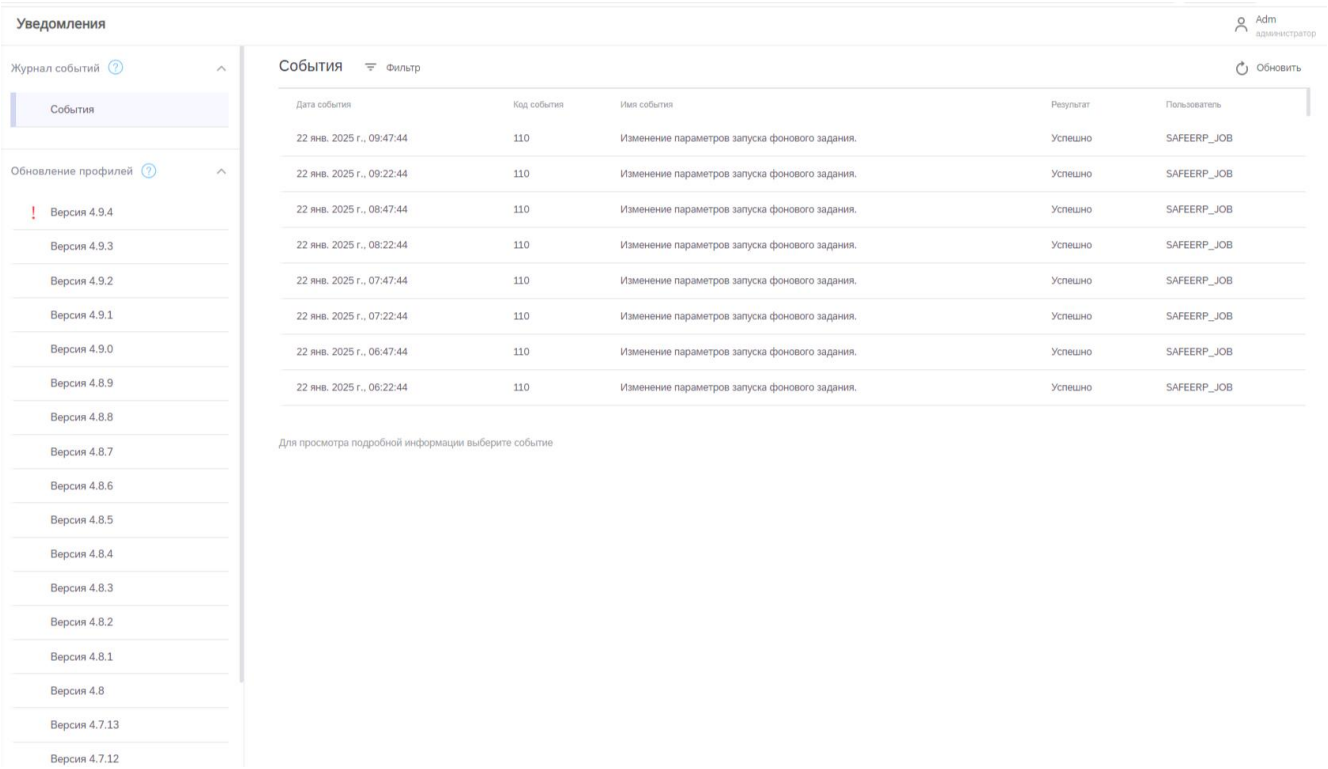


Рисунок 330 – Область уведомлений

7.1.11.1 Журнал событий

Журнал событий предназначен для отображения списка действий в ПК «SafeERP Security Suite», совершенных пользователями за определенное время.

Для просмотра событий необходимо нажать кнопку *«Уведомления»* (см. рис. 330), развернуть вкладку «Журнал событий» (рис. 331), нажать на раздел «События».

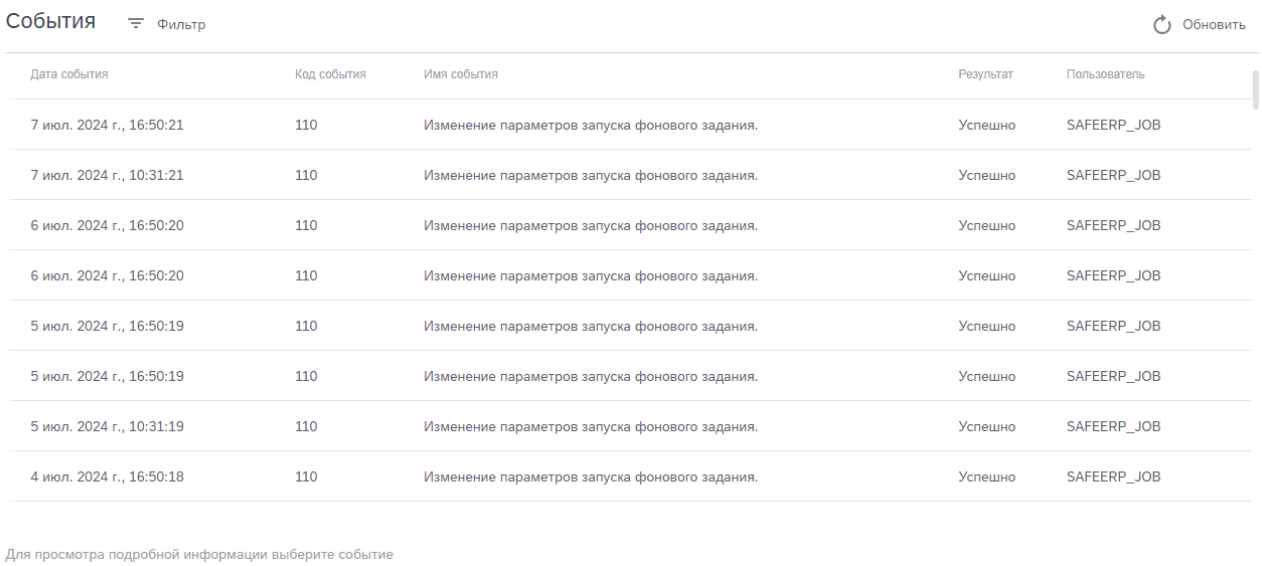


Рисунок 331 – Область «События»

Для просмотра события необходимо выбрать события в области «События» (рис. 331), нажать левой кнопкой мыши. Подробное описание события представлен на рис. 332.

Изменение параметров запуска фонового задания.

Код события:	110	Дата события:	7 июл. 2024 г., 16:50:21
Пользователь:	SAFEERP_JOB	Результат:	Успешно
Параметр 1:	SERVER		
Параметр 2:	Parameters of batch job: LAI_LOG_051MWn4a7joJY07rr9kclm has been changed		
Параметр 3:	Program: SAPCNVE		
Параметр 4:	SAFEERP_JOB		

Рисунок 332 – Подробное описание события

В разделе «Журнал событий» доступен фильтр по следующим параметрам (рис. 333):

- дата события с;
- дата события по;
- пользователь;
- код события;
- источник;
- ID проекта.

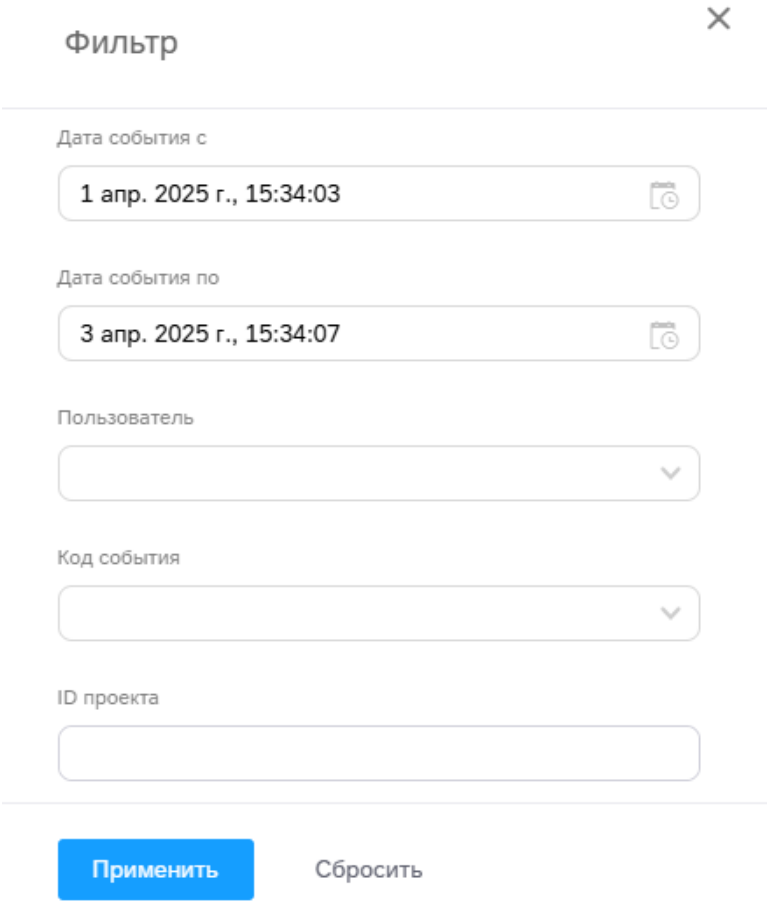


Рисунок 333 – Окно «Фильтр» в разделе «Журнал событий»

7.1.11.2 Обновление профилей

Раздел «Обновление профилей» предназначен для информирования пользователей о произошедших изменениях в проверочных профилях проектов между выпусками обновлений (релизов) ПК «SafeERP Security Suite».

Примечание. Ведение информации об изменениях в проверочных профилях осуществляется в ПК «SafeERP Security Suite», начиная с версии релиза 4.7.10.

Под изменениями в проверочных профилях имеются ввиду изменения количественного (добавление новых проверок/нот, удаление проверок из профилей) и качественного состава проверок в профилях (изменение в алгоритмах проверок, их описаниях и изменение в описании нот).

Для просмотра произошедших изменений в проверочных профилях проектов необходимо одним нажатием левой кнопки мыши активировать пункт «Обновление профилей» и строчку с соответствующим названием релиза. Справа развернется окно для просмотра данных (рис. 334).

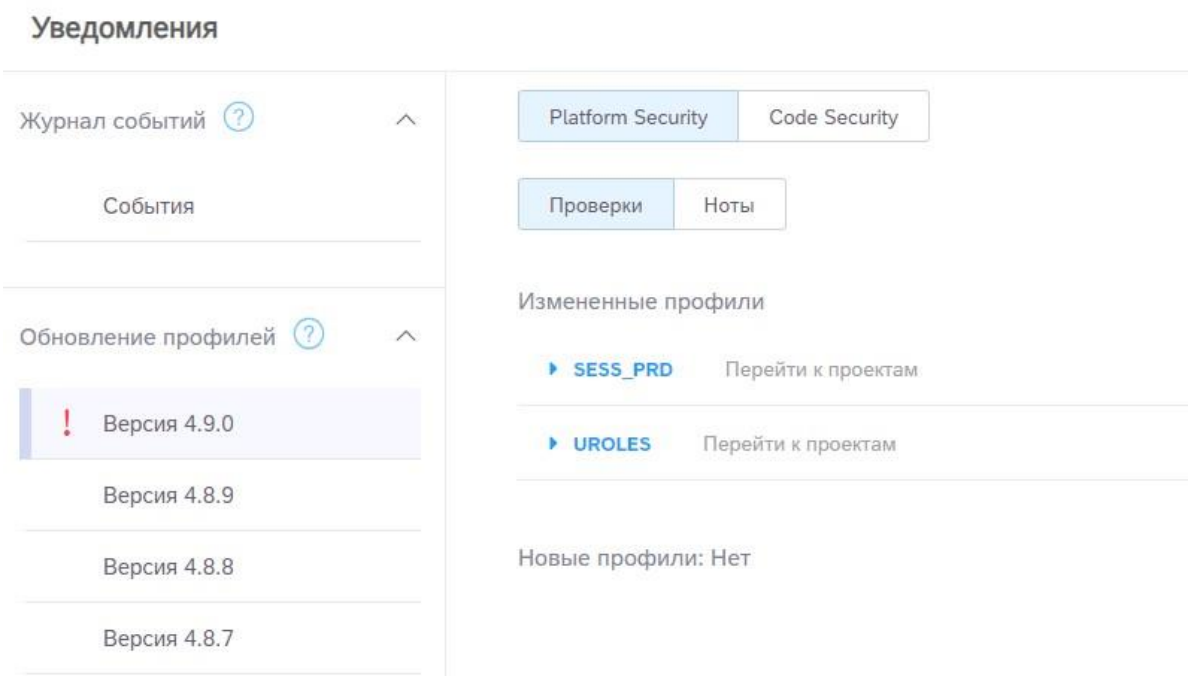


Рисунок 334 – Окно просмотра данных по обновлению профилей

Информация по изменениям проверочных профилей представлена отдельно для модулей «Сканер» и «Анализ кода».

7.1.11.2.1 Обновление профилей модуля «Сканер»

Информация по изменениям в проверочных профилях модуля «Сканер» представлена для проектов типа КН и нот.

Для просмотра данных по изменениям в проверочных профилях необходимо активировать соответствующие вкладки «Platform Security»/«Проверки» и «Platform Secuirty»/«Ноты». Для перехода к списку проверок измененного профиля необходимо нажать один раз левой кнопкой мыши кнопку списка ▸ рядом с его названием (рис. 335).

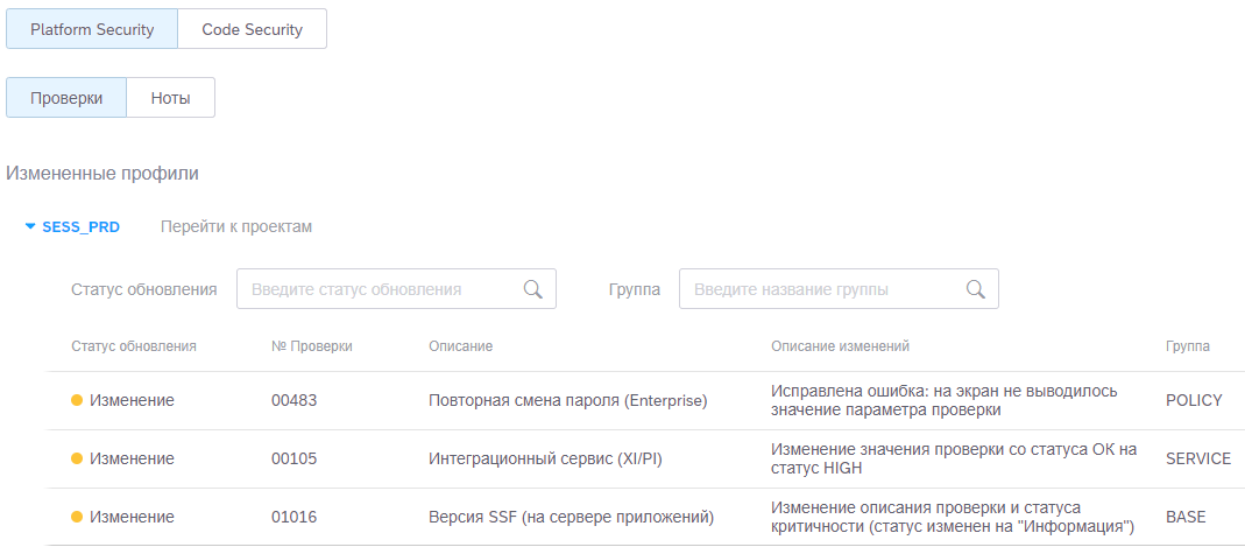


Рисунок 335 – Список проверок измененного профиля модуля «Сканер»

В таблице изменений представлен список проверок с их статусом обновления в профиле. Доступные статусы:

- добавление – новые проверки или добавленные в профиль проверки, в которых не было изменений;
- удаление – удаленные из профиля проверки;
- изменение – измененные проверки профиля.

Для работы с таблицей предусмотрена процедура фильтрации проверок по полям «Статус обновления» и «Группа». Чтобы начать процедуру фильтрации, необходимо задать символьную маску в соответствующей форме поиска и нажать кнопку *«Поиск»*. Для сброса введенных данных предусмотрена кнопка *«Сбросить»*.

Для каждого измененного профиля предусмотрено действие по переходу к списку проектов, в которых он содержится. Для просмотра списка проектов необходимо одним нажатием левой кнопки мыши нажать на действие «Перейти к проектам» (см. рис. 334) рядом с названием профиля. На экране появится отфильтрованный список проектов (рис. 336).

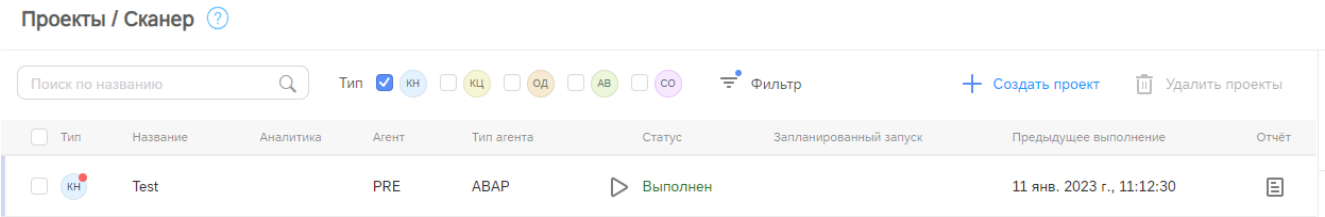


Рисунок 336 – Список проектов модуля «Сканер», содержащих измененный профиль

Проверить корректность фильтрации проектов доступно в окне содержимого проекта в поле «Профиль» (рис. 337).

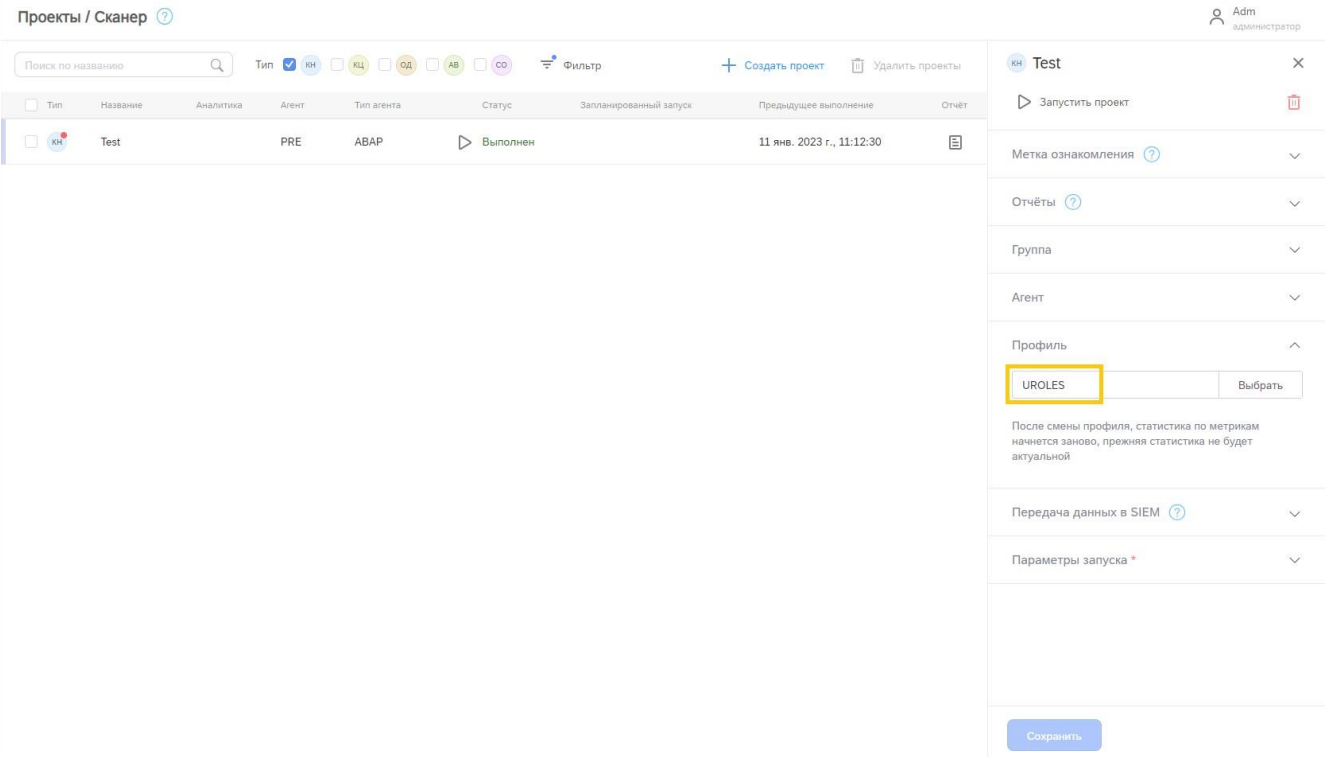


Рисунок 337 – Проверка корректности фильтрации проектов модуля «Сканер»

7.1.11.2.2 Обновление профилей модуля «Анализ кода»

Для просмотра данных по изменениям в проверочных профилях модуля «Анализ кода» необходимо активировать соответствующую вкладку «Code Security». Для перехода к списку проверок измененного профиля необходимо нажать один раз левой кнопкой мыши кнопку списка ▸ рядом с его названием (рис. 338).

Platform Security | Code Security

Измененные профили

10000 Перейти к проектам

Статус обновления: Введите статус обновления; Группа: Введите название группы

Статус обновления	№ Проверки	Описание	Описание изменений	Группа
Изменение	5	Неработающий AUTHORITY-CHECK	Ложное срабатывание проверки sy-subrc	Безопасность
Изменение	34	Отсутствие контроля полномочий до вызова транзакции	Ложное срабатывание проверки sy-subrc	Безопасность
Изменение	103	Контроль авторизации для балансовой единицы в отчётах FI	Исправление алгоритма работы сценария на BUKRS	Безопасность

10001 Перейти к проектам

Статус обновления: Введите статус обновления; Группа: Введите название группы

Статус обновления	№ Проверки	Описание	Описание изменений	Группа
Изменение	5	Неработающий AUTHORITY-CHECK	Ложное срабатывание проверки sy-subrc	Безопасность
Изменение	34	Отсутствие контроля полномочий до вызова транзакции	Ложное срабатывание проверки sy-subrc	Безопасность
	103	Контроль авторизации для балансовой единицы в отчётах FI	Исправление алгоритма работы сценария на BUKRS	Безопасность

Рисунок 338 – Список проверок измененного профиля модуля «Анализ кода»

В таблице изменений представлен список проверок с их статусом обновления в профиле. Доступные статусы:

- добавление – новые проверки или добавленные в профиль проверки, в которых не было изменений;
- удаление – удаленные из профиля проверки;
- изменение – измененные проверки профиля.

Для работы с таблицей предусмотрена процедура фильтрации проверок по полям «Статус обновления» и «Группа». Чтобы начать процедуру фильтрации, необходимо задать символьную маску в соответствующей форме поиска и нажать кнопку *«Поиск»*. Для сброса введенных данных предусмотрена кнопка *«Сбросить»*.

Для каждого измененного профиля предусмотрено действие по переходу к списку проектов, в которых он содержится. Для просмотра списка проектов необходимо нажать один раз на действие «Перейти к проектам» рядом с названием профиля одним нажатием левой кнопки мыши. На экране появится отфильтрованный список проектов (рис. 339).

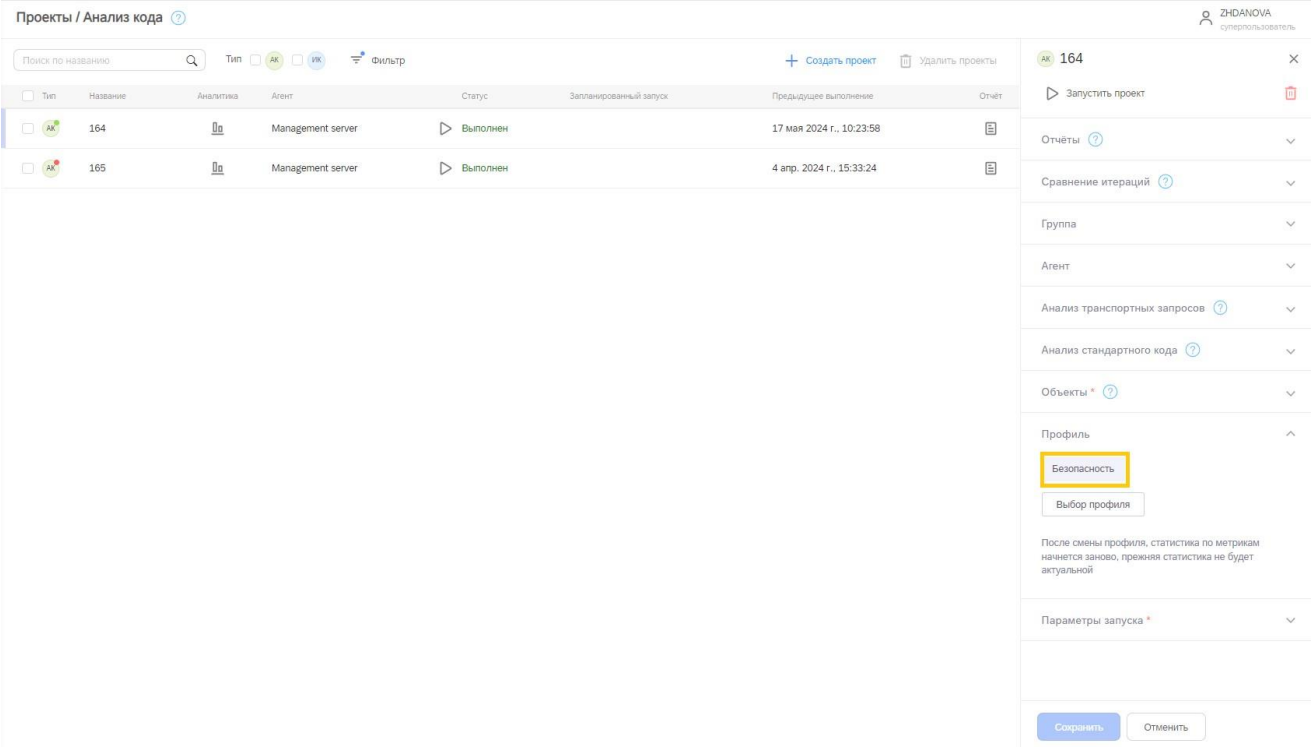


Рисунок 339 – Отфильтрованный список проектов модуля «Анализ кода», содержащих измененный профиль

Проверить корректность фильтрации проектов доступно в окне содержимого проекта в поле «Профиль» (рис. 340).

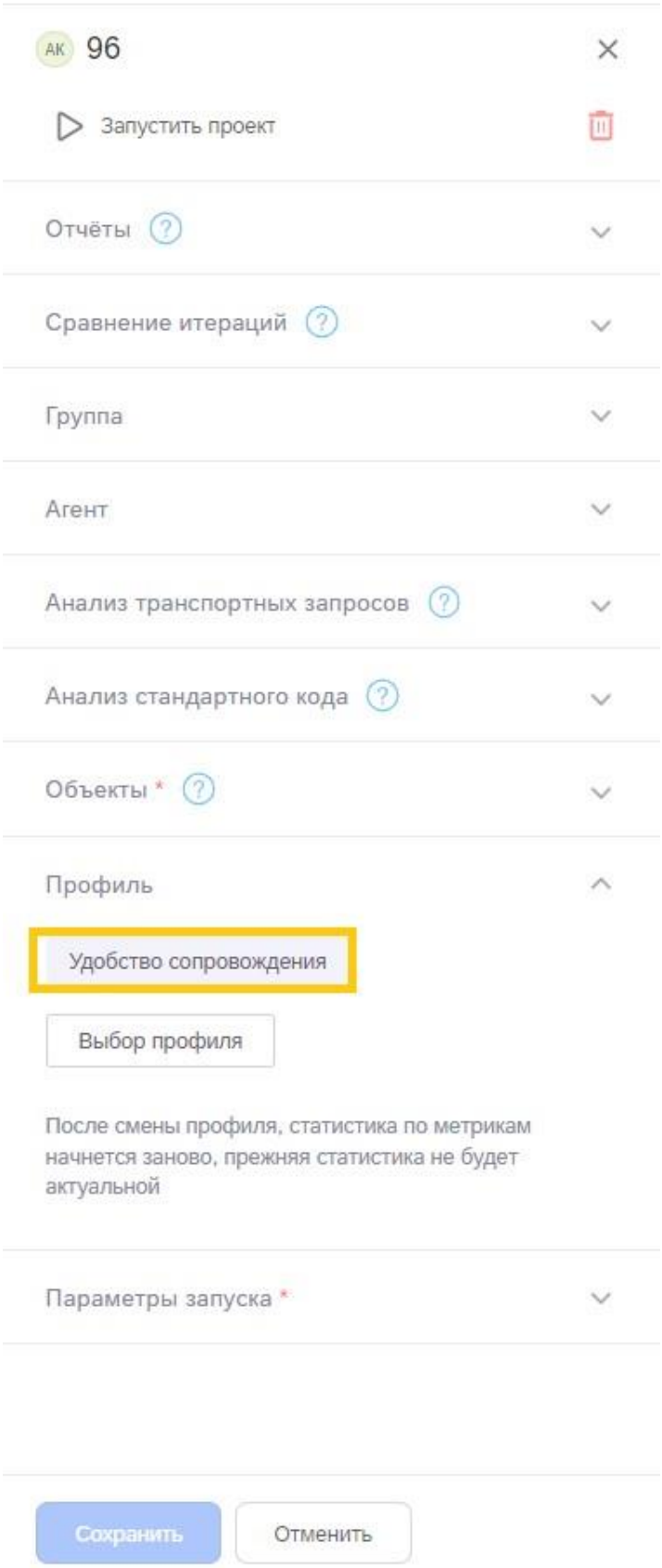


Рисунок 340 – Проверка корректности фильтрации проектов модуля

Приложение 1

Транзакция	Описание
/N/GAZIS/ANKEY_IDM	Ведение исключений сценариев контроля настроек (КН) для модуля интеграции с ANKEY_IDM. Подробное описание работы см. пункт 4.2.7
/N/GAZIS/CHECK_SAFEERP	Проверка веб-сервисов для корректной работы ПК «SafeERP Security Suite» в интерфейсе FIORI. Подробное описание работы см. в подразделе 4.16
/N/GAZIS/CHECK_NAMES	Проверка наименований объектов. Подробное описание см. в подразделе 4.24
/N/GAZIS/CONTROL_RFC	Настройка RFC соединений агентов. Подробное описание работы см. в подразделе 4.17
/N/GAZIS/COMPARE_ITERS	Сравнение двух итераций проекта типа АК. Подробное описание работы см. в подразделе 4.8
/N/GAZIS/COMPARE_ROLE	Сравнение полномочий двух ролей. Подробное описание работы см в подразделе 4.18
/N/GAZIS/SEPS_VULNERS	Инструмент фиксации результатов. Подробное описание см. в подразделе 4.19
/N/GAZIS/EXPORT_PRF	Экспорт профилей. Подробное описание см. в подразделе 4.9
/N/GAZIS/INTEGRAT_TT	Подключение таск-трекера. Подробное описание см. в подразделе 4.21
/N/GAZIS/HIERARCHY	Просмотр иерархии полномочий. Подробное описание см. в подразделе 4.24
/N/GAZIS/HISTORY	Просмотр истории изменений полномочий. Подробное описание см. в подразделе 4.23
/N/GAZIS/MAIL	Настройка почтовых уведомлений для пользователей ПК «SafeERP Security Suite». Подробное описание работы см. в подразделе 4.6
/N/GAZIS/MONJOBS	Мониторинг ФЗ ПК «SafeERP Security Suite». Параметры хэширования: изменения, обзор Подробное описание см. подразделе 4.7
/N/GAZIS/NEST_SCAN_SET /	Настройка вложенности сканирования. Подробное описание см. подразделе 4.14
/N/GAZIS/PSEUDOCOMMENT	Поиск псевдокомментариев в программном коде. Подробное описание см. подразделе 4.13
/N/GAZIS/SACT	Инструмент освобождения. Подробное описание см. в разделе 5

/N/GAZIS/SECS	Запуск ПК «SafeERP CS в SAP GUI. Подробное описание см. в подразделе 4.5
/N/GAZIS/SECS_VULNERS	Инструмент фиксации. Подробное описание см. в подразделе 4.22
/N/GAZIS/SEGA	Настройки ПК «SafeERP Security Suite». Подробное описание см. в подразделе 4.2
/N/GAZIS/SEPS	Запуск SafeERP Platform Security в SAP GUI Подробное описание см. в подразделе 4.4
/N/GAZIS/TRAN_AUTH	Поиск объектов полномочий. Подробное описание см. в подразделе 4.26

Приложение 2

Имя роли	Имя объекта	Имя поля	Значение поля
Z_SAFEERP_ADMINISTRATOR	S_TCODE	TCD	/GAZIS/CHECK_SAFEERP
Z_SAFEERP_ADMINISTRATOR	S_TCODE	TCD	/GAZIS/ACTIVATION
Z_SAFEERP_ADMINISTRATOR	S_TCODE	TCD	/GAZIS/NEWMAIL
Z_SAFEERP_ADMINISTRATOR	S_USER_GRP	CLASS	*
Z_SAFEERP_ADMINISTRATOR	S_USER_GRP	ACTVT	*
Z_SAFEERP_ADMINISTRATOR	S_TABU_NAM	ACTVT	02
Z_SAFEERP_ADMINISTRATOR	S_TABU_NAM	ACTVT	03
Z_SAFEERP_ADMINISTRATOR	S_TCODE	TCD	/GAZIS/NEST_SCAN_SET
Z_SAFEERP_ADMINISTRATOR	S_TABU_NAM	TABLE	/GAZIS/STCSSCS
Z_SAFEERP_ADMINISTRATOR	S_TCODE	TCD	/GAZIS/FLP
Z_SAFEERP_ADMINISTRATOR	ZSBS_ROLE	ACTVT	/GAZIS/SGWP_EXCLUDE_SRV
Z_SAFEERP_ADMINISTRATOR	S_RS_TR	ACTVT	03

Приложение 3

Список стандартных тегов для проектов типа АК (модуль «Анализ кода»):

- Динамический вызов;
- Запись данных;
- Файловый интерфейс;
- Личные данные;
- Шифрование данных;
- Незашифрованные данные;
- Удаление программы;
- Пароль;
- Лог-файлы;
- Команда WAIT;
- Индекс БД;
- Hard-code;
- Удаление файлов;
- Системные переменные;
- Комментарии;
- Псевдоавторизация;
- Загрузка файла с сервера;
- XML-преобразование;
- Инъекция команды ОС;
- Таблицы БД;
- Отправка документа;
- SCI;
- Условный оператор;
- Чтение программы;
- Пользовательская память;
- Буфер;
- COMMIT;
- Системные вызовы;
- Загрузка файла на сервер;
- Функции ядра;
- Мандант;
- Отчёт FI;
- Псевдокомментарий;
- SLIN;
- Устаревший метод;
- Объект полномочий;
- Строковые литералы;
- Хэш пароля;
- Ручной анализ;

- SQL-инъекция;
- Цикл;
- Запуск программы;
- Обработка ошибок;
- Функциональный модуль;
- Журнал изменения данных;
- Внутренние таблицы;
- Активное утверждение;
- ASSERT;
- Стандартные пользователи;
- Логическая БД;
- Debugger;
- ADBC;
- Отладочный код;
- Чтение данных;
- Синтаксическая ошибка;
- Макрос;
- Редактор кода;
- BREAK-POINT;
- WEB;
- Таблица диапазонов;
- FTP;
- Динамический запрос;
- EXEC SQL;
- Фоновое задание;
- База данных;
- Данные о системе;
- DYNPRO;
- Критичные команды ОС;
- Хэширование;
- ООП;
- Системная переменная;
- Обход каталога;
- SQL-инъекции;
- RFC-соединение;
- Проверка полномочий;
- Исходный код;
- AUTHORITY-CHECK;
- HTML;
- Инъекция данных;
- Командная инъекция;

- SQL-запрос;
- Регулярные выражения;
- Буфферные таблицы;
- HANA;
- Класс;
- Структура;
- Пользовательский ввод.