Платформа безопасной разработки «Шерлок»

Руководство по эксплуатации

Москва

2025

Содержание

1. Введение

1.1. Область применения

Платформа безопасной разработки «Шерлок» (далее — Система) предназначена для оптимизации процессов безопасной разработки за счет консолидации информации об ИБ-дефектах, получаемой из различных сканеров, и предоставления возможности централизованной одновременной работы с ними различными пользователями.

1.2. Краткое описание возможностей

Платформа безопасной разработки «Шерлок» обладает следующей функциональностью:

– централизованное управление сканерами (создание задач на сканирование, получение и обработка результатов задач на сканирование), позволяющими идентифицировать ИБ-дефекты (потенциальные уязвимости) в анализируемом программном обеспечении. Система поддерживает следующие типы сканеров:

- Static Application Security Testing (SAST);
- Software Composition Analysis (SCA);
- Container Image Analysis (Image Scan).

– консолидация информации, получаемой в результате реализации задач на сканирование, создаваемых различными сканерами программного обеспечения;

– сокращение информационного «шума» за счет дедупликации идентичных (повторяющихся) результатов, получаемых от различных сканеров;

– управление ИБ-дефектами (изменение статусов, уровня критичности, принятие рисков и т.д.), выявленными в анализируемом программном обеспечении;

– выстраивание процесса по управлению ИБ-дефектами за счет интеграции с системами управления задач (Issue Tracker);

– предоставление сводной информации о состоянии информационной безопасности анализируемого программного обеспечения.

2. Назначение и условия применения

2.1. Программные и аппаратные требования для доступа к Системе

Для работы с Системой пользователь должен обладать:

– автоматизированным рабочим местом. Минимальные требования к автоматизированному рабочему месту:

- процессор с тактовой частотой не менее 2000 МГц;
- оперативная память не менее 4096 Мбайт.

– веб-браузером. Рекомендуется использовать следующие веб-браузеры (версия — актуальная на декабрь 2024 года):

- Google Chrome;
- Microsoft Edge;
- Mozilla Firefox;
- Яндекс Браузер.

3. Подготовка к работе

Для начала работы с Системой необходимо обладать:

– ссылкой (уникальным идентификатором ресурса), по которой опубликована Система.

– логином и паролем для доступа к Системе.

Указанные данные должны быть получены в соответствии с процессами, принятыми в Компании, работником которой является пользователь Системы.

4. Описание операций

4.1. Вход в Систему

При переходе пользователя по ссылке, полученной в соответствии с описанием в Разделе 3, отображается форма для входа пользователя в Систему (Рисунок 1).

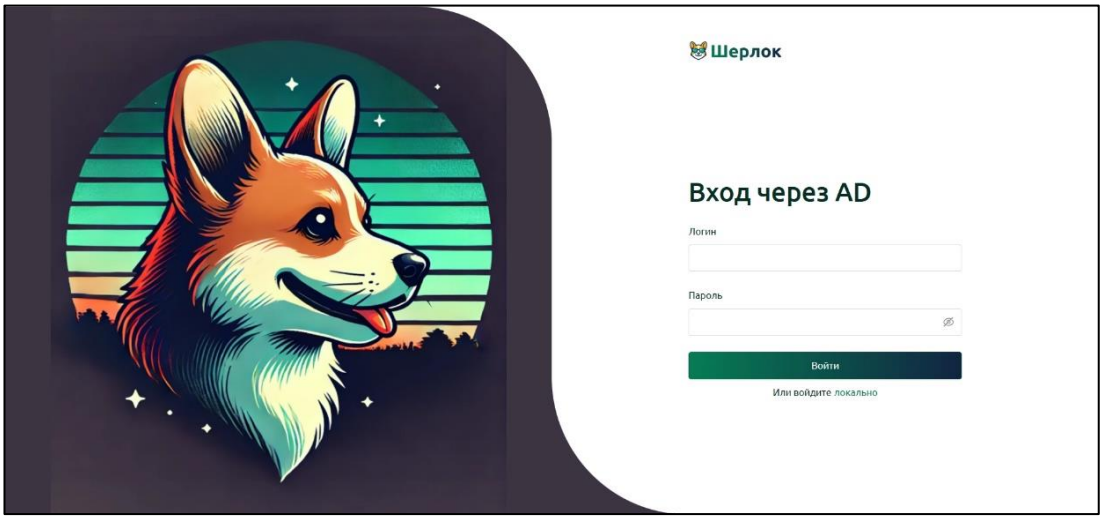


Рисунок 1 — Страница для входа через AD в Систему

Для успешного доступа необходимо ввести свои учетные данные: логин и пароль в соответствующие поля формы (Рисунок 2).

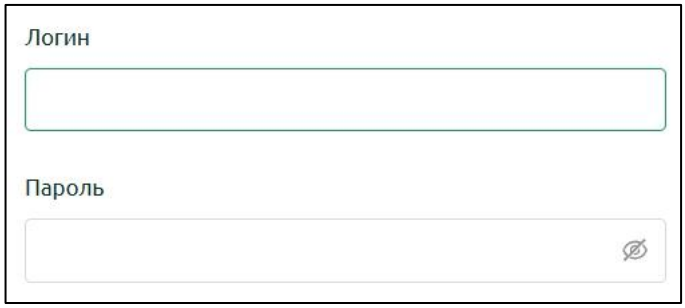
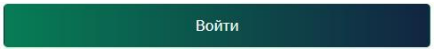


Рисунок 2 — Поля формы входа в Систему

В случае успешной авторизации пользователь будет перенаправлен на главную страницу Системы (Рисунок 5, Рисунок 6).

4.1.1. Вход через AD

По умолчанию при входе пользователю доступен вход через AD. При нажатии на кнопку Войти 

Система проверяет учетные данные. Для входа через AD у пользователя уже должна быть учетная запись в каталоге AD.

4.1.2. Вход локально

Для локального входа необходимо нажать на ссылку «локально» Или войдите локально под кнопкой Войти. На странице входа отобразится форма Локальный вход (Рисунок 3).

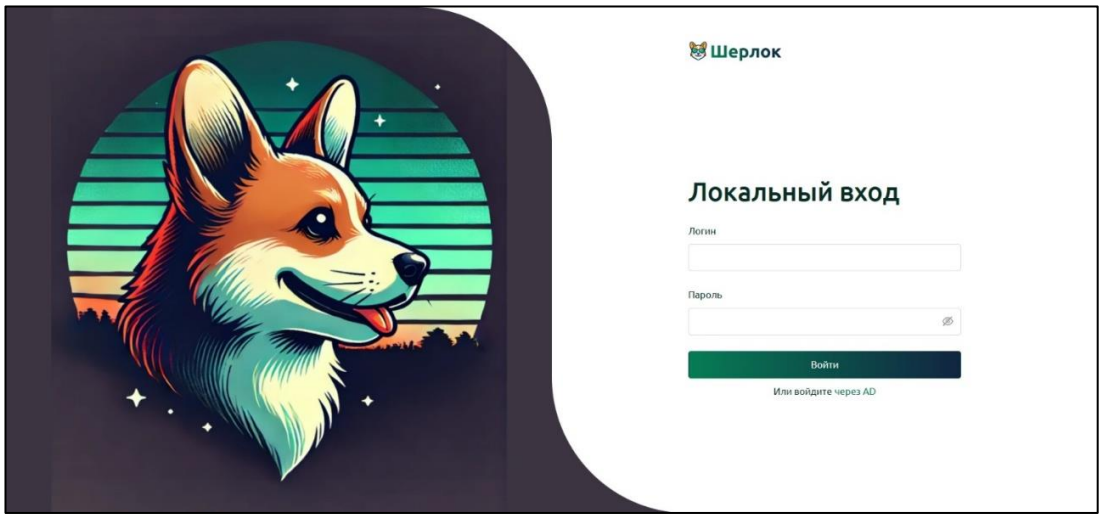


Рисунок 3 — Страница для локального входа в Систему

Аналогично входу через AD, для локального входа в Систему у пользователя уже должна быть учетная запись в Системе. После ввода данных, нажатия кнопки Войти и успешной идентификации и аутентификации пользователь будет перенаправлен на главную страницу Системы (Рисунок 5, Рисунок 6).

4.2. Выход из Системы

Для выхода из Системы необходимо:

1) Нажать на значок с логотипом пользователя в правом верхнем углу S;
2) В выпадающем меню выбрать пункт Выход Выход;
3) В открывшейся форме (Рисунок 4) нажать кнопку Да, выйти Да, выйти.

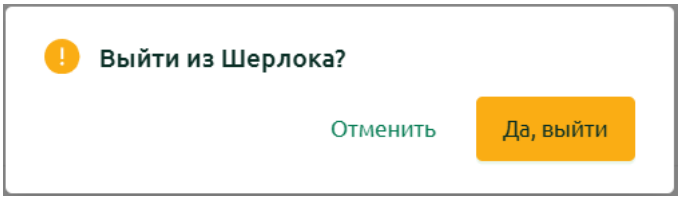


Рисунок 4 — Форма выхода из Системы

4.3. Главная страница

После успешной идентификации и аутентификации Система перенаправляет пользователя на главную страницу Системы (Рисунок 5, Рисунок 6), где доступны следующие элементы и функции в зависимости от прав доступа и наличия групп:

– **Навигационное меню**, предназначенное для перехода в разделы, доступные для роли пользователя. Подробное описание элементов навигационного меню в разделе 4.3.1.

– Форма **Группы**:

а) Если есть хотя бы одна группа, то доступны элементы (Рисунок 5):

– поле поиска групп и проектов;

– элементы фильтрации и сортировки;

– кнопка **Создать группу** + Создать группу (доступна при наличии прав доступа на создание групп на корневом уровне) или кнопка **Создать** + Создать (доступна при наличии прав доступа на создание групп и проектов на не корневом уровне) с пунктами выпадающего меню **Группу** Группу и **Проект** Проект.

– – Основная часть страницы.

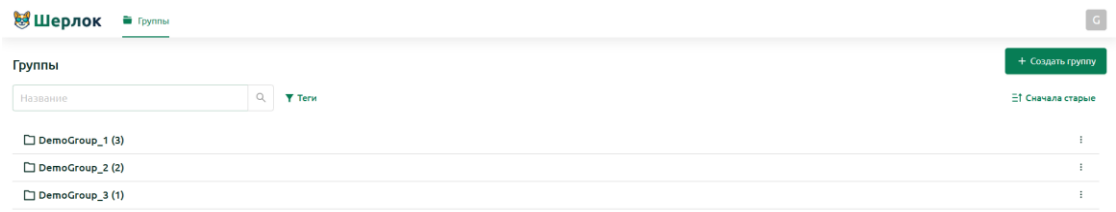


Рисунок 5 – Главная страница Системы с отображением групп

б) Если ни одной доступной для просмотра группы нет, то доступны элементы (Рисунок 6):

– информационное сообщение;

– кнопка **Создать группу** Создать группу (доступна при наличии прав доступа на создание групп на корневом уровне).

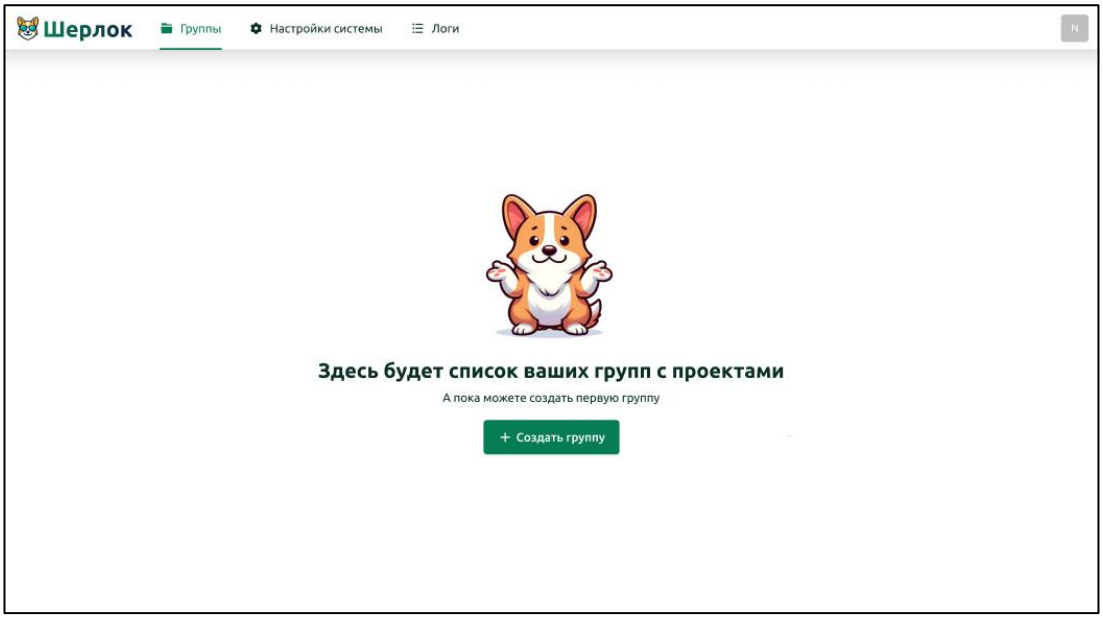


Рисунок 6 — Главная страница Системы без групп

Подробное описание элементов формы Группы в разделах 4.3.2 — 4.3.5.

Подробное описание операций, доступных пользователю на форме Группы, в разделе 4.6.

4.3.1. Навигационное меню

Состав отображаемых элементов навигационного меню может отличаться (отображаться или быть скрытым) в зависимости от настроек прав доступа пользователя. Описание ролей и прав доступа, предусмотренных для работы в Системе, представлено в подразделе 4.4.

В навигационном меню (Рисунок 7) расположены следующие элементы:

– **Логотип: кнопка для перехода на стартовую страницу** Шерлок**;**

– **Группы: ссылка для перехода в раздел Группы** Группы **;**

– **Настройки системы:** выпадающее меню с названиями разделов, предназначенных для настройки Системы Настройки системы ;

– **Логи:** ссылка для перехода на страницу просмотра логов Системы Логи .

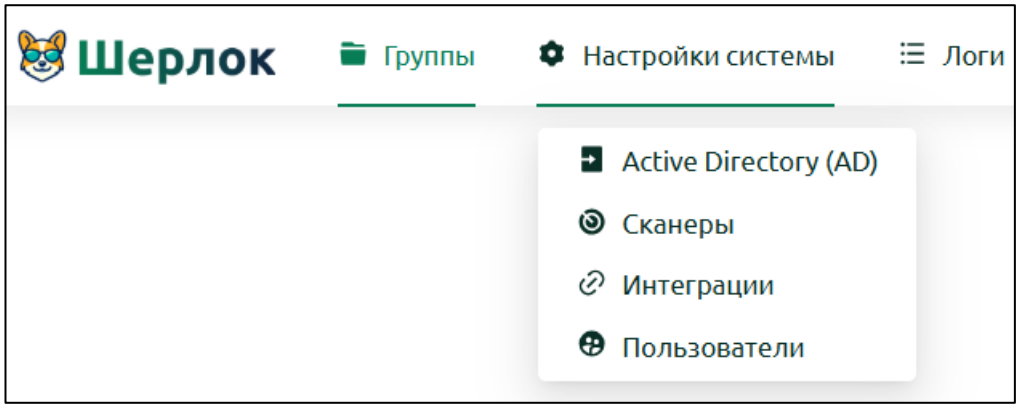


Рисунок 7 — Навигационное меню Системы

4.3.2. Поле поиска групп и проектов

Пользователь может добавлять поисковый запрос в поле для ввода текста (Рисунок 8). После нажатия на кнопку Enter или иконку Система отобразит список групп и проектов, соответствующих критериям поиска.

Рисунок 8 — Поле поиска групп и проектов

4.3.3. Элементы фильтрации и сортировки

Фильтрация списка групп и проектов возможна через выбор тегов Теги.

По умолчанию данные сортируются по дате создания. При необходимости пользователь может изменить поле сортировки.

4.3.4. Кнопка создания групп

При нажатии на кнопку Создать группу + Создать группу или на пункт меню Группу Группу кнопки Создать + Создать открывается форма Создание группы. Порядок работы с формой описан в разделе 4.6.1.2.

4.3.5. Основная часть страницы (при наличии групп)

Основная часть страницы состоит из следующих элементов:

– Список доступных пользователю групп и проектов, отсортированных по дате создания с количеством вложенных в группу элементов;

– Теги, относящиеся к соответствующей группе или проекту pipeline ;

– Меню действий ⋮ со списком операций над группой:

  – Изменить Изменить ;

  – Удалить Удалить .

4.4. Ролевая модель

В Системе предусмотрена двойная ролевая модель:

1) Роли пользователей на уровне Системы (далее — Системная роль). Эти роли позволяют осуществлять действия с Системой в соответствии с возможностями, определенными в ролевой модели (Таблица 1). Перечень Системных ролей:

  – Admin;

  – AppSec Manager System;

  – Member.

2) Роли пользователей на уровне Групп проектов (Групповая роль). Эти роли позволяют пользователям осуществлять действия с Группами проектов и их дочерними элементами (Группами, Проектами) в соответствии с возможностями, определенными в ролевой модели (Таблица 2). Перечень групповых ролей:

  – AppSec Manager (Group);

  – AppSec Specialist;

  – TeamLead;

  – Developer;

  – Product Owner.

Для корректной работы пользователя в Системе ему необходимо назначить роль как на уровне Системы, так и на уровне Группы.

Исключение составляет Системная роль Admin. Пользователям с данной системной ролью доступна вся функциональность Системы (как на уровне Системы, так и на уровне Групп).

Таблица 1 — Описание полномочий ролей на уровне Системы

№	Операция	Системная роль		
		Admin	**AppSec Manager System**	**Member**
Вход и выход из Системы				
1	Вход в Систему	X	X	X
2	Выход из Системы	X	X	X
Журналы (Эксплуатация)				
3	Просмотр системных событий (System Log)	X		
Настройки интеграций на уровне Системы				
4	Создание интеграций на уровне Системы	X		
5	Просмотр интеграций на уровне Системы	X		
6	Изменение интеграций на уровне Системы	X		
7	Удаление интеграций на уровне Системы	X		
Управление пользователями Системы				
8	Просмотр пользователей Системы	X		
9	Создание локального пользователя	X		
10	Удаление локального пользователя	X		
11	Просмотр списка групп для фильтрации пользователей Системы	X		
Управление группами				
12	Создание группы на корневом уровне	X	X	

Таблица 2 — Описание полномочий ролей на уровне Групп (* - предоставление данных только к тем Группам / Проектам, доступ к которым есть у пользователя)

№	Операция	Системная роль	Групповая роль				
		Admin	**AppSec Manager (Group)**	**AppSec Specialist**	**TeamLead**	**Developer**	**Product Owner**
Управление группами и проектами							

№	Операция	Системная роль	Групповая роль				
		Admin	**AppSec Manager (Group)**	**AppSec Specialist**	**TeamLead**	**Developer**	**Product Owner**
1	Просмотр списка групп и проектов	X	X*	X*	X*	X*	X*
2	Создание группы на любом уровне, кроме корневого	X	X*				
3	Изменение группы	X	X*				
4	Удаление группы	X	X*				
Управление тегами							
5	Просмотр тегов в фильтрах списка групп и проектов	X	X*	X*	X*	X*	X*
Управление пользователями группы							
6	Просмотр пользователей в группе	X	X*	X*	X*	X*	
7	Добавление пользователей в группу (с указанием роли)	X	X*		X* (только с ролью Developer)		
8	Изменение роли пользователя в группе	X	X*				
9	Удаление пользователя из группы	X	X*		X* (только с ролью Developer)		
Управление проектами (в списке групп и проектов)							
10	Создание проекта	X	X*				
11	Изменение проекта	X	X*				

№	Операция	Системная роль	Групповая роль				
		Admin	**AppSec Manager (Group)**	**AppSec Specialist**	**TeamLead**	**Developer**	**Product Owner**
12	Удаление проекта	X	X*				
Управление проектами (в карточке проекта)							
Просмотр ИБ-дефектов							
13	Получение общей информации по проекту	X	X*	X*	X*	X*	
14	Просмотр списка ИБ-дефектов с типом SAST	X	X*	X*	X*	X*	
15	Просмотр карточки ИБ-дефекта на вкладке «Общее»	X	X*	X*	X*	X*	
16	Просмотр карточки ИБ-дефекта на вкладке сканера	X	X*	X*	X*	X*	
17	Просмотр списка ИБ-дефектов с типом SCA	X	X*	X*	X*	X*	
18	Просмотр карточки ИБ-дефекта на вкладке «Общее»	X	X*	X*	X*	X*	
19	Просмотр карточки ИБ-дефекта на вкладке сканера	X	X*	X*	X*	X*	
20	Просмотр списка ИБ-дефектов с типом Image Scan	X	X*	X*	X*	X*	

№	Операция	Системная роль	Групповая роль				
		Admin	**AppSec Manager (Group)**	**AppSec Specialist**	**TeamLead**	**Developer**	**Product Owner**
21	Просмотр карточки ИБ-дефекта на вкладке «Общее»	X	X*	X*	X*	X*	
22	Просмотр карточки ИБ-дефекта на вкладке сканера	X	X*	X*	X*	X*	
Управление ИБ-дефектами							
23	Изменение статуса ИБ-дефекта	X	X*	X*			
24	Изменения уровня критичности ИБ-дефекта	X	X*	X*			
25	Создание комментариев к ИБ-дефекту	X	X*	X*	X*	X*	
26	Просмотр комментариев к ИБ-дефекту	X	X*	X*	X*	X*	
27	Изменение комментариев к ИБ-дефекту	X	X*	X* (только собственных)	X* (только собственных)	X* (только собственных)	
28	Удаление комментариев к ИБ-дефекту	X	X*	X* (только собственных)	X* (только собственных)	X* (только собственных)	
Управление исключениями							
29	Добавление ИБ-дефекта в исключения	X	X*	X*			
30	Просмотр исключенных ИБ-дефектов	X	X*	X*			
31	Удаление ИБ-дефекта	X	X*	X*			

№	Операция	Системная роль	Групповая роль				
		Admin	**AppSec Manager (Group)**	**AppSec Specialist**	**TeamLead**	**Developer**	**Product Owner**
	(отзыв) из исключений						
Управление задачами в Jira							
32	Создание задачи в Jira	X	X*	X*			
Управление сканированиями							
33	Создание задач сканирования Проекта (в ручном режиме)	X	X*	X*			
34	Просмотр истории сканирования	X	X*	X*			
35	Отмена задачи на сканирование	X	X*	X*			
36	Ручной импорт результатов сканирования в проект	X	X*	X*			
Управление аналитикой (дашборды)							
37	Просмотр дашборда	X	X*	X*	X*	X*	X*
Управление Security Gates							
38	Создание Security Gates	X	X*				
39	Просмотр настроек Security Gates	X	X*				
40	Изменение настроек Security Gates	X	X*				
41	Удаление Security Gates	X	X*				
Управление настройками проекта							

№	Операция	Системная роль	Групповая роль				
		Admin	AppSec Manager (Group)	AppSec Specialist	TeamLead	Developer	Product Owner
42	Просмотр настроек проекта	X	X*				
43	Добавление и изменение настроек проекта	X	X*				

4.5. *Описание операций администратора*

В данном разделе описаны функции, доступные только пользователям с системной ролью **Admin**.

4.5.1. Администрирование учетных записей пользователей Системы

Для администрирования учетных записей пользователей Системы администратору необходимо в навигационном меню в разделе **Настройки системы** Настройки системы выбрать пункт **Пользователи** Пользователи

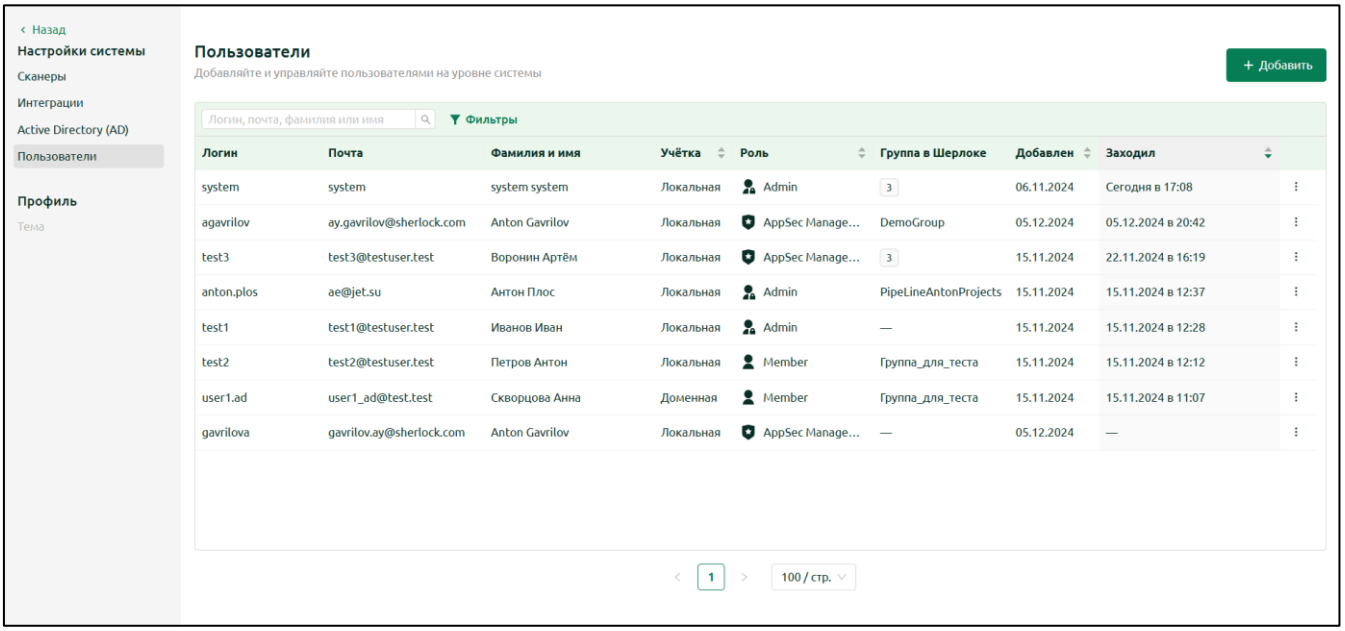


Рисунок 9 — Страница администрирования учетных записей пользователей

На странице **Пользователи** (Рисунок 9) доступны следующие функции:

– просмотр списка учетных записей всех пользователей Системы (локальных и доменных);

– создание учетной записи пользователя (только локальной);

– изменение учетной записи пользователя (локальной и доменной);

– блокирование учетной записи пользователя (только доменной);

– разблокирование учетной записи пользователя (только доменной);

– удаление учетной записи пользователя (только локальной).

4.5.1.1. Создание локальной учетной записи пользователя Системы

В разделе **Настройки системы** Настройки системы в подразделе **Пользователи** Пользователи доступно создание только локальных учетных записей.

Для создания новой локальной учетной записи необходимо:

1) В разделе **Пользователи** нажать кнопку **Добавить** + Добавить и выбрать в выпадающем меню пункт **Локально** Локально ;

2) В открывшейся форме **Добавление пользователя** (Рисунок 10) заполнить поля, описанные в таблице 3;

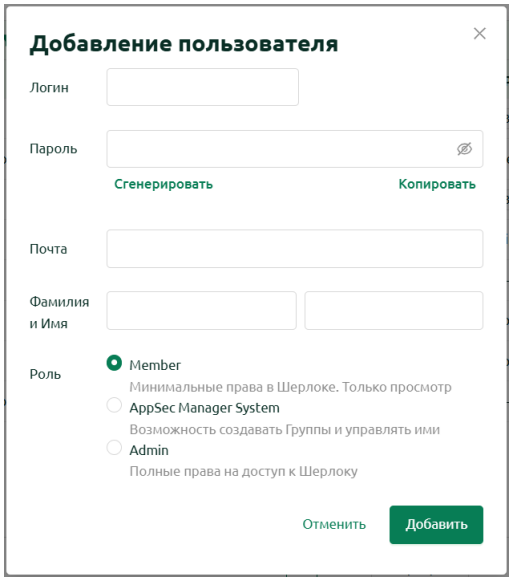


Рисунок 10 — Форма Добавление локального пользователя

3) Нажать кнопку **Добавить** 

. После этого Система сохранит новую локальную учетную запись.

Таблица 3 — Описание полей формы Добавление или изменение локального пользователя

№	Наименование поля	Описание поля	Обязательное для заполнения	Порядок заполнения
1	Логин	Логин пользователя для входа в Систему	Да	Заполнить вручную текстовое поле
1 2	Пароль	Пароль пользователя для входа в Систему	Да	Заполнить вручную текстовое поле
2 3	Почта	Адрес электронной почты пользователя	Да	Заполнить вручную текстовое поле
3 4	Фамилия и Имя	Фамилия и имя пользователя	Да	Заполнить вручную текстовое поле
4 5	Роль	Список системных ролей	Да	Выбрать системную роль в списке. Описание системных ролей представлено в подразделе

4.5.1.2. Изменение учетной записи пользователя Системы

Для изменения учетной записи необходимо:

1) В разделе **Пользователи** (Рисунок 9) найти учетную запись, для которой требуется изменение;

2) Нажать в меню действий ⋮ на пункт **Изменить** 

.

Если учетная запись локальная, то откроется форма **Изменение локального пользователя** (Рисунок 11) с полями, описанными в таблице 3;

3) В открывшейся форме **Изменение локального пользователя** отредактировать необходимые поля.

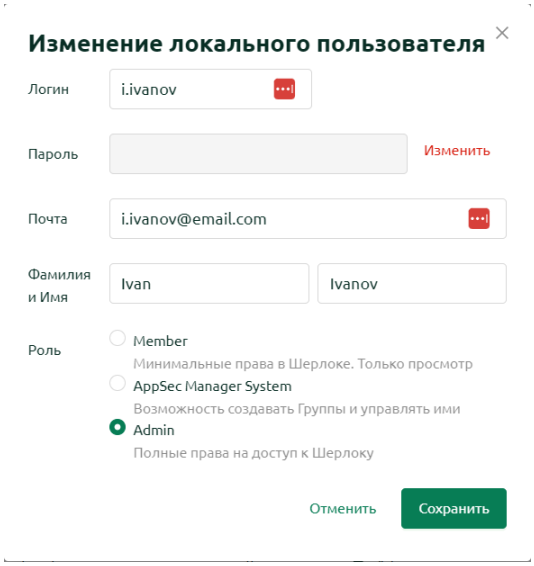
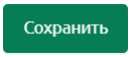


Рисунок 11 — Форма Изменение локального пользователя

4) Нажать кнопку **Сохранить** 

. После этого Система обновит локальную учетную запись.

Если учетная запись доменная, то откроется форма **Изменение роли пользователя из AD** (Рисунок 12) с полями, описанными в таблице 4;

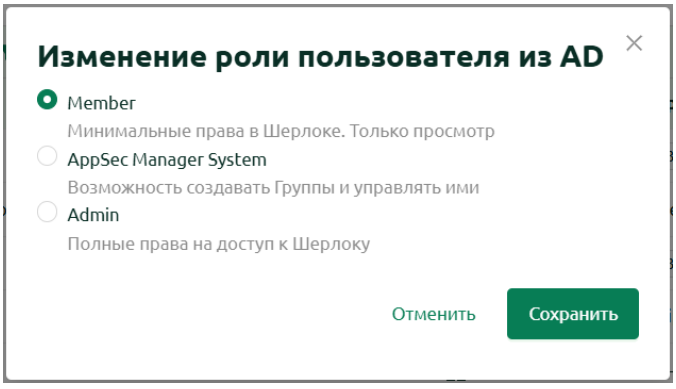


Рисунок 12 — Форма Изменение доменного пользователя

Таблица 4 — Описание полей формы Изменение роли пользователя из AD

№	Наименование поля	Описание поля	Обязательное для заполнения	Порядок заполнения
1	Роль	Список системных ролей	Да	Выбрать системную роль в списке. Описание системных ролей представлено в подразделе 4.4

5) В открывшейся форме **Изменение роли пользователя из AD** выбрать новую системную роль;

6) Нажать кнопку **Сохранить** Сохранить. После этого Система обновит доменную учетную запись.

4.5.1.3. Удаление локальной учетной записи пользователя Системы

Удалить можно только локальную учетную запись. После удаления пользователь не сможет войти в Систему под своими учетными данными.

Для удаления учетной записи необходимо:

1) В разделе **Пользователи (**Рисунок 9**)** найти учетную запись, которую требуется удалить;

2) Нажать в меню действий ⋮ на пункт **Удалить** Удалить;

3) В открывшейся форме **Удалить пользователя <Логин пользователя>?** (Рисунок 13) нажать на кнопку **Удалить** Удалить**.** После этого Система удалит учетную запись.

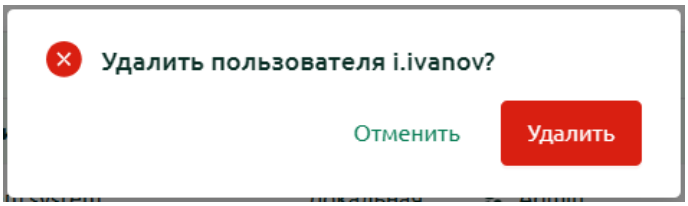


Рисунок 13 — Форма удаления локального пользователя

4.5.1.4. Блокировка доменной учетной записи

Заблокировать можно только доменную учетную запись. После блокировки пользователь не сможет войти в Систему под своими учетными данными.

Для блокировки доменной учетной записи необходимо:

1) В разделе **Пользователи (**Рисунок 9**)** найти доменную учетную запись, которую требуется заблокировать;

2) Нажать в меню действий ⋮ на пункт **Заблокировать** Заблокировать;

3) В открывшейся форме **Заблокировать пользователя <Логин пользователя>?** (Рисунок 14) нажать на кнопку **Заблокировать** Заблокировать**.** После этого Система заблокирует доменную учетную запись пользователя .

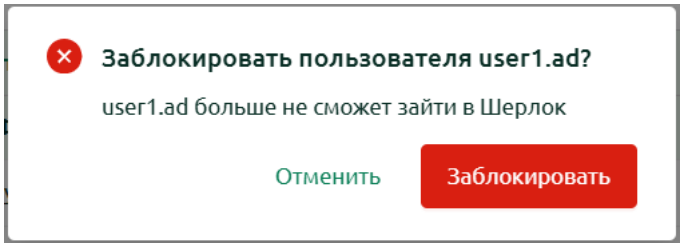


Рисунок 14 — Форма блокировки доменного пользователя

4.5.1.5. Разблокировка доменной учетной записи

Разблокировать можно только заблокированную доменную учетную запись. После разблокировки пользователь сможет войти в Систему под своими учетными данными.

Для разблокировки доменной учетной записи необходимо:

1) В разделе **Пользователи** (Рисунок 9) найти заблокированную доменную учетную запись, которую требуется разблокировать;

2) Нажать в меню действий ⋮ на пункт **Разблокировать** Разблокировать;

3) В открывшейся форме **Разблокировать пользователя <Логин пользователя>?** (Рисунок 15) нажать на кнопку **Разблокировать** Разблокировать. После этого Система разблокирует доменную учетную запись пользователя.

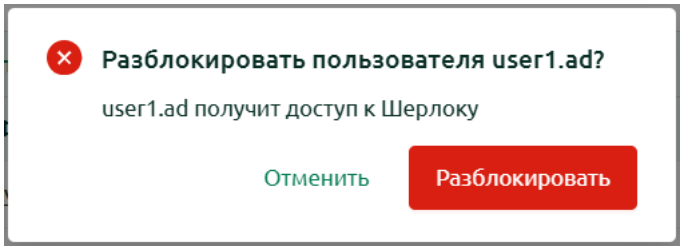


Рисунок 15 — Форма разблокировки доменного пользователя

4.5.2. Настройки интеграции Системы

Для создания задач в системе управления задачами требуется интеграция Системы с Jira. Для настройки интеграции Системы с Jira необходимо:

1) В меню **Настройки системы** Настройки системы в разделе **Интеграции** Интеграции нажать на кнопку **Подключить** Подключить, расположенную в блоке Jira (Рисунок 16);

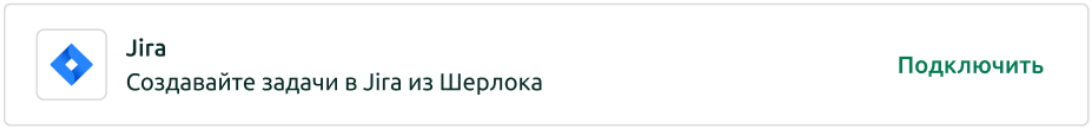


Рисунок 16 — Блок интеграции с Jira

2) В открывшейся форме **Подключение к Jira** (Рисунок 17) заполнить поля, описанные в таблице 5;

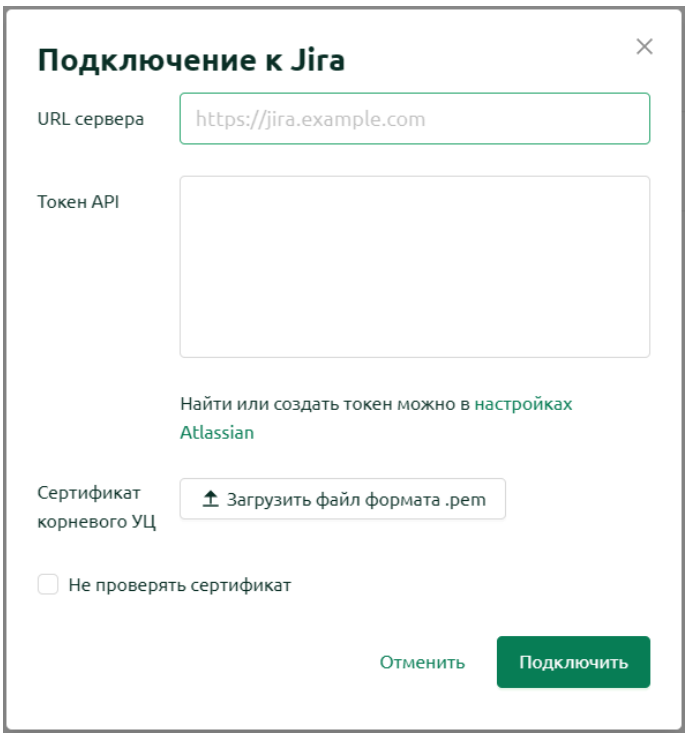


Рисунок 17 — Форма Подключение Системы к Jira

Таблица 5 — Описание полей формы Подключение к Jira

№	Наименование поля	Описание поля	Обязательное для заполнения	Порядок заполнения
1	URL сервера	Ссылка на сервер Jira	Да	Заполнить вручную текстовое поле
2	Токен API	Токен доступа к Jira	Да	Заполнить вручную текстовое поле
3	Сертификат корневого УЦ	Файл сертификата	Нет	Загрузить файл в формате PEM
4	Не проверять сертификат	Смена состояний чекбокса	Да	По умолчанию, установлено значение **Нет**, т.е. требуется

№	Наименование поля	Описание поля	Обязательное для заполнения	Порядок заполнения
				проверка сертификата Если проверка сертификата не требуется, то нужно переключить чекбокс в значение **Да**

3) Нажать на кнопку **Подключить** Подключить. После этого Система добавит интеграцию с Jira, что позволит создавать в ней задачи из интерфейса Системы;

4) Для изменения настроенного подключения с Jira необходимо нажать на кнопку **Изменить** , расположенную в блоке Jira. Настройки изменения подключения аналогичны тем, что используются и при его создании;

5) Для отключения интеграции с Jira необходимо нажать на кнопку Удалить ×, расположенную в блоке Jira;

6) В открывшейся форме **Отключить Jira?** (Рисунок 18) нажать на кнопку **Отключить** Отключить. После этого Система удалит интеграцию с Jira.

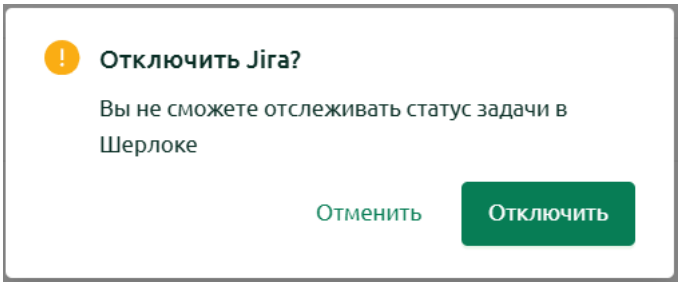


Рисунок 18 — Форма отключения интеграции с Jira

4.5.3. Настройки интеграции с AD

Для настройки интеграции с AD необходимо:

1) В меню **Настройки системы** Настройки системы в разделе **Active Directory (AD)** Active Directory (AD) заполнить форму **Настройка интеграции с Active Directory** (**Ошибка! Источник ссылки не найден.**), поля которой описаны в Таблица 6;

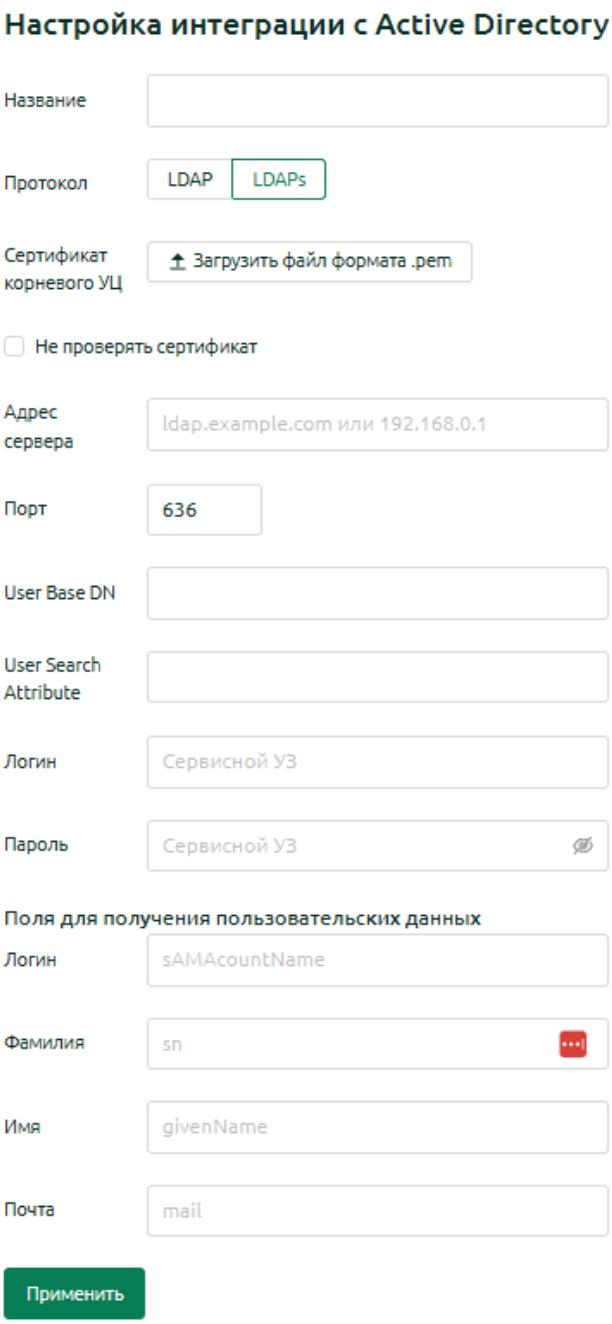


Рисунок 19 — Форма настройки интеграции с Active Directory (LDAPs)

Таблица 6 — Описание полей формы интеграции с Active Directory

№	Наименование поля	Описание поля	Обязательное для заполнения	Порядок заполнения
1	Название	Название интеграции	Да	Заполнить вручную текстовое поле
2	Протокол	Протокол передачи данных для подключения к AD	Да	Выбрать одну из двух вкладок

№	Наименование поля	Описание поля	Обязательное для заполнения	Порядок заполнения
3	Сертификат корневого УЦ (только LDAPs)	Файл сертификата	Нет	Загрузить файл в формате PEM
4	Не проверять сертификат (только LDAPs)	Смена состояний чекбокса	Нет	По умолчанию, установлено значение **Нет**, т.е. требуется проверка сертификата Если проверка сертификата не требуется, то нужно переключить чекбокс в значение **Да**
5	Адрес сервера	Адрес севера AD	Да	Заполнить вручную текстовое поле
6	Порт	Порт сервера AD	Да	Заполнить вручную текстовое поле
7	User Base DN	Атрибут для поиска отдельной записи LDAP	Да	Заполнить вручную текстовое поле
8	User Search Attribute	Атрибут для поиска и идентификации пользователей в AD	Да	Заполнить вручную текстовое поле
9	Логин	Логин пользователя для создания интеграции с AD	Да	Заполнить вручную текстовое поле
10	Пароль	Логин пользователя для создания интеграции с AD	Да	Заполнить вручную текстовое поле
11	Логин	Атрибут в AD, в котором хранится логин пользователя	Да	Заполнить вручную текстовое поле
12	Фамилия	Атрибут в AD, в котором хранится фамилия пользователя	Да	Заполнить вручную текстовое поле
13	Имя	Атрибут в AD, в котором хранится имя пользователя	Да	Заполнить вручную текстовое поле
14	Почта	Атрибут в AD, в котором хранится почта пользователя	Да	Заполнить вручную текстовое поле

2) Нажать на кнопку **Применить** 

. После этого Система сохранит интеграцию с Active Directory;

3) Для изменения настроенной интеграции с Active Directory необходимо отредактировать форму **Настройка интеграции с Active Directory** (**Ошибка! Источник ссылки не найден.**) и нажать на кнопку **Применить** Применить. Настройки изменения интеграции с AD аналогичны тем, что используются и при его создании.

4.5.4. Настройки интеграции со сканерами

Для настройки интеграции со сканерами необходимо:

1) В меню **Настройки системы** Настройки системы в разделе **Сканеры** Сканеры нажать на кнопку **Подключить** Подключить, расположенную в разделе **Можно подключить** в блоке подключаемого сканера (на примере сканера SAST PT Application Inspector) (Рисунок 20);

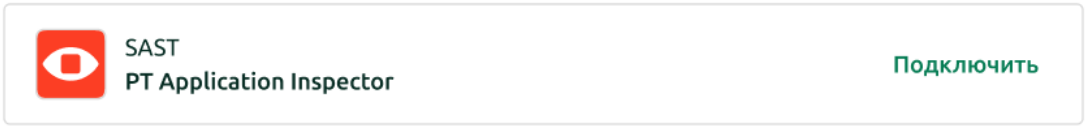


Рисунок 20 — Блок интеграции со сканером PT Application Inspector

2) В открывшейся форме **Подключение к <Название сканера>** (Рисунок 21) заполнить поля, описанные в Таблица 7;

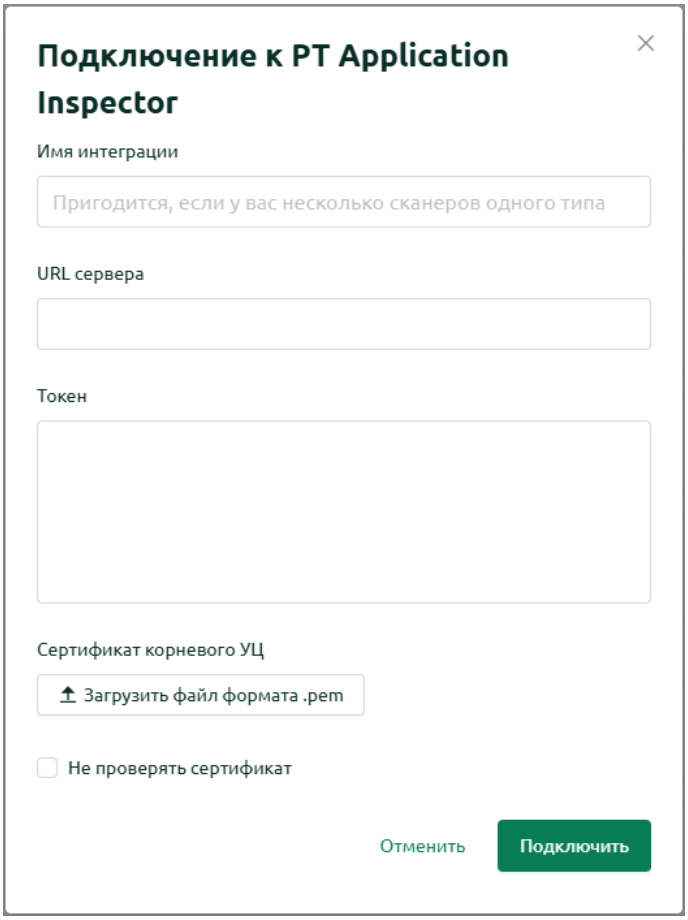


Рисунок 21 — Форма подключения сканера PT Application Inspector к Системе

Таблица 7 — Описание полей формы интеграции со сканером PT Application Inspector

№	Наименование поля	Описание поля	Обязательное для заполнения	Порядок заполнения
1	Имя интеграции	Имя интеграции со сканером	Да	Заполнить вручную текстовое поле
2	URL сервера	Ссылка на сервер сканера	Да	Заполнить вручную текстовое поле
3	Токен	Токен доступа к сканеру	Да	Заполнить вручную текстовое поле
4	Сертификат корневого УЦ	Файл сертификата	Нет	Загрузить файл в формате PEM
5	Не проверять сертификат	Смена состояний чекбокса	Да	По умолчанию, установлено значение **Нет**, т.е. требуется проверка сертификата Если проверка сертификата не требуется, то нужно переключить чекбокс в значение **Да**

№	Наименование поля	Описание поля	Обязательное для заполнения	Порядок заполнения

3) Нажать на кнопку **Подключить** Подключить. После этого Система добавит интеграцию с сканером, что позволит запускать сканирование проекта из интерфейса Системы;

4) Для изменения настроенного подключения со сканером необходимо нажать на кнопку **Изменить** , расположенную в разделе **Подключенные** в блоке подключенного сканера. Настройки изменения подключения аналогичны тем, что используются и при его создании;

5) Для отключения интеграции со сканером необходимо нажать на кнопку Удалить ×, расположенную в разделе **Подключенные** в блоке подключенного сканера;

6) В открывшейся форме **Отключить <Название сканера>?** (Рисунок 22) нажать на кнопку **Отключить** Отключить**.** После этого Система удалит интеграцию со сканером.

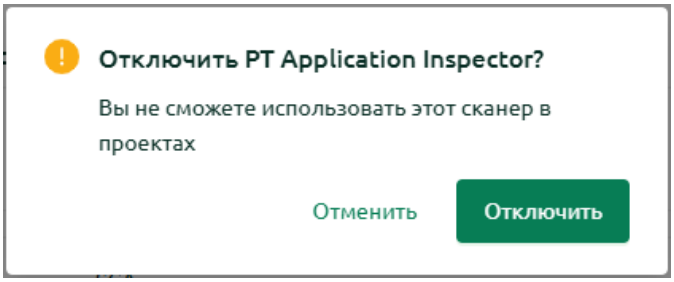


Рисунок 22 — Форма отключения интеграции со сканером PT Application Inspector

4.6. Описание операций в разделе Группы

В разделе пользователю доступны функции:

- управление группами и проектами (Раздел 4.6.1);
- работа в карточке проекта (Раздел 4.6.2).

4.6.1. Работа со списком групп и проектов

Пользователю доступны следующие функции:

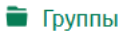
- просмотр списка групп и проектов (Раздел 4.6.1.1);
- создание группы (Раздел 4.6.1.2);
- изменение группы (Раздел 4.6.1.3);
- удаление группы (Раздел 4.6.1.4);
- создание проекта (Раздел 4.6.1.5);

– изменение проекта (Раздел 4.6.1.6);

– удаление проекта (Раздел 4.6.1.7);

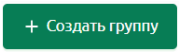
– просмотр и настройка прав доступа к группе и вложенным проектам (Разделы 4.6.1.8 — 4.6.1.14).

4.6.1.1. Просмотр списка групп и проектов

Для просмотра списка групп и проектов необходимо в навигационном меню перейти в раздел **Группы**  (Рисунок 5, Рисунок 6).

Группы в Системе представлены в виде вложенного списка. На каждом уровне иерархии Система отображает количество вложенных в группу элементов. Вложенными элементами группы могут быть группы и проекты.

При переходе пользователя в группу возможно отображение в одном из двух вариантов:

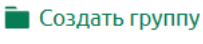
– еслив группе нет вложенных групп или проектов, то пользователю отображается страница с кнопкой **Создать группу**  (Рисунок 6);

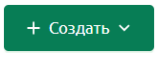
– если в группе есть вложенные группы или проекты, то пользователю отображается список вложенных групп и проектов, к которым у него есть права доступа на просмотр (Рисунок 5).

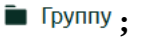
4.6.1.2. Создание группы

Группы можно создавать как на корневом уровне, так и на любом дочернем уровне вложенности, с учетом ограничения — не более 20 уровней вложенности.

Для создания группы необходимо:

1) Если в группе нет вложенных групп или проектов, то нажать кнопку **Создать группу**  ;

2) Если в группе есть вложенные группы или проекты, то нажать на кнопку **Создать**  ;

3) В выпадающем меню выбрать пункт **Группу**  ;

4) В открывшейся форме **Создание группы** (Рисунок 23) заполнить поля, описанные в таблице 8;

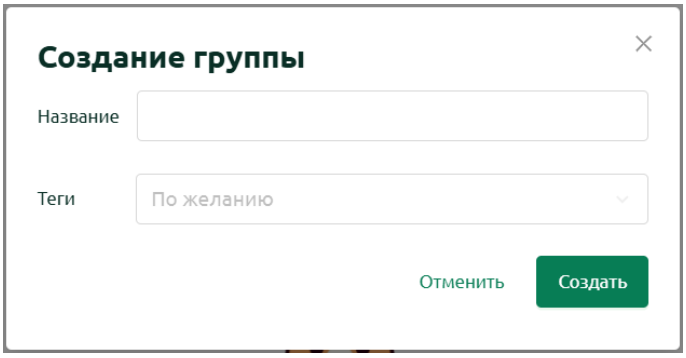


Рисунок 23 — Форма Создание группы

Таблица 8 — Описание полей формы Создание группы

№	Наименование поля	Описание поля	Обязательное для заполнения	Порядок заполнения
1	Название	Название группы	Да	Заполнить вручную текстовое поле
2	Теги	Отличительная метка группы	Нет	Заполнить вручную текстовое поле или выбрать из выпадающего списка название тега

5) Нажать на кнопку **Создать** Создать. После этого Система добавит новый проект.

4.6.1.3. Изменение группы

Для изменения группы необходимо:

1) В разделе Группы Группы (Рисунок 5) найти группу, которую требуется изменить;

2) Нажать в меню действий ⋮ на пункт **Изменить** Изменить;

3) В открывшейся форме **Изменение группы** (Рисунок 24) отредактировать необходимые поля;

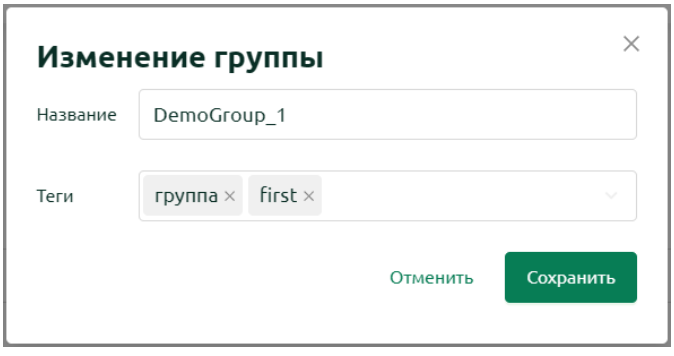
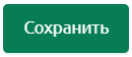


Рисунок 24 — Форма Изменение группы

4) Нажать на кнопку **Сохранить** 

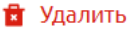
. После этого Система обновит данные группы.

4.6.1.4. Удаление группы

Для удаления группы необходимо:

1) В разделе **Группы** 

(Рисунок 5) найти группу, которую требуется удалить;

2) Нажать в меню действий на пункт **Удалить** 

;

3) Далее возможны следующие варианты поведения Системы:

а) Если в группе есть вложенные элементы, то отобразится форма **Сначала удалите содержимое группы** (Рисунок 25)**.** В данном случае для удаления группы необходимо предварительно удалить все ее вложенные элементы;

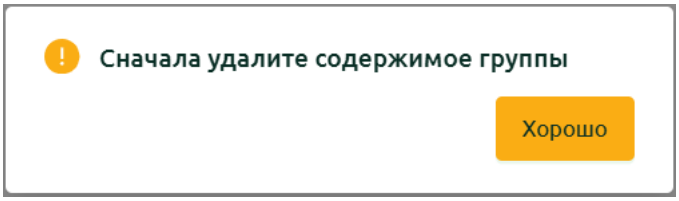
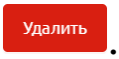


Рисунок 25 — Форма-предупреждение о наличии вложенных групп или проектов в удаляемой группе

б) Если в группе нет вложенных элементов, то отобразится форма **Удалить группу <Название группы>?** (Рисунок 26);

4) В открывшейся форме **Удалить группу <Название группы>?** (Рисунок 26) нажать на кнопку **Удалить** 

. После этого Система удалит группу.

Рисунок 26 — Форма удаления группы

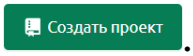
4.6.1.5. Создание проекта

Проект можно создать только внутри группы. Для создания проекта необходимо:

1) Перейти в ранее созданную группу;

2) Возможны следующие варианты:

а) Если в группе нет созданных групп или проектов:

– нажать на кнопку **Создать проект** 

.

В открывшейся форме Создание проекта **(Рисунок 27) заполнить поля, описанные в Таблице 9;**

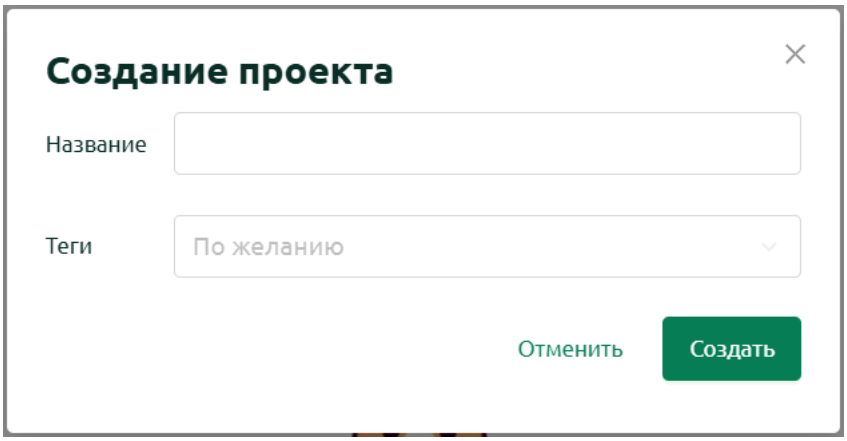


Рисунок 27 — Форма Создание проекта

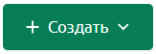
Таблица 9 — Описание полей формы Создание проекта

№	Наименование поля	Описание поля	Обязательное для заполнения	Порядок заполнения
1	Название	Название проекта	Да	Заполнить вручную текстовое поле
2	Теги	Отличительная метка проекта	Нет	Заполнить вручную текстовое поле или выбрать из выпадающего списка название тега

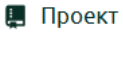
– нажать на кнопку **Создать** 

. После этого Система добавит новый проект.

б) Если в группе есть созданные группы или проекты:

– нажать на кнопку **Создать** 

;

– в выпадающем меню выбрать пункт **Проект** 

.

В открывшейся форме Создание проекта **(Рисунок 27) заполнить поля, описанные в таблице 9;**

– нажать на кнопку **Создать** 

. После этого Система добавит новый проект.

4.6.1.6. Изменение проекта

При необходимости внесения изменений в проект (как элемента группы) пользователю необходимо:

1) В разделе **Группы** Группы (Рисунок 5) найти проект, который требуется изменить;

2) Нажать в меню действий ⋮ на пункт **Изменить** Изменить;

3) В открывшейся форме **Изменение проекта** (Рисунок 28) отредактировать необходимые поля;

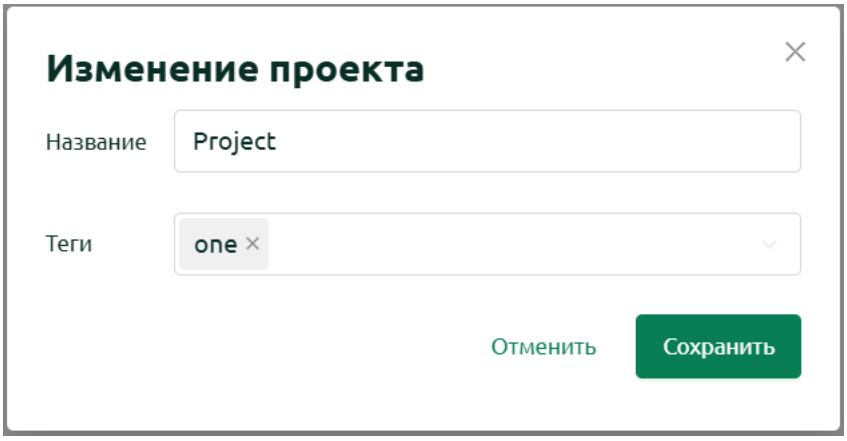


Рисунок 28 — Форма Изменение проекта

4) Нажать на кнопку **Сохранить** Сохранить. После этого Система обновит данные проекта.

4.6.1.7. Удаление проекта

Для удаления проекта необходимо:

1) В разделе Группы Группы (Рисунок 5) найти проект, который требуется удалить;

2) Нажать в меню действий ⋮ на пункт **Удалить** Удалить;

3) В открывшейся форме **Удалить проект <Название проекта>?** (Рисунок 29) ввести в поле для ввода слово «Подтверждаю»;

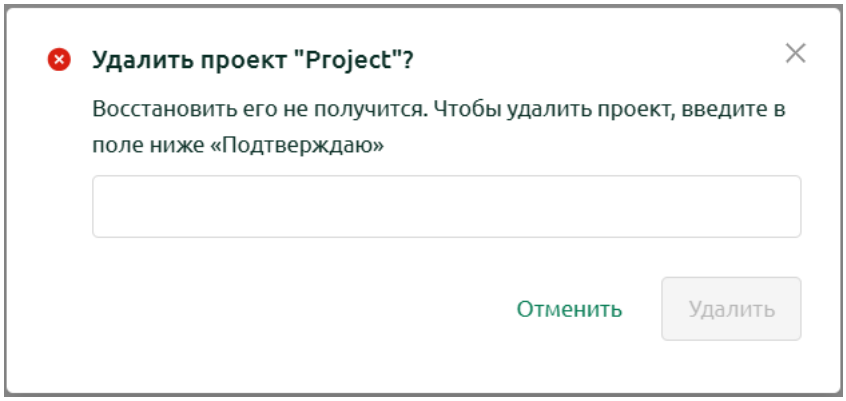


Рисунок 29 — Форма удаления проекта

4) Нажать на кнопку **Удалить** Удалить. После этого Система удалит проект.

4.6.1.8. Просмотр пользователей группы

Для просмотра пользователей группы необходимо:

1) На странице **<Название группы>** (Рисунок 30) нажать на кнопку **Пользователи** Пользователи;

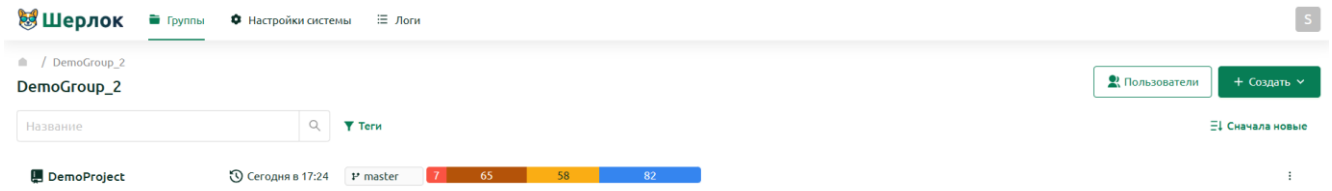


Рисунок 30 — Страница проекта

2) Система отобразит во вкладке **Пользователи** Пользователи (3) таблицу (Рисунок 31) с полем поиска, кнопкой фильтра и колонками, описанными в Таблица 10.

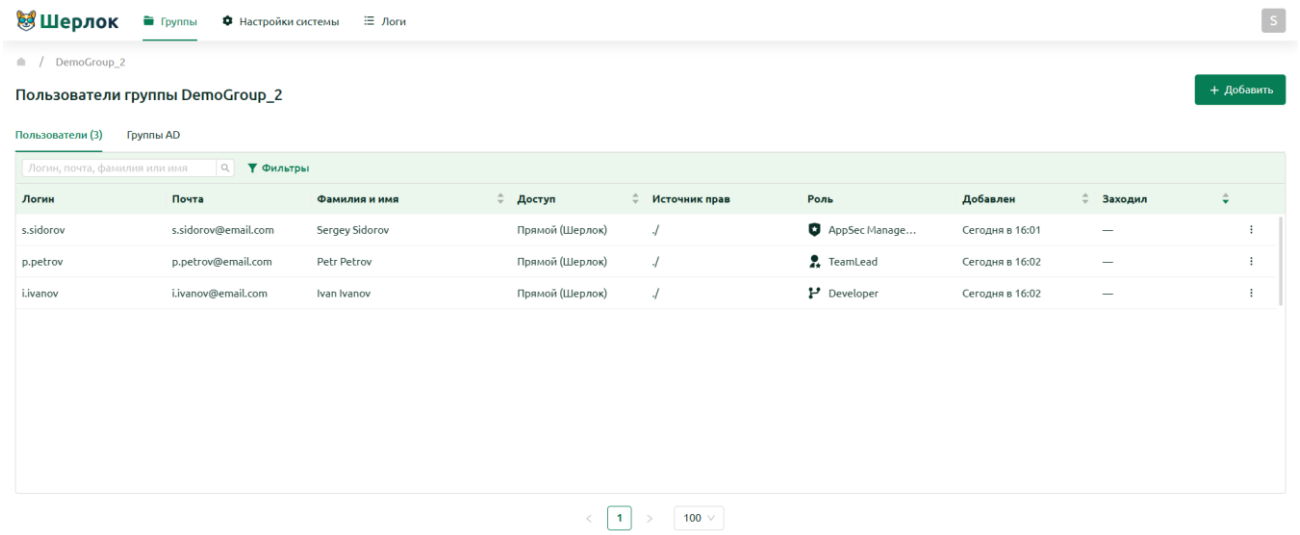


Рисунок 31 — Пользователи группы

Таблица 10 — Колонки таблицы пользователей группы

№	Наименование поля	Описание поля
1	Логин	Логин пользователя в Системе
2	Почта	Email пользователя в Системе
3	Фамилия и имя	Фамилия и имя пользователя в Системе
4	Доступ	Доступен только один из возможных значений: – Прямой (Шерлок); – Прямой (AD); – Наследование
5	Источник прав	Путь до корневой группы, в которую был впервые добавлен пользователь
6	Роль	Возможна только одна из возможных групповых ролей: – AppSec Manager (Group); – AppSec AppSec Specialist; – TeamLead; – Developer; – Product Owner
7	Добавлен	Дата добавления пользователя в группу
8	Заходил	Дата последнего входа в Систему
9	Меню действий	Функционал меню: - Изменить роль пользователя (Раздел 4.6.1.10). - Удалить пользователя из группы (Раздел 4.6.1.11)

4.6.1.9. Добавление пользователя в группу (локально)

Для добавления пользователя в группу (локально) необходимо:

1) В разделе **Пользователи группы <Название группы>** (Рисунок 32) нажать на кнопку **Добавить** + Добавить;

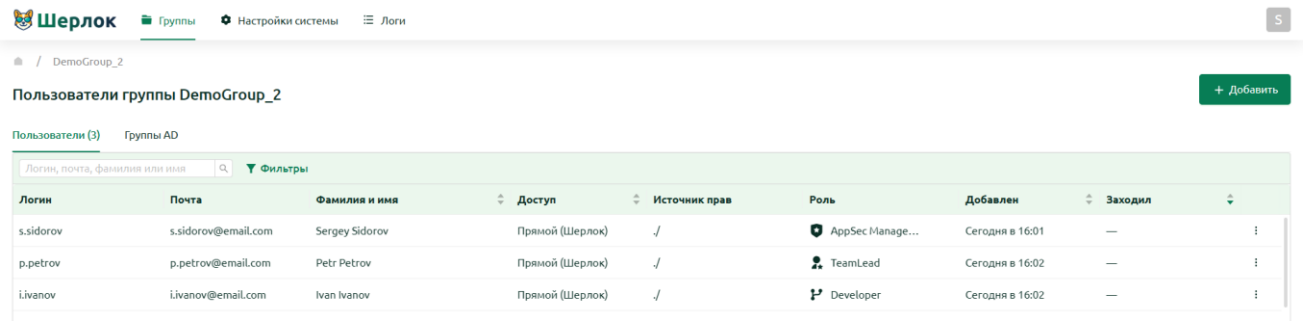


Рисунок 32 — Таблица пользователей группы

2) В выпадающем меню нажать на пункт **Локально** Локально **;**

3) В открывшейся форме **Добавление пользователя** (Рисунок 33) заполнить поля, описанные в Таблица 11;

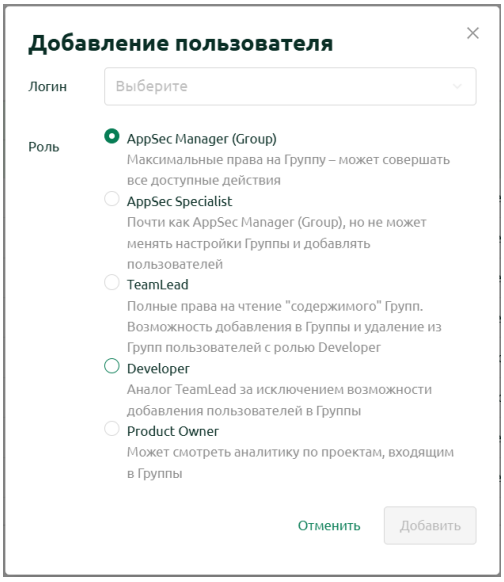


Рисунок 33 — Форма Добавление пользователя (локально)

Таблица 11 — Описание полей формы Добавление пользователя

№	Наименование поля	Описание поля	Обязательное для заполнения	Порядок заполнения
1	Логин	Логин пользователя в Системе	Да	Заполнить вручную текстовое поле или выбрать из выпадающего списка

№	Наименование поля	Описание поля	Обязательное для заполнения	Порядок заполнения
2	Роль	Групповая роль пользователя	Да	Выбрать из списка групповых ролей

4) Нажать на кнопку **Добавить** Добавить. После этого пользователь добавится в текущую и во все вложенные группы.

4.6.1.10. Изменение роли пользователя группы

Для изменения групповой роли пользователя необходимо:

1) В разделе **Пользователи группы <Название группы>** (Рисунок 32) найти пользователя, которого требуется изменить;

2) Нажать в меню действий ⋮ на пункт **Изменить** Изменить;

3) В открывшейся форме **Изменение роли пользователя** (Рисунок 34) отредактировать необходимые поля;

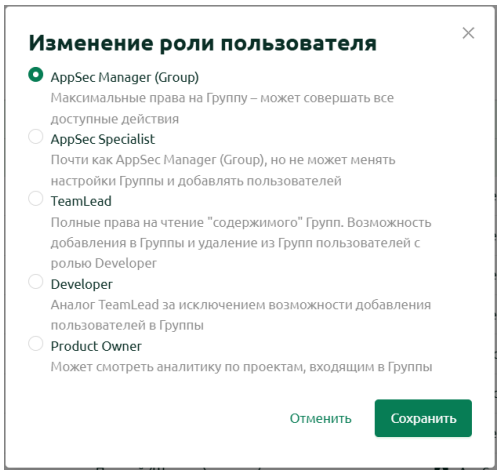


Рисунок 34 — Форма Изменение роли пользователя

4) Нажать на кнопку Сохранить Сохранить. После этого Система обновит роль пользователя.

4.6.1.11. Удаление пользователя из группы

Для удаления пользователя из группы необходимо:

1) В разделе **Пользователи группы <Название группы>** (Рисунок 32) найти пользователя, которого требуется удалить;

2) Нажать в меню действий ⋮ на пункт **Удалить** Удалить ;

3) В открывшейся форме **Удалить пользователя <Логин пользователя>** (Рисунок 35) нажать на кнопку **Да, удалить** Да, удалить. После этого пользователь удалится из текущей и всех вложенных групп.

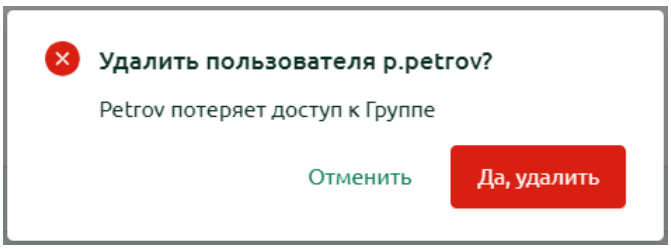


Рисунок 35 — Форма удаления пользователя из группы

4.6.1.12. Просмотр групп AD

Для просмотра групп AD, которые соотносятся с группой «Шерлока», необходимо:

1) В разделе **Пользователи группы <Название группы>** (Рисунок 32) нажать на кнопку Пользователи Пользователи ;

2) Перейти во вкладку **Группы AD** Группы AD (10) ;

3) Система отобразит таблицу **Группы** (Рисунок 36) с колонками, описанными в Таблица 12.

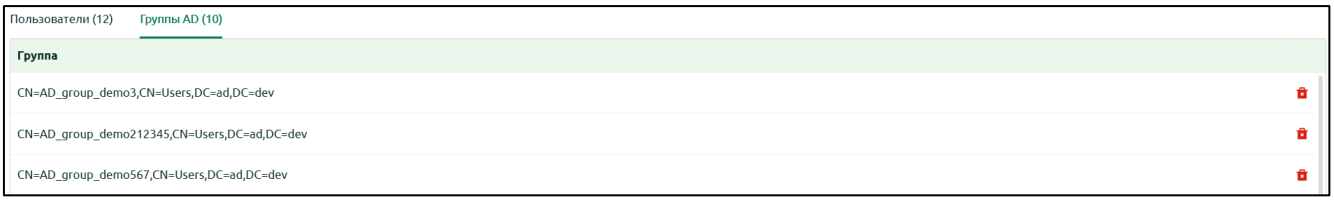


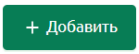
Рисунок 36 — Группы AD

Таблица 12 — Колонки таблицы групп AD

№	Наименование поля	Описание поля
1	Группа	Distinguished Name: уникальное имя объекта в AD
2	Удаление группы	Удаление группы AD (Раздел 4.6.1.14)

4.6.1.13. Добавление групп AD

Для добавления пользователя в группу (из AD) необходимо:

1) В разделе **Пользователи группы <Название группы>** (Рисунок 32) нажать на кнопку **Добавить** 

;

2) В выпадающем меню нажать на пункт **Из AD** 

;

3) В открывшейся форме **Добавление пользователей из AD** (Рисунок 37) заполнить поля, описанные в Таблица 13;

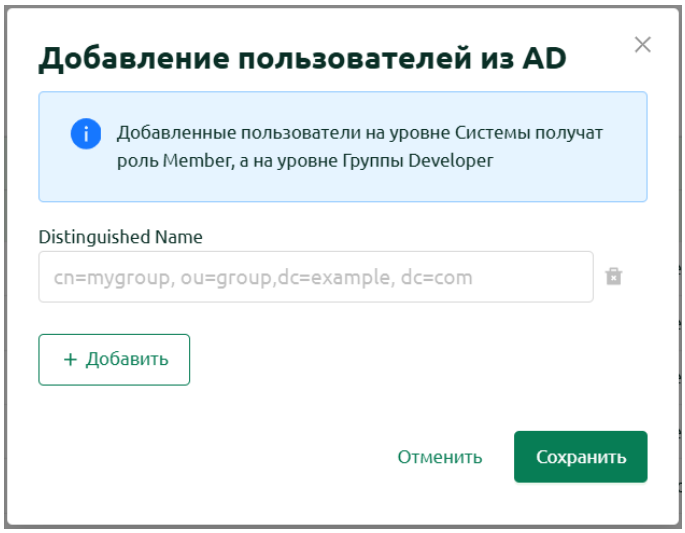
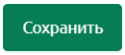


Рисунок 37 — Форма Добавление пользователей из AD

Таблица 13 — Описание полей формы Добавление пользователей из AD

№	Наименование поля	Описание поля	Обязательное для заполнения	Порядок заполнения
1	Distinguished Name	Distinguished Name: уникальное имя объекта в AD	Да	Заполнить вручную текстовое поле

4) Нажать на кнопку **Сохранить** 

. После этого пользователи из AD добавятся в текущую и во все вложенные группы.

4.6.1.14. Удаление групп AD

Для удаления группы AD необходимо:

1) В разделе **Пользователи группы <Название группы>** (Рисунок 32), во вкладке **Группы AD** 

, в таблице **Группы** (Рисунок 36) найти группу, которую требуется удалить;

2) Нажать на кнопку **Удалить** ;

3) В открывшейся форме **Удалить группу AD <Distinguished Name>?** (Рисунок 38) нажать на кнопку **Да, удалить** Да, удалить. После этого группа AD удалится из группы Системы.

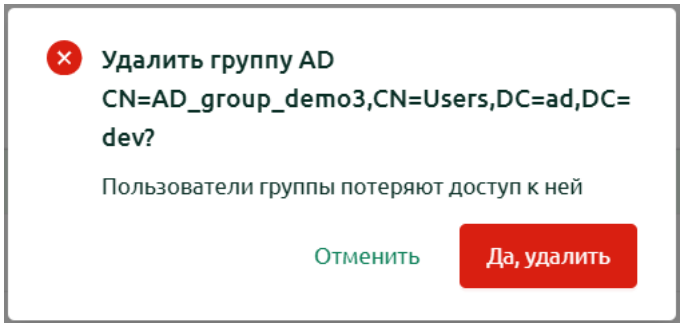


Рисунок 38 — Форма удаления группы AD

4.6.2. Работа в карточке проекта

При переходе пользователя в проект ему будет доступен один из следующих вариантов отображения **Карточки проекта**:

– если не настроена интеграция с GitLab, то пользователь увидит экран, отображенный на рисунке 39;

– если настроена интеграция с GitLab и информация об ИБ-дефектах отсутствует, то пользователь увидит экран, отображенный на рисунке 40;

– если настроена интеграция с GitLab и информация об ИБ-дефектах присутствует, то пользователь увидит экран, отображенный на рисунке 41;

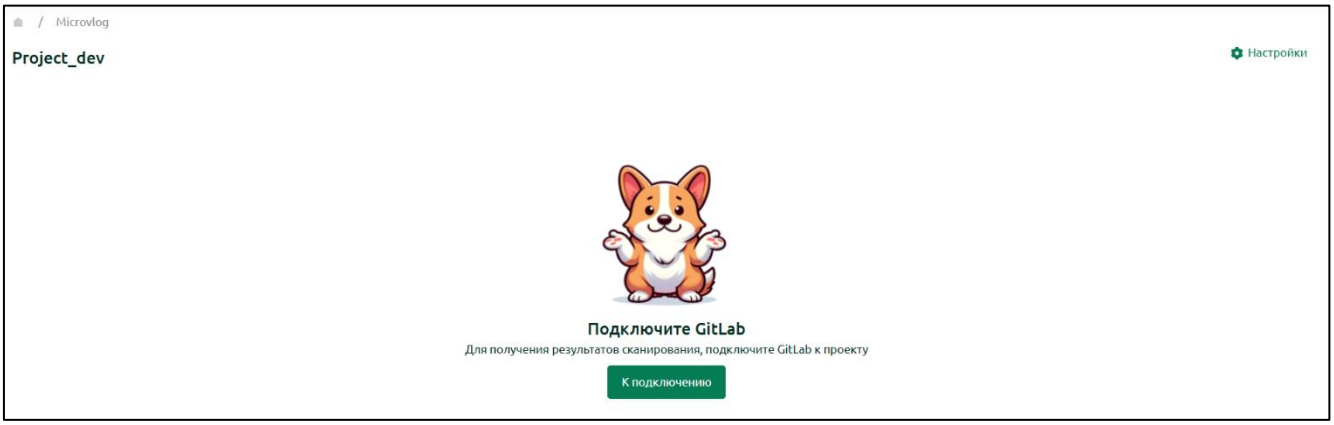


Рисунок 39 — Карточка проекта (GitLab не подключен)

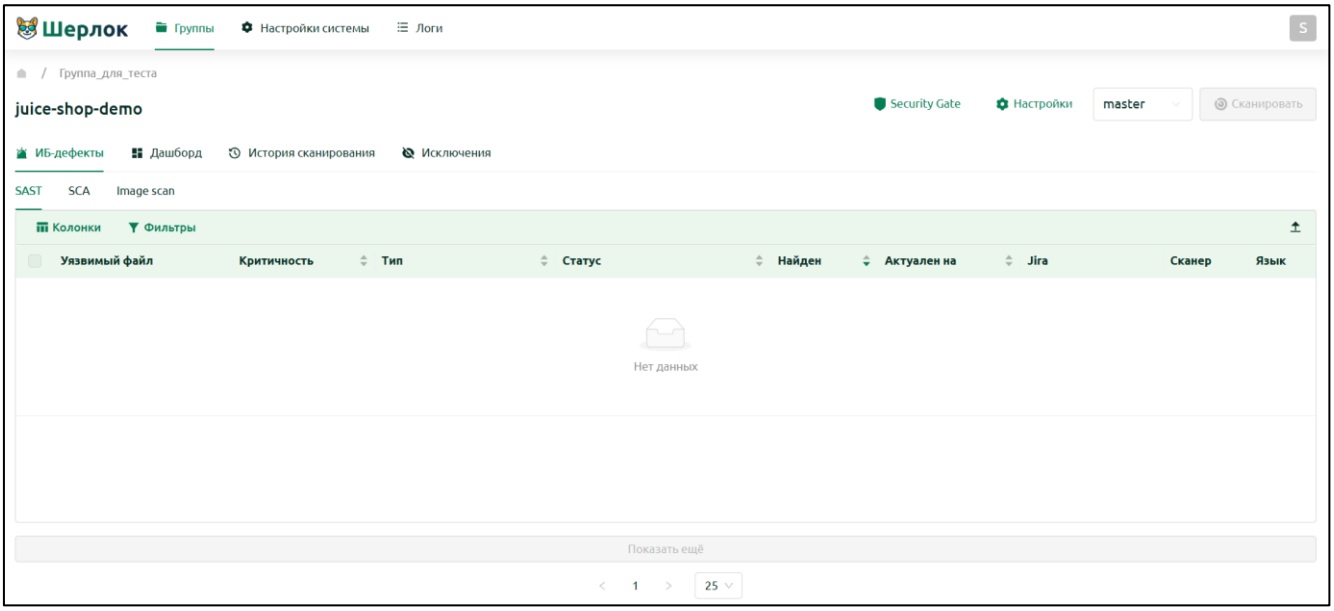


Рисунок 40 — Карточка проекта (GitLab подключен, ИБ-дефекты отсутствуют)

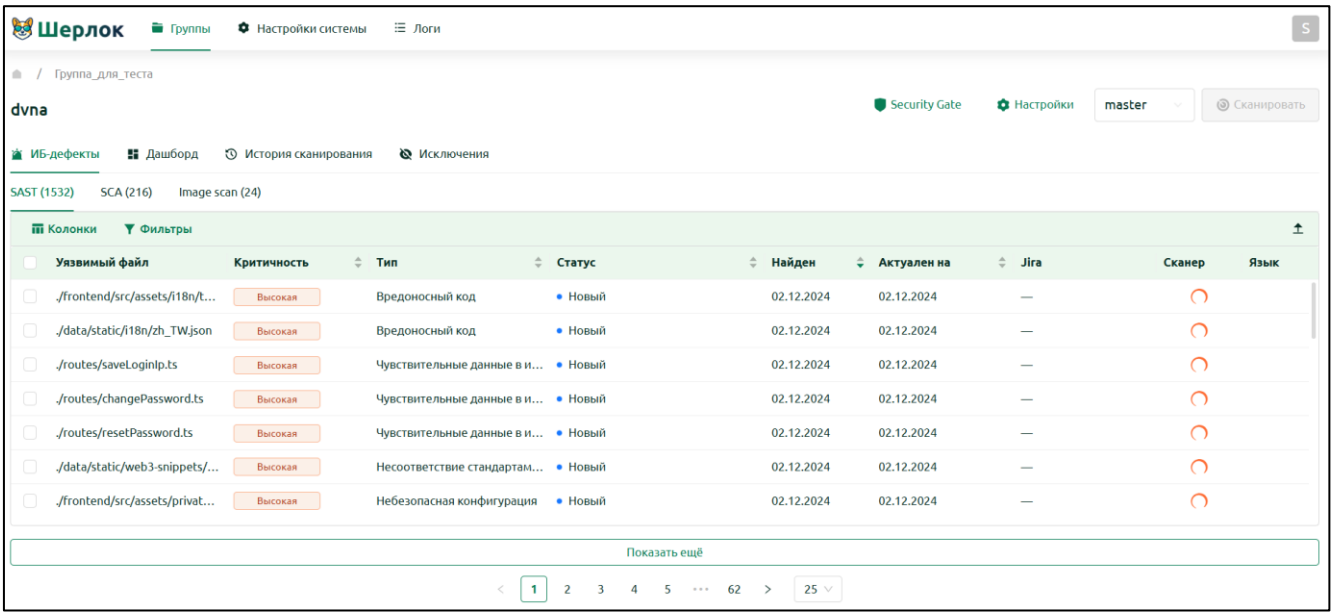


Рисунок 41 — Карточка проекта (GitLab подключен, ИБ-дефекты присутствуют)

В карточке проекта пользователю доступны следующие функции:

– Настройки проекта. Подробное описание в разделе 4.6.2.1;

– Настройка правил Security Gate. Подробное описание в разделе 4.6.2.2;

– Работа с ИБ-дефектами (запуск сканирования, импорт результатов сканирования, просмотр списка ИБ-дефектов и информации по каждому ИБ-дефекту). Подробное описание в разделе 4.6.2.3;

– Просмотр статистической информации в дашборде. Подробное описание в разделе 4.6.2.4;

– Просмотр Истории сканирования. Подробное описание в разделе 4.6.2.5;

– Просмотр исключенных ИБ-дефектов. Подробное описание в разделе 4.6.2.6.

4.6.2.1. Настройки проекта

Для управления настройками проекта пользователю необходимо перейти из **Карточки проекта** в раздел **Настройки проекта** (Рисунок 42).

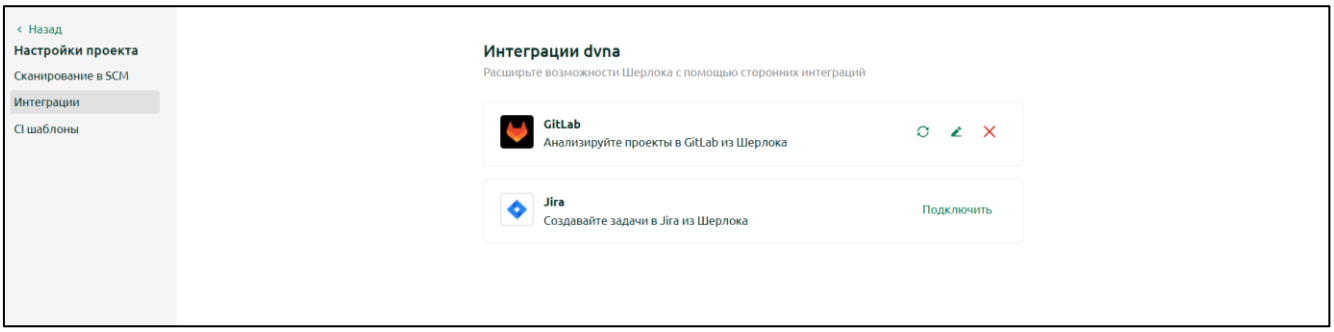


Рисунок 42 — Страница настроек проекта

Дальнейшие разделы (4.6.2.1.1 — 4.6.2.1.3) описаны исходя из предположения, что пользователь находится в разделе **Настройки проекта**.

4.6.2.1.1. Сканирование в SCM

Для управления настройками сканирования в SCM пользователю необходимо перейти в раздел **Сканирование в SCM** (Рисунок 43) раздела **Настройки проекта**.

Рисунок 43 — Страница настроек сканирования в SCM

Сканирование в SCM доступно только для сканеров типа SAST и SCA:

– SAST:
  – Solar appScreener (appScreener);
  – Positive Technologies Application Inspector (PT AI).
– SCA:
  – CodeScoring.

Перед тем как настраивать сканирование в SCM для определенного проекта, необходимо подключить сканеры на уровне Системы. (Подробнее об этом написано в разделе 2).

Если сканеры не подключены в Системе, то будет отображена ссылка для перехода в настройки Системы или текстовое сообщение о необходимости обратиться к администратору для настройки Системы (Рисунок 44, Рисунок 45).

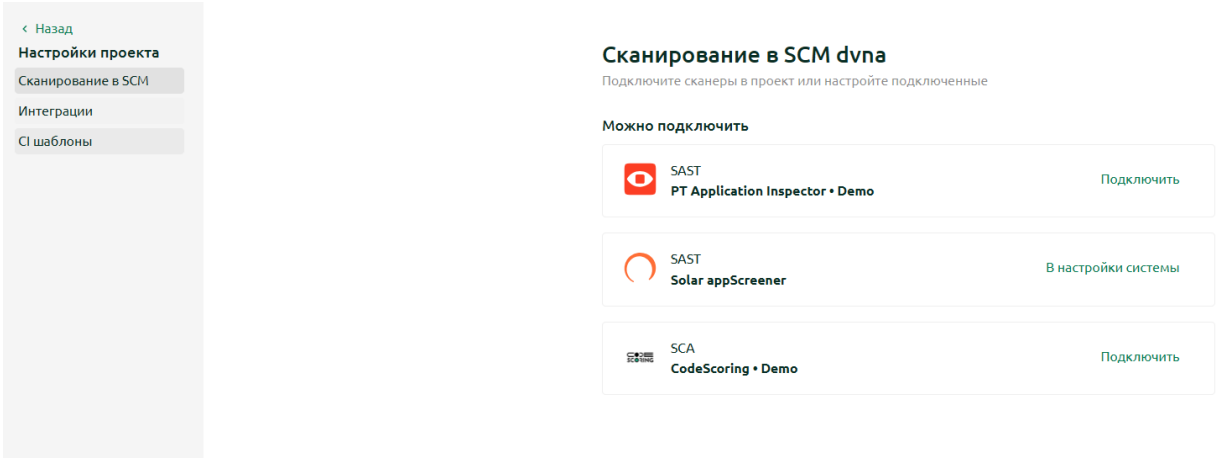


Рисунок 44 — Страница настроек сканирования в SCM (сканеры не подключены на уровне Системы, отображение информации для пользователя с ролью Admin)

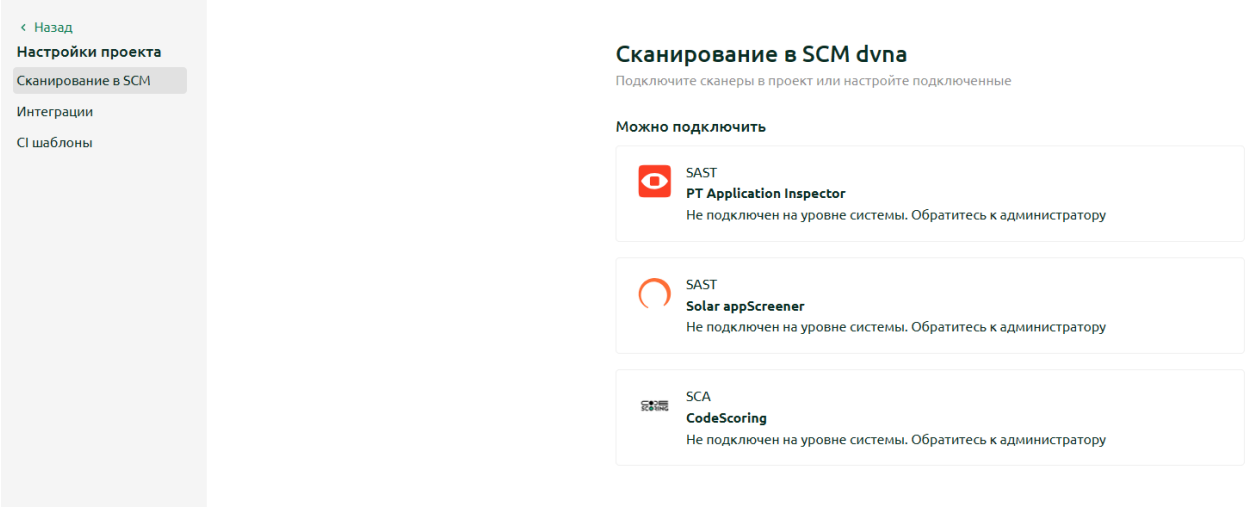


Рисунок 45 — Страница настроек сканирования в SCM (сканеры не подключены на уровне Системы, отображение информации для пользователя с ролью, отличной от Admin)

Все подключенные на уровне Системы сканеры отобразятся в блоке **Можно подключить** в разделе **Сканирование в SCM.** Для всех сканеров из блока **Можно подключить** пользователю доступно подключение проекта Системы к проектам сканеров.

Пользователю доступно подключение проекта Системы к нескольким проектам сканера.

Для подключения к проектам сканера с разными ветками репозитория с исходным кодом необходимо добавить отдельные настройки.

После подключения сканера Система позволит осуществлять сканирование в SCM для заданной ветки репозитория.

Подключенные сканеры будут отображаться в блоке **Подключенные** раздела **Сканирование в SCM** с указанием ветки репозитория (Рисунок 46).

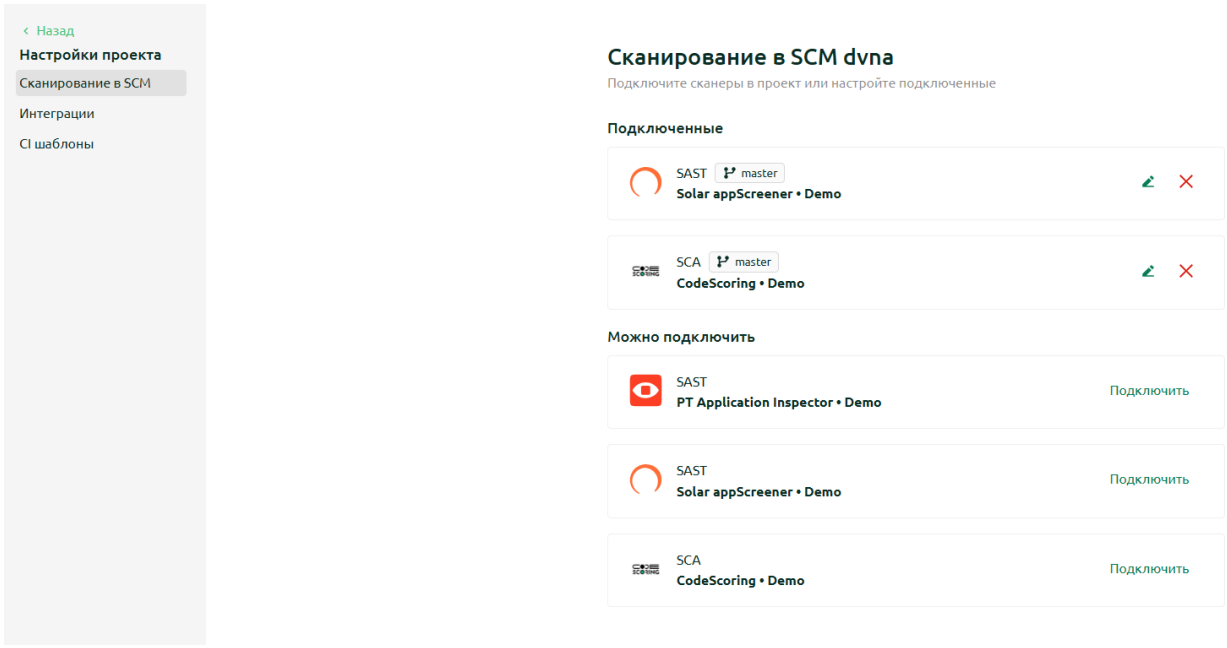


Рисунок 46 — Подключенные сканеры проекта для сканирования в SCM

Для подключения к проекту сканера необходимо:

1) На странице **Настроек проекта** в разделе **Сканирование в SCM** нажать кнопку **Подключить**, расположенную в блоке с нужным сканером;

2) В открывшейся форме подключения сканера заполнить поля, описанные в таблице 14;

3) Нажать кнопку **Подключить**. После этого Система добавит новый сканер, что позволит осуществлять сканирование в SCM.

Таблица 14 — Описание полей формы подключения сканера для сканирования в SCM

№	Сканер	Наименование поля	Описание поля	Обязательное для заполнения	Порядок заполнения
1	PT AI	ProjectID или ссылка на проект в PT AI	Идентификатор анализируемого проекта в PT AI	Да	Заполнить вручную текстовое поле. Возможные варианты заполнения: – полная ссылка на проект в PT AI. Пример: https://%ptaiurl%/ui/projects/20815d64-8d4a-4fdc-8093-697aeb8a950d/scan/2d7012cd-1c3a-43ba-b576-772bb8dc0415 – UUID проекта в PT AI. Пример: 20815d64-8d4a-4fdc-8093-697aeb8a950d

№	Сканер	Наименование поля	Описание поля	Обязательное для заполнения	Порядок заполнения
2	appScreener*	ProjectID или ссылка на проект в Solar	Идентификатор анализируемого проекта в appScreener	Да	Заполнить вручную текстовое поле. Возможные варианты заполнения: – полная ссылка на проект в appScreener. Пример: https://%appscreenerurl%/projects/1b436a11-719e-4b26-b250-2d9b57b3151b/summary_data?scan=… – UUID проекта в appScreener. Пример: 1b436a11-719e-4b26-b250-2d9b57b3151b
3	CodeScoring	ProjectID или ссылка на проект в CodeScoring	Идентификатор анализируемого проекта в CodeScoring	Да	Заполнить вручную текстовое поле. Возможные варианты заполнения: – полная ссылка на проект в CodeScoring. Пример: https://%codescoringurl%/cabinet/projects/184/sca – ID проекта в CodeScoring. Пример: 184

***Важно:** у подключаемого проекта appScreener в обязательном порядке должны быть указаны параметры:

– ветка репозитория Git. Если ее не указывать, appScreener будет анализировать ветку master. Однако для интеграции с Системой ветку необходимо указать явно;

Настройка приватного репозитория. Сейчас Система поддерживает только вариант «Персональный токен». С иными вариантами настроить корректную реализацию интеграции для запуска сканирования SCM из пользовательского интерфейса в Системе не получится.

При необходимости внесения изменений в настроенные подключения сканеров для сканирования в SCM пользователю Системы необходимо нажать на иконку рядом с интересующим подключением и поменять настройки. Настройки при изменении подключения аналогичны тем, что используются при его создании.

Для удаления подключения пользователю необходимо нажать на иконку рядом с интересующим подключением и подтвердить операцию в открывшейся форме.

4.6.2.1.2. Интеграции

Для управления настройками интеграций пользователю необходимо перейти в раздел **Интеграции** (Рисунок 47) раздела **Настройки проекта**.

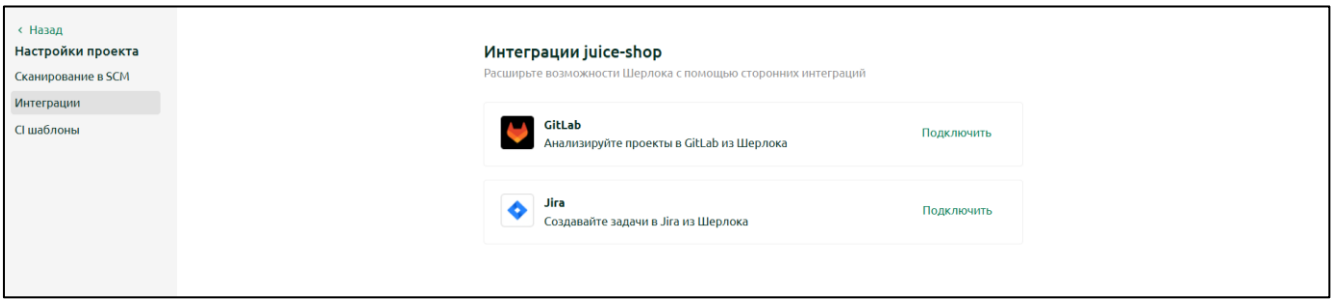


Рисунок 47 — Страница настроек интеграции проекта

Для подключения **GitLab** необходимо:

1) На странице **Настроек проекта** в разделе **Интеграции** нажать кнопку **Подключить**, расположенную в блоке с GitLab;

2) В открывшейся форме подключения GitLab заполнить поля, описанные в таблице 15;

Таблица 15 — Описание полей формы подключения GitLab

№	Наименование поля	Описание поля	Обязательное для заполнения	Порядок заполнения
1	URL проекта	URL репозитория, который нужно подключить	Да	Заполнить вручную текстовое поле. Примечание: важно указать именно URL репозитория, а не полную ссылку на *.git-проект. Т.е. вариант «https://%gitlaburl%/%path%/%to%/%project%» подойдет, а вариант «https://%gitlaburl%/%path%/%to%/%project**.git**%» — нет
2	Токен проекта	Personal Access Token, Group Access Token (минимальная роль — Developer) или Project Access Token (минимальная роль — Developer), обладающий полномочиями: – read_api – read_repository	Да	Заполнить вручную текстовое поле

3) Нажать кнопку **Подключить.** После этого Система добавит интеграцию с GitLab, что позволит работать с результатами сканирования и синхронизировать ветки.

Перед тем как настраивать интеграцию с Jira для определенного проекта, необходимо подключить Jira на уровне Системы. Подробнее об этом написано в разделе 4.5.2.

Если Jira не подключена в Системе, то будет отображена ссылка для перехода в настройки Системы или текстовое сообщение о необходимости обратиться к администратору для настройки Системы (Рисунок **48**, Рисунок 49).

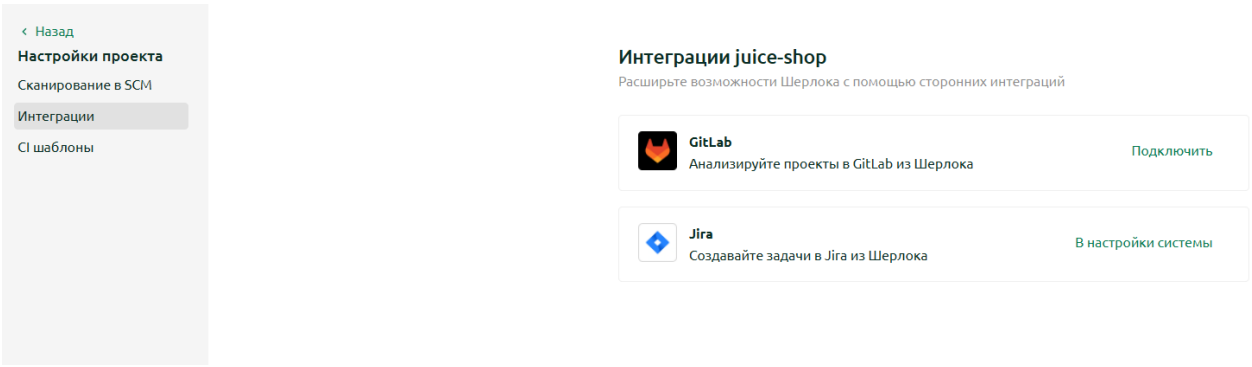


Рисунок 48 **— Страница настроек интеграций проекта (Jira не подключена на уровне Системы, отображение информации для пользователя с ролью Admin)**

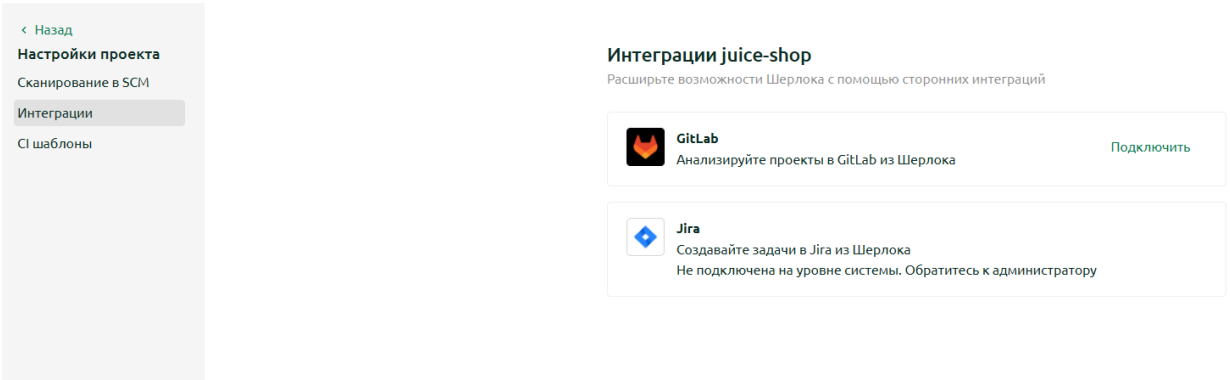


Рисунок 49 — Страница настроек интеграций проекта (Jira не подключена на уровне Системы, отображение информации для пользователя с ролью, отличной от Admin)

Для подключения **Jira** необходимо:

1) На странице **Настроек проекта** в разделе **Интеграции** нажать кнопку **Подключить**, расположенную в блоке с Jira;

2) В открывшейся форме подключения Jira заполнить поля, описанные в таблице 16;

Таблица 16 — Описание полей формы подключения Jira

№	Наименование поля	Описание поля	Обязательное для заполнения	Порядок заполнения
1	Код проекта	Уникальный идентификатор проекта в Jira	Да	Заполнить вручную текстовое поле

3) Нажать кнопку **Подключить.** После этого Система добавит интеграцию с Jira, что позволит создавать в ней задачи и синхронизировать типы задач.

Для внесения изменений в настроенные подключения GitLab и/или Jira пользователю необходимо нажать на иконку  рядом с интересующим подключением и поменять настройки. Настройки при изменении подключения аналогичны тем, что используются при его создании.

Для синхронизации веток в GitLab и/или синхронизации типов задач в Jira пользователю необходимо нажать на кнопку  рядом с соответствующей системой.

Для удаления подключения пользователю необходимо нажать на иконку  рядом с интересующим подключением и подтвердить операцию в открывшейся форме.

4.6.2.1.3. CI-шаблоны

Для управления интеграцией Системы в CI пользователю необходимо перейти в раздел **CI-шаблоны** раздела **Настройки проекта**.

Перед тем как получить доступ к CI-шаблонам для определенного проекта, необходимо подключить сканеры на уровне Системы. (Подробнее об этом написано в разделе 2).

Если сканеры не подключены в Системе, то будет отображена ссылка для перехода в настройки Системы или текстовое сообщение о необходимости обратиться к администратору для настройки Системы (Рисунок 50, Рисунок 51, блок Можно подключить).

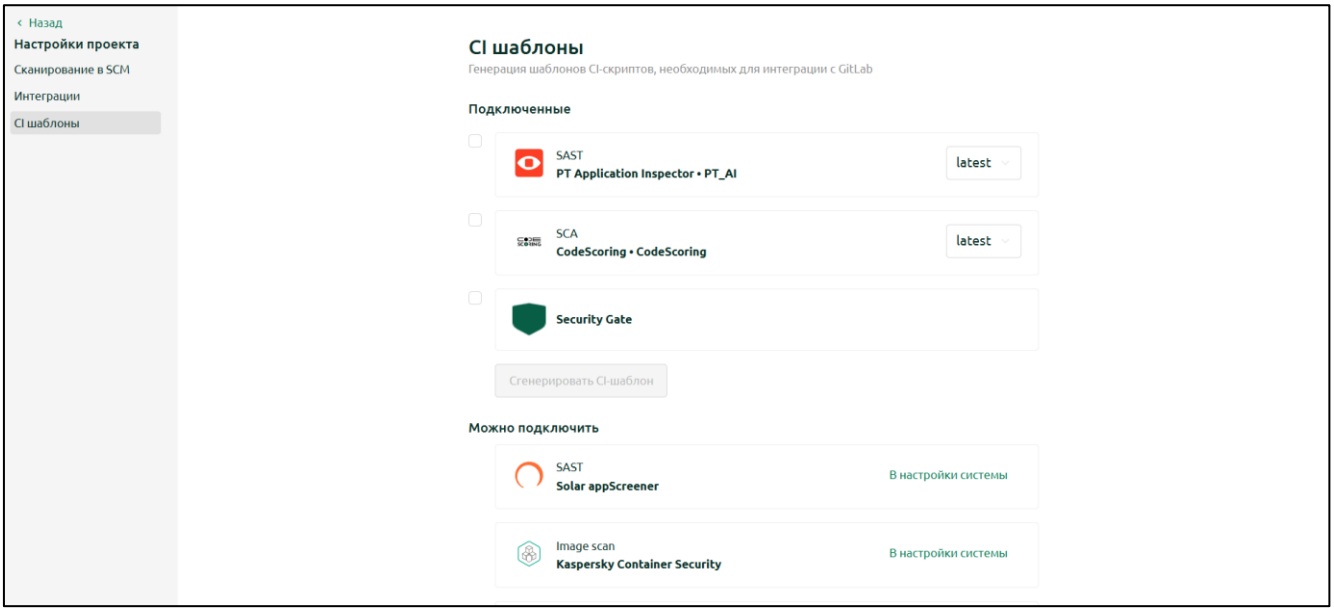


Рисунок 50 — Страница CI-шаблонов (сканеры не подключены на уровне Системы, отображение информации для пользователя с ролью Admin)

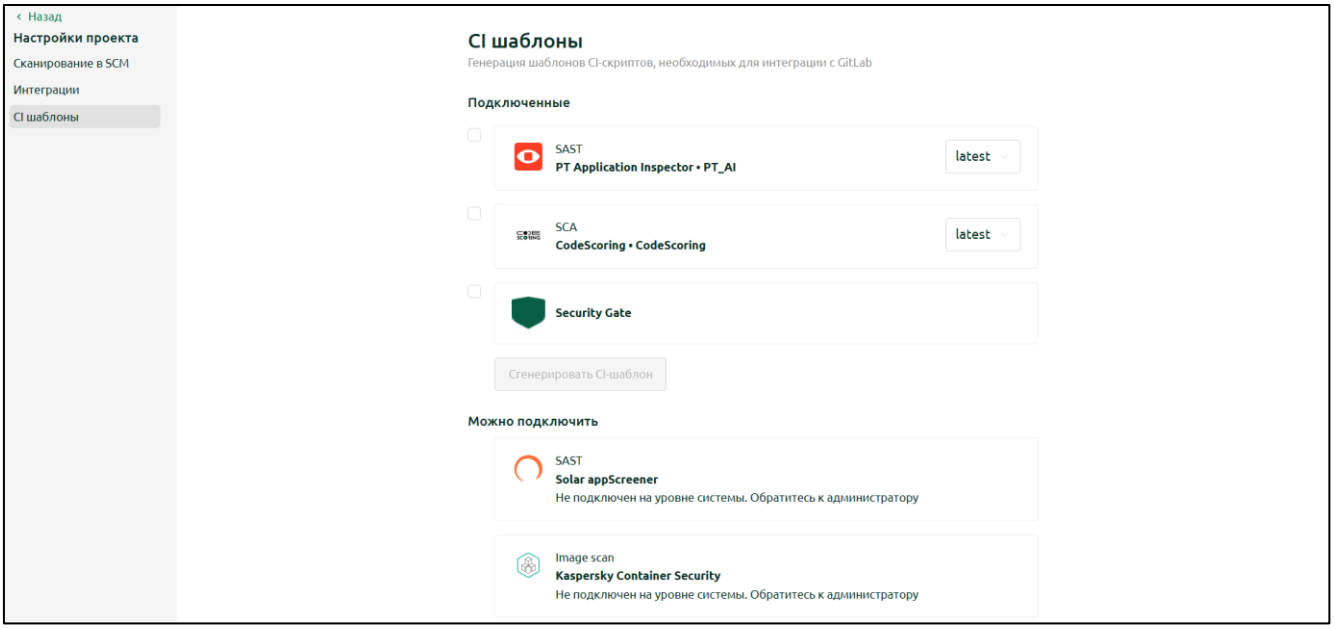


Рисунок 51 — Страница CI-шаблонов (сканеры не подключены на уровне Системы, отображение информации для пользователя с ролью, отличной от Admin)

CI-шаблоны доступны для всех сканеров, поддерживаемых Системой, и для Security Gate:

- SAST:
  - Solar appScreener (appScreener);
  - Positive Technologies Application Inspector (PT AI).

- SCA:
  - CodeScoring.
- Image Scan
  - Kaspersky Container Security;
  - Trivy.

Для генерации CI-шаблонов необходимо:

1) На странице **Настроек проекта** в разделе **CI-шаблоны** выбрать интересующие сканеры и/или Security Gate и нажать кнопку **Сгенерировать CI-шаблон;**
2) Скопировать CI-шаблон(ы) из открывшейся формы:
   а) Для копирования конкретного CI-шаблона необходимо нажать на кнопку **Копировать**, расположенную рядом с ним;
   б) Для копирования всех CI-шаблонов необходимо нажать на кнопку **Копировать все.**

Важно: необходимо адаптировать CI-шаблон под собственные нужды, например:

- указать требуемые stage, на которых должен отработать сгенерированный CI-шаблон;
- указать корректный адрес репозитория, в котором будет расположена CLI-утилита Системы, указываемый в разделе image;
- указать нужный runner в разделе tags;
- создать переменную окружения GitLab CI и поместить в нее SHERLOCK_TOKEN, использовать созданную переменную в CI-скрипте;
- создать необходимые переменные окружения в GitLab для того, чтобы CI-скрипт мог запуститься.

4.6.2.2. Настройка правил Security Gate

Для управления правилами Security Gate пользователю необходимо перейти из карточки проекта в раздел **Security Gate** (Рисунок 52, Рисунок 53).

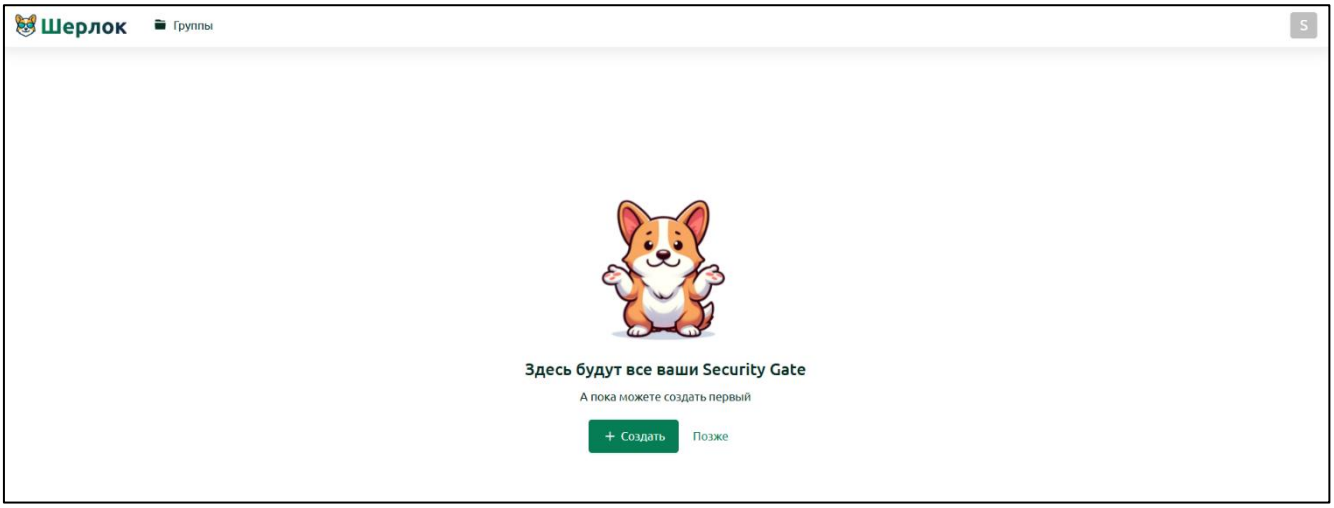


Рисунок 52 — Страница создания и настроек правил Security Gate (пример, когда нет ни одного правила)

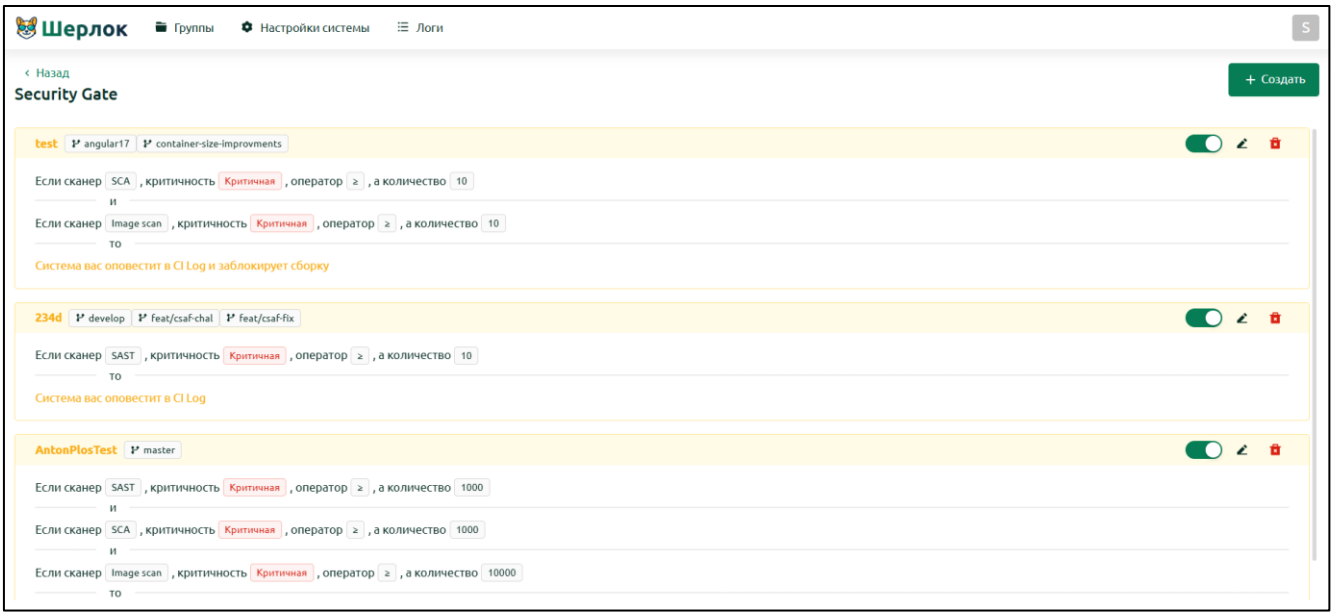


Рисунок 53 — Страница создания и настроек правил Security Gate (пример, когда есть правила)

Перед тем как создавать и настраивать правила Security Gate для определенного проекта, необходимо подключить GitLab. Подробнее об этом написано в разделе 4.6.2.1.2.

Для создания **правила Security Gate** необходимо:

1) На странице Создания и настроек правил Security Gate нажать кнопку **Создать**;

2) В открывшейся форме создания правила Security Gate заполнить поля, описанные в таблице 17;

Таблица 17 — Описание полей формы создания правила Security Gate

№	Наименование поля	Описание поля	Обязательное для заполнения	Порядок заполнения
1	Название	Произвольно название создаваемого Security Gate	Да	Заполнить вручную текстовое поле
2	Ветка	Ветка подключенного GitLab-репозитория, на которую будет распространяться Security Gate	Да	Выбрать ветку из предложенного списка
3	Блокировать сборку	Флаг, который позволяет запретить дальнейший процесс сборки в CI-системе в случае, если условия, описанные в правиле Security Gate для рассматриваемой ветки, не были пройдены	Нет	Установить флаг или оставить поле без изменений. По умолчанию флаг не устанавливается
Условия. Можно создать как одно, так и несколько условий. Для добавления условия необходимо нажать кнопку + Условие и заполнить соответствующие поля. Объединение условий осуществляется с использованием «логического И»				
4	Сканер	Тип сканера, для которого описывается условие	Да	Выбрать сканер из предложенного списка
5	Критичность	Уровень критичности правила, на которое будет распространяться условие	Да	Выбрать уровень критичности из предложенного списка
6	Количество	Количество уязвимостей определенного уровня критичности для определенного типа сканера, на которое будет распространяться условие	Да	Заполнить вручную численное поле

3) Нажать кнопку **Создать**. После этого Система добавит новое правило Security Gate.

Пользователь может создавать множество правил Security Gate:

– для разных веток анализируемого GitLab-репозитория;

– для одной и той же ветки анализируемого GitLab-репозитория. В этом случае проверяться будут все активные правила.

Пользователь может управлять набором активных правил Security Gate. Для этого на странице Создания и настроек Security Gate ему необходимо нажать на иконку  рядом с интересующим правилом:

–  – означает, что правило Security Gate активно;

–  – означает, что правило Security Gate не активно.

При необходимости внесения изменений в созданные правила Security Gate пользователь Системы может нажать на иконку  рядом с интересующим правилом и изменить его. Настройки при изменении правила Security Gate аналогичны тем, что используются при его создании.

Для удаления правила Security Gate пользователю необходимо нажать на иконку  рядом с интересующим правилом и подтвердить операцию в открывшейся форме.

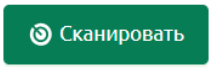
4.6.2.3. Работа в разделе ИБ-дефекты

4.6.2.3.1. Запуск сканирования

Перед запуском сканирования в Системе должны быть настроены:

1) Интеграция с GitLab в проекте. (Описание в разделе 4.6.2.1.2.)
2) Подключение сканера к проекту. (Описание в разделе 4.6.2.1.1.)

Для запуска сканирования необходимо:

1) Перейти в **Проект**;
2) Нажать на кнопку **Сканировать** 

;
3) В выпадающем меню выбрать пункт с названием сканера, например, **CodeScoring (SCA)** 

;
4) После завершения сканирования Система отобразит найденные ИБ-дефекты.

4.6.2.3.2. Импорт результатов сканирования

Для импорта результатов сканирования пользователю необходимо перейти в раздел **ИБ-дефекты** карточки проекта и выполнить следующие действия:

1) В разделе с ИБ-дефектами нажать на иконку  . Указанная иконка расположена в правом верхнем углу таблицы, содержащей информацию об ИБ-дефектах (Рисунок 54).
2) В открывшейся форме **Загрузка результатов сканирования** выбрать требуемый сканер:

а) PT Application Inspector (возможен импорт результатов сканирования в формате JSON);
б) Solar appScreener (возможен импорт результатов сканирования в формате SARIF);

в) CodeScoring (возможен импорт SBOM-файла в формате JSON);

г) Kaspersky Container Security (возможен импорт результатов сканирования в формате JSON);

д) Trivy (возможен импорт результатов сканирования в формате JSON).

3) Приложить файл соответствующего формата и размера (не более 5 Мбайт):

а) Нажать на область (Рисунок 55) и выбрать необходимый файл из открывшегося проводника;

б) Перетащить необходимый файл на область (Рисунок 55).

4) Нажать кнопку **Загрузить**. После этого Система загрузит результаты сканирования.

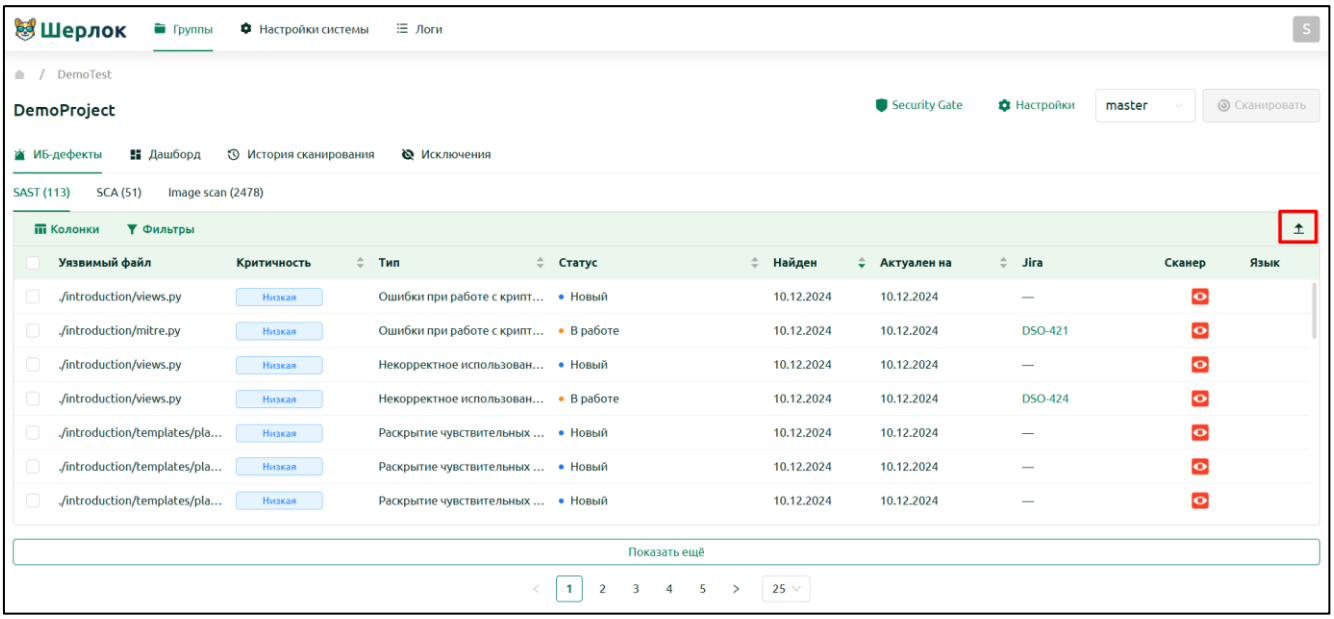


Рисунок 54 — Расположение иконки импорта результатов сканирования

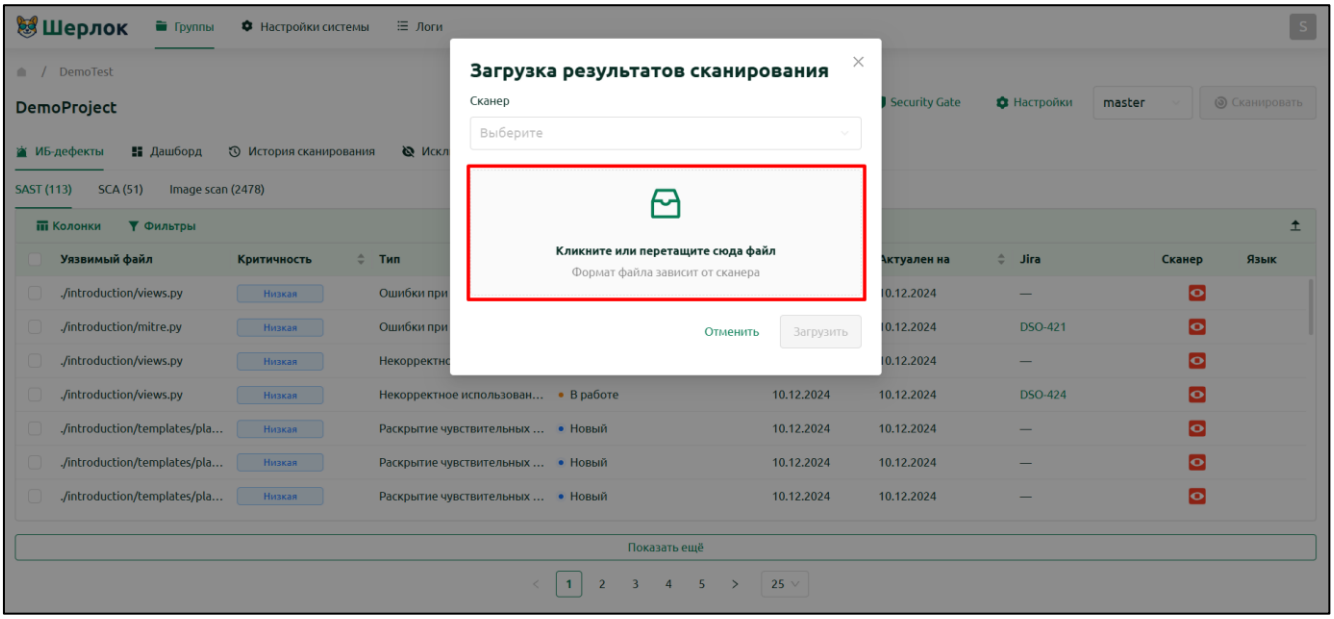


Рисунок 55 — Область для загрузки результатов сканирования

4.6.2.3.3. Работа со списком ИБ-дефектов

Для анализа результата сканирования Система отображает ИБ-дефекты трех видов сканера: SAST, SCA, Image Scan.

4.6.2.3.3.1. SAST

Для просмотра ИБ-дефектов типа сканера SAST необходимо:

1) Перейти в **Проект**;

2) Перейти в раздел **ИБ-дефекты** ИБ-дефекты;

3) Перейти во вкладку **SAST** SAST (22);

4) Система отобразит таблицу (Рисунок 56) с кнопками и колонками, описанными в Таблица 18 и Таблица 19.

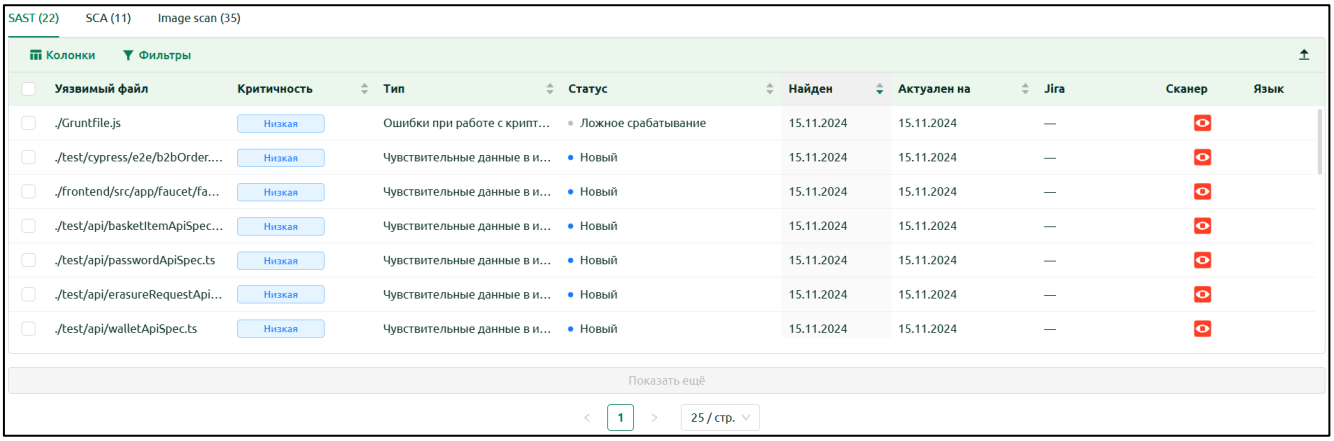


Рисунок 56 — Таблица с ИБ-дефектами сканера типа SAST

Таблица 18 — Заголовок таблицы с ИБ-дефектами сканера типа SAST

№	Наименование кнопки	Описание кнопки
1	Колонки	Выбор отображаемых в таблице колонок
2	Фильтры	Выбор отображаемых в таблице данных

Таблица 19 — Колонки таблицы ИБ-дефектов сканера типа SAST

№	Наименование поля	Описание поля
1	Выбор строк	Выбор строк для множественных операций
2	Уязвимый файл	Файл в репозитории с ИБ-дефектом
3	Критичность	Уровень критичности ИБ-дефекта. Возможные значения: – Критичная; – Высокая; – Средняя; – Низкая
4	Тип	Тип ИБ-дефекта
5	Статус	Статус ИБ-дефекта. Возможные значения: – Новый; – Подтвержден; – Ложное срабатывание; – В работе; – Риск принят; – Устранен; – Повторно найден; – Проигнорирован
6	Найден	Дата первого обнаружения ИБ-дефекта
7	Актуален на	Дата повторного обнаружения ИБ-дефекта

№	Наименование поля	Описание поля
8	Jira	Ссылка на задачу в Jira
9	Сканер	Логотип сканера, обнаружившего ИБ-дефект
10	Язык	Язык программирования, на котором написан уязвимый файл, содержащий ИБ-дефект

4.6.2.3.3.2. SCA

Для просмотра ИБ-дефектов типа сканера SCA необходимо:

1) Перейти в **Проект** (ссылка на раздел);

2) Перейти в раздел **ИБ-дефекты** ИБ-дефекты;

3) Перейти во вкладку **SCA** SCA (11);

4) Система отобразит таблицу (Рисунок 57) с кнопками, аналогичными кнопкам в таблице 24, и колонками, описанными в Таблица 20.

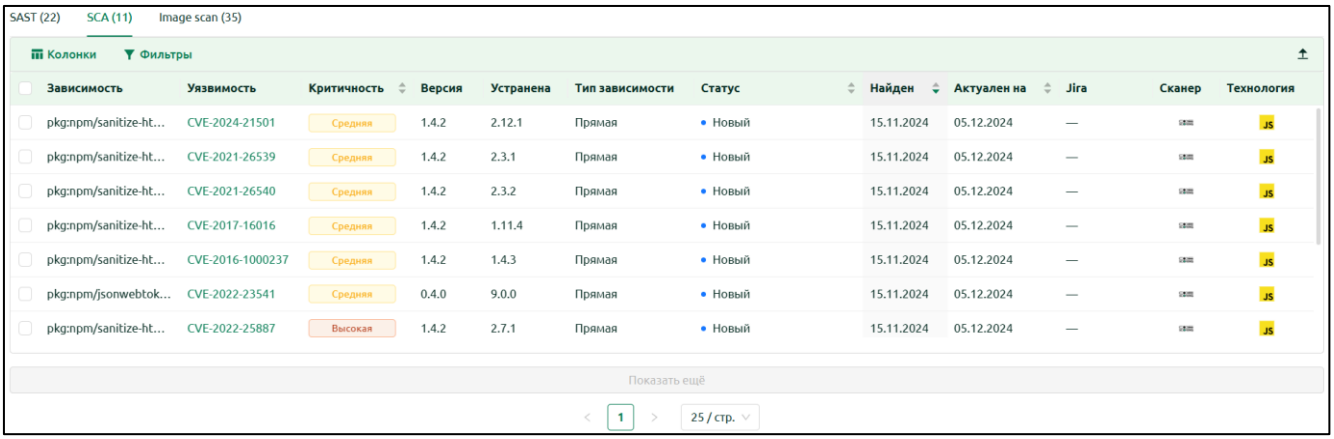


Рисунок 57 — Таблица с ИБ-дефектами сканера типа SCA

Таблица 20 — Колонки таблицы ИБ-дефектов сканера типа SCA

№	Наименование поля	Описание поля
1	Выбор строк	Выбор строк для множественных операций
2	Зависимость с версией	Путь до файла в репозитории, в котором найден ИБ-дефект с версией
3	Уязвимость	Ссылка на описание уязвимости
4	Критичность	Уровень критичности ИБ-дефекта. Возможные значения: – Критичная; – Высокая; – Средняя; – Низкая
5	Версия	Версия зависимости

№	Наименование поля	Описание поля
6	Устранена	Дата устранения ИБ-дефекта в зависимости
7	Тип зависимости	Тип зависимости ИБ-дефекта. Возможные значения: – Прямая; – Транзитивная
8	Статус	Статус ИБ-дефекта. Возможные значения: – Новый; – Подтвержден; – Ложное срабатывание; – В работе; – Риск принят; – Устранен; – Повторно найден; – Проигнорирован
9	Найден	Дата первого обнаружения ИБ-дефекта
10	Актуален на	Дата повторного обнаружения ИБ-дефекта
11	Jira	Ссылка на задачу в Jira
12	Сканер	Логотип сканера, обнаружившего ИБ-дефект
13	Технология	Язык программирования или технология, на которой написан уязвимый файл, содержащий ИБ-дефект

4.6.2.3.3.3. Image Scan

Для просмотра ИБ-дефектов типа сканера Image Scan необходимо:

1) Перейти в **Проект** (ссылка на раздел);

2) Перейти в раздел **ИБ-дефекты** ИБ-дефекты;

3) Перейти во вкладку **Image Scan** Image scan (35);

4) Система отобразит таблицу (Рисунок 58) с кнопками, аналогичными кнопкам в таблице 23, и колонками, описанными в Таблица 21.

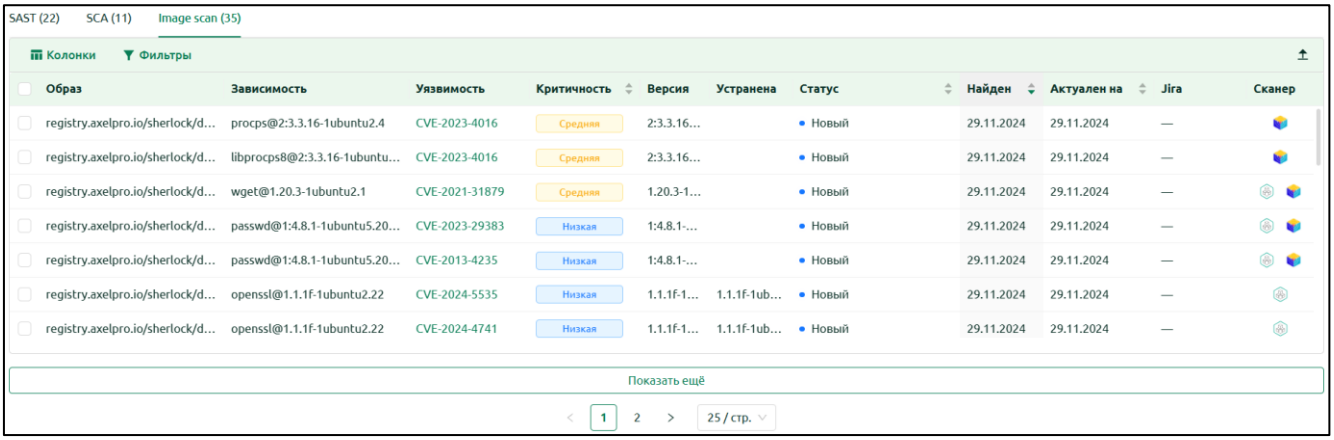


Рисунок 58 — Таблица с ИБ-дефектами сканера типа Image Scan

Таблица 21 — Колонки таблицы ИБ-дефектов сканера типа Image Scan

№	Наименование поля	Описание поля
1	Выбор строк	Выбор строк для множественных операций
2	Образ	Путь до образа, в котором содержится ИБ-дефект
3	Уязвимость	Ссылка на описание уязвимости
4	Критичность	Уровень критичности ИБ-дефекта. Возможные значения: – Критичная; – Высокая; – Средняя; – Низкая
5	Версия	Версия зависимости
6	Устранена	Дата устранения ИБ-дефекта в зависимости
7	Тип зависимости	Тип зависимости ИБ-дефекта. Возможные значения: – Прямая; – Транзитивная
8	Статус	Статус ИБ дефекта. Возможные значения: – Новый; – Подтвержден; – Ложное срабатывание; – В работе; – Риск принят; – Устранен; – Повторно найден; – Проигнорирован
9	Найден	Дата первого обнаружения ИБ-дефекта
10	Актуален на	Дата повторного обнаружения ИБ-дефекта

№	Наименование поля	Описание поля
11	Jira	Ссылка на задачу в Jira
12	Сканер	Логотип сканера, обнаружившего ИБ-дефект
13	Технология	Язык программирования или технология, на которой написан уязвимый файл, содержащий ИБ-дефект

4.6.2.4. Работа в разделе Дашборд

Для просмотра аналитической информации об ИБ-состоянии анализируемого проекта пользователю необходимо перейти в раздел **Дашборд** (Рисунок 59, Рисунок 60, Рисунок 61) карточки проекта.

Во всех информационных панелях и диаграммах Дашборда система получает статистические данные как среднее значение количества ИБ-дефектов или времени на устранение ИБ-дефектов в зависимости от выбранного периода времени с учетом фильтров по типу сканера, критичности (если это применимо для диаграммы). Под данными, релевантными для указанного временного интервала, Система понимает отношение количества ИБ-дефектов к количеству сканирований за период.

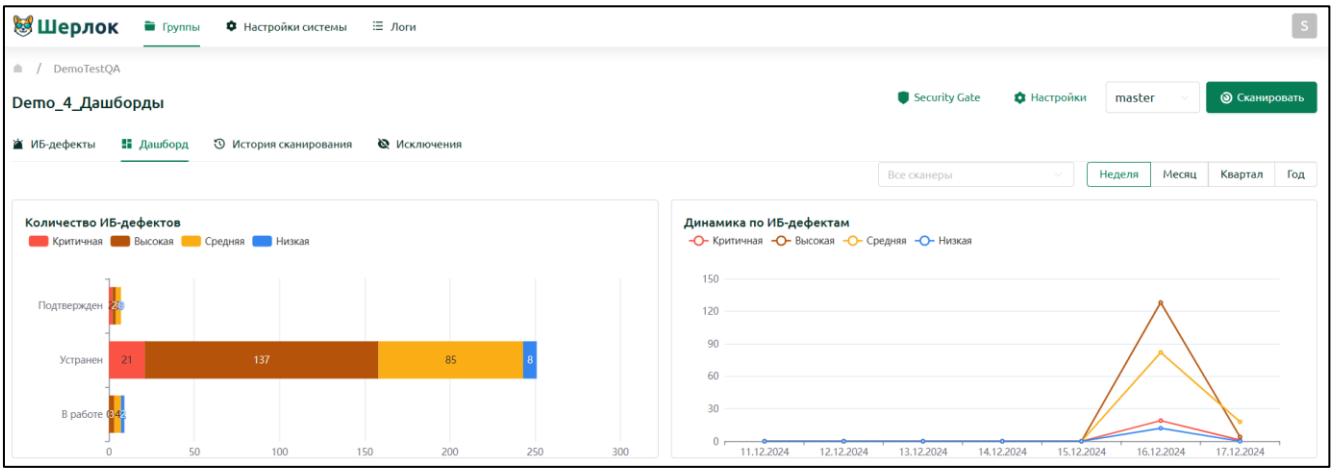


Рисунок 59 — Раздел Дашборд, диаграммы Количество ИБ-дефектов и Динамика по ИБ-дефектам

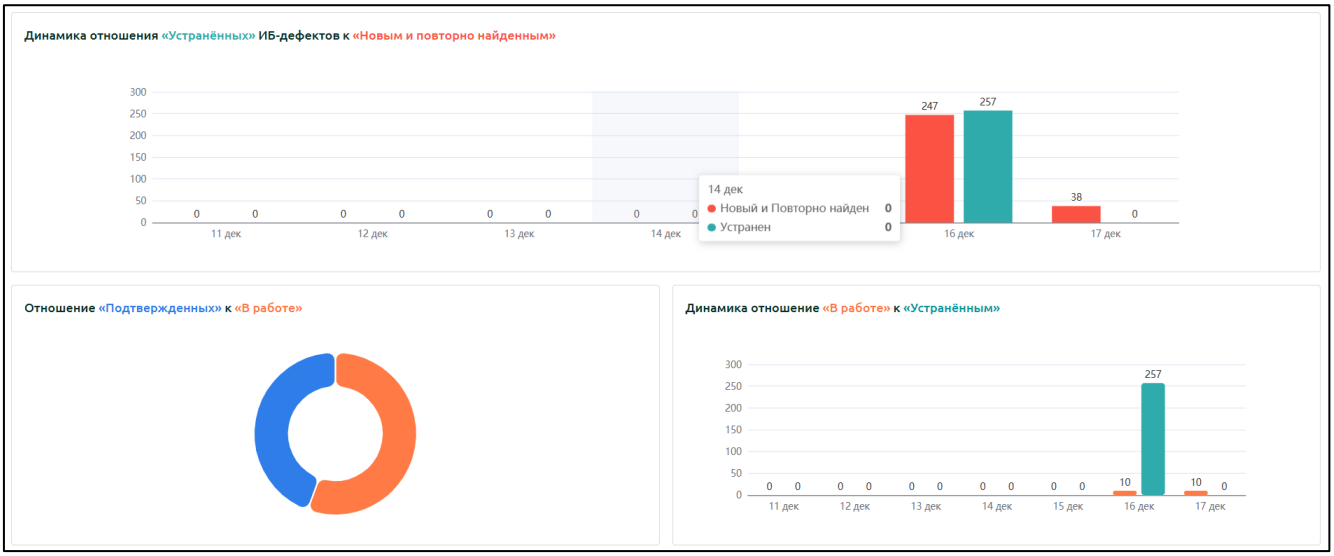


Рисунок 60 — Раздел Дашборд, диаграммы Динамика отношения «Устраненных» ИБ-дефектов к «Новым и повторно найденным», Отношение «Подтвержденных» в «В работе» и Динамика отношение «В работе» к «Устраненным»

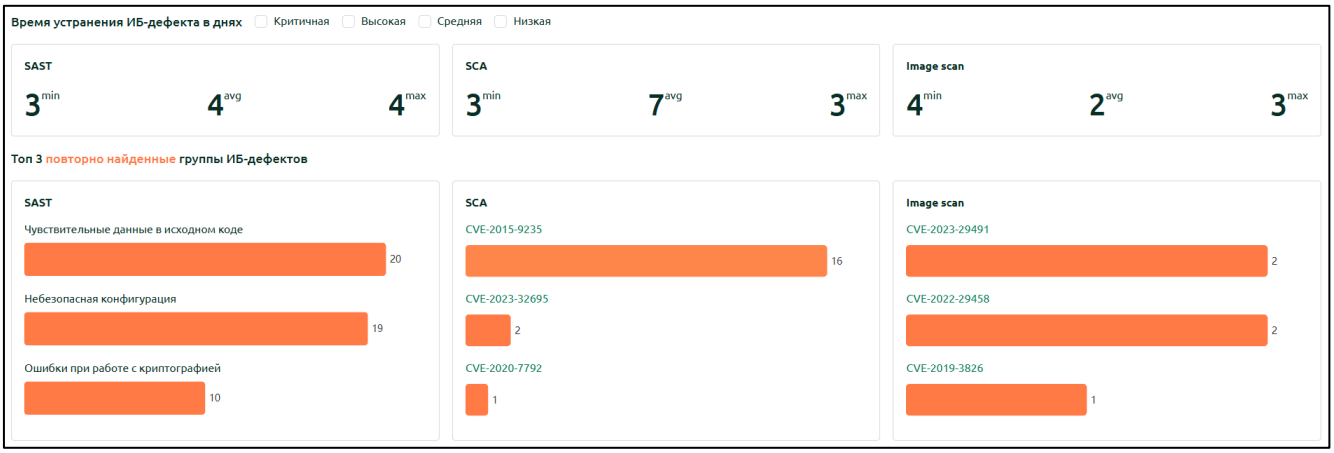


Рисунок 61 — Раздел Дашборд, информационные панели Время устранения ИБ-дефекта в днях и Топ-3 повторно найденные группы ИБ-дефектов

В разделе **Дашборд** представлена следующая информация:

1) Диаграмма **Количество ИБ-дефектов** с разбивкой по статусам (Устранен, В работе, Подтвержден) и по уровням критичности (Критичная, Высокая, Средняя, Низкая). По умолчанию график отображает информацию для всех уровней критичности ИБ-дефектов. Для того чтобы отобразить информацию для определенного уровня критичности, пользователю необходимо:

– на странице **Дашборд**, в графике **Количество ИБ-дефектов** нажать на интересующий уровень критичности;

– после этого Система отобразит данные, релевантные для обновленной выборки.

2) Диаграмма **Динамика по ИБ-дефектам** с разбивкой по уровням критичности (Критичная, Высокая, Средняя, Низкая). По умолчанию график отображает информацию для всех уровней критичности ИБ-дефектов. Для того чтобы отобразить информацию для определенного уровня критичности, пользователю необходимо:

- на странице **Дашборд**, в графике **Динамика по ИБ-дефектам** нажать на интересующий уровень критичности;
- после этого Система отобразит данные, релевантные для обновленной выборки.

3) Диаграмма **Динамика отношения «Устраненных» ИБ-дефектов к «Новым и повторно найденным»;**

4) Диаграмма Отношение «Подтвержденных» к «В работе»;

5) Диаграмма Динамика отношения «В работе» к «Устраненным»;

6) Информационная панель **Время устранения ИБ-дефекта в днях** для каждого класса сканеров (SAST, SCA, Image Scan): Минимальное (Min), Среднее (Avg), Максимальное (Max). По умолчанию Система отображает информацию для всех уровней критичности ИБ-дефектов. Для того чтобы отобразить информацию для определенного уровня критичности, пользователю необходимо:

- на странице **Дашборд**, в графике **Время устранения ИБ-дефекта в днях** нажать на интересующий уровень критичности;
- после этого Система отобразит данные, релевантные для обновленной выборки.

7) Информационная панель **Топ 3 повторно найденные группы ИБ-дефектов** (отдельно для сканеров классов SAST, SCA, Image Scan).

По умолчанию описанные выше диаграммы и информационные панели отображаются для всех типов сканеров (SAST, SCA, Image Scan).

Для получения аналитической информации по определенным типам сканеров пользователю необходимо:

- на странице **Дашборд** выбрать один или несколько типов сканеров в выпадающем списке (Рисунок 62);
- после этого Система отобразит данные, релевантные для выбранных типов сканеров.

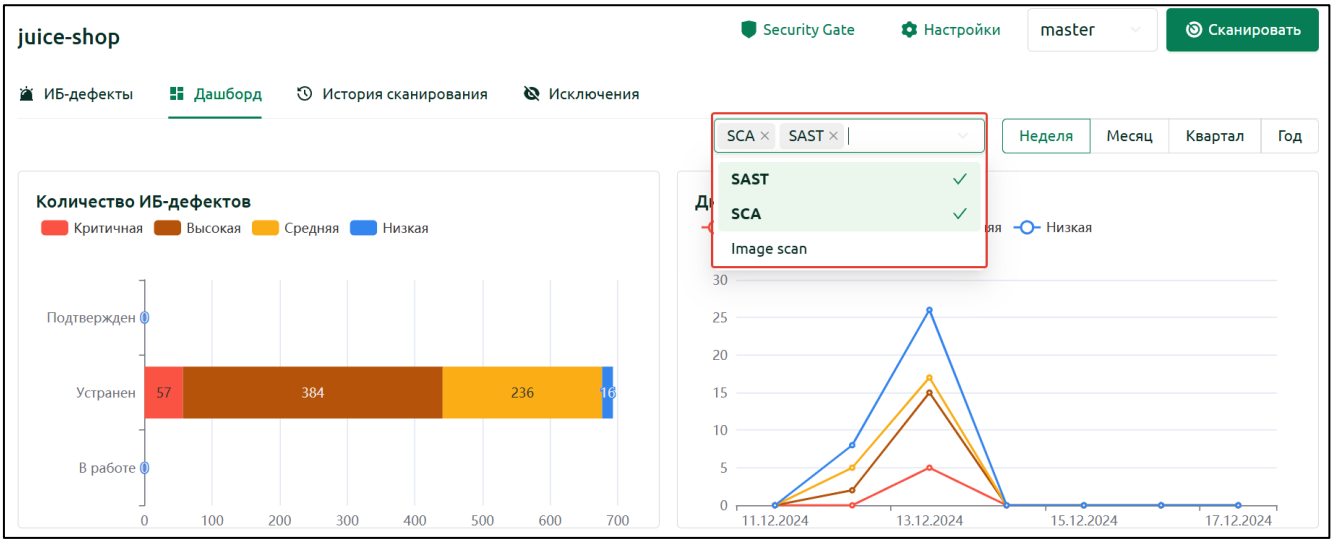


Рисунок 62 — Раздел Дашборд, выбор типов сканера для фильтрации данных

Для получения аналитической информации за определенный временной интервал пользователю необходимо:

– на странице **Дашборд** нажать на кнопку, отображающую интересующий временной интервал (Рисунок 63):

– Неделя;

– Месяц;

– Квартал;

– Год.

– после этого Система отобразит данные, релевантные для указанного временного интервала.

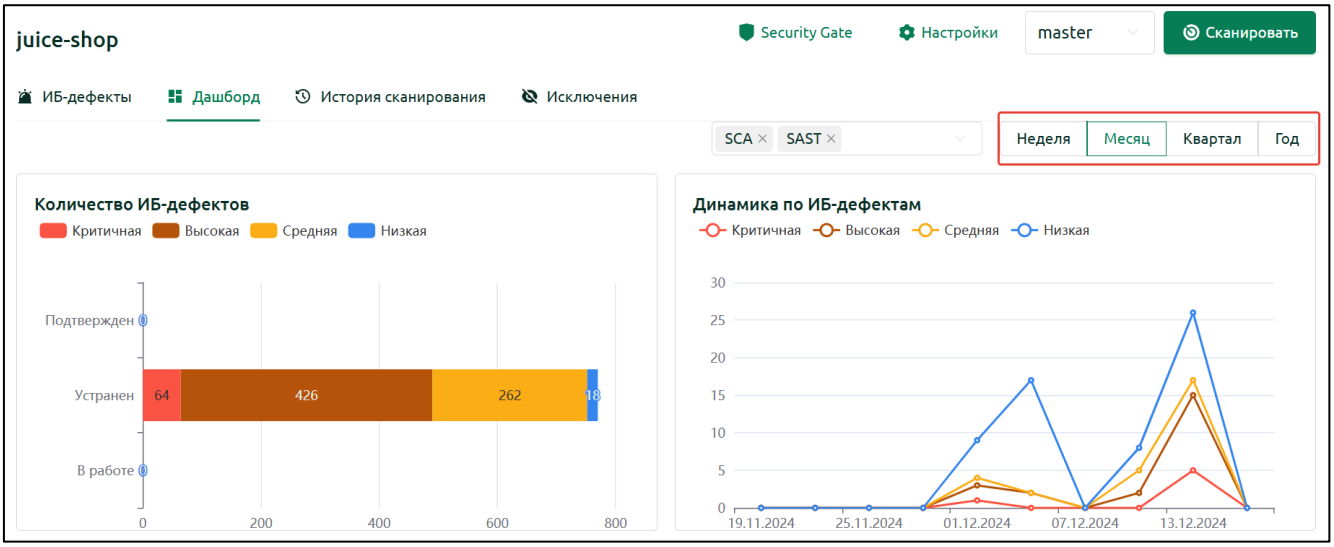


Рисунок 63 — Раздел Дашборд, выбор временного интервала для фильтрации данных

4.6.2.5. Работа в разделе История сканирования

Все запуски сканирований хранятся в разделе **История сканирования**. Для просмотра информации о сканированиях необходимо:

1) Перейти в **Проект**;

2) Перейти в раздел История сканирования История сканирования ;

Система отобразит таблицу (Рисунок 64) с кнопкой и колонками, описанными в таблице 24.

Рисунок 64 — Таблица историй сканирования ИБ-дефектов

Таблица 22 — Колонки таблицы истории сканирования проекта

№	Наименование поля	Описание поля
1	Запустили	Дата и время запуска сканирования
2	Длилось	Продолжительность сканирования

№	Наименование поля	Описание поля
3	Инициатор	Инициатор запуска сканирования. Возможные значения: – CI/CD; – Логин пользователя
4	Сканер	Логотип сканера, обнаружившего ИБ-дефект
5	Критичность	Шкала с количеством найденных ИБ-дефектов определенного уровня критичности
6	Результат	Результат запуска сканирования. Возможные значения: – Успех (сканирование завершилось); – Номер и описание ошибки при неуспешном завершении процесса сканирования

4.6.2.6. Работа в разделе Исключения

Для управления исключениями пользователю необходимо перейти в раздел **Исключения** (Рисунок 65, Рисунок 66) карточки проекта.

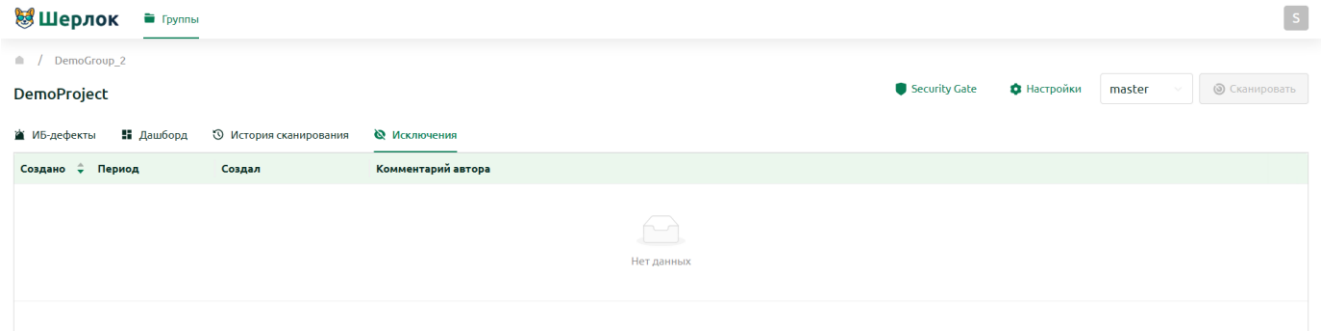


Рисунок 65 — Страница управления исключениями (пример, когда нет ни одного исключения)

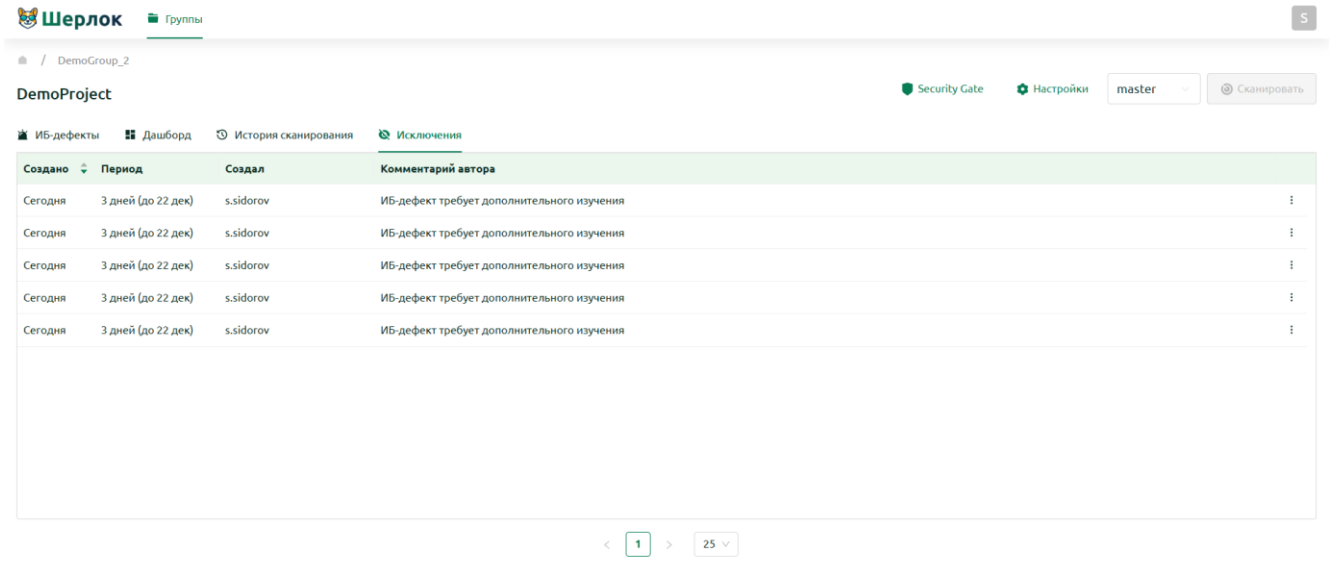


Рисунок 66 — Страница управления исключениями (пример, когда есть исключения)

В разделе **Исключения** приводится краткая информация о созданных исключениях:

– Создано. Дата создания исключения;

– Период. Временной интервал, в течение которого действует исключение. По завершении периода исключение будет автоматически удалено (отозвано);

– Создал. Логин пользователя, который создал исключение;

– Комментарий автора. Обязательное указание причины, из-за которой было принято решение об исключении ИБ-дефекта.

Также пользователь может получить информацию об ИБ-дефекте, для которого создано исключение, и/или удалить (отозвать) исключение.

Для получения информации об ИБ-дефекте, для которого создано исключение, необходимо:

1) На странице **Исключения** нажать на иконку ⋮ рядом с интересующим исключением;

2) В открывшейся форме нажать кнопку **К дефекту**. После этого Система перенаправит пользователя на расширенную версию карточки ИБ-дефекта.

Для удаления (отзыва) исключения ИБ-дефекта необходимо:

1) На странице Исключения нажать на иконку ⋮ рядом с интересующим исключением;

2) В открывшейся форме нажать кнопку **Удалить**;

3) В открывшейся форме нажать кнопку **Да, удалить**.

5. Перечень терминов и сокращений

Термин, сокращение	Описание
AD	Active Directory. Сервис управления и хранения информации о пользователях, компьютерах и других ресурсах в компьютерных сетях
API	Application Programming Interface. Набор правил, позволяющих одному программному продукту взаимодействовать с другим
CI/CD	Continuous Integration / Continuous Delivery. Технология автоматизации тестирования и доставки новых модулей разрабатываемого проекта заинтересованным сторонам
CI-скрипт	Сценарий, который используется в CI-системе
CI-шаблон	Шаблон с данными, необходимый для настройки конвейера сборки ПО в CI-системе
CLI	Command Line Interface. Интерфейс командной строки, позволяющий управлять различными процессами в компьютере с помощью текстовых команд
Image Scan	Сканирование образов контейнеров для идентификации уязвимостей, вредоносного ПО и чувствительной информации (например, секреты)
JSON	JavaScript Object Notation. Текстовый формат обмена данными, который используется для хранения данных и их передачи между различными системами и приложениями
LDAP	Lightweight Directory Access Protocol. Протокол быстрого доступа к каталогам
PEM	Privacy Enhanced Mail. Формат контейнера, содержащий криптографическую информацию
PT AI	PT Application Inspector. Инструмент для статического анализа кода
SARIF	Static Analysis Results Interchange Format. Формат обмена результатами статического анализа на основе JSON для вывода инструментов статического анализа
SAST	Static Application Security Testing, статический анализатор кода Класс решений, позволяющий анализировать программный код, байт-код и бинарные файлы для идентификации конструкций, которые могут являться ИБ-дефектами. Могут применяться на этапах разработки и тестирования жизненного цикла программного обеспечения. Например, Solar appScreener
SBOM	Software Bill of Materials. Список всех модулей и библиотек, необходимых для сборки программного продукта, а также указателей их связи друг с другом
SCA	Software Composition Analysis, анализ состава ПО Класс решений, которые позволяют идентифицировать ИБ-дефекты (уязвимости, лицензионные ограничения) в зависимостях (компонентах с открытым исходным кодом), используемых при разработке ПО. Могут применяться на этапах разработки и тестирования жизненного цикла программного обеспечения
SCM	Source Code Management, система управления исходными кодами Класс решений, которые позволяют управлять версиями программного кода, отслеживать изменения в программном коде и организовать централизованную работу разработчиков с одним или несколькими проектами (репозиториями)
Security Gate	Этап жизненного цикла программного обеспечения (ПО), на котором проверяется, что все заранее определенные требования по информационной безопасности, предъявляемые к нему, были выполнены. Необходимо для

	оценки возможности перехода к последующим этапам жизненного цикла ПО
Token	Идентификатор, который используется для представления доступа к ресурсам или выполнения определенных операций
URL	Uniform Resource Locator. Унифицированный адрес электронного ресурса
UUID	Universally Unique Identifier. Стандарт идентификации, используемый в создании программного обеспечения
ИБ	Информационная безопасность
ИБ-дефект	Дефект информационной безопасности (ИБ). Ошибка кода или инфраструктуры, которая требует внимания и устранения
ИБ-состояние	Состояние информационной безопасности (ИБ)
МГц	Мегагерц. Единица измерения частоты периодических процессов в Международной системе единиц
Сканер	Средство анализа поддерживаемой Системы (см. SAST, SCA, Image Scan)
УЦ	Удостоверяющий центр. Доверенная организация, которая имеет право выпускать сертификаты электронной подписи