Программное обеспечение для электронно-вычислительных машин
«Платформа управления внешними угрозами SENTRA»

Руководство пользователя

Листов 23

г. Москва, 2025 г.

СОДЕРЖАНИЕ

ТЕРМИНЫ, ОПРЕДЕЛЕНИЯ, СОКРАЩЕНИЯ 3
1. Введение 4
1.1. Общие сведения 4
2. Начало работы 6
2.1 Вход в систему 6
2.2 Навигация 6
2.3 Раздел «Главная» 7
3. Работа с профилем пользователя 9
4. Раздел «Активы» 11
5. Раздел «Уязвимости» 16
6. Раздел «Сканирования» 19
7. Раздел «Сотрудники» 20
8. Раздел «Уведомления» 22
9. Раздел «Документы» 23

ТЕРМИНЫ, ОПРЕДЕЛЕНИЯ, СОКРАЩЕНИЯ

Термин	Определение
Актив	IP-адрес или домен
ПО	Программное обеспечение
ЭВМ	Электронно-вычислительная машина
CIDR	Бесклассовая междоменная маршрутизация (Classless Inter-Domain Routing)
ASN	Номер автономной системы (Autonomous System Number)

1. Введение

Программное обеспечение для ЭВМ «Платформа управления внешними угрозами SENTRA» (Далее - ПО «SENTRA CTEM») – облачное решение (SaaS – Software as a Service / Программное обеспечение как сервис), предназначенное для инвентаризации корпоративных цифровых активов, доступных из сети Интернет, и выявления уязвимостей, возникающих в результате использования устаревшего программного обеспечения, программных ошибок и ошибок конфигурации.

Область применения:

Инвентаризация и контроль доступных из сети Интернет IT-ресурсов на наличие уязвимостей и ошибок конфигурации.

Функциональные возможности:

ПО «SENTRA CTEM» обеспечивает автоматизированную проверку корпоративных ресурсов в течение 24 часов, анализируя сетевые уровни L3-L7, идентифицируя открытые порты (0-65535, TCP/UDP), выявляя уязвимости и ошибки конфигурации сервисов.

Доступ к сервису предоставляется ООО «ЗАЩИЩЕННЫЕ СИСТЕМЫ» по подписке, условия которой зависят от количества анализируемых ресурсов и выбранных опций. Пользователь получает доступ к личному кабинету на весь срок действия подписки.

Функциональность ПО «SENTRA CTEM» включает:

- автоматизированный поиск корпоративных ресурсов, доступных из сети Интернет;
- регулярное обогащение списка ресурсов;
- регулярный мониторинг портов сервисов;
- выявление уязвимостей систем, сервисов и веб-приложений;
- классификацию уязвимостей по уровню критичности;
- автоматизированный подбор паролей для ssh, ftp, telnet, mssql, postgresql, imap, pop3, smtp, snmp, mysql, vmauthd, vnc, mongodb, asterisk, oracle, xmpp, rdp;
- подбор доменных учетных данных;
- анализ настроек доступа к файлам и папкам веб-серверов с целью предотвращения утечек конфиденциальных данных;
- управление и контроль процесса устранения уязвимостей при экспертной поддержке специалистов ООО «ЗАЩИЩЕННЫЕ СИСТЕМЫ».

1.1.Общие сведения

ПО «SENTRA CTEM» размещено в ЦОД ООО "Яндекс.Облако" (Yandex Cloud), расположенных на территории Российской Федерации.

Для получения достоверных результатов работы сервиса необходимо внести адреса, предоставляемые ООО «ЗАЩИЩЕННЫЕ СИСТЕМЫ», в списки исключения на периметровых средствах защиты информации (WAF, antiDDoS, NGFW/UTM).

Веб-браузер должен поддерживать выполнение JavaScript-кода и быть совместимым с React 18. Поддерживается последними версиями браузеров:

- Edge 15 или новее,
- Firefox 59 или новее,
- Opera 12.10 или новее,
- Google Chrome 66 или новее.

Рекомендуется регулярно обновлять браузер для обеспечения стабильной работы ПО.

Неподдерживаемые веб-браузеры:

- Internet Explorer,
- Opera версий до версии 12.02,
- прочие браузеры.

Для удобства работы с техническими отчетами, выгружаемыми из интерфейса в формате CSV, рекомендуется установить офисный пакет (например, LibreOffice или Microsoft Office).

1.2.Уровень подготовки пользователя

Все пользователи Системы должны иметь навыки работы с браузерами и являться уверенными пользователями ПК. Наличие профильного образования или сертификата о переподготовке позволит быстрее погрузиться в существующие процессы управления уязвимостями и оценки цифровых угроз.

Для получения доступа к ресурсам Системы пользователю необходимо использовать автоматизированное рабочее место (АРМ) в виде электронного вычислительного устройства, имеющего доступ в сеть Интернет, с установленным браузером.

2. Начало работы

2.1 Вход в систему

Для входа в Систему необходимо ввести логин и пароль на стартовой странице (Рис. 1). Логин и пароль для первого входа предоставляет менеджер.

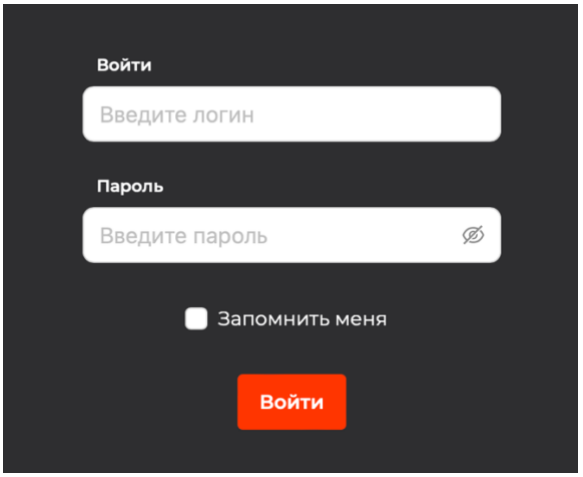

Рисунок 1. Форма авторизации

Для того, чтобы пароль отобразился при вводе, необходимо нажать на кнопку « » на поле ввода пароля.

Чтобы скрыть вводимые данные, нужно нажать на кнопку « ».

Для того, чтобы Система каждый раз при закрытии браузера не запрашивала авторизацию пользователя заново, необходимо поставить галочку в поле «Запомнить меня».

После ввода адреса электронной почты и пароля следует нажать на кнопку «Войти».

После авторизации станет доступен личный кабинет.

2.2 Навигация

Пользователю в личном кабинете доступны следующие функциональные разделы: «Главная», «Активы», «Уязвимости», «Сканирования», «Сотрудники», «Уведомления», «Документы», доступные в боковом меню в левой части экрана (Рис. 2).

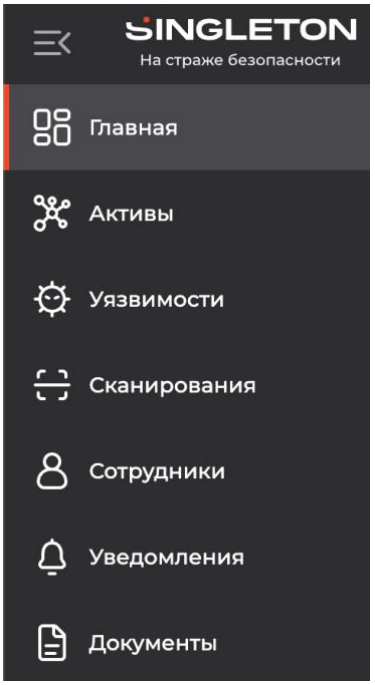

Рисунок 2. Разделы навигации

Для того, чтобы свернуть боковое меню (Рис. 3), необходимо нажать на кнопку «  » в левом верхнем углу экрана.

Рисунок 3. Компактный вид бокового меню

Для отмены изменений и возврату к более подробному меню необходимо нажать на кнопку «  » в левом верхнем углу экрана.

2.3 Раздел «Главная»

В данном разделе отображается статистика по организации. Представленные виджеты (Рис. 3) позволяют получить информацию о сканированиях, динамике изменения количества уязвимостей, активов и портов.

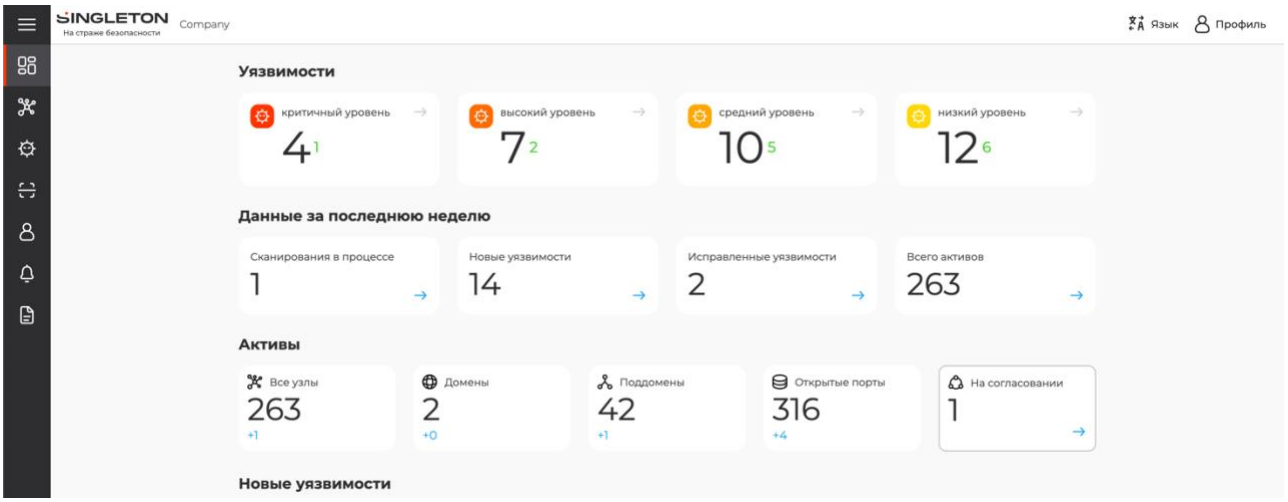

Рисунок 4. Раздел «Главная» личного кабинета пользователя

Для смены языка интерфейса необходимо нажать на кнопку «Язык» в правой верхней части экрана (Рис. 5) и выбрать желаемый язык (Рис. 6).

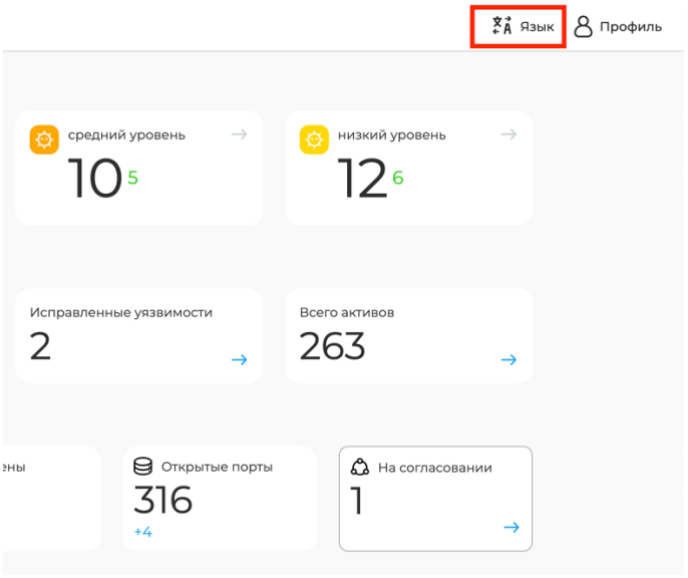

Рисунок 5. Кнопка смены языка интерфейса

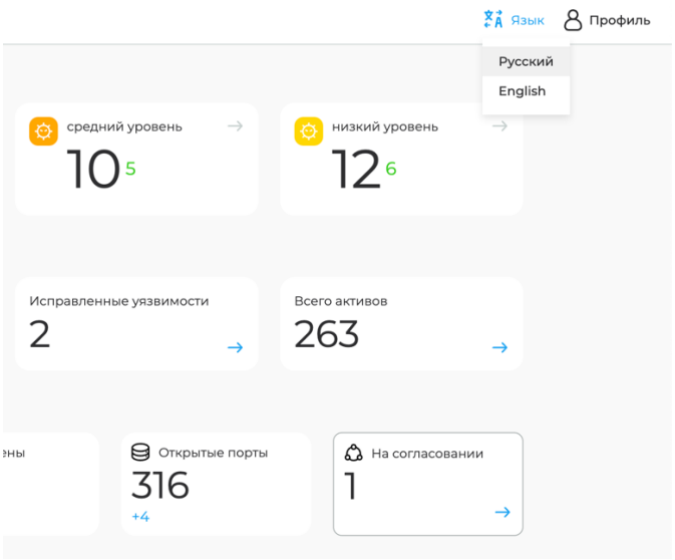

Рисунок 6. Выбор языка интерфейса личного кабинета

3. Работа с профилем пользователя

Для начала работы с профилем пользователя необходимо нажать на кнопку «Профиль» в правом углу интерфейса. После нажатия на указанную кнопку откроется раздел просмотра информации о пользователе (Рис. 7).

Пользователь может редактировать информацию о себе, изменить свой пароль, а также завершить текущую сессию (кнопка – «Выйти из аккаунта).

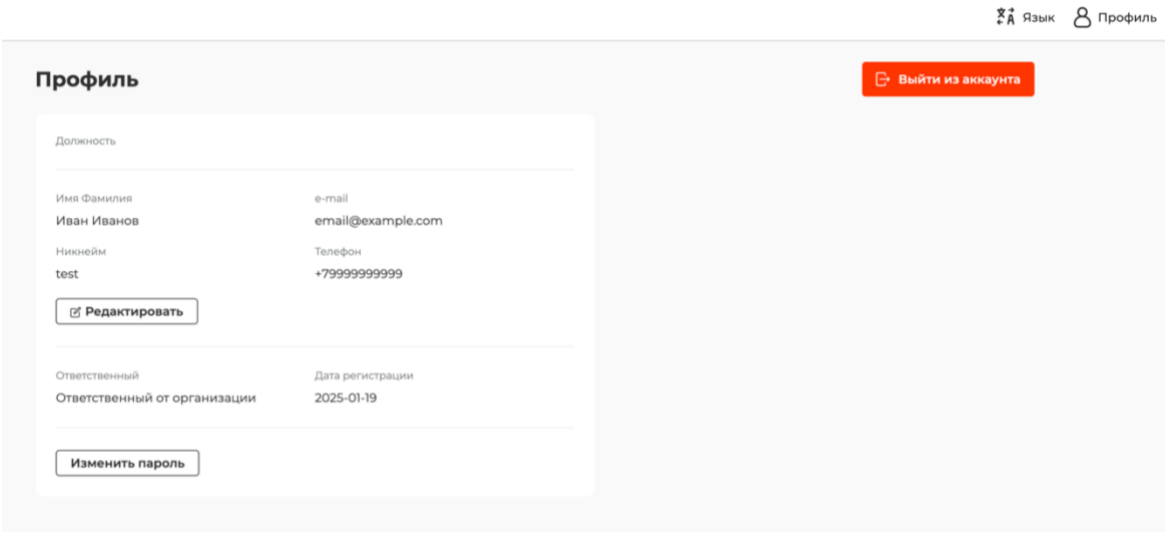

Рисунок 7. Просмотр профиля пользователя

Для редактирования профиля необходимо нажать на кнопку «Редактировать» в карточке пользователя. В результате откроется окно редактирования данных с полями для ввода данных (Рис. 8). Для сохранения введенных изменений необходимо нажать на кнопку «Сохранить». Чтобы вернуться обратно на страницу профиля, следует нажать на кнопку «Назад».

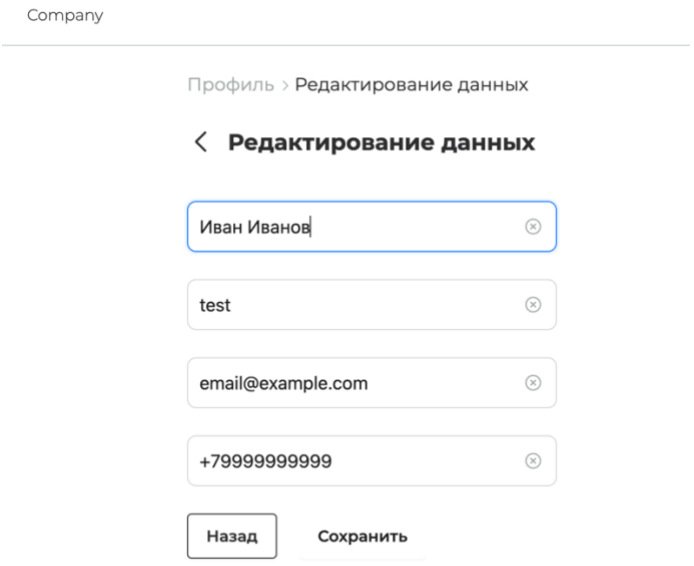

Рисунок 8. Редактирование данных профиля пользователя

Для изменения пароля необходимо нажать на кнопку «Изменить пароль» в карточке пользователя. В результате откроется окно редактирования данных с полями для ввода

паролей (Рис. 9). Для сохранения введенных изменений необходимо нажать на кнопку «Сохранить». Чтобы вернуться обратно на страницу профиля, следует нажать на кнопку «Назад».

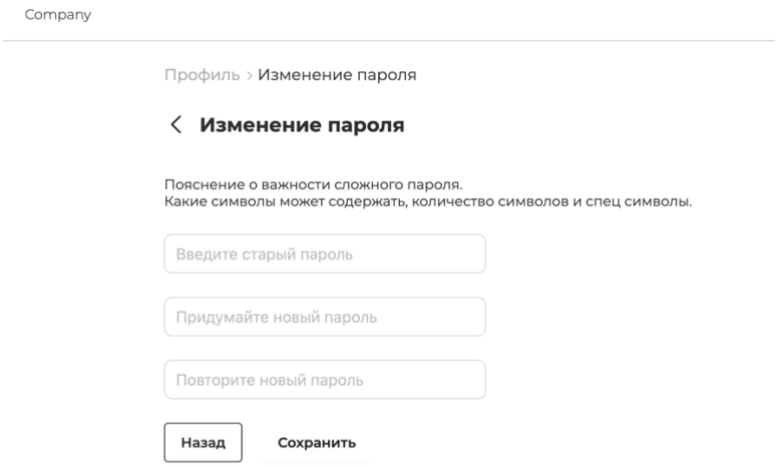

Рисунок 9. Изменение пароля пользователя

4. Раздел «Активы»

Для начала работы с активами необходимо нажать на кнопку «Активы» в левом боковом меню или на кнопку «  » свернутого бокового меню. После нажатия на указанную кнопку откроется таблица с информацией об активах (Рис. 10).

Активы включают IP-адреса и домены и доступны для просмотра по данным категориям раздельно (Рис. 11, Рис. 12). Для переключения между типами активов необходимо нажать на соответствующую вкладку («IP-адреса» или «Домены») в верхней части интерфейса раздела (цифра 1 на Рис. 10).

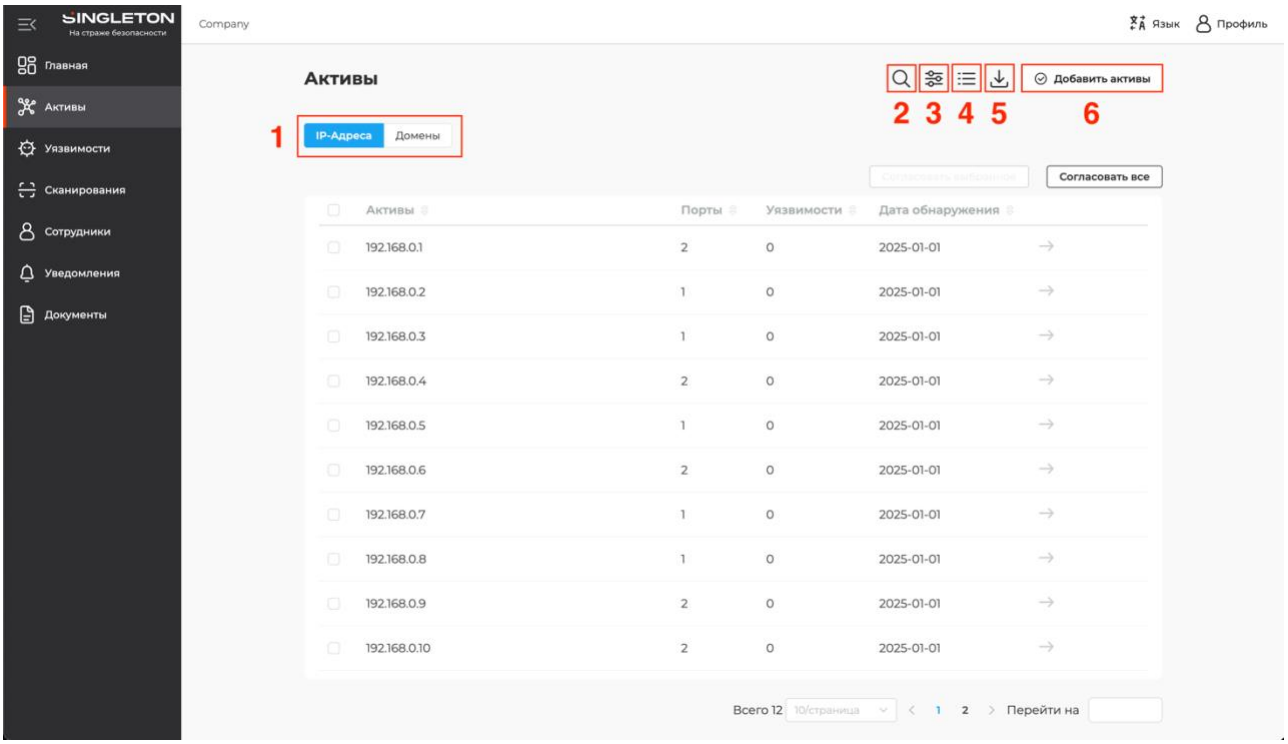

Рисунок 10. Работа с активами организации

Пользователю также доступны:

- поиск активов (цифра 2 на Рис. 10),
- фильтрация активов (цифра 3 на Рис. 10),
- выбор режима просмотра активов (в виде карточек / таблицы) (цифра 4 на Рис. 10),
- выгрузка информации об активах в формате .xlsx (цифра 5 на Рис. 10),
- добавление активов (цифра 6 на Рис. 10).

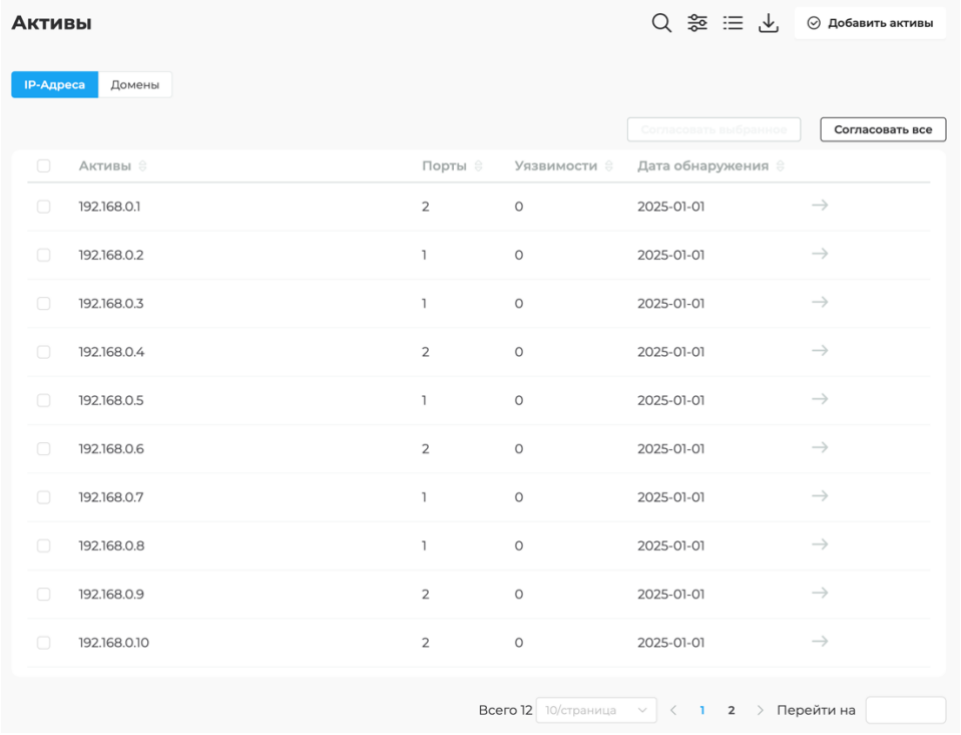

Рисунок 11. Просмотр IP-адресов организации

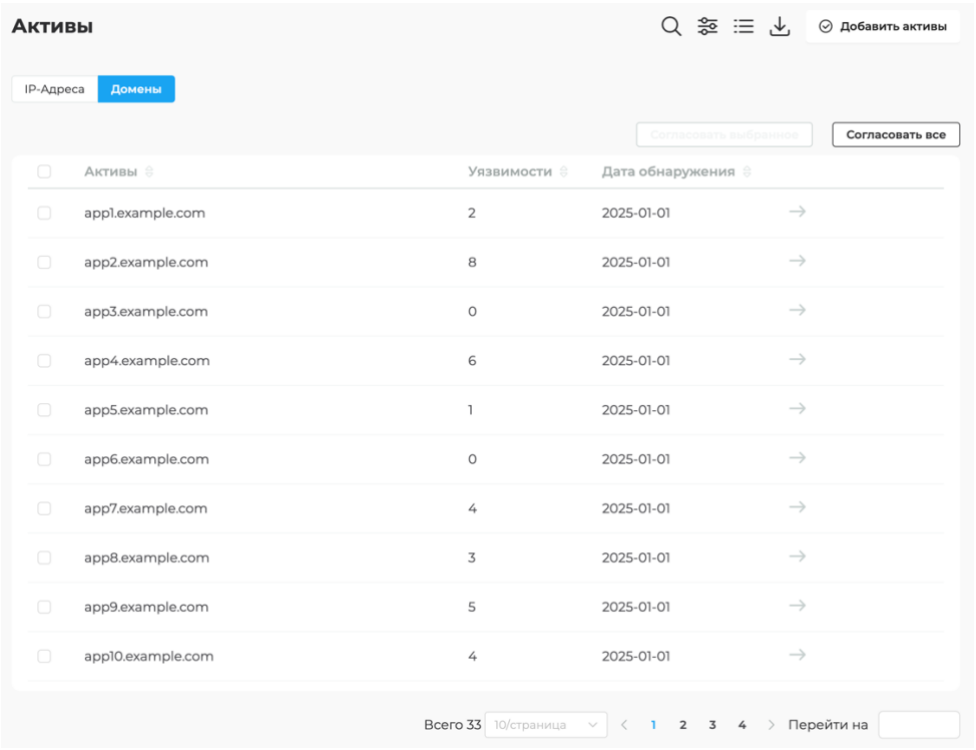

Рисунок 12. Просмотр доменов организации

При просмотре таблицы с активами можно перемещаться по страницам. Для этого следует выбрать нужную страницу в нижней части таблицы или ввести номер страницы в поле для ввода (Рис. 13).

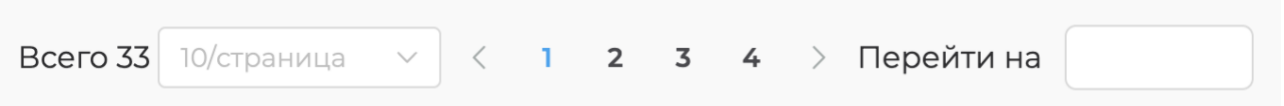

Рисунок 13. Перемещение по страницам

Регулярные сканирования запускаются только для согласованных компанией активов. Для согласования активов необходимо проставить отметку рядом с желаемым активом в соответствующей строке и нажать на кнопку «Согласовать выбранное» (Рис. 14). В случае, когда необходимо согласовать все активы, следует поставить отметку в заголовке таблицы и нажать на кнопку «Согласовать все» (Рис. 15). В таком случае отметка проставится рядом со всеми активами и все активы из списка будут согласованы.

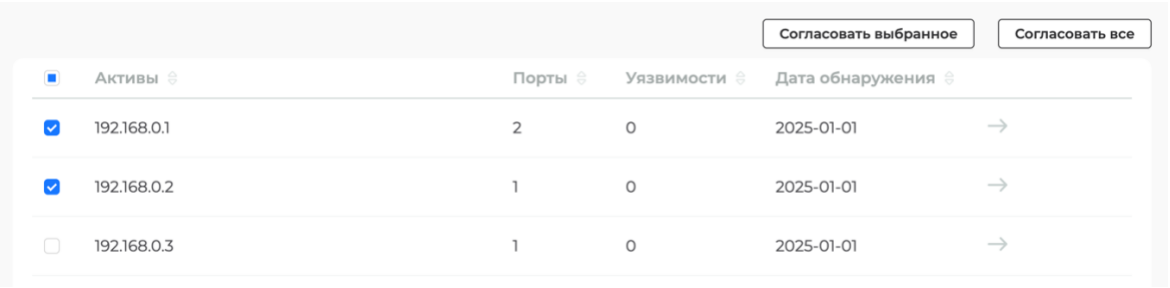

Рисунок 14. Согласование выбранных активов

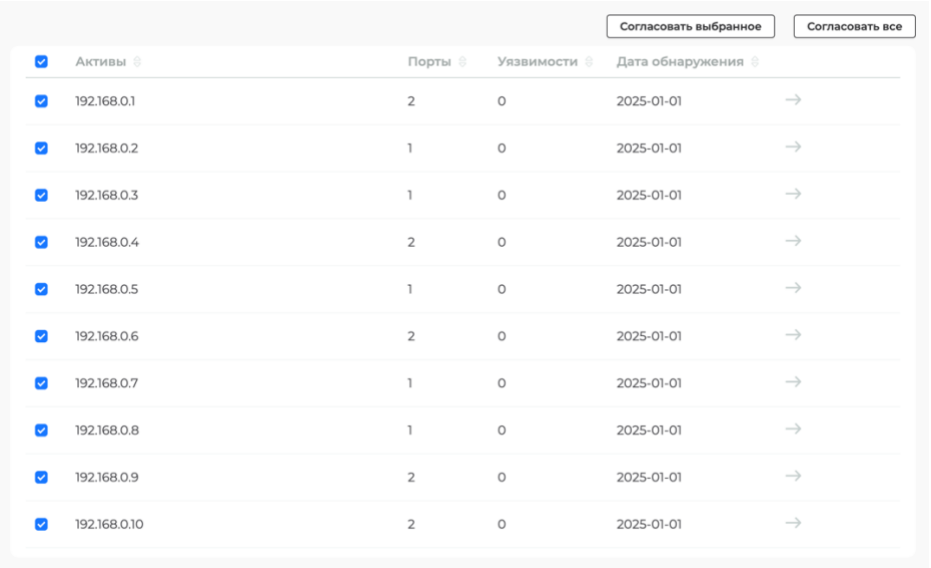

Рисунок 15. Согласование всех активов

При нажатии на кнопку экспорта данных (цифра 5 на Рис. 10) открывается окно конфигурации экспортируемого файла (Рис. 16). Пользователь может поставить / убрать отметки рядом с желаемыми сведениями об активе и нажать на кнопку «Скачать .xlsx» в открывшемся окне. Для возврата к разделу активов необходимо нажать на кнопку «Отмена».

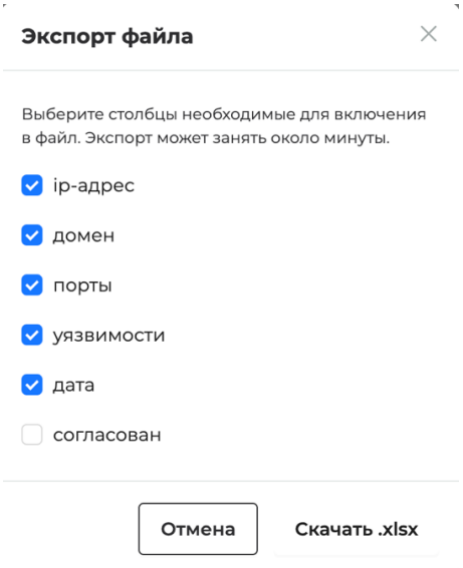

Рисунок 16. Настройка экспортируемых данных об активах

Для добавления новых активов необходимо нажать на кнопку «Добавить активы» (цифра 6 на Рис. 10). В открывшейся вкладке будет доступна форма ввода активов в формате IP-адреса, домена, CIDR и ASN (Рис. 17). Пользователь может вводить активы в любом указанном формате построчно. Для сохранения введенных данных необходимо нажать на кнопку «Добавить», для возврата к странице активов – на кнопку «Назад».

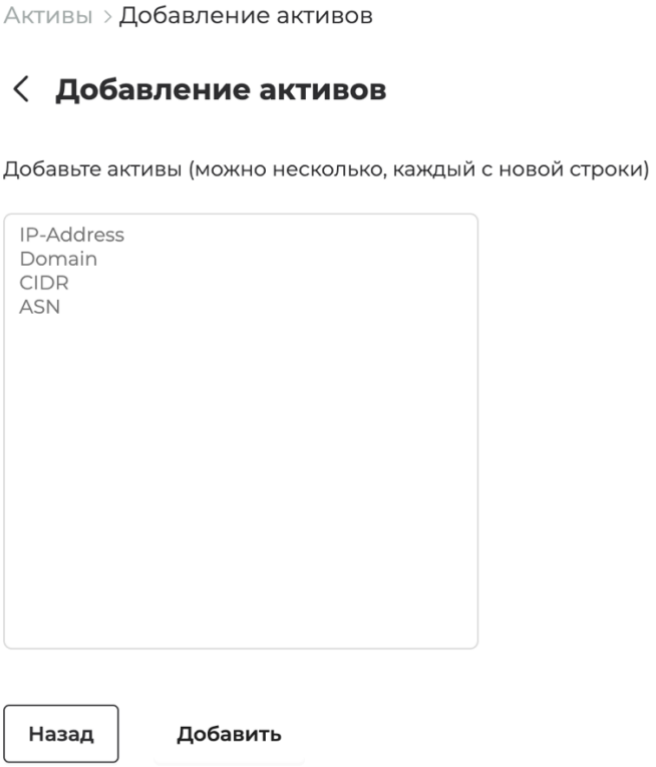

Рисунок 17. Добавление активов

Для просмотра более подробной информации об активе необходимо нажать на кнопку « → » в строке / карточке актива (цифра 1 на Рис. 18).

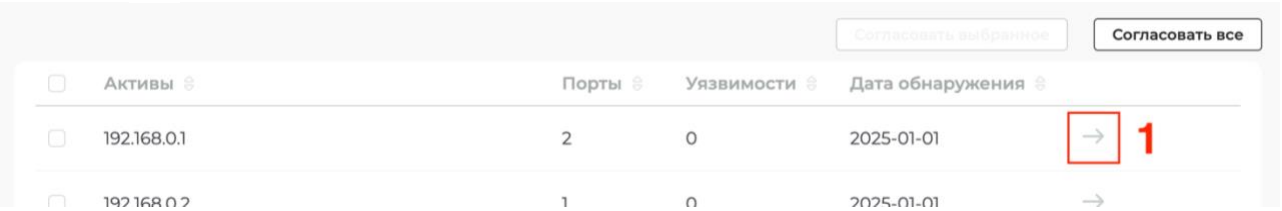

Рисунок 18. Переход на страницу актива

В открывшейся вкладке (Рис. 19) пользователь сможет получить следующую информацию об активе:

- дата обнаружения актива,
- статус согласования,
- сведения об обнаруженных портах,
- найденные уязвимости,
- обнаруженные технологии,
- скриншоты страницы веб-приложения.

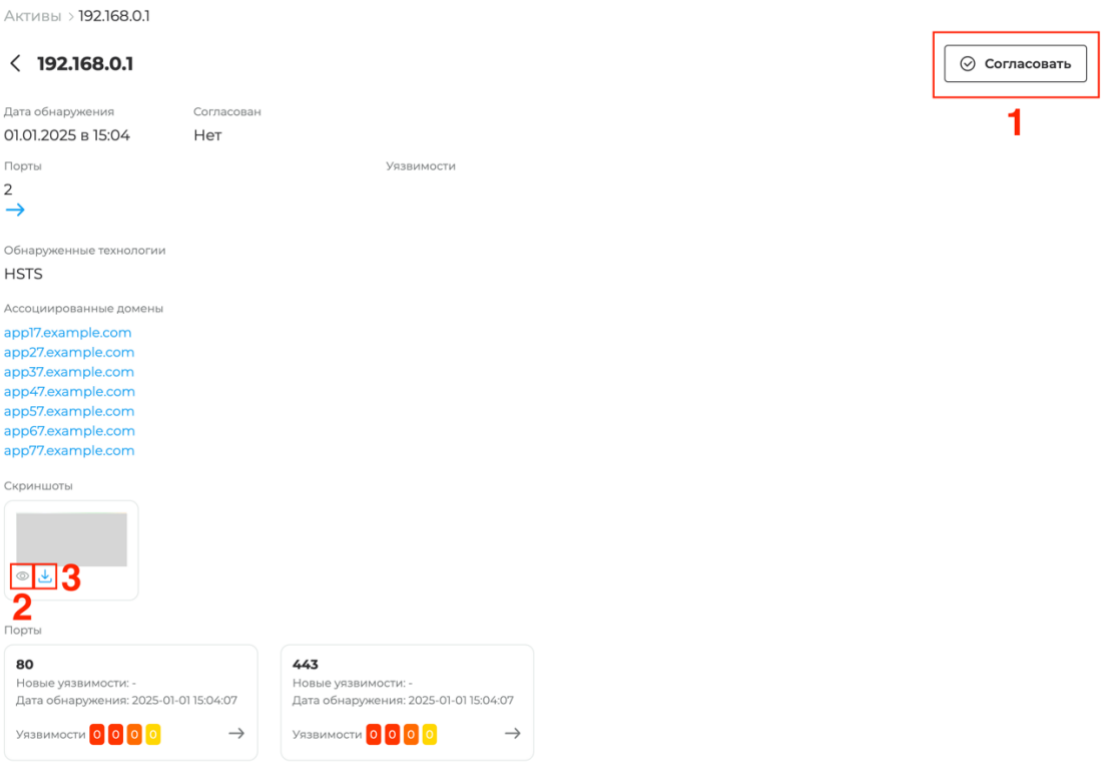

Рисунок 19. Переход на страницу актива

Если актив не согласован, пользователь может его согласовать, нажав на кнопку «Согласовать» в правом верхнем углу вкладки (цифра 1 на Рис. 19).

Пользователь также может посмотреть прикрепленные к активу скриншоты (при наличии) (Рис. 20). Для открытия скриншота необходимо нажать на кнопку « » (цифра 2 на Рис. 19). Для скачивания скриншота необходимо нажать на кнопку « » (цифра 3 на Рис. 19).

При просмотре скриншота возможно уменьшать или увеличивать скриншот с помощью кнопок « » и « » соответственно. Для перемещения между скриншотами необходимо нажимать на кнопки « » и « ». Для закрытия скриншота необходимо нажать на кнопку « ».

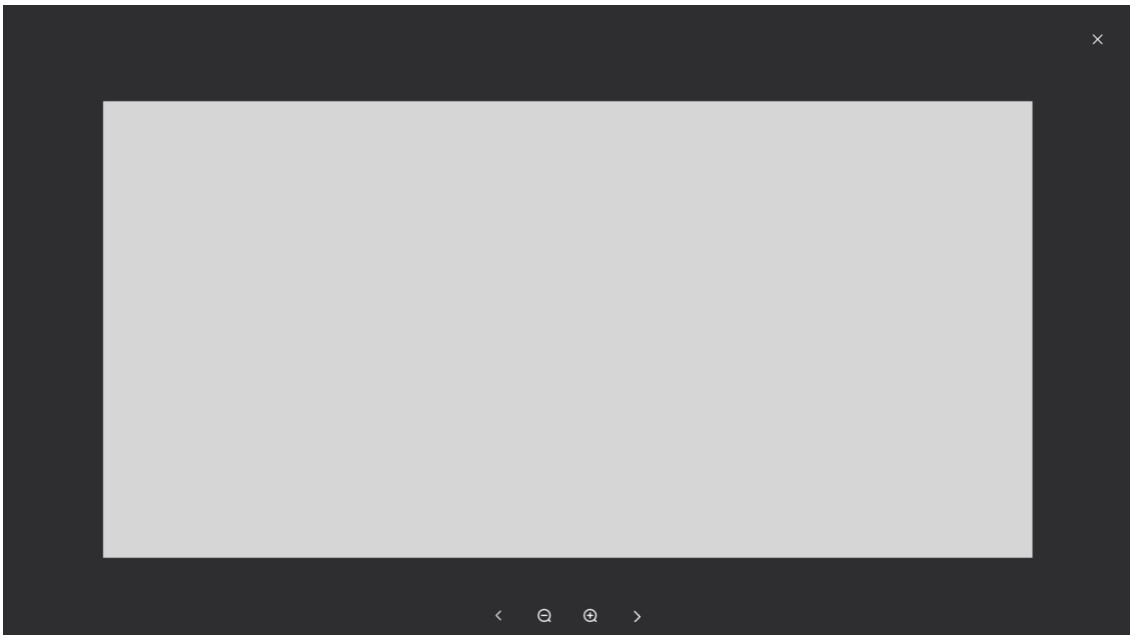

Рисунок 20. Просмотр скриншотов

5. Раздел «Уязвимости»

Для начала работы с уязвимостями необходимо нажать на кнопку «Уязвимости» в левом боковом меню или на кнопку «  » свернутого бокового меню. После нажатия на указанную кнопку откроется таблица с уязвимостями (Рис. 21).

В данном разделе пользователь может:

- получить информацию о найденных уязвимостях,
- выполнить поиск по уязвимостям (цифра 1 на Рис. 21),
- отфильтровать уязвимости (цифра 2 на Рис. 21),
- добавить уязвимость (цифра 3 на Рис. 21),
- перейти в карточку уязвимости (цифра 5 на Рис. 21).

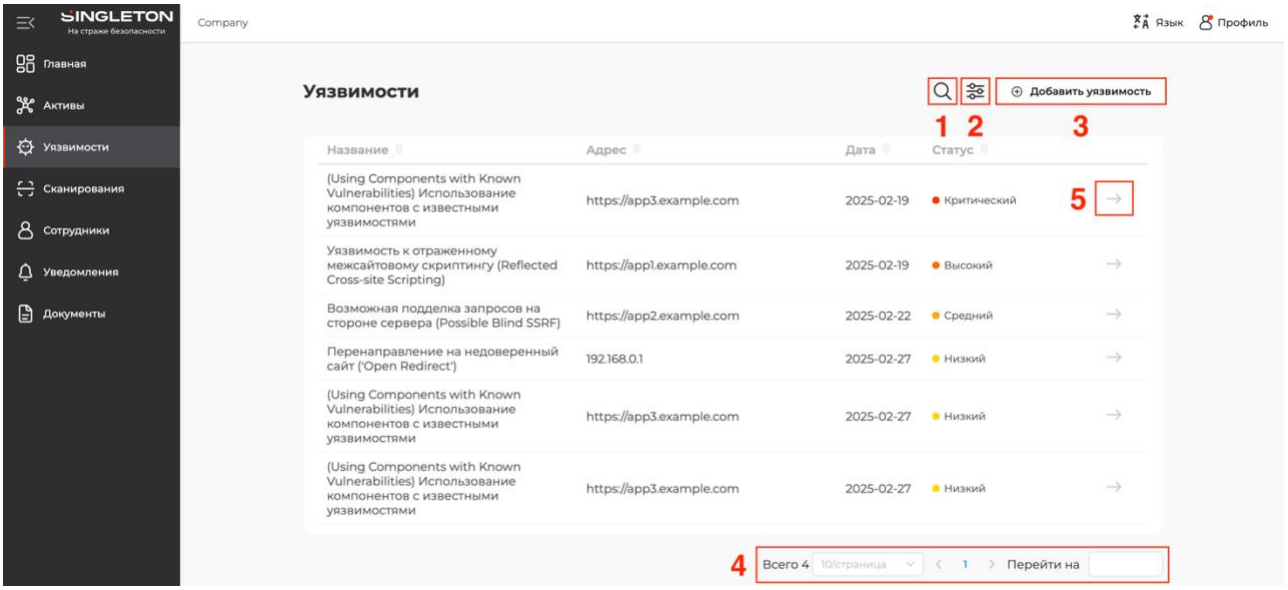

Рисунок 21. Работа с уязвимостями

Для перемещения между страницами с уязвимостями следует выбрать нужную страницу в нижней части таблицы или ввести номер страницы в поле для ввода (цифра 4 на Рис. 21).

Для добавления уязвимости необходимо нажать на кнопку «Добавить уязвимость» (цифра 3 на Рис. 21). В открывшейся вкладке (Рис. 22) будут доступны следующие поля для ввода информации об уязвимости:

- название,
- адрес уязвимого ресурса,
- степень риска,
- описание уязвимости.

Пользователь также может загрузить в карточку уязвимости файлы с устройства (цифра 1 на Рис. 22).

Для добавления уязвимости следует нажать на кнопку «Добавить Уязвимость», расположенную внизу формы. Для возврата к странице уязвимостей необходимо нажать на кнопку «Назад».

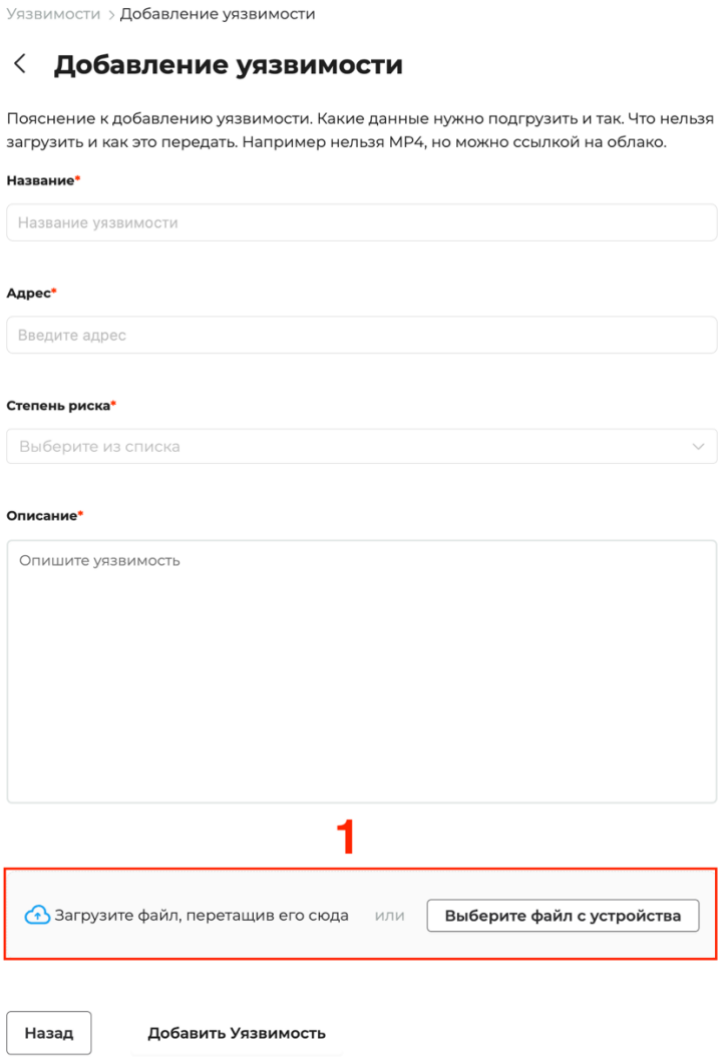

Рисунок 22. Добавление уязвимости

Для перехода в карточку уязвимости следует нажать на кнопку « → » в строке уязвимости (цифра 5 на Рис. 21). Открывшаяся вкладка позволяет получить информацию об уязвимости и вести переписку со специалистами ООО «ЗАЩИЩЕННЫЕ СИСТЕМЫ» (Рис. 23, Рис. 24).

Рисунок 23. Просмотр карточки уязвимости (часть 1)

Рисунок 24. Просмотр карточки уязвимости (часть 2)

В случае, когда необходимо открыть уязвимость, следует нажать на кнопку «Открыть уязвимость», расположенную в правом верхнем угле вкладки, и в открывшемся окне нажать на кнопку «Да». В ином случае следует нажать на кнопку «Отмена».

Карточка уязвимости также позволяет оставлять комментарии к уязвимости (цифра 1 на Рис. 24). К комментарию можно прикрепить файлы (цифра 2 на Рис. 24). Для добавления комментария следует нажать на кнопку «Добавить комментарий». Для перемещения между комментариями можно прокручивать страницу, а также использовать окно перемещения между страницами (цифра 3 на Рис. 24).

Для просмотра прикрепленных к уязвимости скриншотов необходимо нажать на кнопку « » (цифра 4 на Рис. 24). Для скачивания скриншота необходимо нажать на кнопку « » (цифра 5 на Рис. 24).

При просмотре скриншота возможно уменьшать или увеличивать скриншот с помощью кнопок « » и « » соответственно. Для перемещения между скриншотами необходимо нажимать на кнопки « » и « ». Для закрытия скриншота необходимо нажать на кнопку « ».

Для возврата из карточки уязвимости к списку всех уязвимостей следует нажать на кнопку «Назад», расположенную в нижней левой части вкладки уязвимости.

6. Раздел «Сканирования»

Для работы со сканированиями необходимо нажать на кнопку «Сканирования» в левом боковом меню или на кнопку «  » свернутого бокового меню. После нажатия на указанную кнопку откроется таблица со сканированиями (Рис. 25).

В данном разделе пользователь может:

- получить информацию о запущенных сканированиях (тип сканирования, дата запуска и статус сканирования),
- выполнить поиск по сканированиям (цифра 1 на Рис. 25),
- отфильтровать сканирования (цифра 2 на Рис. 25).

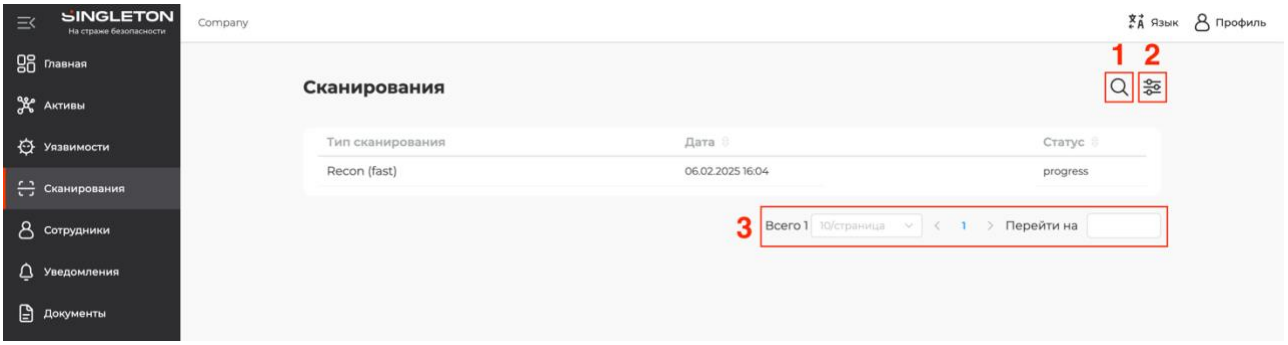

Рисунок 25. Работа со сканированиями

Для перемещения между страницами со сканированиями следует выбрать нужную страницу в нижней части таблицы или ввести номер страницы в поле для ввода (цифра 3 на Рис. 25).

7. Раздел «Сотрудники»

Для работы с сотрудниками необходимо нажать на кнопку «Сотрудники» в левом боковом меню или на кнопку «  » свернутого бокового меню. После нажатия на указанную кнопку откроется таблица с сотрудниками (Рис. 26).

В данном разделе пользователь может:

- посмотреть список сотрудников организации,
- выполнить поиск по сотрудникам (цифра 1 на Рис. 26),
- отфильтровать сотрудников (цифра 2 на Рис. 26),
- добавить сотрудника,
- перейти в карточку сотрудника (цифра 4 на Рис. 26).

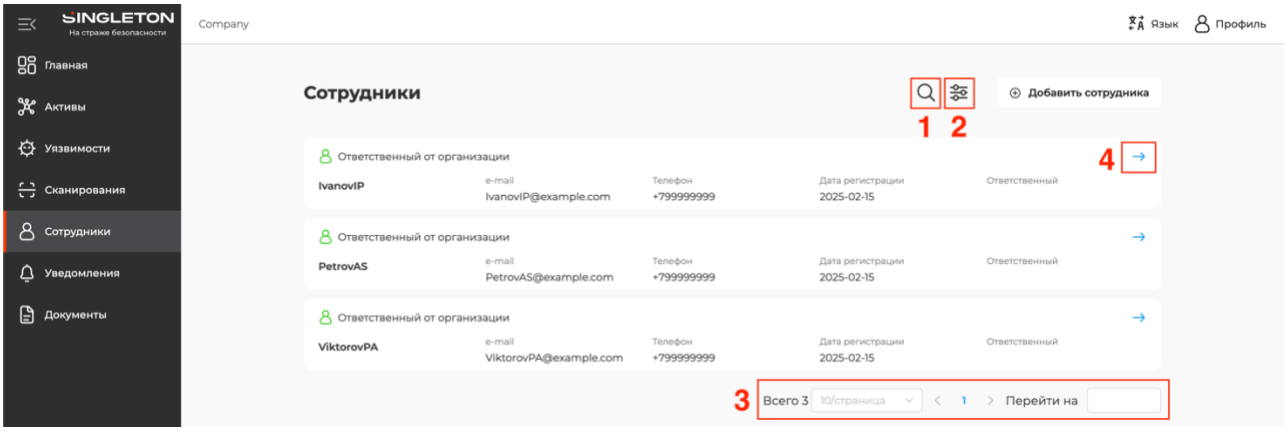

Рисунок 26. Работа с сотрудниками

Для перемещения между страницами с сотрудниками следует выбрать нужную страницу в нижней части таблицы или ввести номер страницы в поле для ввода (цифра 3 на Рис. 26).

Для добавления сотрудника необходимо нажать на кнопку «Добавить сотрудника», расположенную в правой верхней части раздела. В результате откроется форма добавления сотрудника с доступными полями для ввода информации. Для добавления сотрудника необходимо нажать на кнопку «Пригласить», для возврата к странице с таблицей сотрудников – нажать на кнопку «Назад». После приглашения сотрудника на введенный адрес электронной почты придет письмо с одноразовым паролем для входа.

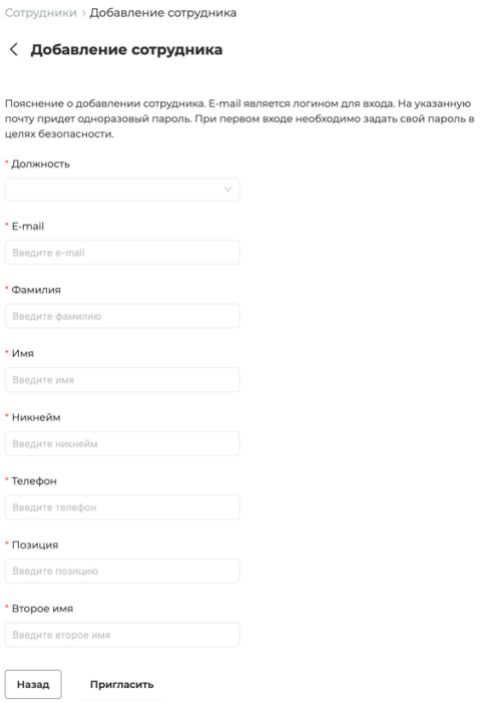

Рисунок 27. Работа с сотрудниками

Для перехода к карточке сотрудника необходимо нажать на кнопку « → » в строке сотрудника (цифра 4 на Рис. 26). Если пользователь имеет роль «Менеджер», в открывшейся вкладке он сможет получить информацию о пользователе (Рис. 27) и сбросить пользователю пароль (путем нажатия на кнопку «Сбросить пароль»). В случае, если роль пользователя – «IT-инженер», получить доступ к карточке сотрудника, не удастся.

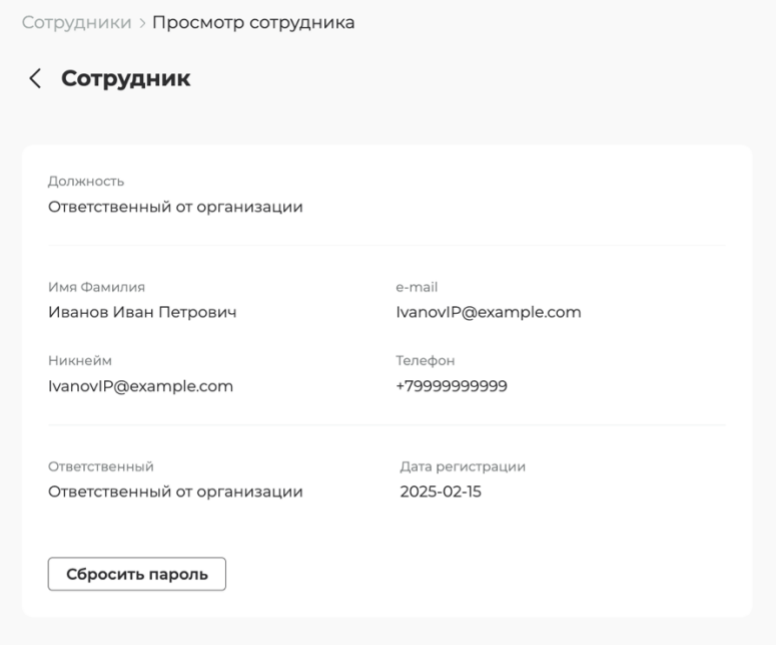

Рисунок 27. Просмотр карточки сотрудника

8. Раздел «Уведомления»

Для работы с уведомлениями необходимо нажать на кнопку «Уведомления» в левом боковом меню или на кнопку «  » свернутого бокового меню. После нажатия на указанную кнопку откроется список уведомлений (Рис. 28).

В данном разделе пользователь может:

- посмотреть сведения о системных сообщениях,
- выполнить поиск по уведомлениям (цифра 1 на Рис. 28),
- отфильтровать уведомления (цифра 2 на Рис. 28),
- прочитать уведомления,
- сконфигурировать отправку уведомлений.

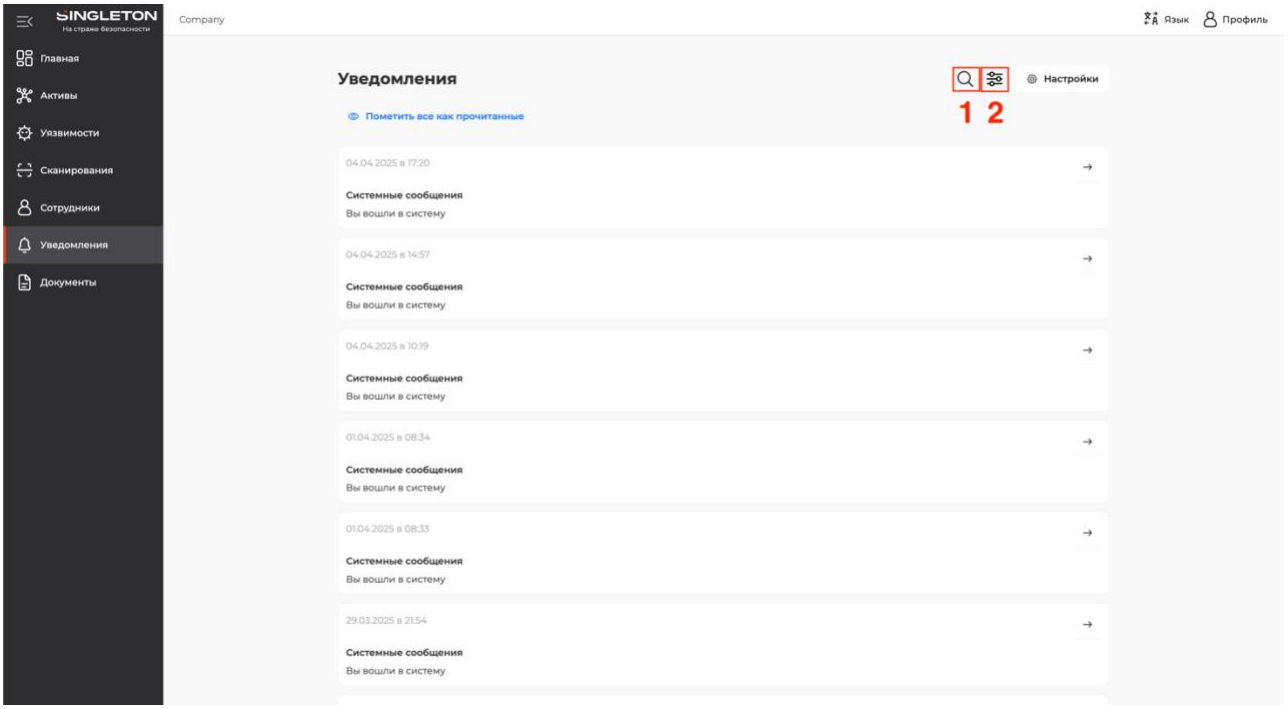

Рисунок 28. Работа с уведомлениями

Для того, чтобы отметить все системные сообщения, как прочитанные, необходимо нажать на кнопку «Пометить все как прочитанные» в верхней левой части раздела.

Для конфигурации отправки уведомлений следует нажать на кнопку «Настройки», расположенную в правой верхней части раздела. В результате откроется вкладка настроек (Рис. 29). Для конфигурации уведомлений следует поставить отметки рядом с выбранной настройкой. Для подключения уведомлений следует нажать на кнопку «Подключить уведомления», расположенную в правой верхней части вкладки.

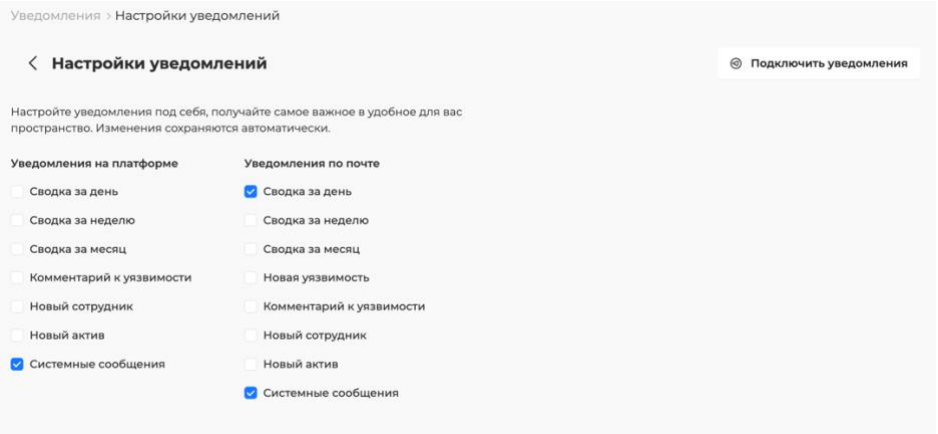

Рисунок 29. Настройка уведомлений

9. Раздел «Документы»

Для работы с документами необходимо нажать на кнопку «Документы» в левом боковом меню или на кнопку «  » свернутого бокового меню. После нажатия на указанную кнопку откроется список документов (Рис. 30).

В данном разделе пользователь может:

- посмотреть информацию о загруженных документах,
- связаться с ботом технической поддержки (путем нажатия на кнопку «Написать нам»).

Рисунок 30. Работа с документами