Общество с ограниченной ответственностью
"АН-СЕКЬЮРИТИ КИБЕР-БЕЗОПАСНОСТЬ"
195027, Санкт-Петербург, ул. Конторская, д.11, литера А, офис 421
+7 (812) 318 4000, доб. 2222
an-cyber.ru

An-Canary

Управление навыками информационной безопасности сотрудников

руководство пользователя

1. Общая информация – назначение, область применения, уровень подготовки

Web-приложение «AN-Canary» предназначено для тестирования сотрудников предприятий на знание основ кибербезопасности и цифровой гигиены. Для этого используются канареечные токены (цифровые маячки). Имеется возможность создания групповых тестирований с рассылкой сгенерированных токенов на e-mail адреса целей, а также создание индивидуальных токенов различных типов для выборочной проверки сотрудников.

Для кого разработано: операторы SoC (security operation center), администраторы ИБ, системные администраторы.

Уровень подготовки пользователей: базовый пользователь ПК.

Уровень подготовки администраторов: продвинутый пользователь ПК.

2. Условия использования

Наличие любого браузерного приложения.

3. Компоненты приложения

Два основных компонента приложения – сервер Nginx и стек контейнеров docker-compose, в котором запущены все основные элементы функционирования программного продукта (ПП).

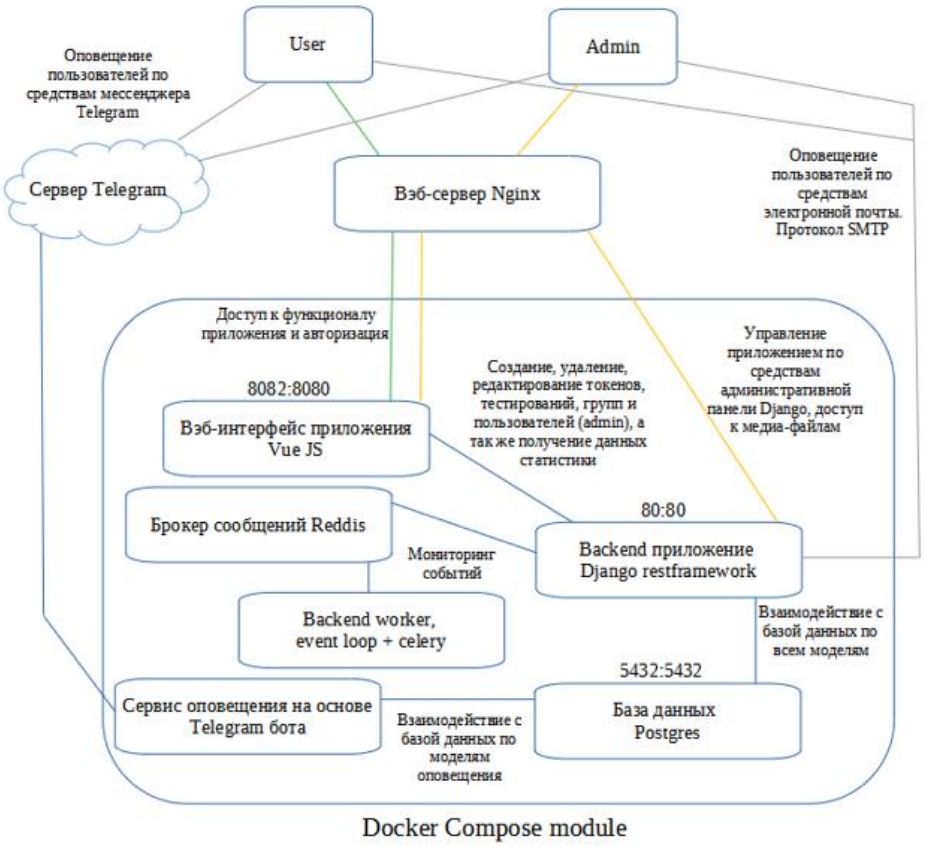

Рис.1 Основные компоненты ПП

4. Запуск приложения

Получить доступ к web-интерфейсу приложения можно получить на сайте https://an-canary.ru/ по предоставленным учетным данным.

Доступ для ознакомления с внутренней структурой ПП и его компонентами можно получить по предоставленному адресу и учетным данным.

5. Принцип функционирования

Приложение представляет из себя web-интерфейс с тремя видами пользовательских прав: клиент, модератор и администратор.

Клиентский интерфейс предусматривает создание как одиночных канареечных токенов (цифровая ловушка, отправляющая создателю уведомление о срабатывании) различных видов (url-ссылки, qr-коды, папки Windows и исполняемые файлы), так и групповых фишинг-тестов с функционалом автоматической рассылки фишинговых писем на почтовые ящики сотрудников (далее - цель) выбранной проверочной группы (далее - группа), а так же тестов (далее - тест) с возможностью автоматической рассылки группе. Клиентский интерфейс также позволяет создавать, редактировать состав и удалять проверочные группы; изменять настройки уведомлений фишинг-тестов; удалять токены, тесты и фишинг-тесты; редактировать их настройки, а также просматривать статистику по фишинг-тестам и сводную статистику по группе.

Пользователь с правами «модератор» может приглашать в приложение других пользователей (на почтовый ящик приглашенного отправляется письмо с данными для регистрации).

Интерфейс администратора расширен функционалом редактирования списка пользователей приложения, а также возможностью просмотра созданных другими пользователями токенов, фишинг- тестов и групп.

Приложение поддерживает возможность отправки уведомлений посредством мессенджера Telegram. Для этого используется телеграмм-бот, функционирующий на отдельном сервере. Привязка Telegram ID к аккаунту приложения происходит через регистрацию идентификатора аккаунта в интерфейсе бота. В результате пользователь получает возможность в онлайн режиме принимать уведомления о срабатывании созданных им токенов в мессенджере Telegram.

6. Проверка работоспособности

В случае если ПП не запускается, то следует обратиться по электронной почте или телефону, указанному на коробке или в колонтитулах данного документа. Перед обращением подготовьте информацию о покупателе для идентификации.

7. Руководство пользователя

Для доступа к функционалу приложения необходима авторизация в системе, которая основана на токенах доступа, генерируемых бэкенд-фреймворко Django Restframework с дополнительной валидацией фронтенд-фреймворка VueJS.

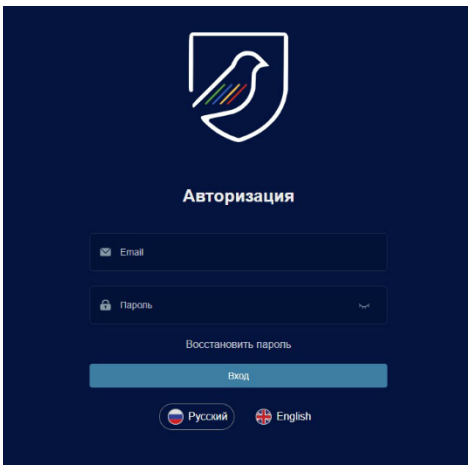

Рис.1. Окно авторизации для входа в систему.

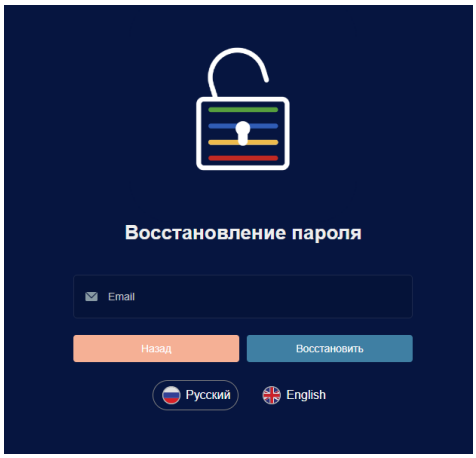

Рис. 2. Окно восстановления пароля.

Для восстановления пароля необходимо ввести e-mail адрес, который уже был зарегистрирован в системе. Далее на указанный почтовый ящик будет отправлено письмо с ссылкой для перехода на страницу восстановления пароля.

Рис. 3. Письмо с ссылкой для восстановления пароля

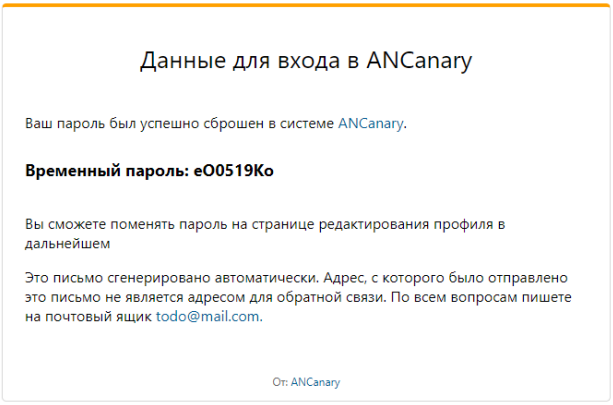

Рисунок 4. Письмо с временным паролем для входа в систему

После входа в систему пользователь попадает на домашнюю страницу приложения. В левой стороне окна присутствует панель навигации для доступа к различным страницам приложения.

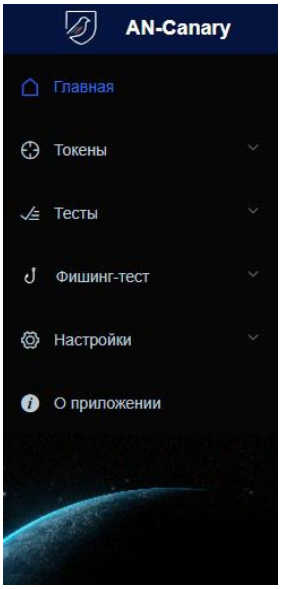

Рисунок 5. Боковая панель навигации.

На домашней странице присутствует 4 панели, на которых отображается различная информация приложения. Слева расположена карточка пользователя, в которой представлена краткая общая статистика пользователя, аватар пользователя с возможностью настройки (выбор из предоставленного списка). Сверху посередине карточка активностей в приложении, где отображены действия пользователя по созданию, удалению токенов, групп, тестирований, а также по срабатыванию одиночных токенов в порядке от новых к старым. Элементы в таймлайне активностей при клике переадресовывают на соответствующие страницы. Справа сверху расположена карточка редактирования профиля. В обычном состоянии поля в ней отключены для редактирования. При нажатии кнопки «настройка» поля становятся активными. В карточке редактирования профиля пользователь может сменить свои имя, фамилию, e-mail адрес, произвести отвязку аккаунта от Telegram, а также изменить пароль. В нижней части страницы расположена карточка, в которой отображается статистика по последней проверке с кнопкой для перехода на страницу статистики.

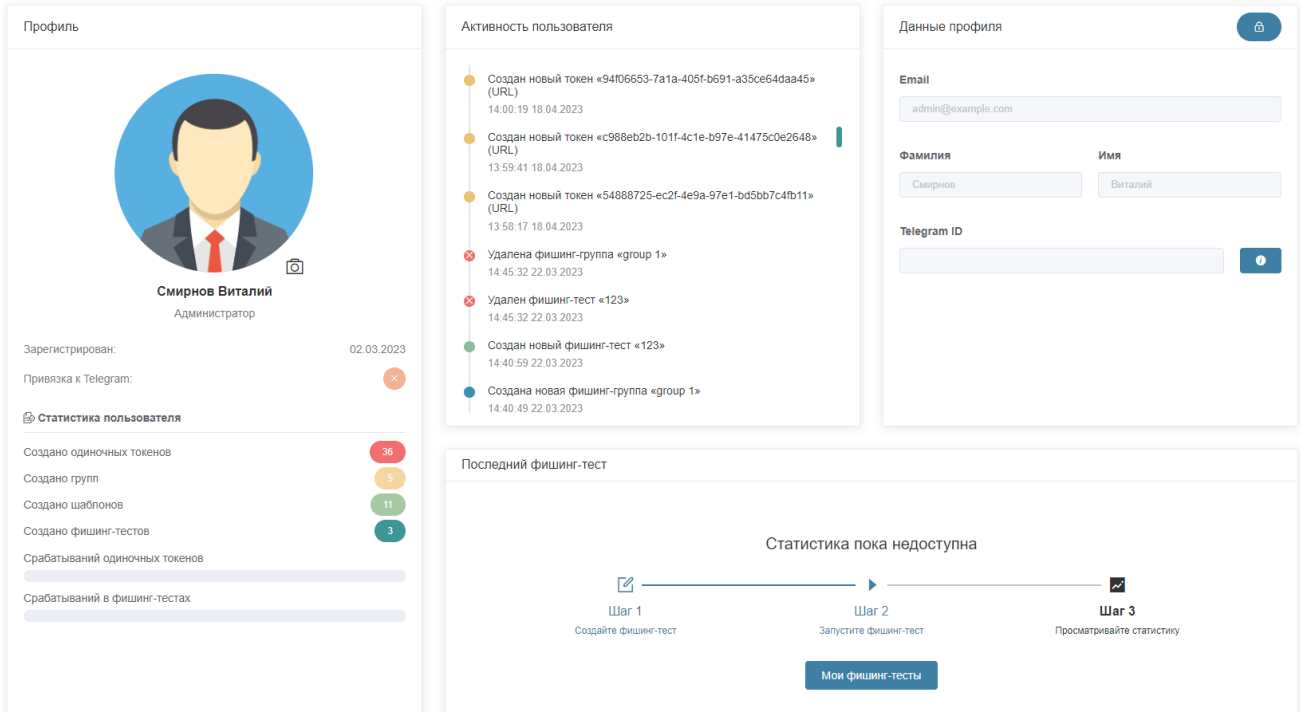

Рис. 6. Внешний вид домашней страницы.

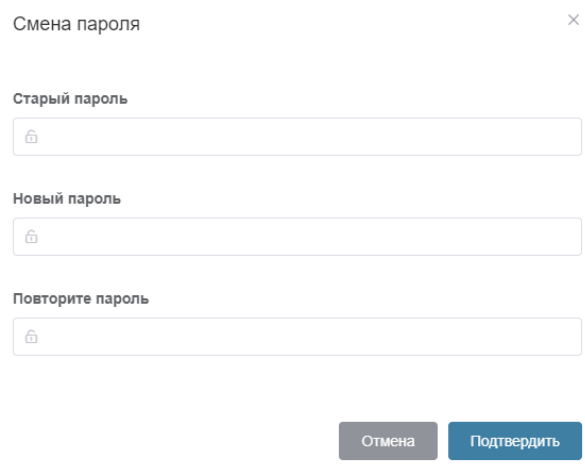

Рис. 7. Модальное окно смены пароля.

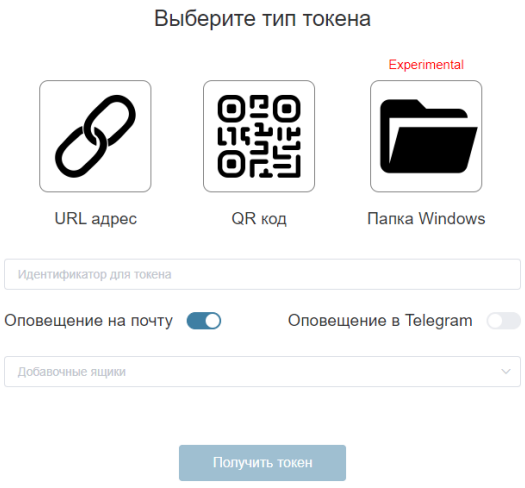

Рис. 8. Окно создания токена.

В окне создания токена необходимо выбрать тип токена в выпадающем списке. От типа токена зависят дополнительные поля. При выборе типов «URL адрес» и «qr-код» появляется поле «Ссылка для перенаправления» (при переходе по ссылке токена пользователь будет незаметно переадресован на указанную в этом поле страницу). При выборе типа «Папка Windows» появляется опция «невидимая папка», включение которой сделает созданный токен-папку невидимой в проводнике. Поле «Напоминание для токена» служит для персонализации токена в системе и указывается в дальнейшем в уведомлениях при срабатываниях. Переключатели «оповещение на почту», «Оповещение в Telegram» включают/выключают уведомления на почту и в мессенджер Telegram (в том случае, если к аккаунту привязан Telegram ID). Поле «Добавочные ящики» позволяет прикрепить к токену дополнительные e-mail адреса для уведомлений. Добавление осуществляется вводом адреса и нажатием клавиши <Enter>.

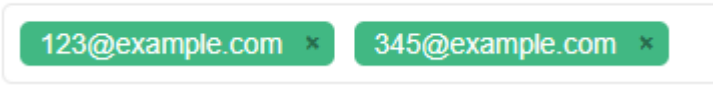

Рис. 9. Поле «добавочные ящики».

После создания токена типа «URL-адрес» пользователь переадресовывается на страницу получения ссылки. Вы сможете скопировать сгенерированную ссылку и воспользоваться ей по своему усмотрению или сгенерировать HTML-код, имитирующий иконки популярных приложений для офиса, для вставки в электронное письмо.

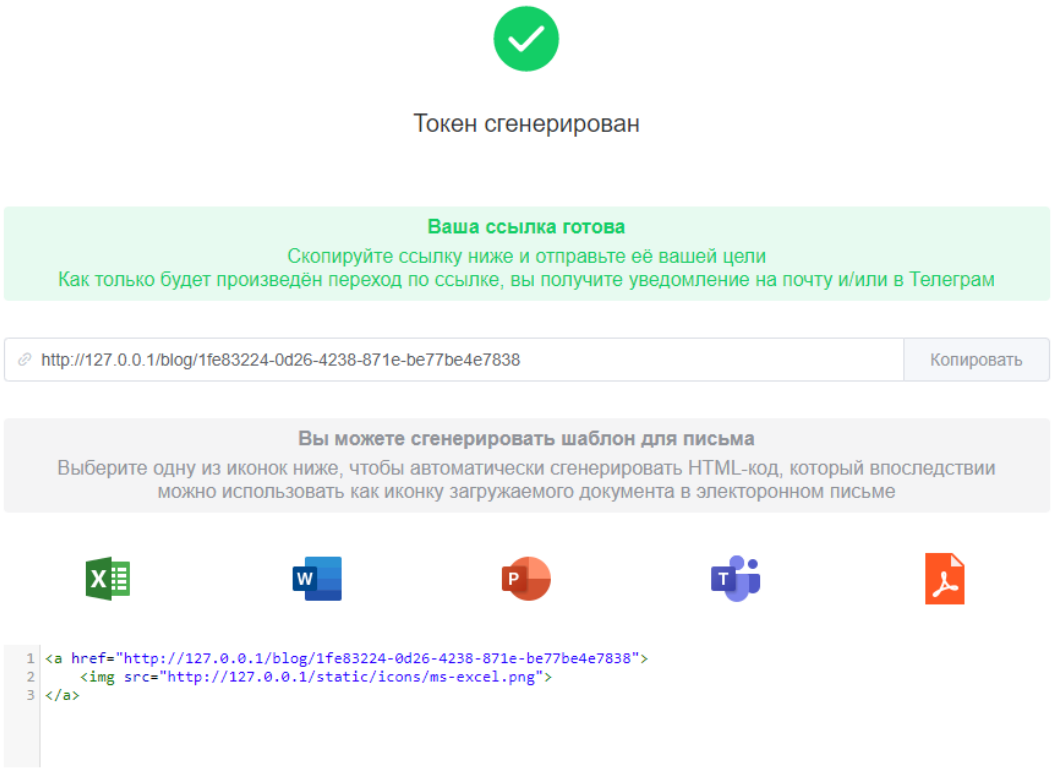

Рис. 10. Страница получения ссылки.

После создания токена типа «Папка Windows» и «Исполняемый файл» пользователь переадресовывается на страницу получения файла. Файл скачивается в виде архива в формате .zip. После скачивания файла можно использовать его по своему усмотрению (например, распаковать в директорию, доступ к которой не должны получить посторонние).

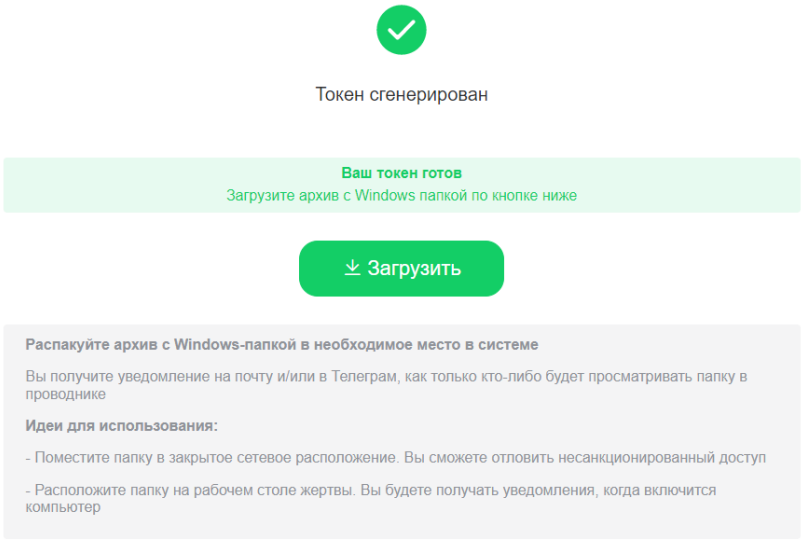

Рис. 11. Страница получения файла

После создания токена типа «qr-код» пользователь переадресовывается на страницу получения qr-кода, где сможет открыть файл как картинку в браузере и скачать ее. Далее картинку можно использовать по своему усмотрению.

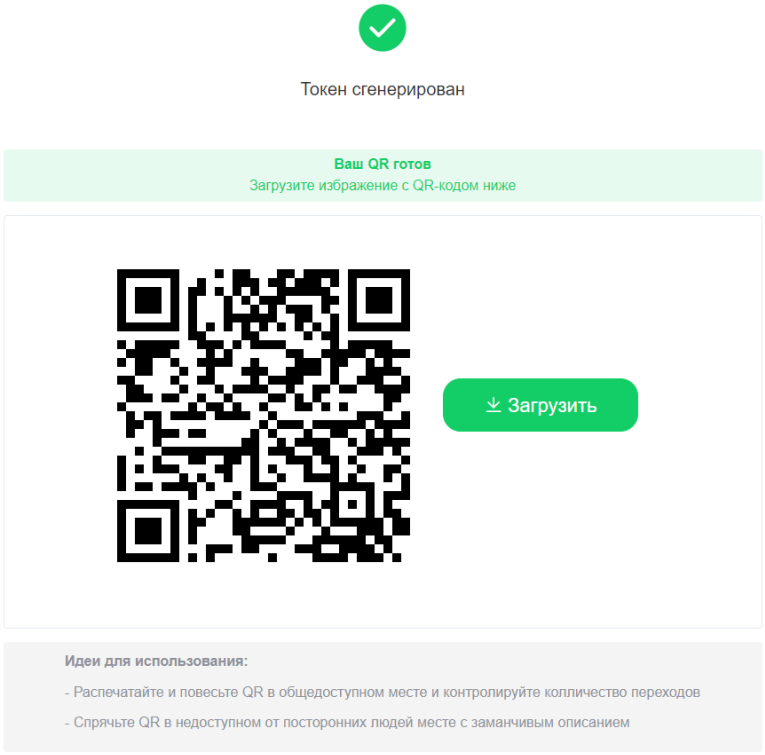

Рисунок 12. Страница получения «qr-кода»

Страница управления созданными одиночными токенами представляет из себя таблицу со списком токенов. В столбце «Токен», в зависимости от его типа, находится кнопка с возможностью скопировать ссылку или скачать файл. В столбце «Срабатывания», если по данному токену были срабатывания имеется ссылка для перехода на страницу просмотра инцидентов. В столбце «Действия» можно редактировать настройки токена (настройки уведомлений, дополнительных почтовых ящиков, напоминание для токена), удалять ненужные токены. В верхней панели находится поле ввода для поиска токенов по напоминаниям, кнопка для перехода на страницу создания токенов и, в случае если пользователь является администратором – переключатель «Все токены/только свои».

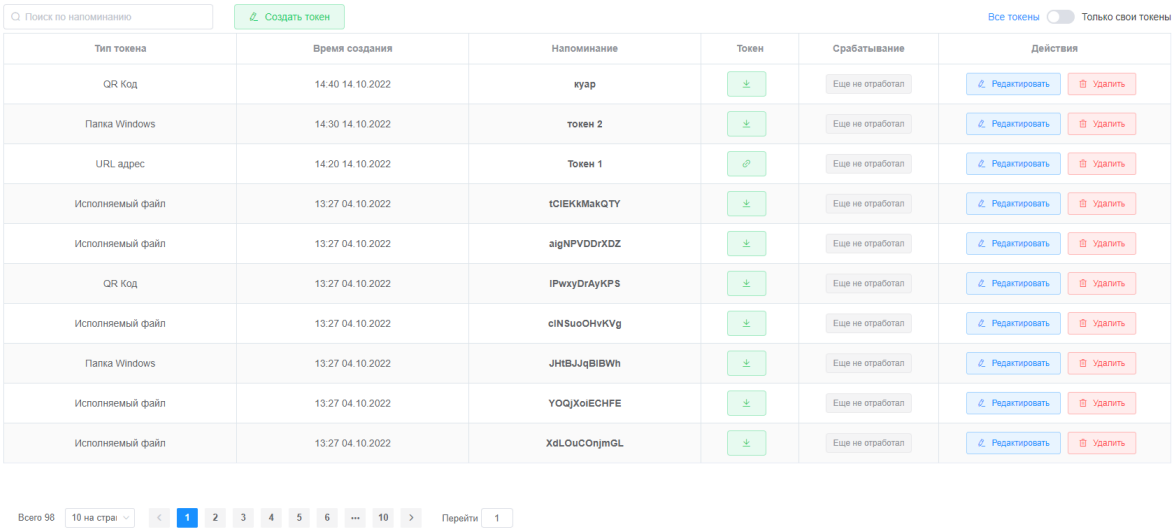

Рис. 13. Страница управления токенами.

На странице инцидентов представлен выпадающий список инцидентов, при нажатии на который отображается детальная информация по каждому инциденту. В правом верхнем углу списка присутствует кнопка загрузки отчета в форматах Excel, JSON, CSV. С левой стороны страницы расположена карта, где отмечается геопозиция устройств, с которых происходили переходы по токенам (данная информация является ознакомительной и не дает 100% точность отображения координат).

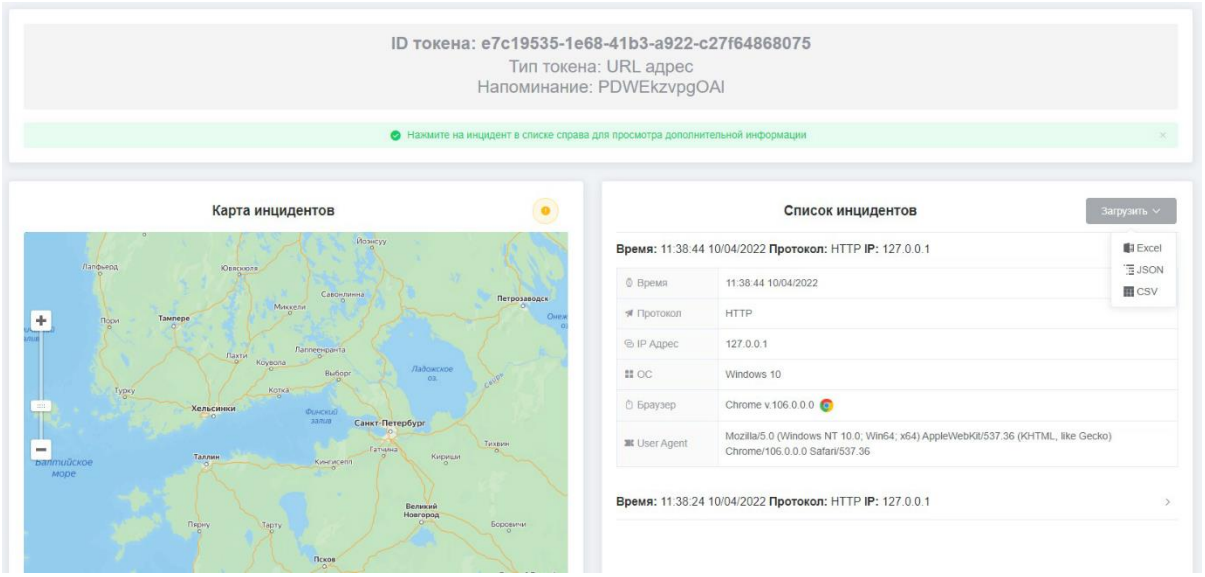

Рис. 14. Страница инцидентов.

Создание фишинг-теста проходит в 4 этапа. На первом – из выпадающего списка выбирается группа для фишинг-теста.

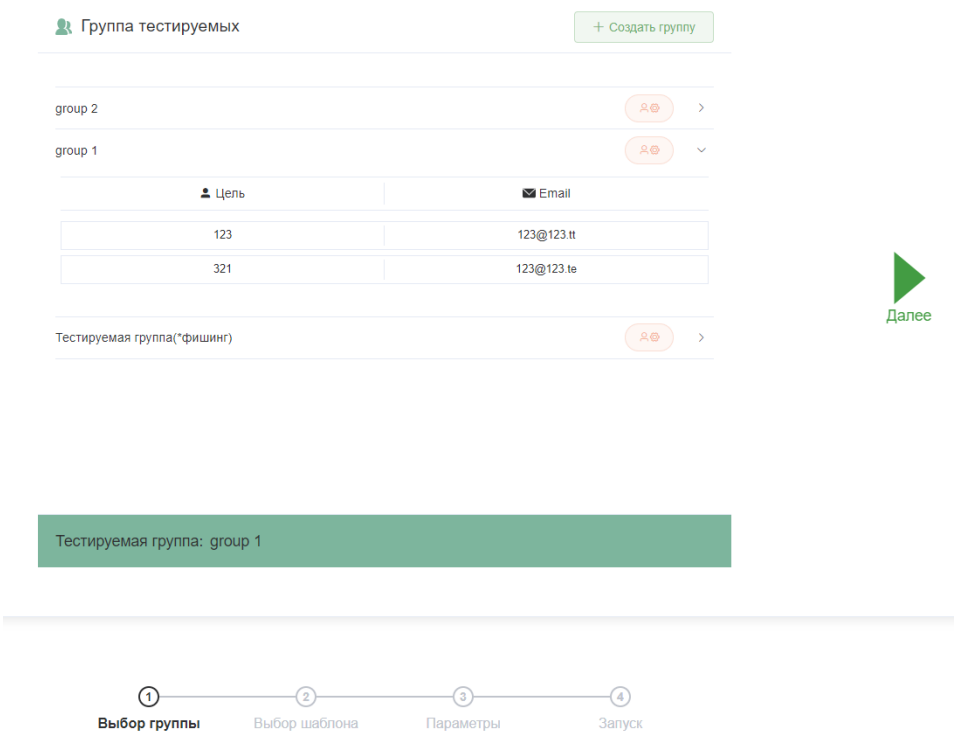

Рис. 15. Первый этап создания фишинг-теста.

На втором этапе происходит выбор шаблона фишингового письма. Переключение между шаблонами происходит при нажатии на нужный шаблон или при переключении «карусели» стрелками по бокам элемента.

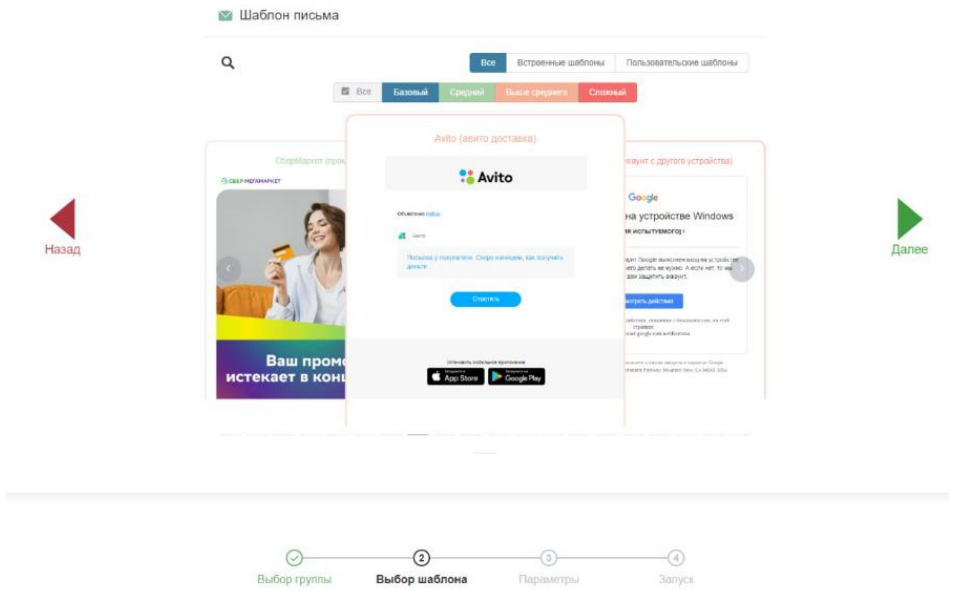

Рис. 16. Второй этап создания тестирования.

На третьем этапе создания фишинг-теста указывается название фишинг-теста и параметры уведомлений при срабатываниях. Так же можно выбрать заранее созданный тест, который будет отправлен цели фишинг-теста на почтовый ящик в том случае, если она перейдет по ссылке в фишинговом письме.

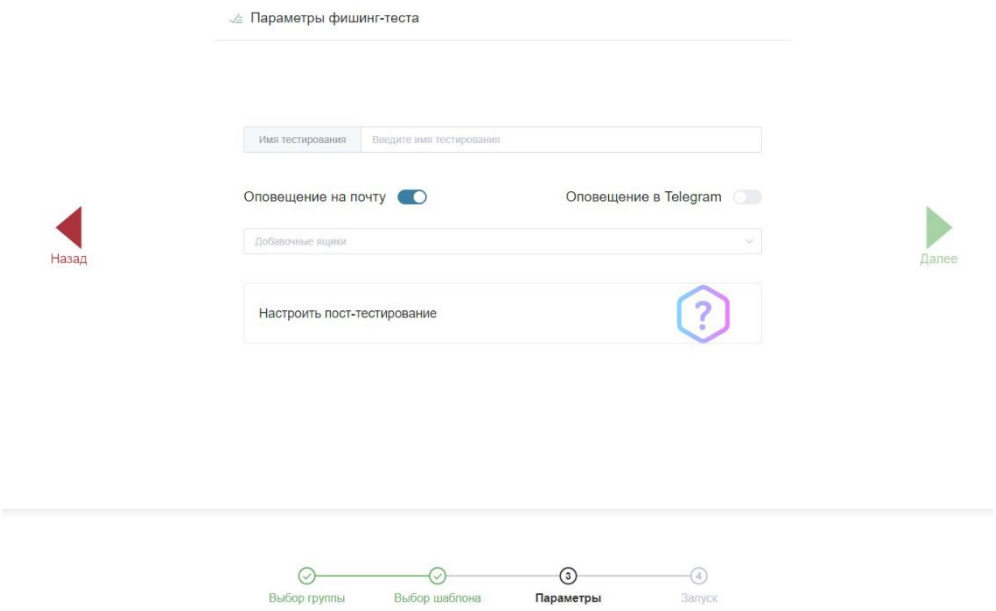

Рис. 17. Третий этап создания фишинг-теста.

На заключительном этапе создания фишинг-теста выбираются опции запуска (отложенный запуск, запуск сейчас и запуск потом на странице управления фишинг- тестами).

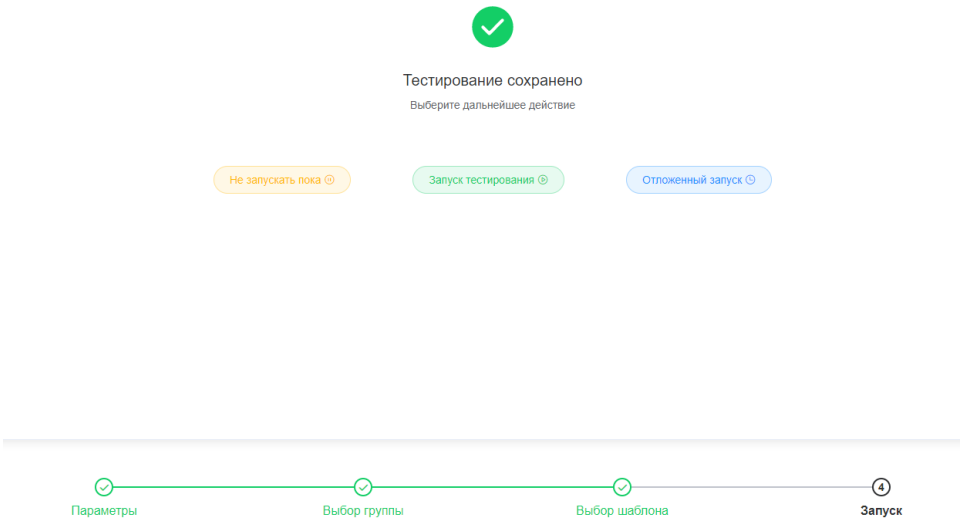

Рис. 18. Заключительный этап создания фишинг-теста.

Страница управления фишинг-тестами представляет собой два выпадающих списка: перечень тестирований и перечень групп. В верхней части списков – панель управления отображением: кнопка отображения поисковой строки, кнопка «только свои/все» (видна только пользователю с правами администраторами), а также выбор опций сортировки (новые, старые и по алфавиту). Если фишинг-тест запущен – справа отображается кнопка управления уведомлениями, нажатие которой вызывает модальное окно. В подменю запущенного фишинг-теста можно посмотреть список целей, а также остановить и удалить фишинг-тест (удаляются все токены фишинг- теста, уведомления по фишинг-тесту не отправляются), посмотреть статистику. В подменю незапущенного фишинг-теста присутствует меню запуска (отложенный запуск и запуск сейчас), а также кнопка удаления фишинг-теста. В шапке таблицы групп присутствует кнопка создания новой группы, нажатие которой вызывает модальное окно. Справа в строке каждой группы находится кнопка редактирования состава группы.

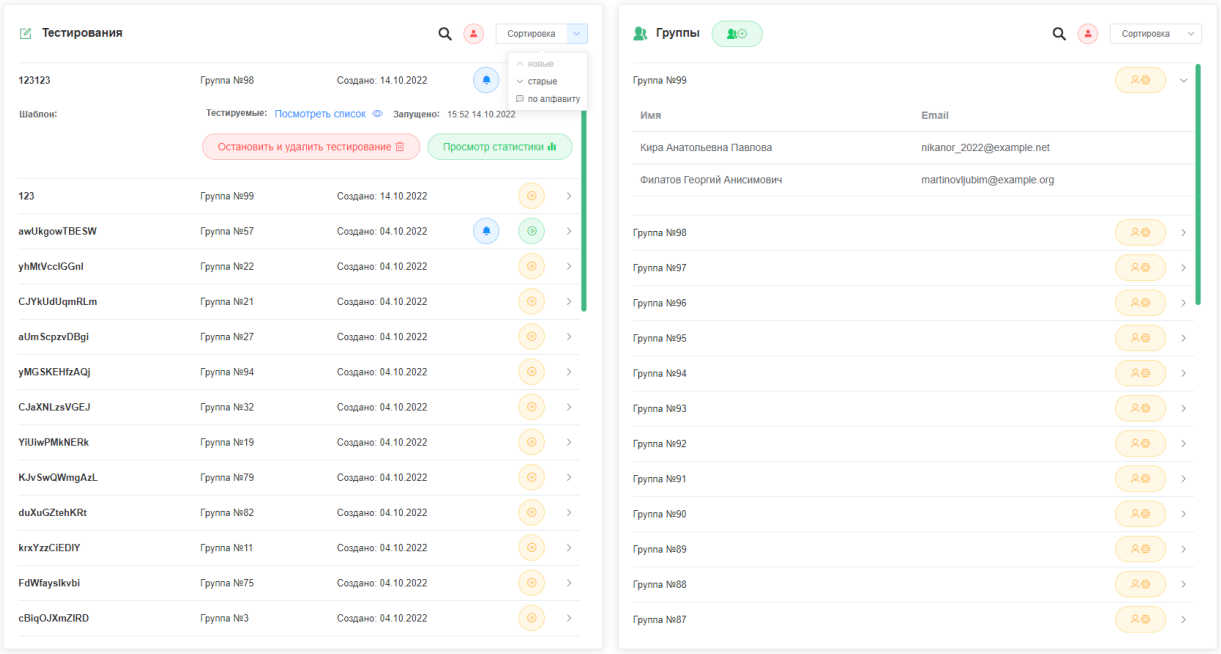

Рис. 19. Страница управления фишинг-тестами.

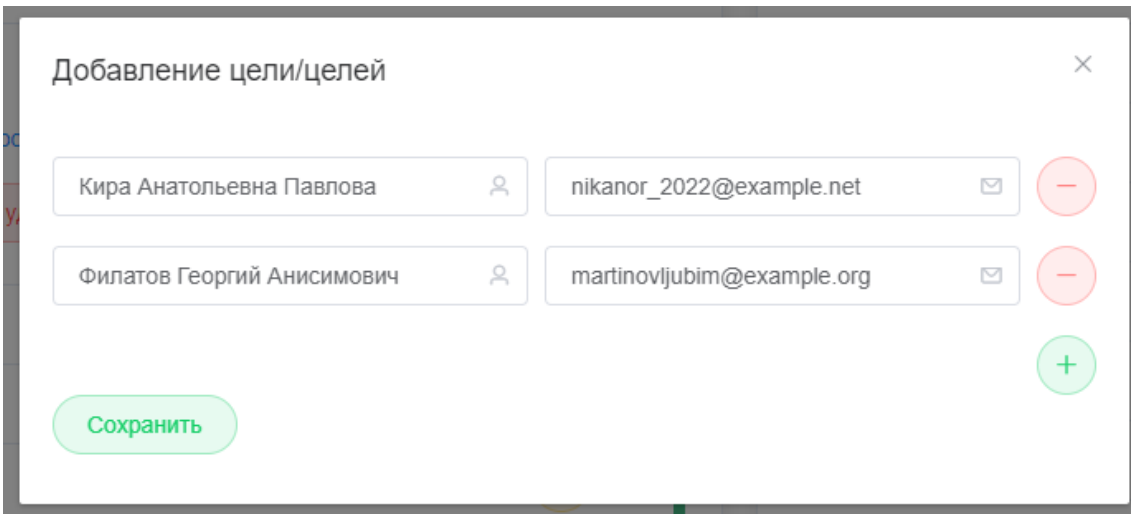

Рис. 20. Модальное окно редактирования состава группы.

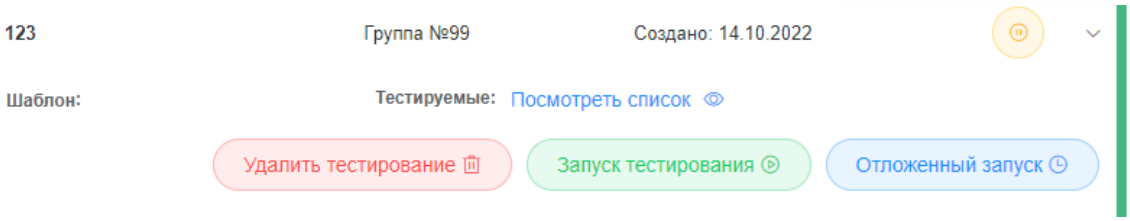

Рис. 21. Подменю незапущенного фишинг-теста

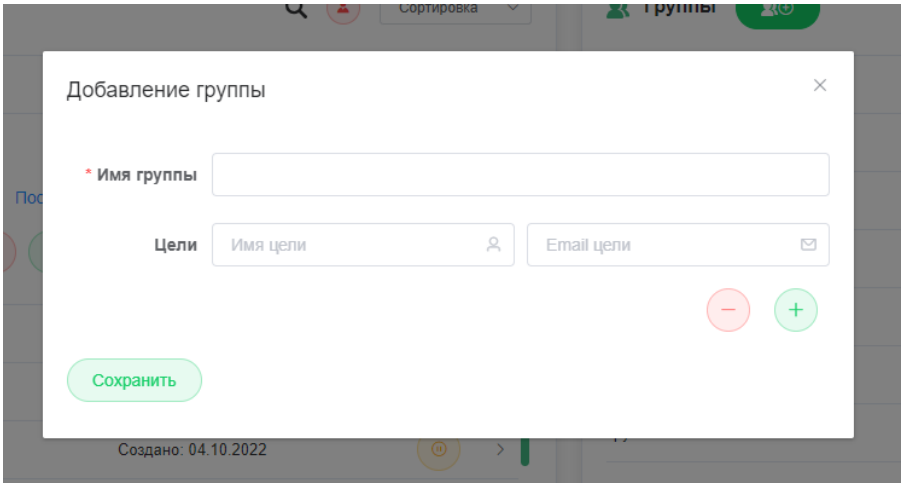

Рис. 22. Модальное окно создания группы

В верхней части страницы статистики отображена общая статистика активности пользователя. В списке слева отображается перечень групп, с описанной выше панелью управлением отображением. Поле справа занимают графики статистики. При нажатии на группу показывается список тестирований этой группы и отображается сводная статистика по группе. При нажатии на определенное тестирование выводится также и статистика по тестированию.

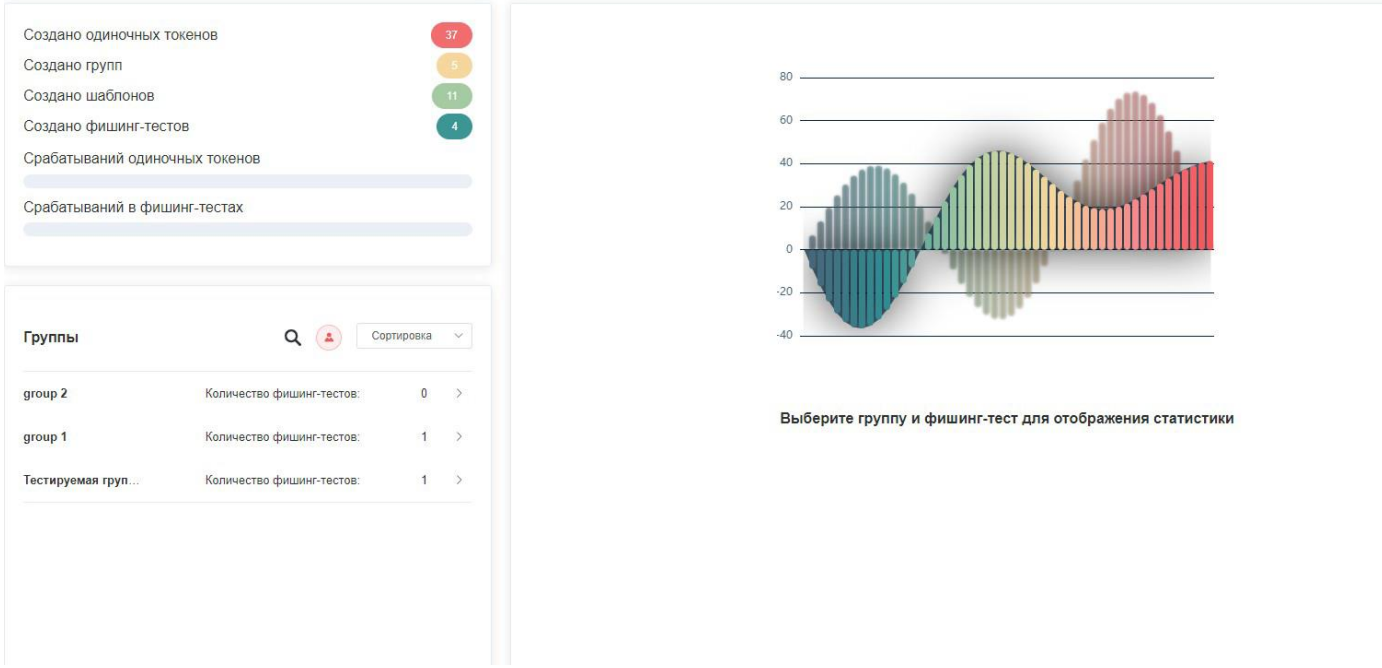

Рис. 23. Страница статистики без отображения статистики по конкретной группе и фишинг-тесту.

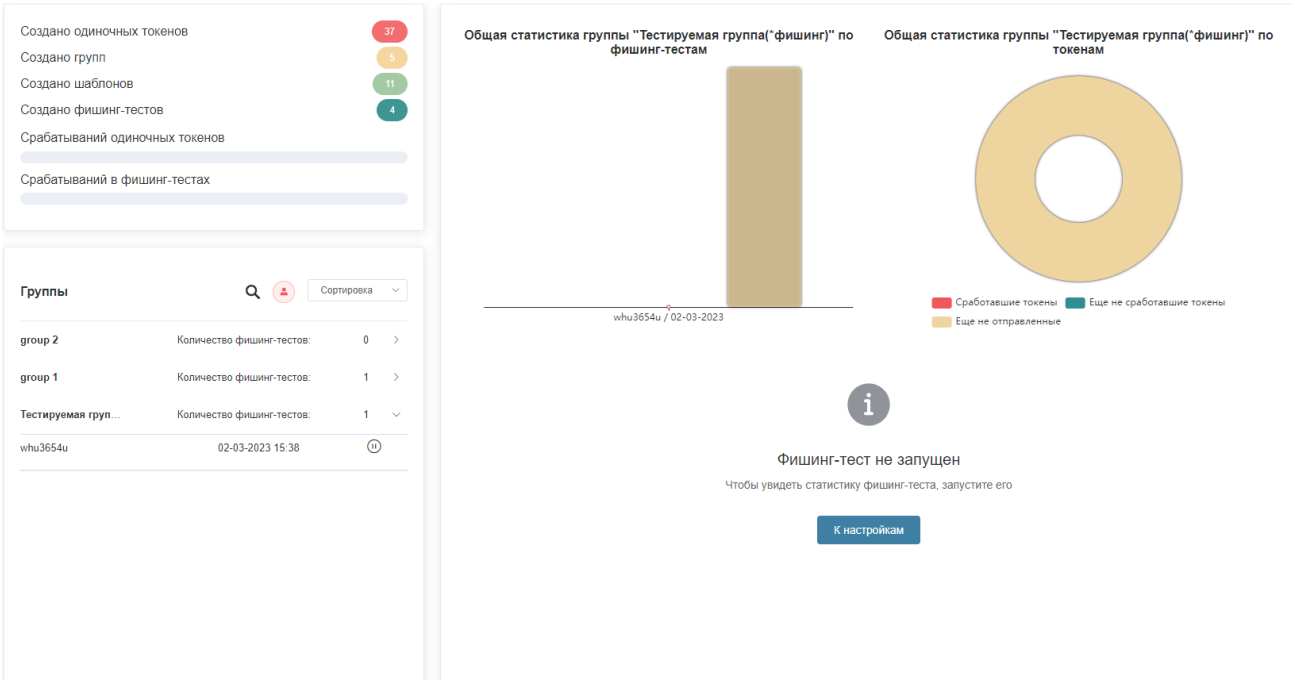

Рис. 24. Отображение статистики группы и тестирования.

Страница редактирования пользователей доступна только пользователям с правами администраторов. На ней отображается список пользователей. Цветом обозначены права и статус пользователей (не активированные профили, модераторы, администраторы, профили обычных пользователей). В столбце «Действия» пользователь может удалить профиль (для удаления обязательным условием является подтверждение паролем) либо изменить данные профиля (имя, фамилия, права модератора).

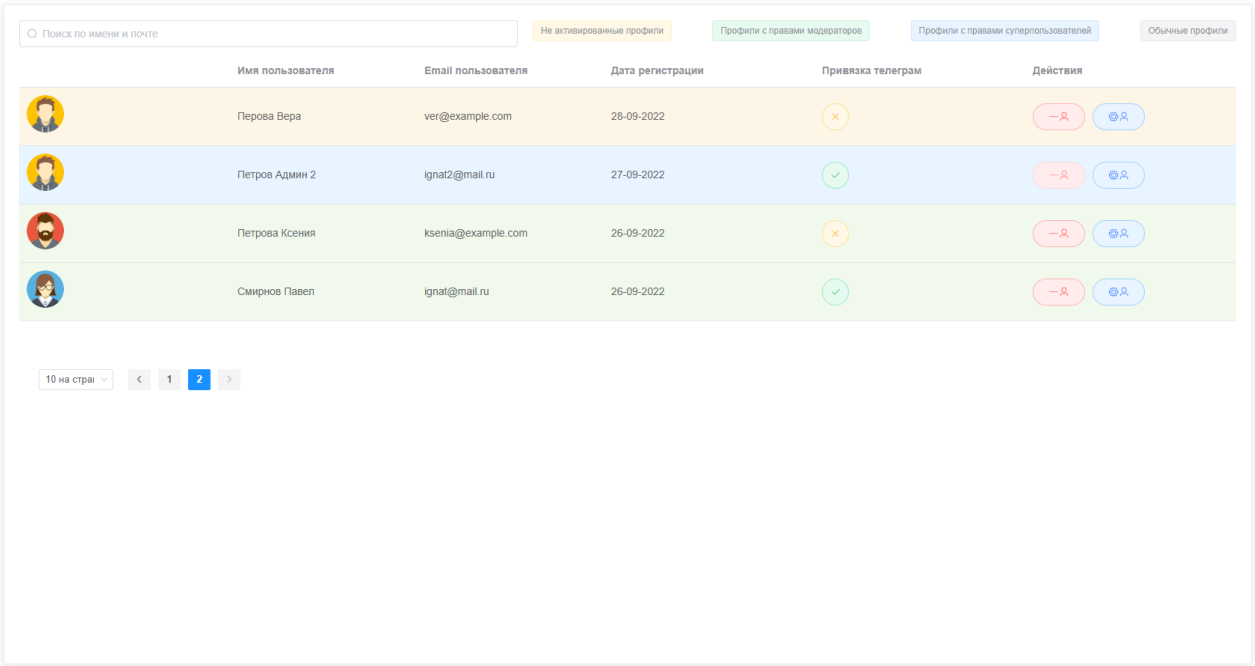

Рис. 25. Страница редактирования пользователей.

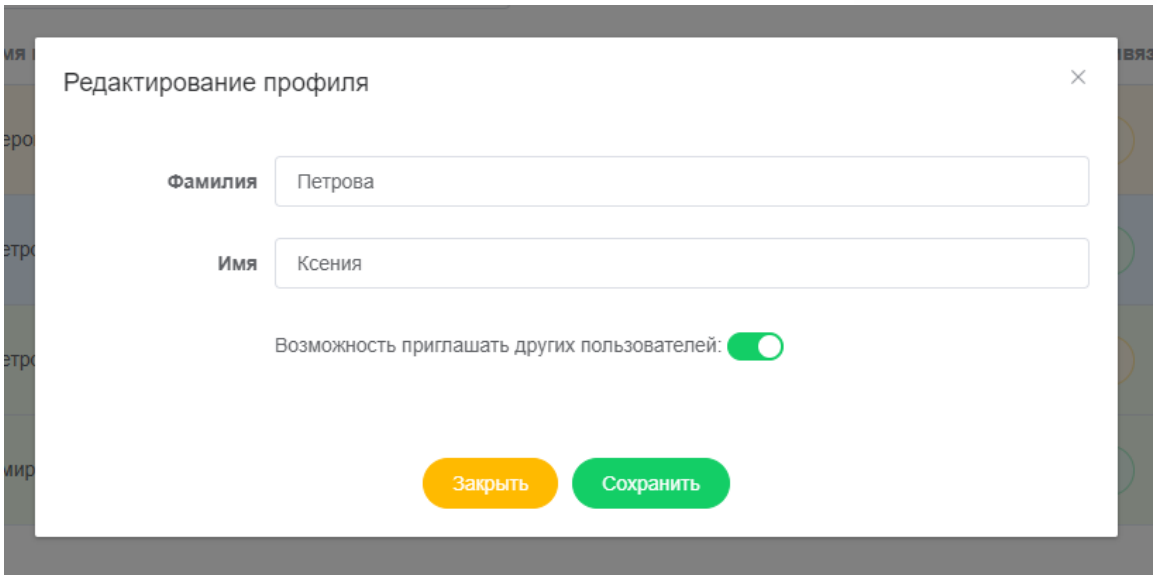

Рис. 26. Модальное окно редактирования пользователя.

Страница приглашения пользователей доступна пользователям с правами администраторов и модераторов. После ввода данных и валидации формы на указанный email адрес поступит письмо с приглашением и данными для входа.

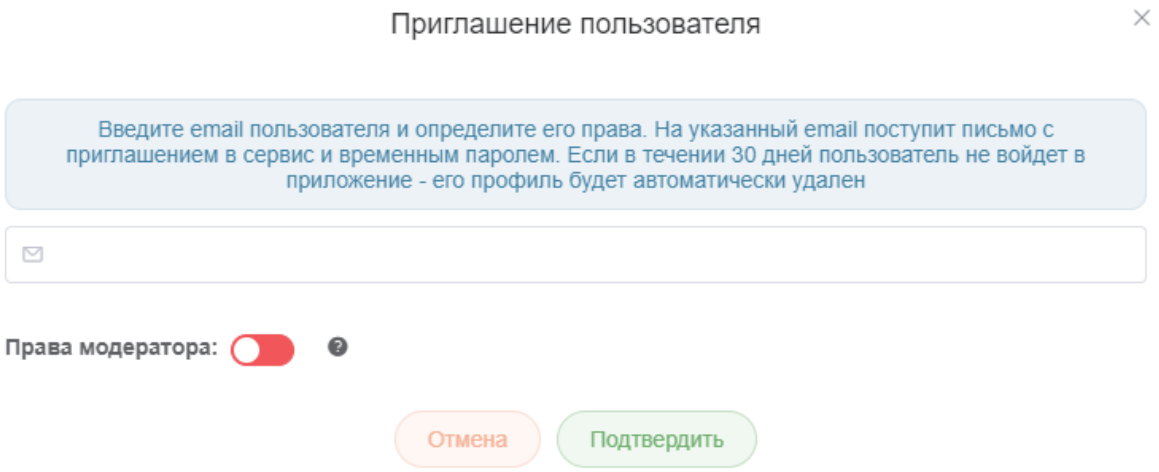

Рис. 27. Страница приглашения пользователя.

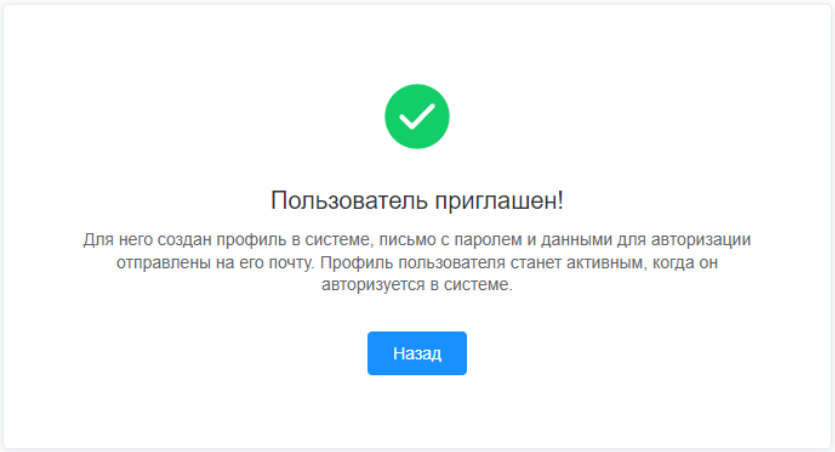

Рис. 28. Страница успешного приглашения

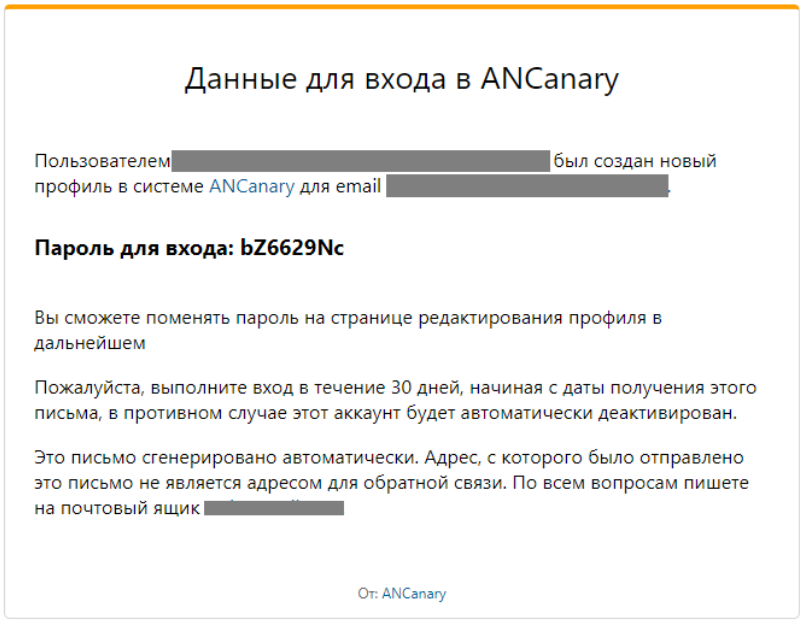

Рис. 29. Пригласительное письмо.

Так же для пользователей доступна страница настройки приложения. Обычные пользователи и модераторы имеют доступ к настройкам отображения приложения и общим настройкам пользовательского интерфейса, администраторы могут менять настройки системы оповещения (токен Telegram-бота, данные сервера SMTP и почтового ящика службы поддержки).

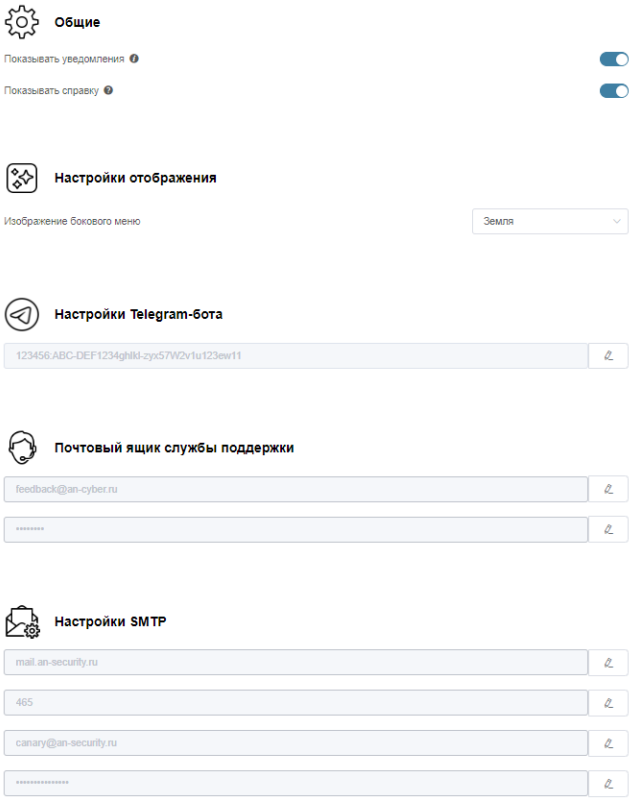

Рис. 30. Страница настроек (для администратора).

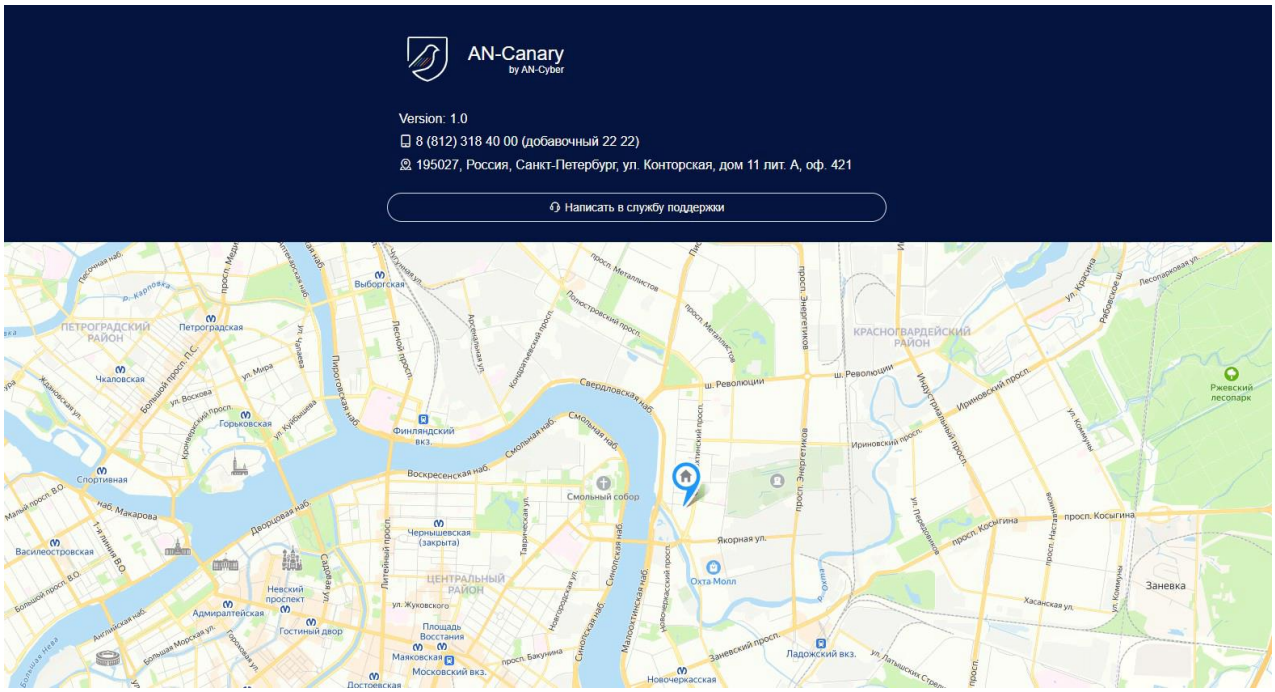

Рис. 31. Страница информации о приложении.

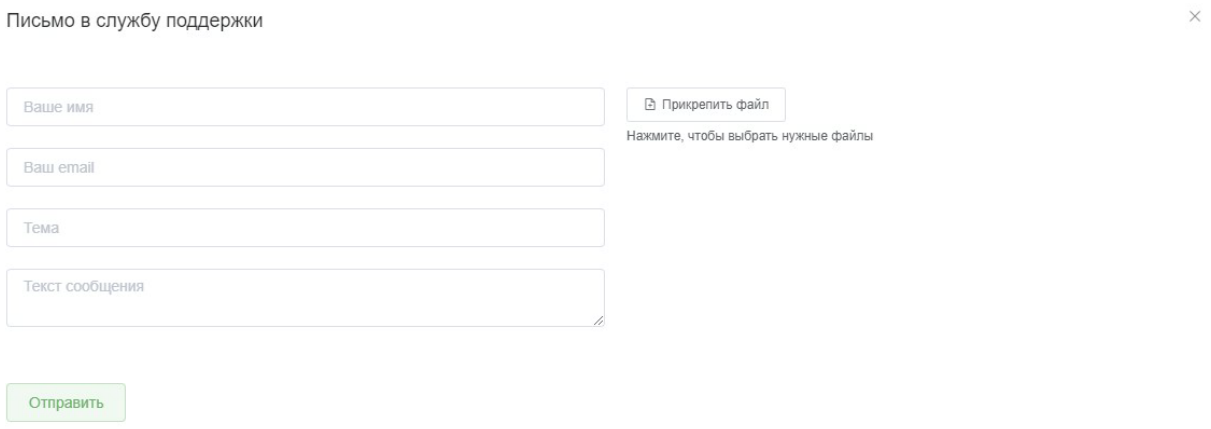

Рис. 32. Форма обратной связи.

Дополнительным функционалом приложения является создание классических тестов для организации учебного процесса и проверки знаний. Форма создания теста позволяет редактировать содержание каждого вопроса, количество балов за правильный ответ, добавлять новые варианты ответов, прикреплять изображения и создавать комментарии к каждому вопросу, а так же указывать проходной порог балов, создавать предисловие и послесловие для теста.

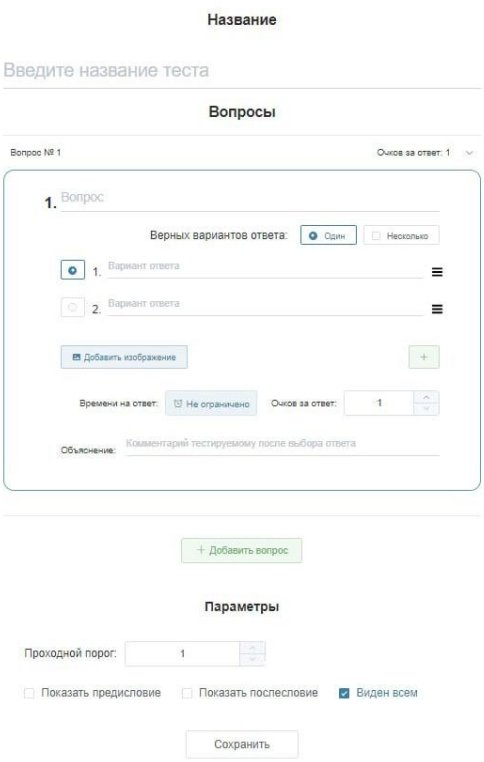

Рис. 33. Форма создания теста.

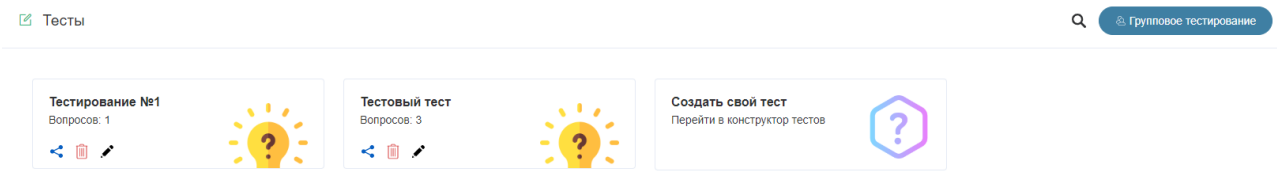

Рис. 34. Страница управления тестами.

На странице информации о тесте отображаются кратко вопросы теста с правильными ответами, а также модальное окно параметров теста, модальное окно настроек публичного доступа (тест будет доступен по ссылке даже не зарегистрированным в системе пользователям), а также информация по результатам теста в тестированиях групп, пост-тестах (тестах, которые отправляются не прошедшим фишинг-тест целям) или публичных тестах.

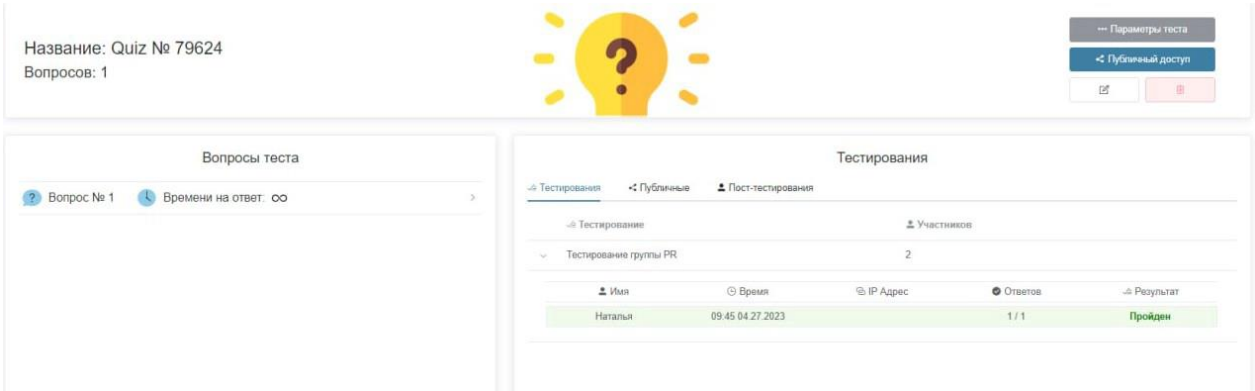

Рис. 35. Страница информации о тесте.

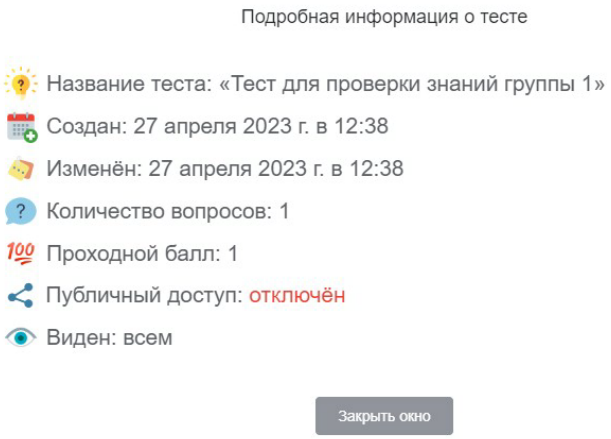

Рис. 36. Модальное окно параметров теста

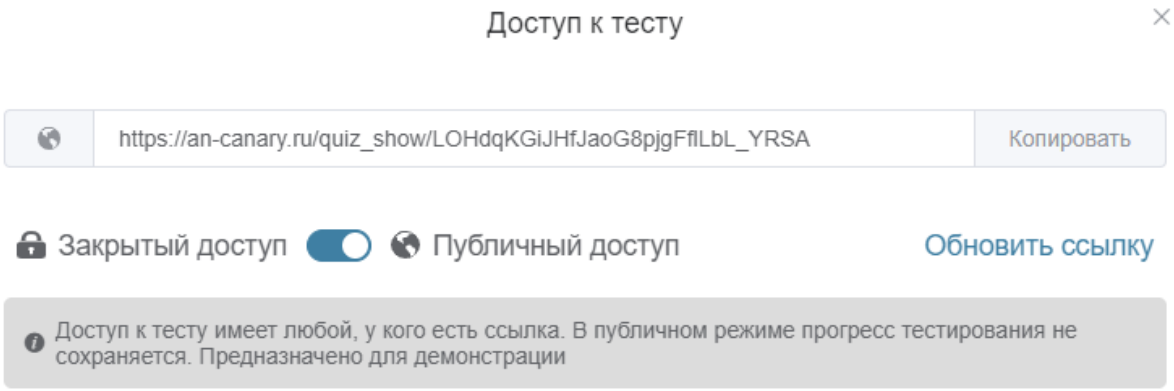

Рис. 37. Модальное окно настроек публичного доступа к тесту.

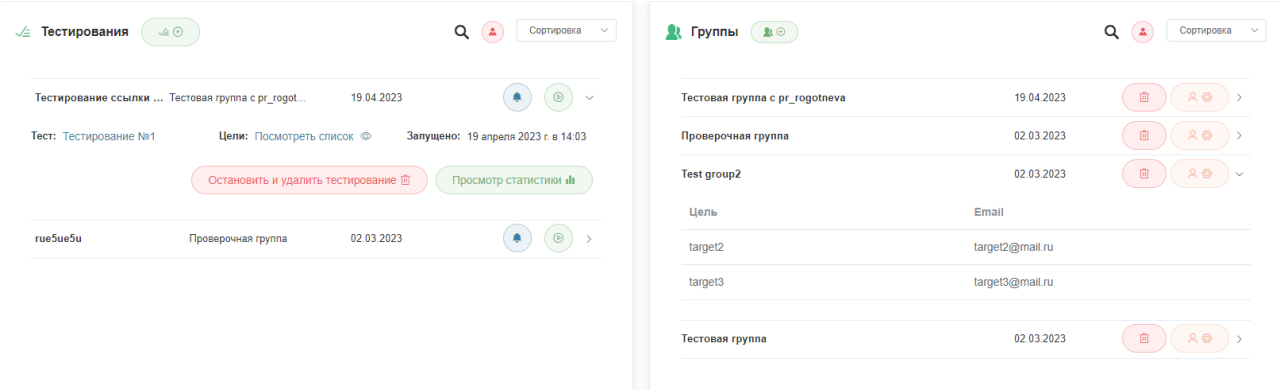

Рис. 38. Страница настроек тестирований (аналогична странице управления фишинг-тестами)