

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

V 1.0

Система тестирования персонала на знание основ информационной безопасности

Документация по программной среде

Общие сведения

1.1 Наименование программы

1.1.1 Полное наименование программы

Система тестирования персонала на знание основ информационной безопасности

1.1.2 Условное обозначение программы

«AN-Canary»

1.1.3 Описание

AN-Canary – это инструмент для тестирования сотрудников предприятия на знание основ информационной безопасности, а так же для создания механизмов раннего предупреждения проникновения посторонних лиц в закрытые корпоративные системы, созданные на базе ОС Windows.

1.2 Условия использования

Наличие любого браузерного приложения

1.3 Программные средства и языки программирования

Стек технологий, использованный для реализации ПО:

- Python 3.10.5
- Django Restframework 3.13.1, Django 4.1.0
- VueJS 2.6.10, Vuex 3.1.0
- Vue Element Admin 4.4.0
- Docker, docker-compose
- Celery5.2.7, Redis 7.0.4
- Nginx

Разработка осуществлялась с помощью интегрированных сред разработки:

- PyCharm Community Edition 2022.1.3
- Visual Studio Code 1.69
- Pgadmin

Технические характеристики

2.1 Минимальные системные требования (для развертывания приложения на сервере)

- OS Ubuntu Server 20.04 LTS, либо любая GNU/Linux система, совместимая с Debian пакетами

- Установленный на сервере инструмент контейнеризации Docker последней версии и инструмент управления контейнерами docker-compose версии не ниже 3.9
- не менее 2 Гб свободного места на жестком диске

2.2 Компоненты программы:

Два основных компонента приложения – сервер Nginx и стек контейнеров docker-compose, в котором запущены все основные элементы функционирования ПО.

2.3 Компонентная архитектура программы

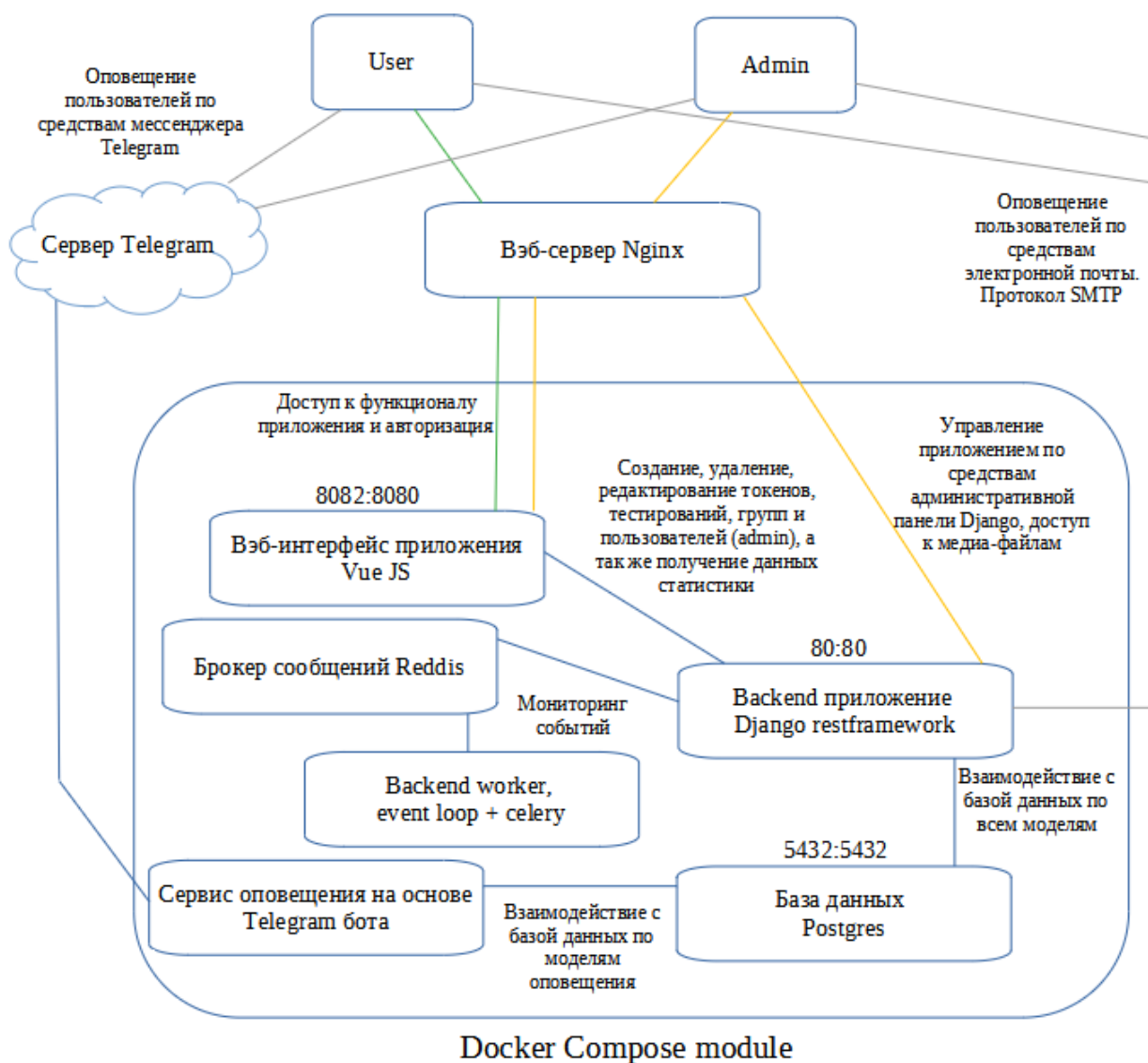


Схема 1. Основные компоненты ПО

Используемые технические средства

4.1 Для эксплуатации программы необходимы следующие технические средства

Техническое средство	Характеристики
Сервер	OS Ubuntu Server 20.04 LTS, либо любая GNU/Linux система, совместимая с Debian пакетами Процессор: не менее 1,8 ГГц Оперативная память: 4 ГБ Дисковое пространство: не менее 2 Гб свободного места Сетевое соединение
PyCharm Community Edition 2022.13 или аналогичная IDE	Требуется для эксплуатации: нет Требуется для разработки: да
Visual Studio Code	Требуется для эксплуатации: нет Требуется для разработки: да
Docker, docker-compose	Требуется для эксплуатации: нет Требуется для разработки: да Требуется для развертывания экземпляра ПО: да

Таблица 1. Требования к программно-аппаратному окружению для эксплуатации ПО.

Запуск и использование

4.1 Получение доступа к функционалу ПО

Доступ к веб-интерфейсу приложения можно получить на сайте «<https://an-canary.ru/>» по предоставленным учетным данным.

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

Принцип функционирования

Приложение представляет из себя веб-интерфейс с тремя видами пользовательских прав – клиентским, модераторским и администраторским. Клиентский интерфейс предусматривает создание как одиночных канареечных токенов (цифровая ловушка, отправляющая создателю уведомление о срабатывании) (Далее - токен) различных видов (url-ссылки, qr-коды, папки Windows и исполняемые файлы), так и групповых тестирований (Далее - тестирование) с функционалом автоматической рассылки фишинговых писем на почтовые ящики членов (Далее - цель) выбранной проверочной группы (Далее - группа). Клиентский интерфейс так же позволяет создавать, редактировать состав и удалять проверочные группы, изменять настройки уведомлений тестирований, удалять токены и тестирования, редактировать их настройки, а также просматривать статистику по тестированиям 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, тестирований и групп. Приложение поддерживает возможность отправки уведомлений по средствам 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».

Руководство пользователя

5.1 Интерфейс пользователя

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

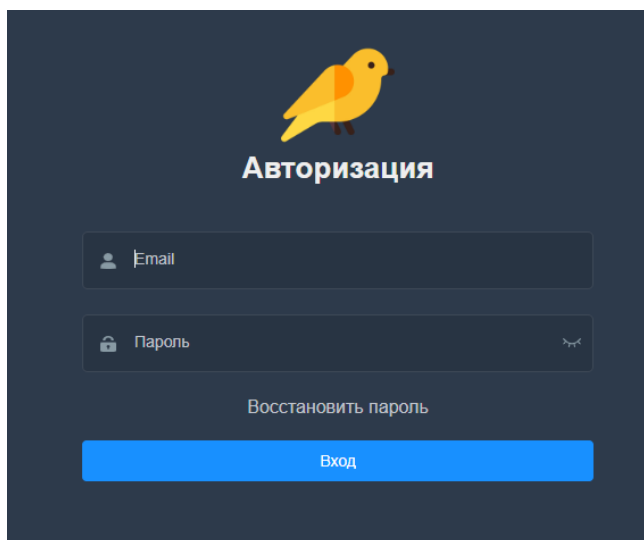


Рисунок 1. Окно авторизации для входа в систему.

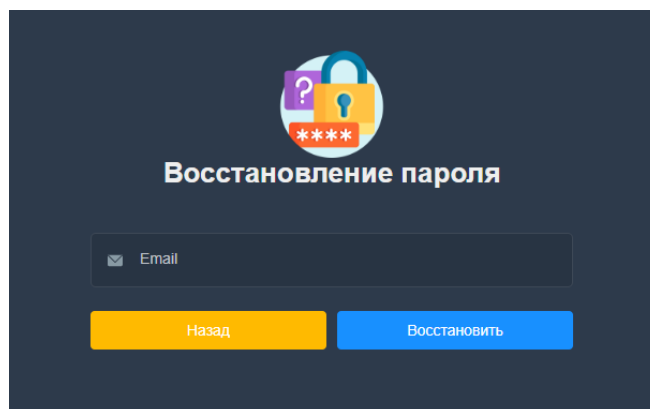


Рисунок 2. Окно восстановления пароля.

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

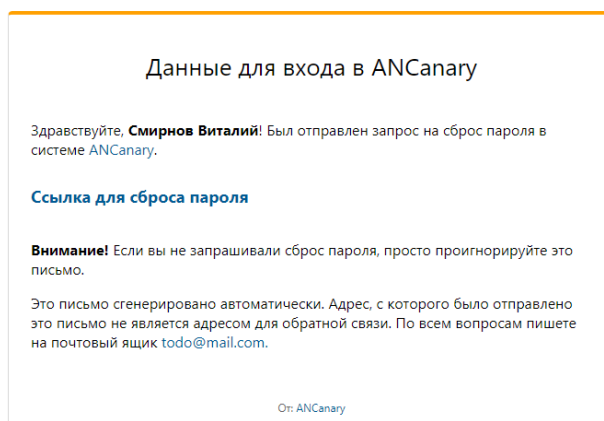


Рисунок 3. Письмо с ссылкой для восстановления пароля

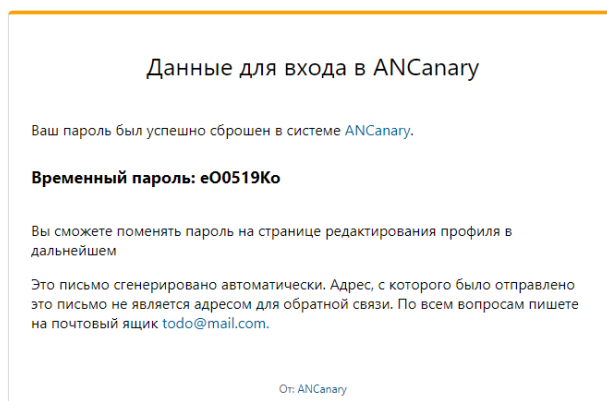


Рисунок 4. Письмо с временным паролем для входа в систему

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

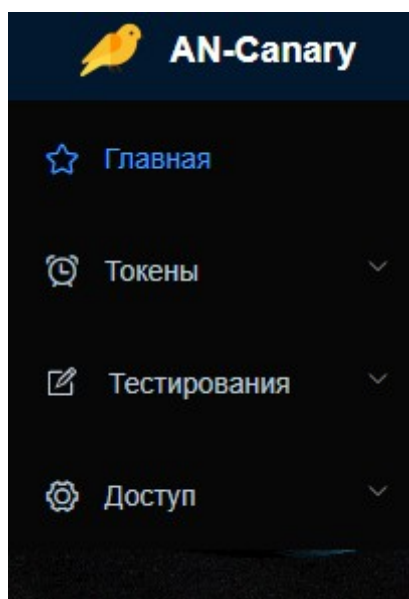


Рисунок 5. Боковая панель навигации.

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, email 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.

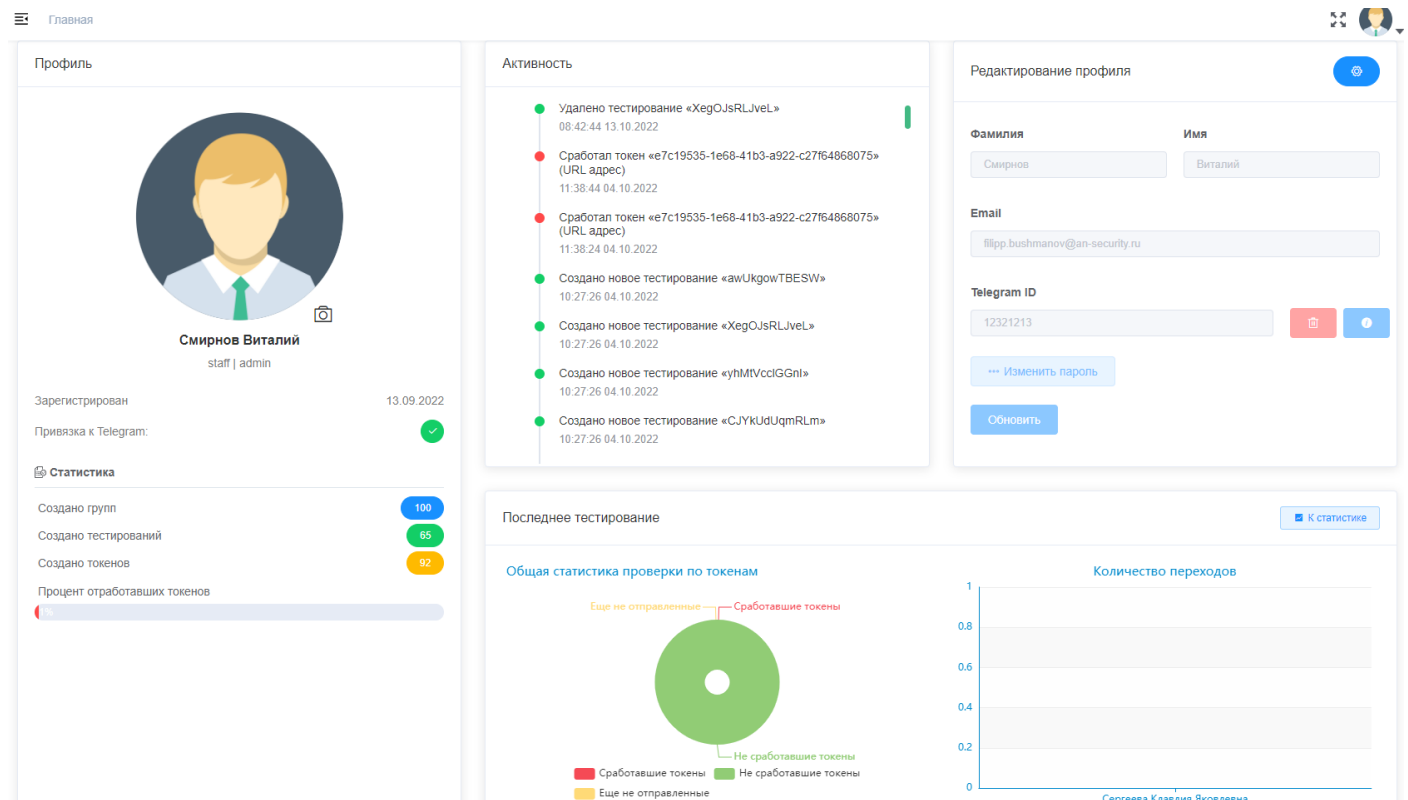


Рисунок 6. Внешний вид домашней страницы.

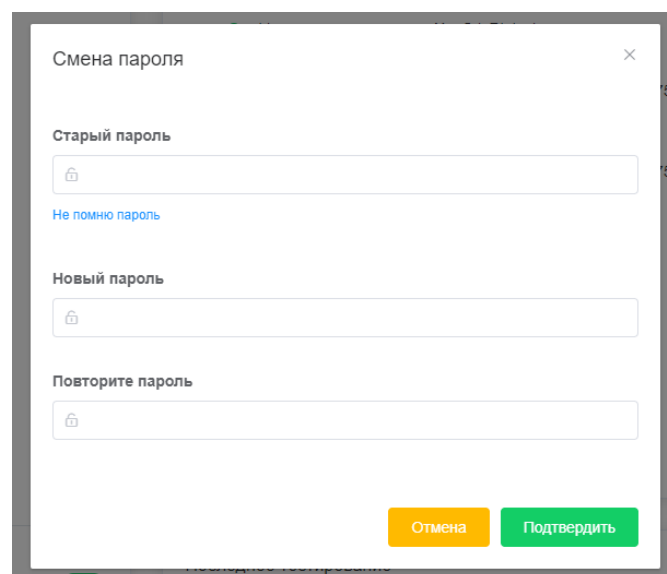


Рисунок 7. Модальное окно смены пароля.

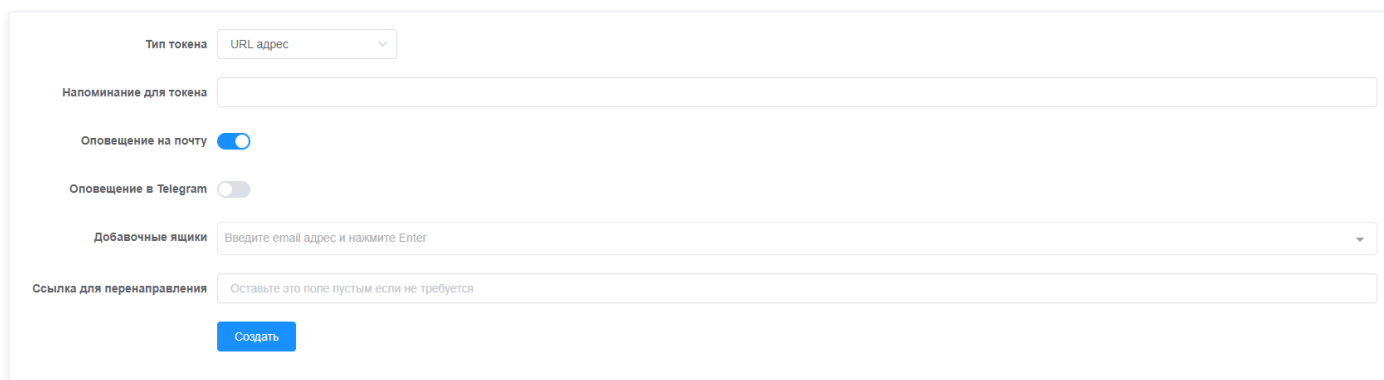


Рисунок 8. Окно создания токена.

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 токenu дополнительные email адреса для уведомлений. Добавление осуществляется вводом адреса и нажатием клавиши Enter.

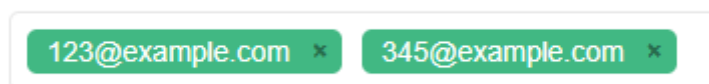


Рисунок 9. Поле «добавочные ящики».

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.



Токен сгенерирован

Ваша ссылка готова

Скопируйте ссылку ниже и отправьте её вашей цели
Как только будет произведён переход по ссылке, вы получите уведомление на почту и/или в Телеграм

<http://127.0.0.1/blog/1fe83224-0d26-4238-871e-be77be4e7838>

Копировать

Вы можете сгенерировать шаблон для письма

Выберите одну из иконок ниже, чтобы автоматически сгенерировать HTML-код, который впоследствии можно использовать как иконку загружаемого документа в электронном письме



```
1 <a href="http://127.0.0.1/blog/1fe83224-0d26-4238-871e-be77be4e7838">  
2   
3 </a>
```

Рисунок 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)



Токен сгенерирован

Ваш токен готов

Загрузите архив с Windows папкой по кнопке ниже

↓ Загрузить

Распакуйте архив с Windows-папкой в необходимое место в системе

Вы получите уведомление на почту и/или в Телеграм, как только кто-либо будет просматривать папку в проводнике

Идеи для использования:

- Поместите папку в закрытое сетевое расположение. Вы сможете отловить несанкционированный доступ
- Расположите папку на рабочем столе жертвы. Вы будете получать уведомления, когда включится компьютер

Рисунок 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.

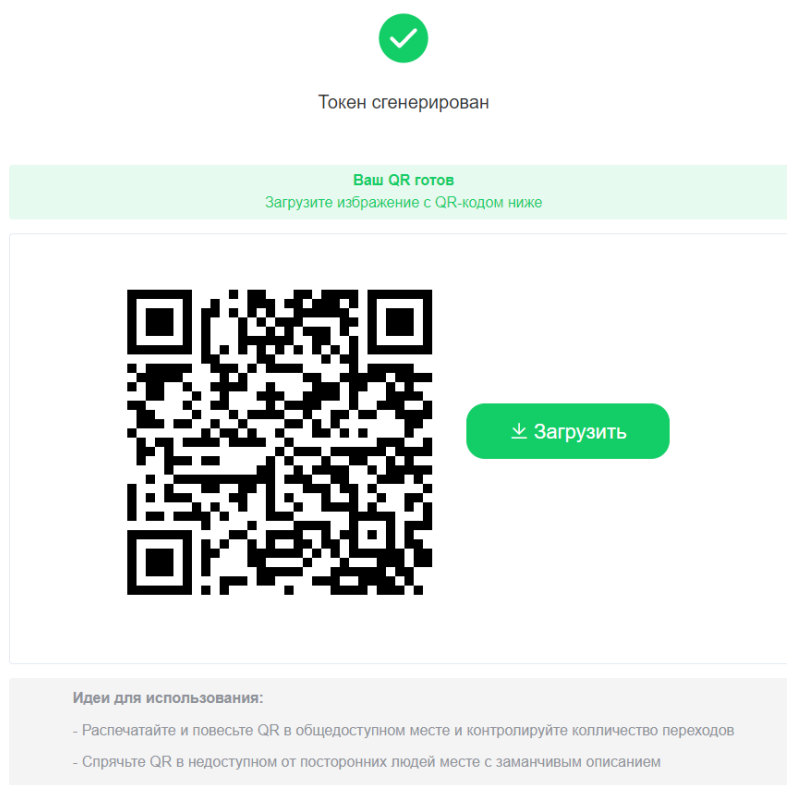


Рисунок 12. Страница получения «qr-кода»

Страница управления созданными одиночными токенами представляет из себя таблицу со списком токенов. В столбце «Токен», в зависимости от типа токена, находится кнопка с возможностью скопировать ссылку или скачать файл. В столбце «Срабатывания», в том случае, если по данному токену были срабатывания находится ссылка для перехода на страницу просмотра инцидентов. В столбце «Действия» можно редактировать настройки токена (настройки уведомлений, дополнительных почтовых ящиков, напоминание для токена), а также 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».

Поиск по напоминанию Создать токен Все токены Только свои токены

Тип токена	Время создания	Напоминание	Токен	Срабатывание	Действия
QR Код	14:40 14.10.2022	куар		Еще не отработал	Редактировать Удалить
Папка Windows	14:30 14.10.2022	токен 2		Еще не отработал	Редактировать Удалить
URL адрес	14:20 14.10.2022	Токен 1		Еще не отработал	Редактировать Удалить
Исполняемый файл	13:27 04.10.2022	tSIEKkMakQTY		Еще не отработал	Редактировать Удалить
Исполняемый файл	13:27 04.10.2022	aigNPVDDrXZDZ		Еще не отработал	Редактировать Удалить
QR Код	13:27 04.10.2022	IPwxyDrAyKPS		Еще не отработал	Редактировать Удалить
Исполняемый файл	13:27 04.10.2022	ciNSuoOHvKVg		Еще не отработал	Редактировать Удалить
Папка Windows	13:27 04.10.2022	JNBVJqBIBWh		Еще не отработал	Редактировать Удалить
Исполняемый файл	13:27 04.10.2022	YOQJXoiECHFE		Еще не отработал	Редактировать Удалить
Исполняемый файл	13:27 04.10.2022	XdLouCOmjGL		Еще не отработал	Редактировать Удалить

Всего 98 < 1 2 3 4 5 6 ... 10 > Перейти

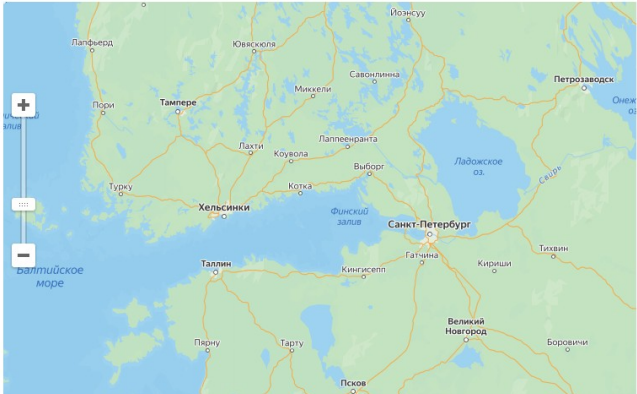
Рисунок 13. Страница управления токенами.

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)

ID токена: e7c19535-1e68-41b3-a922-c27f64868075
 Тип токена: URL адрес
 Напоминание: PDWEkzvpGOAI

Нажмите на инцидент в списке справа для просмотра дополнительной информации

Карта инцидентов



Список инцидентов

Загрузить

Время: 11:38:44 10/04/2022 Протокол: HTTP IP: 127.0.0.1

⌚ Время	11:38:44 10/04/2022
📡 Протокол	HTTP
🌐 IP Адрес	127.0.0.1
🖥️ ОС	Windows 10
🌐 Браузер	Chrome v.106.0.0.0
📄 User Agent	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/106.0.0.0 Safari/537.36

Время: 11:38:24 10/04/2022 Протокол: HTTP IP: 127.0.0.1 >

Рисунок 14. Страница инцидентов.

Создание тестирования проходит в 4 этапа. На первом – указывается название тестирования и параметры уведомлений при срабатываниях (при большом количестве целей тестирования уведомления будут приходить на каждое срабатывание каждого отправленного целям токена, поэтому рекомендуется отключить напоминания для тестирований).

Название тестирования

Оповещение на почту

Оповещение в Telegram

Добавочные ящики

Далее ▶



Рисунок 14. Первый этап создания тестирования.

На втором этапе из выпадающего списка выбирается группа для тестирования.

Группа тестируемых

Имя	Email
🔍 Кира Анатольевна Павлова	✉ nikanor_2022@example.net
🔍 Филатов Георгий Анисимович	✉ martinovjubim@example.org

◀ Назад Далее ▶



Рисунок 15. Второй этап создания тестирования.

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

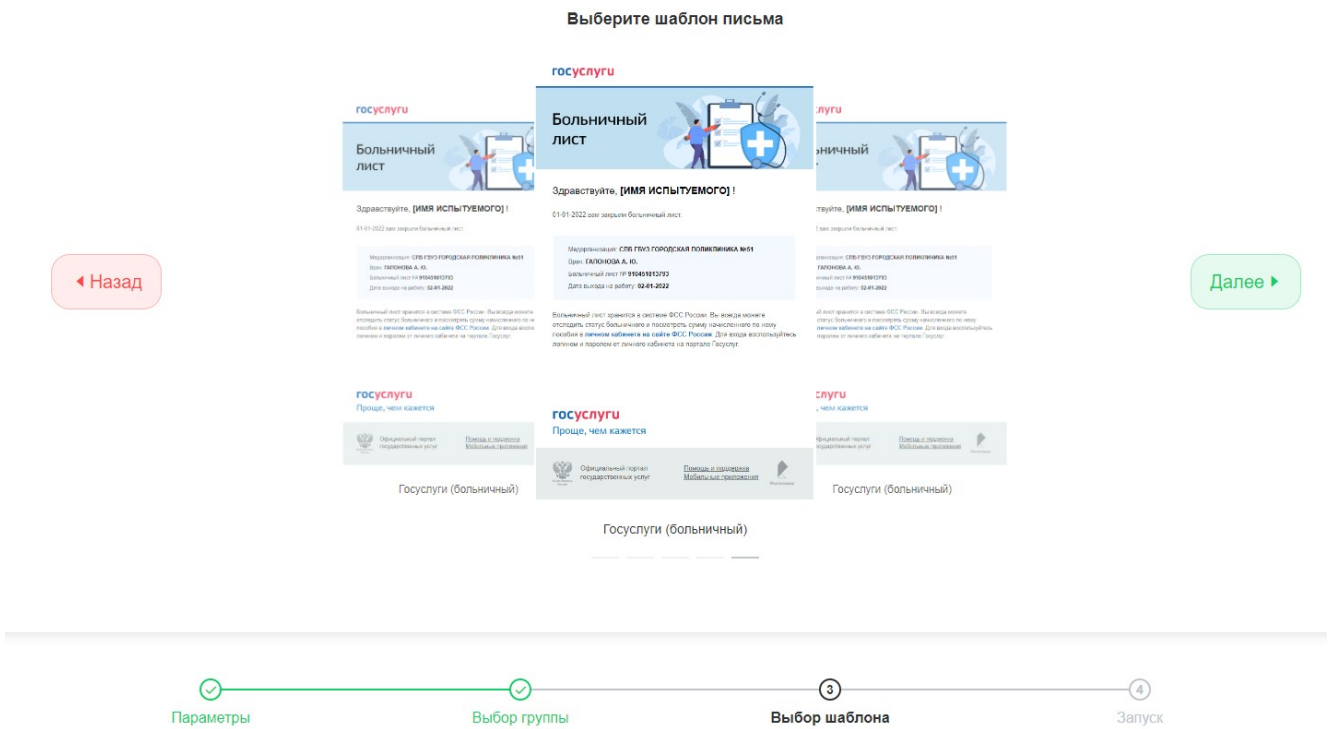


Рисунок 16. Третий этап создания тестирования.

На заключительном этапе создания тестирования выбираются опции запуска (отложенный запуск, запуск сейчас и запуск потом (на странице управления тестирования)).

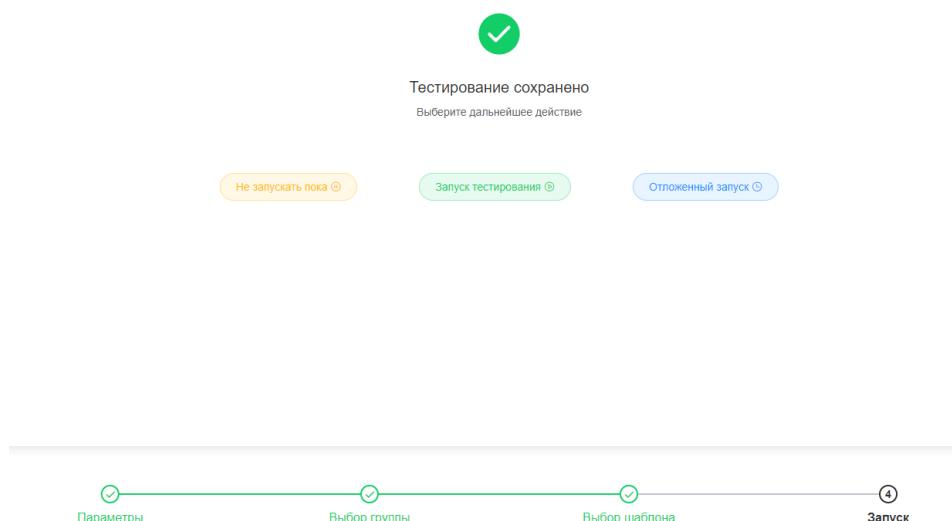


Рисунок 17. Заключительный этап создания тестирования.

Страница управления тестированиями 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 тестирование запущено – справа отображается кнопка управления уведомлениями, нажатие которой вызывает модальное окно. В подменю запущенного тестирования можно посмотреть список целей, а также остановить и удалить тестирование (удаляются все токены тестирования, уведомления по тестированию не отправляются), посмотреть статистику. В подменю незапущенного тестирования присутствует меню запуска (отложенный запуск и запуск сейчас), а также кнопка удаления тестирования. В шапке таблицы групп присутствует кнопка создания новой группы, нажатие которой вызывает модальное окно. Справа в строке каждой группы находится кнопка редактирования состава группы.

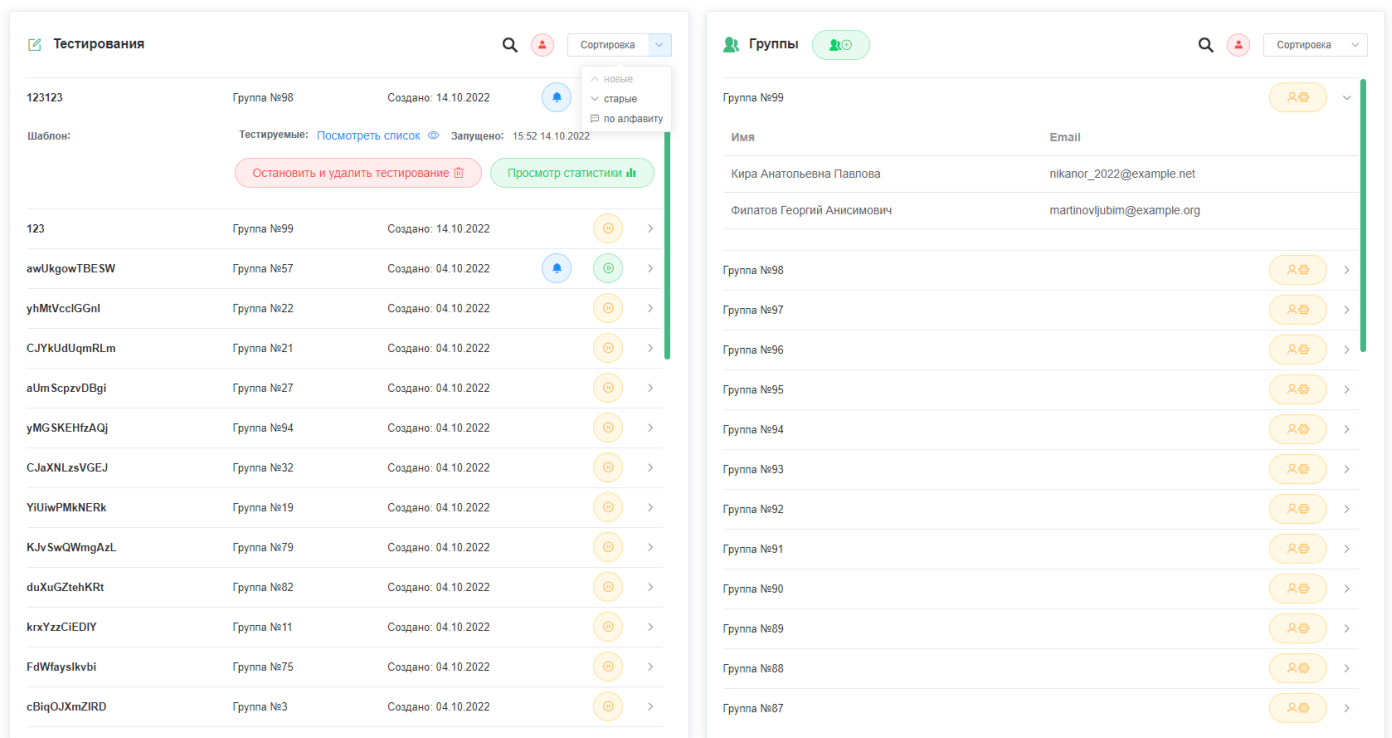


Рисунок 17. Страница управления тестированиями.

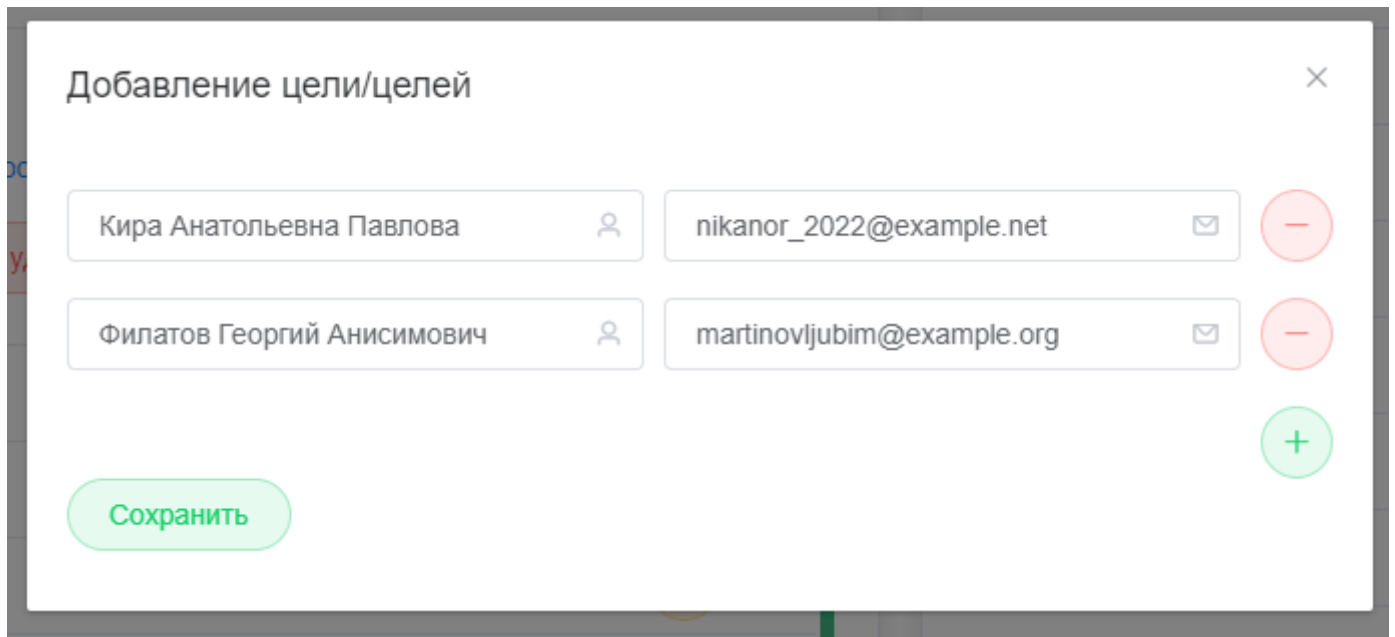


Рисунок 18. Модальное окно редактирования состава группы.

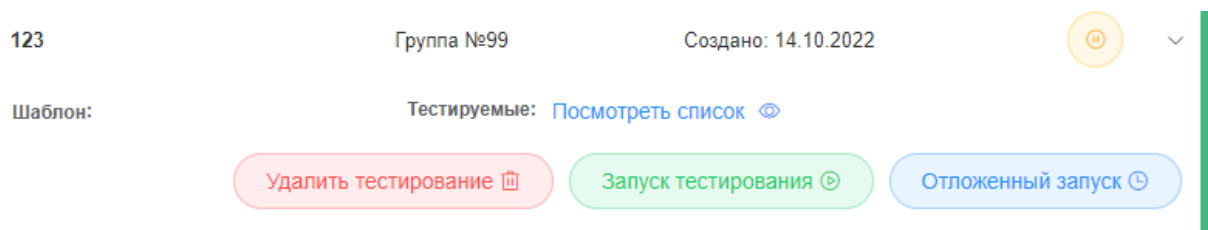


Рисунок 18. Подменю незапущенного тестирования.

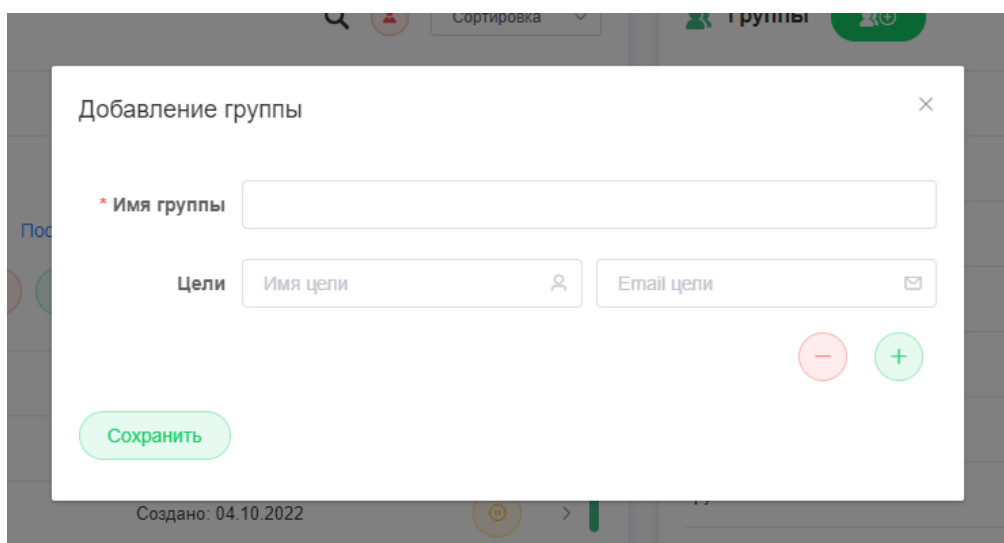


Рисунок 19. Модальное окно создания группы

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.

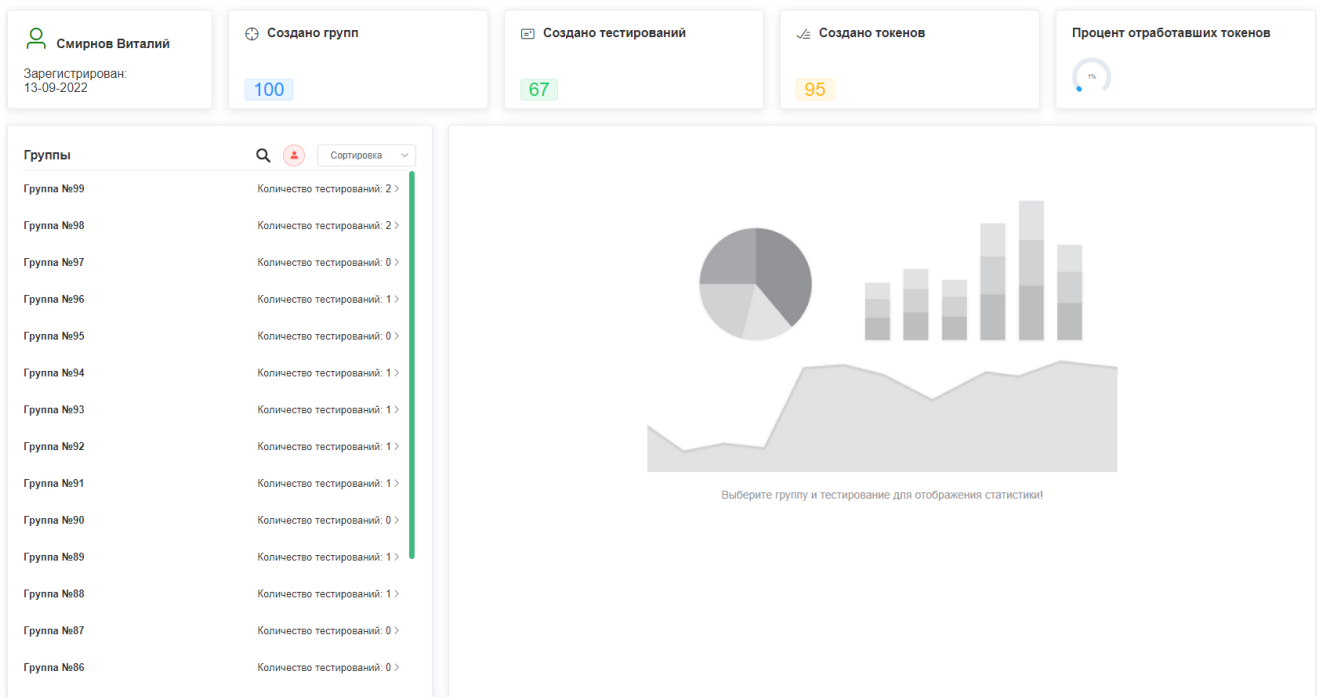


Рисунок 20. Страница статистики без отображения статистики по конкретной группе и тестированию.

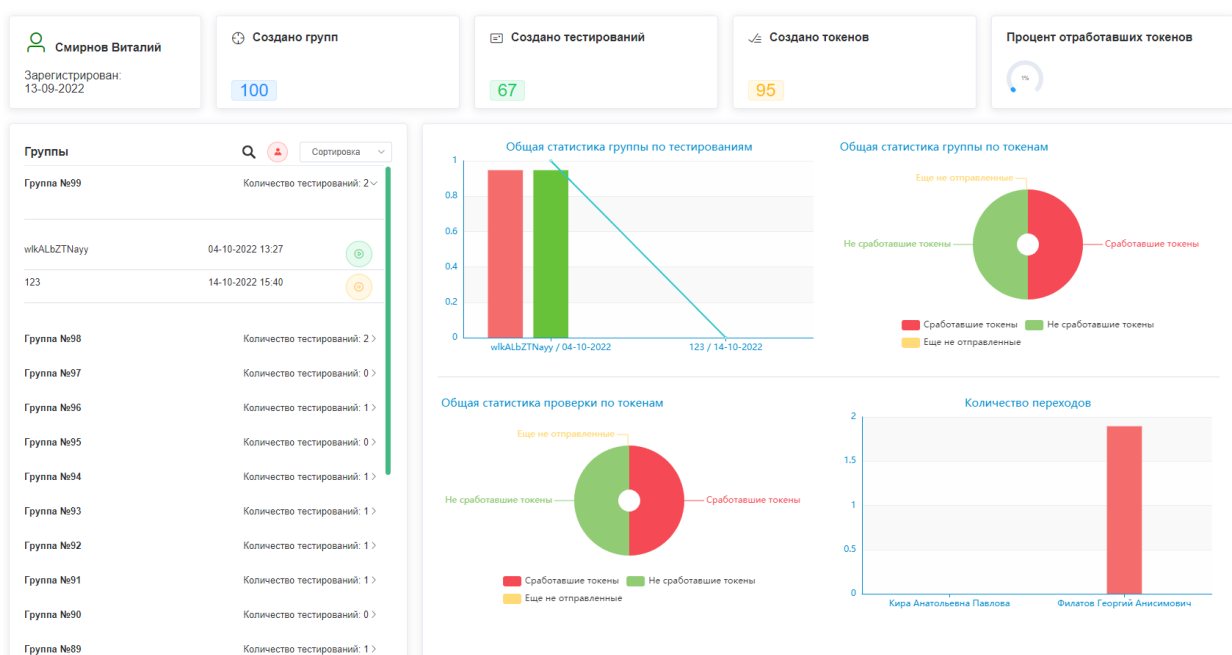


Рисунок 21. Отображение статистики группы и тестирования.

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)

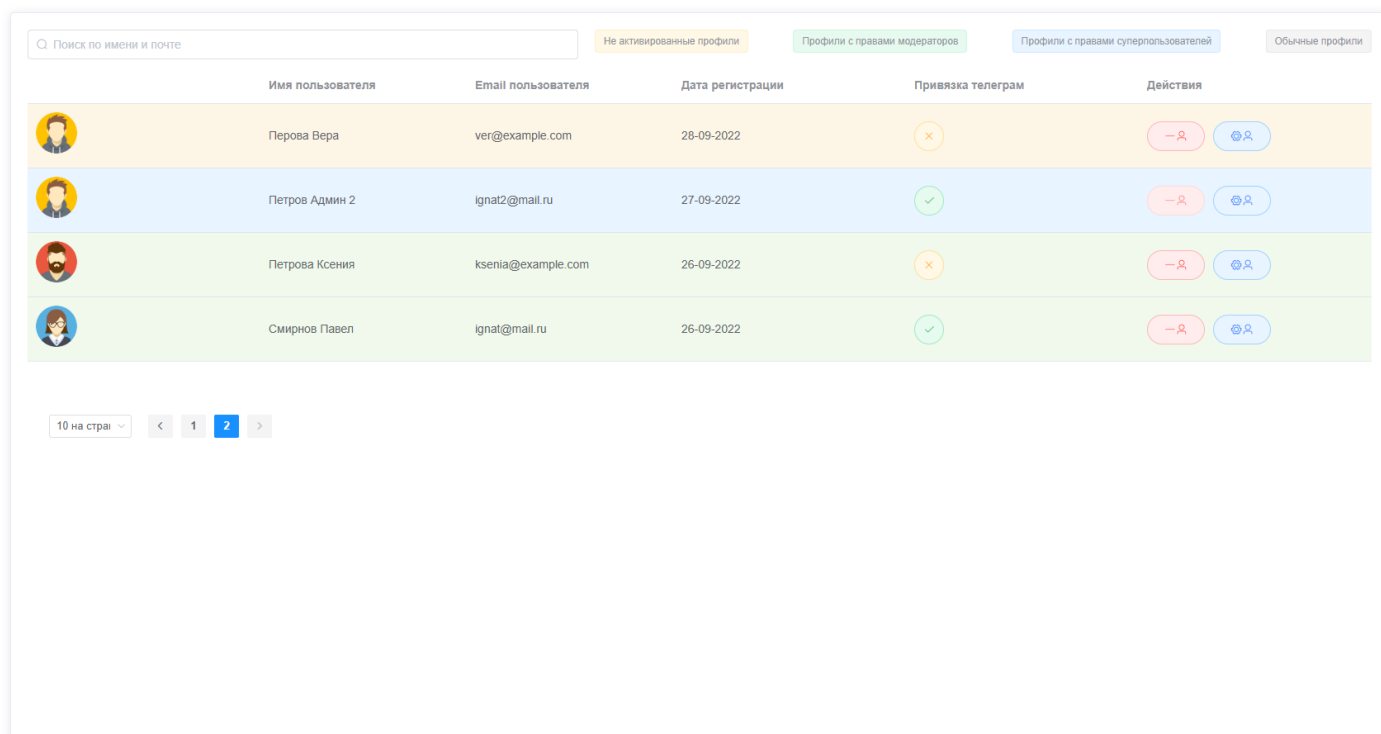


Рисунок 22. Страница редактирования пользователей.

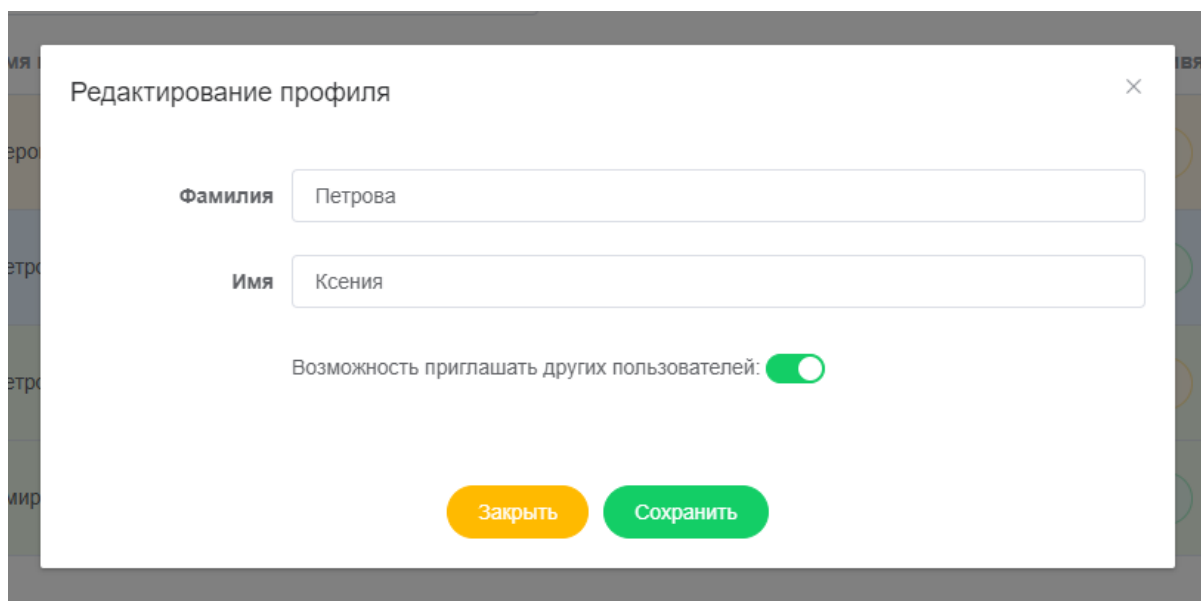
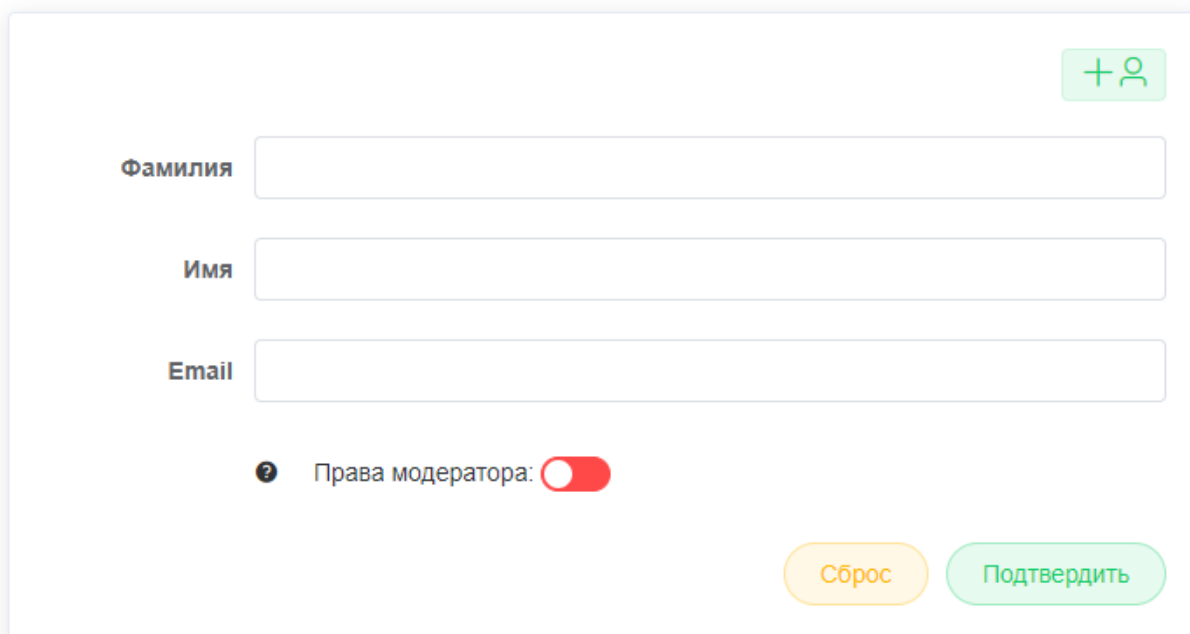


Рисунок 23. Модальное окно редактирования пользователя.

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.



Фамилия

Имя

Email

Права модератора:

Сброс Подтвердить

Рисунок 24. Страница приглашения пользователя.

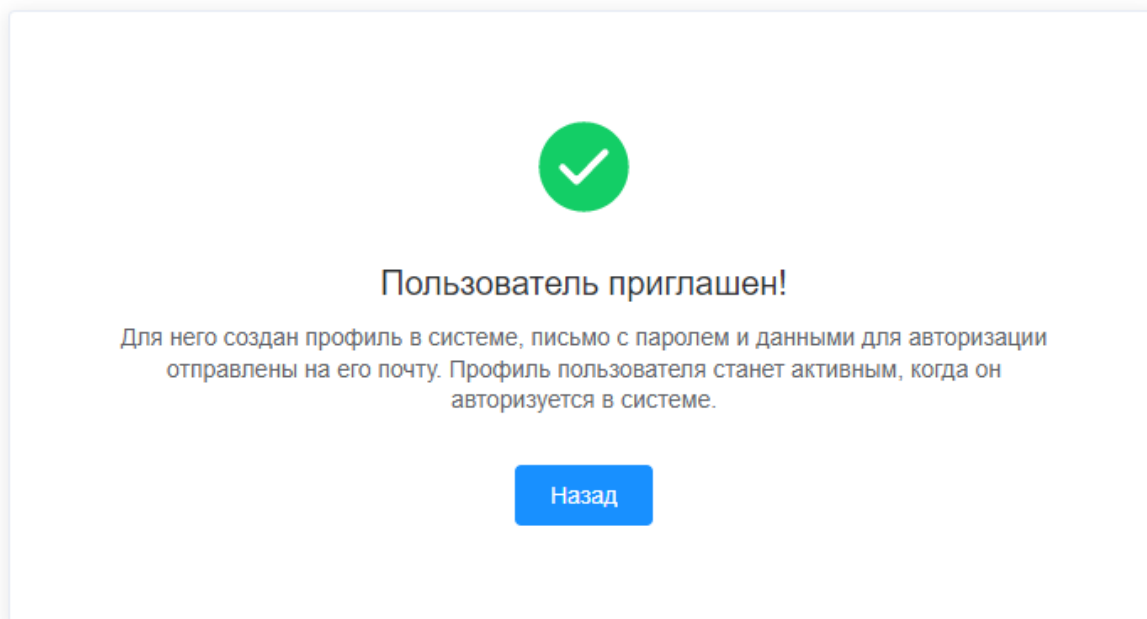


Рисунок 25. Страница успешного приглашения

Данные для входа в ANCanary

Пользователем [REDACTED] был создан новый профиль в системе ANCanary для email [REDACTED].

Пароль для входа: bZ6629Nc

Вы сможете поменять пароль на странице редактирования профиля в дальнейшем

Пожалуйста, выполните вход в течение 30 дней, начиная с даты получения этого письма, в противном случае этот аккаунт будет автоматически деактивирован.

Это письмо сгенерировано автоматически. Адрес, с которого было отправлено это письмо не является адресом для обратной связи. По всем вопросам пишете на почтовый ящик [REDACTED]

От: ANCanary

Рисунок 26. Пригласительное письмо.