RT Protect Awareness

Платформа по повышению
осведомленности сотрудников в сфере ИБ

Что такое RT Protect Awareness?

Это платформа по повышению осведомленности сотрудников в сфере информационной безопасности с понятным запоминающимся контентом и возможностью проверить знания сотрудников при помощи имитированных фишинговых атак.

Проблема

01. Большинство сотрудников не знают основ цифровой гигиены, поэтому халатно относятся к информационной безопасности при использовании личных и корпоративных устройств.

02. У компаний отсутствует возможность контролировать уровень знаний своих сотрудников.

03. В компаниях отсутствует инструмент, с помощью которого можно проверить действия сотрудников в ситуациях, приближённых к реальной атаке.

04. У руководителей нет подробной аналитики по уровню подготовки сотрудников и степени их уязвимости к действиям злоумышленников.

Решение

Теоретическая составляющая

Обучающие курсы

Тестовые задания

Практическая составляющая

Имитация фишинга

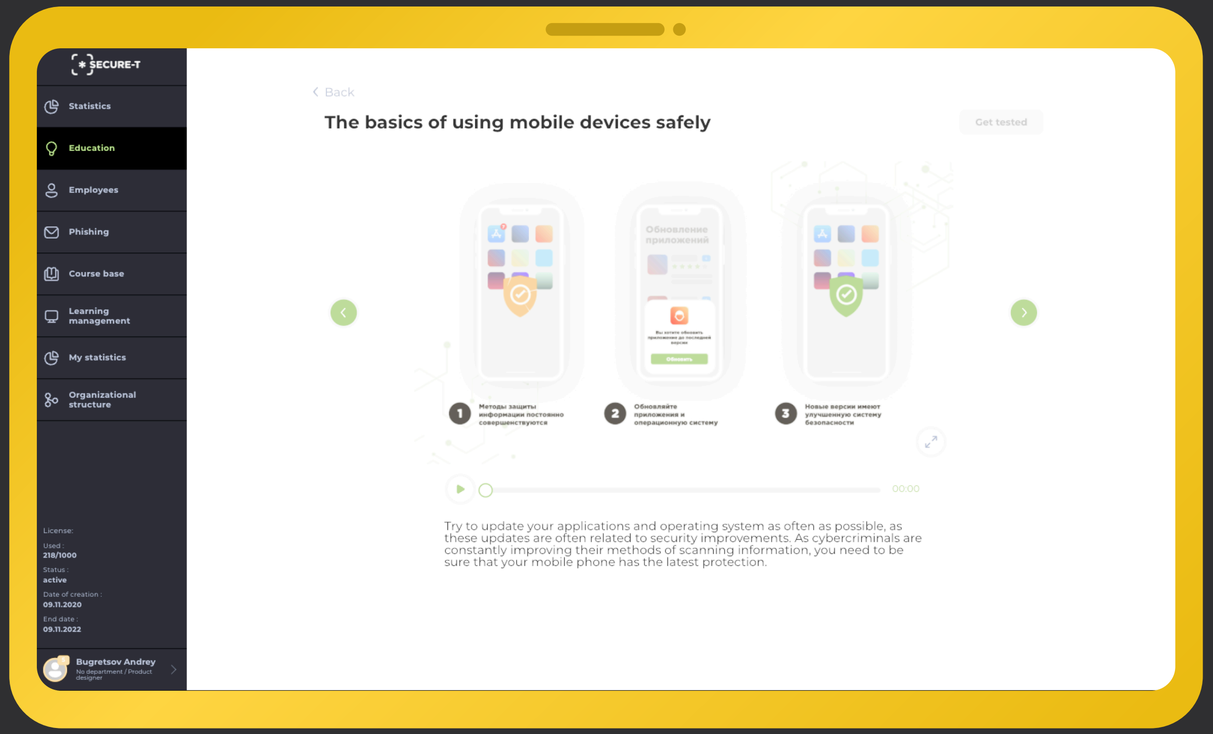
Вирусные вложения

RT Protect Awareness в лёгкой и понятной форме повышает осведомлённость сотрудников при помощи имитации фишинговых рассылок. У компании есть возможность проверить степень уязвимости сотрудников к действиям злоумышленника.

Подробная аналитика

Поиск уязвимых сотрудников

Набор курсов

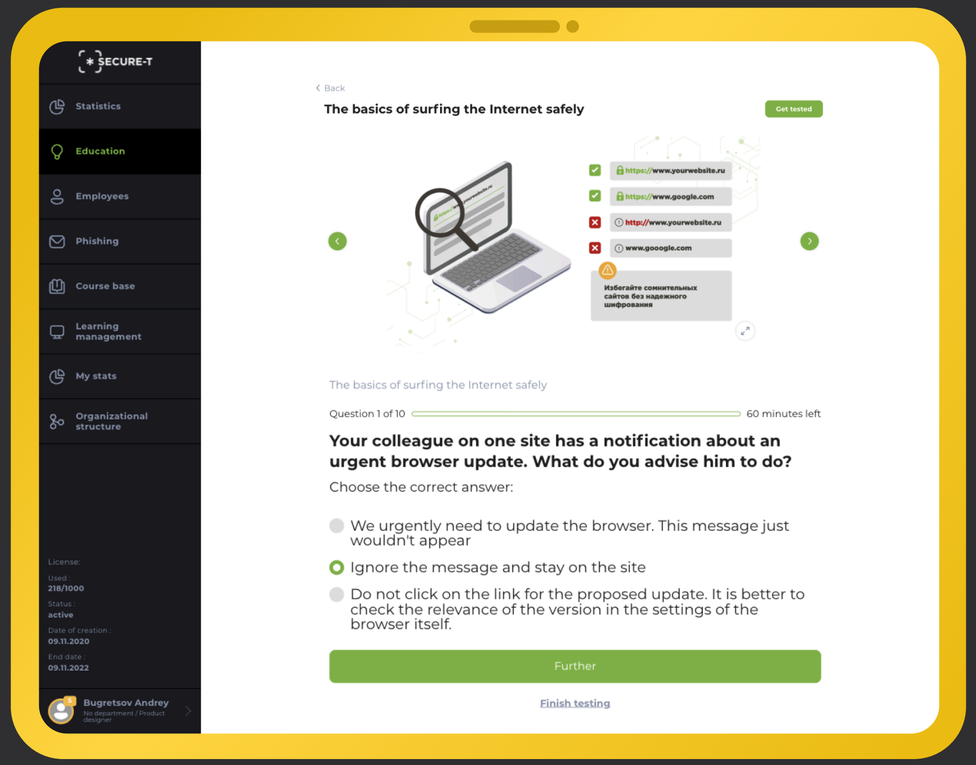


Платформа содержит в себе материалы и набор теоретических блоков — всё необходимое для обучения базовым понятиям и правилам работы с информационными ресурсами.

Более 50 курсов для обучения сотрудников

- Правила обращения с учетными записями.
- Конфиденциальные данные.
- Безопасная разработка ПО (SSDLC).
- Управление рисками информационной безопасности.
- Основы безопасности КИИ.
- Основные правила безопасности при удаленной работе.
- 152-ФЗ "О персональных данных.

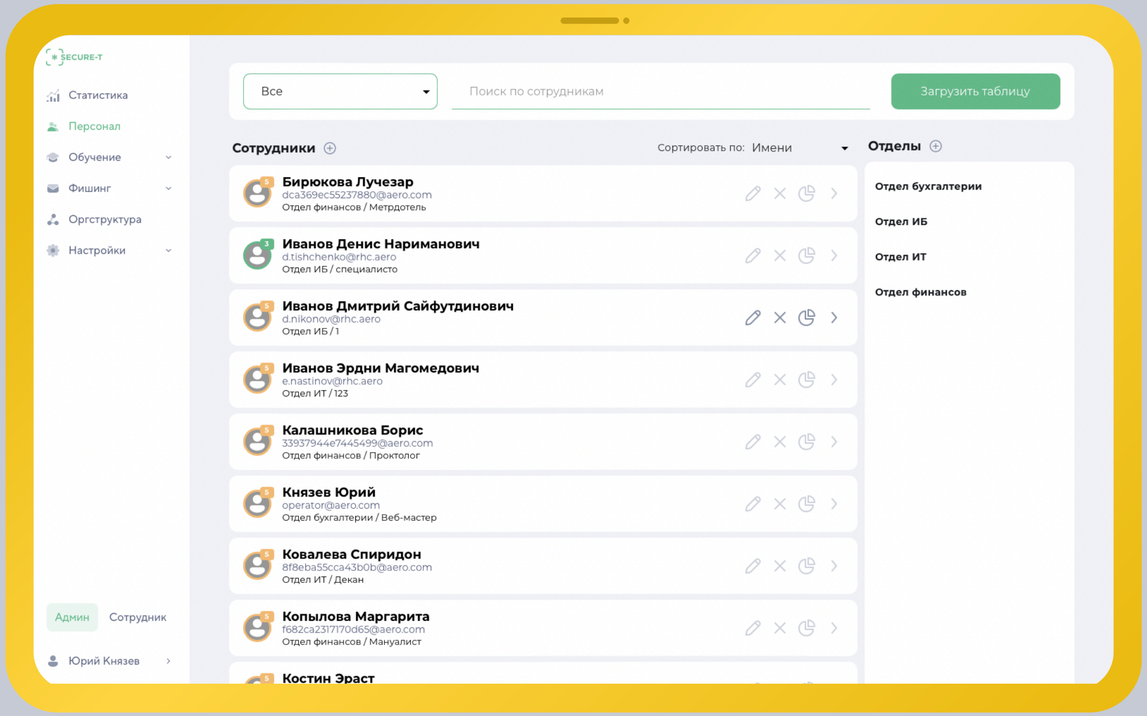
Имитация фишинга



Встроенный в систему фишинговый модуль проверяет, как поведут себя сотрудники компании при реальной атаке, и вычисляет, кто из них наиболее уязвим к этому виду социальной инженерии.

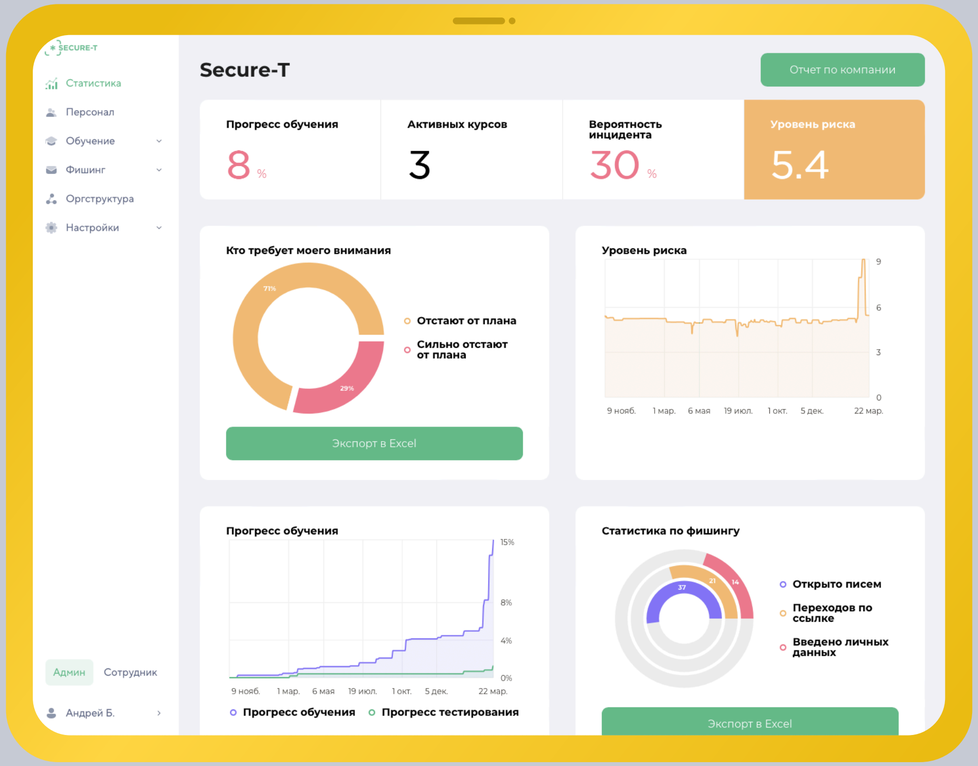
Преимущества

Простая интеграция



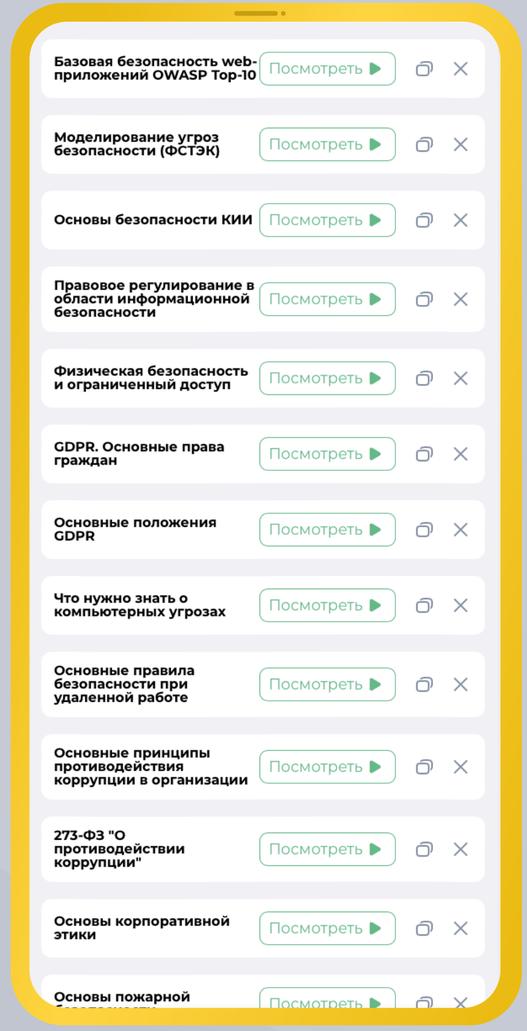
Интеграция платформы очень проста:
загрузите список пользователей с минимальным набором информации — можно начинать работать. Внедрение системы не требует большого количества трудозатрат.

Аналитический шаблон



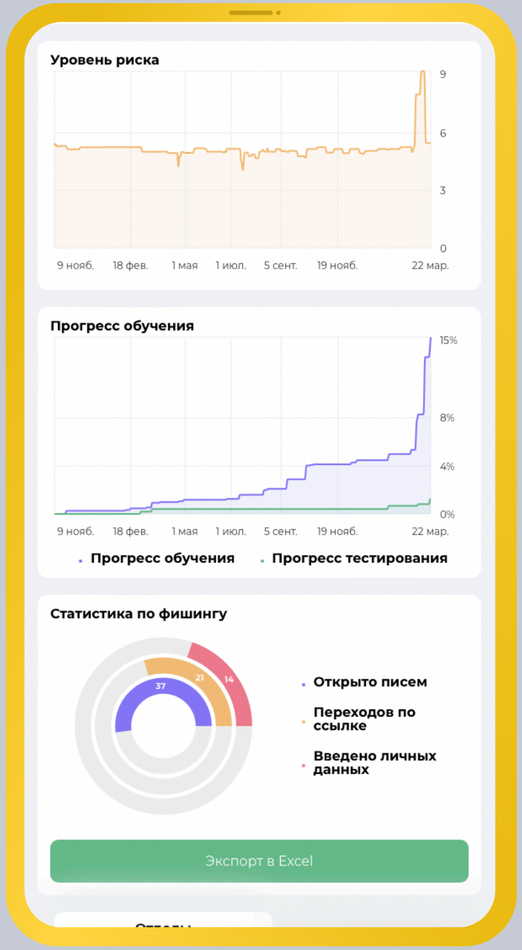
Встроенный в систему фишинговый модуль проверяет, как поведут себя сотрудники компании при реальной атаке, и вычисляет, кто из них наиболее уязвим к этому виду социальной инженерии.

Преимущества



Авторские курсы

Квалифицированные специалисты РТ-Информационная безопасность могут разработать авторские курсы для соответствия платформы целям и задачам компании.

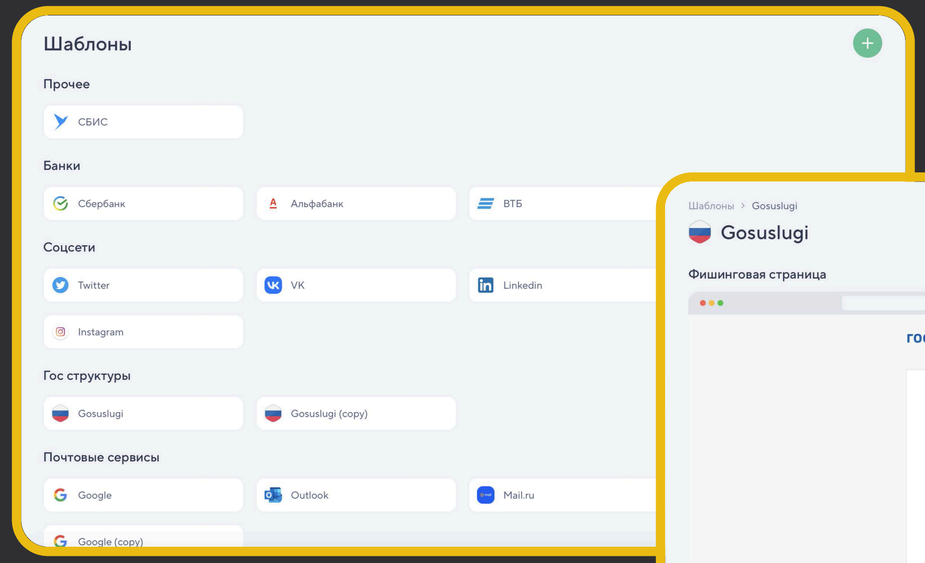


Адаптация под требования

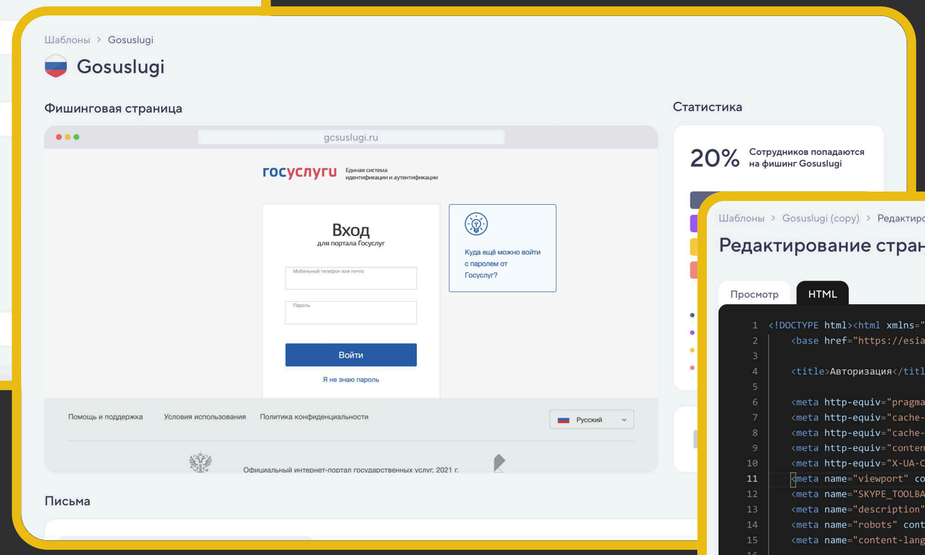
Благодаря гибкости платформы каждый заказчик может адаптировать периодичность обучения, необходимый набор курсов и частоту фишинговых рассылок для соответствия внутренней политики безопасности компании.

Редактор шаблонов

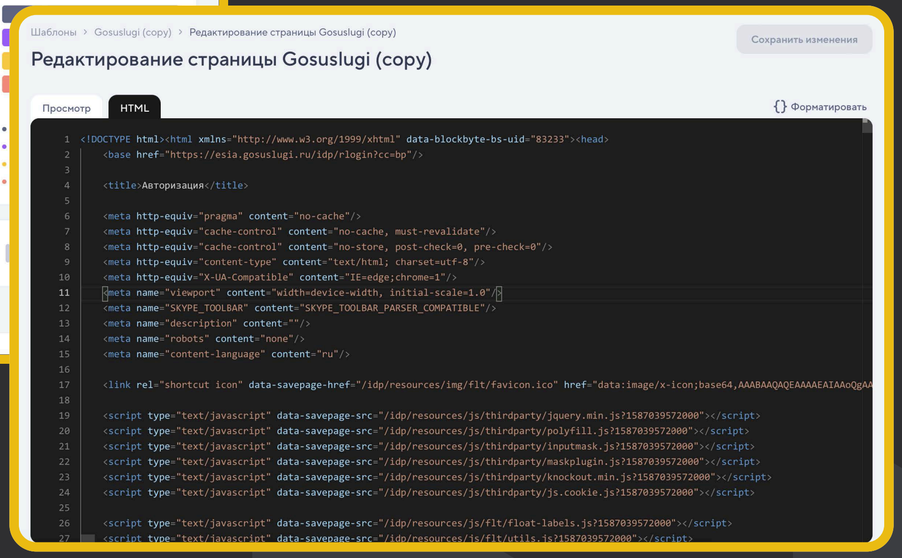
Возможность редактировать и создавать собственные фишинговые шаблоны прямо в системе при помощи пары кликов без потребности покупать домены.



Используйте готовые



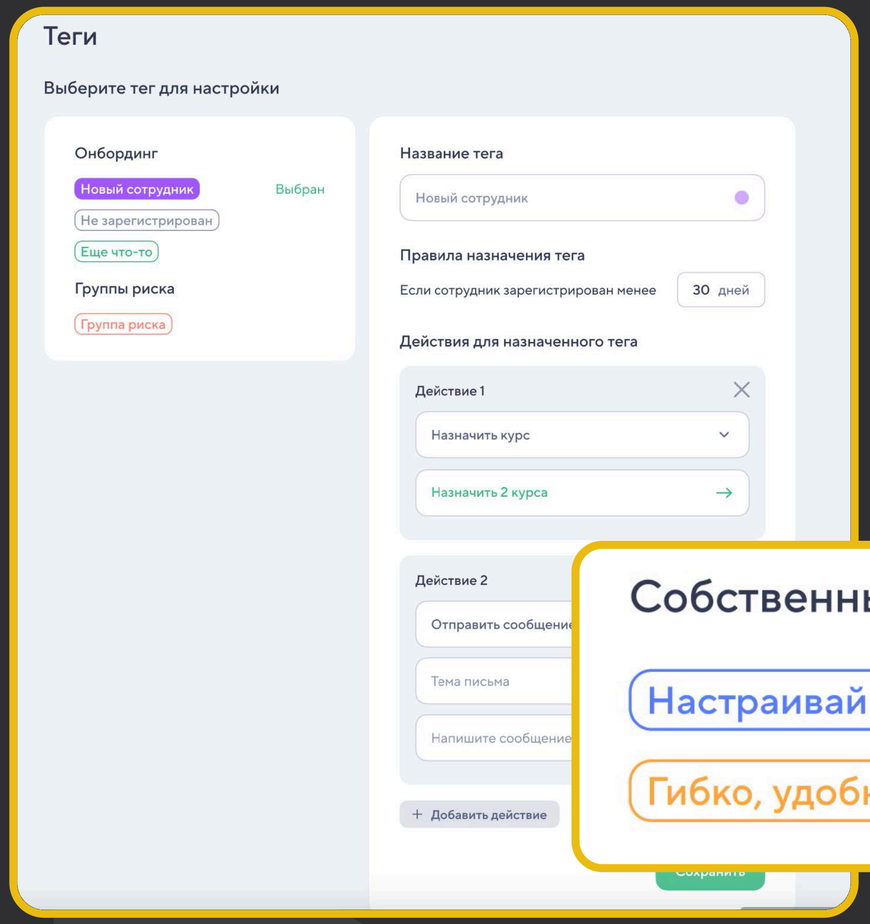
Создавайте свои



Редактируйте

Система тегирования

Онбординг — обучение для новых пользователей

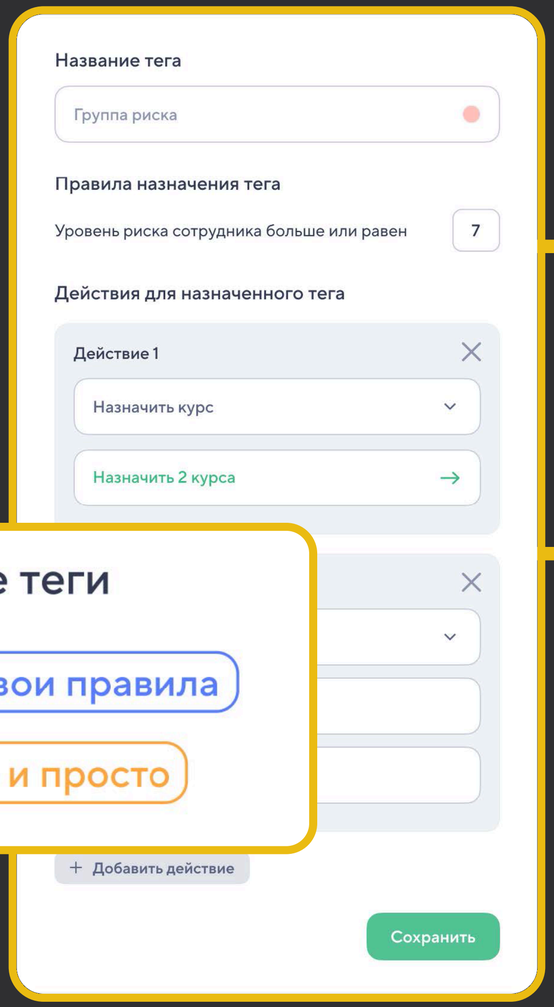


Собственные теги

Настраивай свои правила

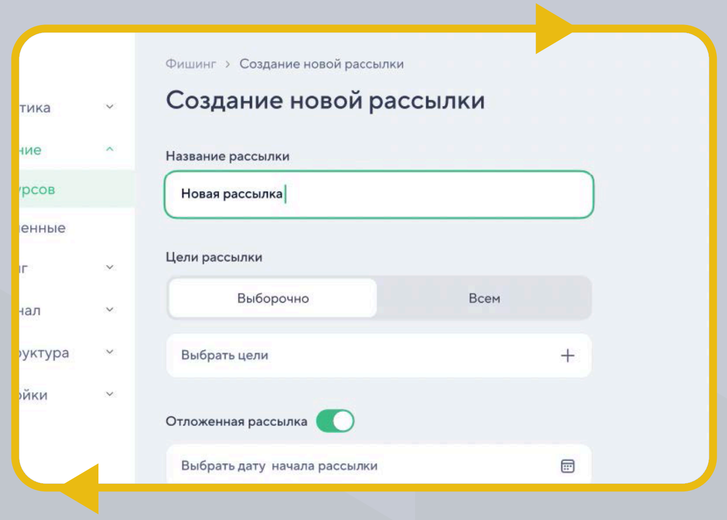
Гибко, удобно и просто

Группа риска — отслеживай уязвимых



Возможность создавать произвольные группы пользователей и назначать свои правила, автоматизируя платформу.

Как работает имитация фишинга?

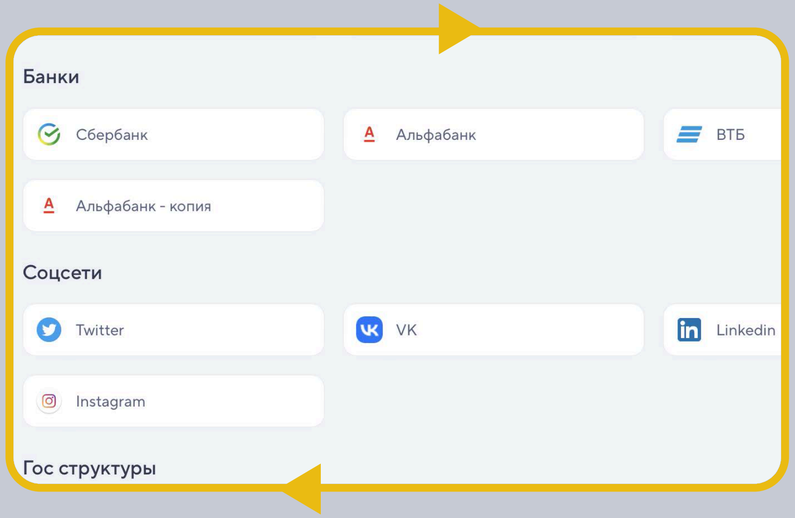


Создание рассылки

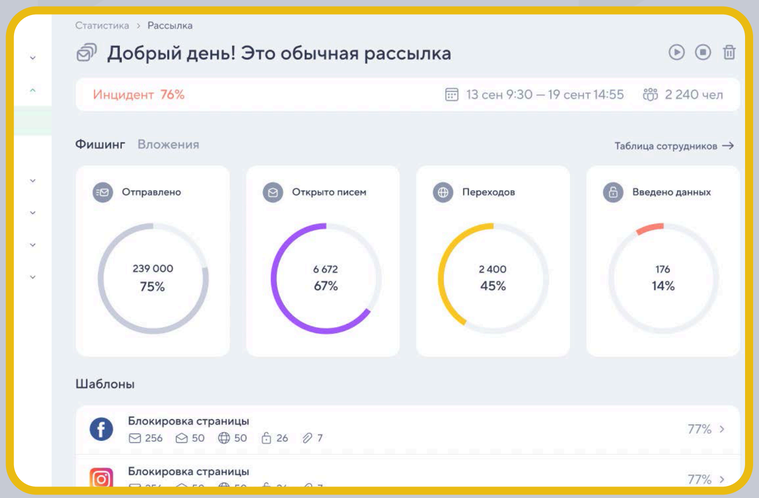
При создании рассылки её можно настроить под ваши цели: выбрать сотрудников, время рассылки, письма, настроить автоматическое назначение курса для тех, кто попался на фишинг.

Набор шаблонов с письмами

На платформе есть готовые шаблоны с известными компаниями для рассылки фишинговых писем. Также есть возможность самим создавать и редактировать письма.

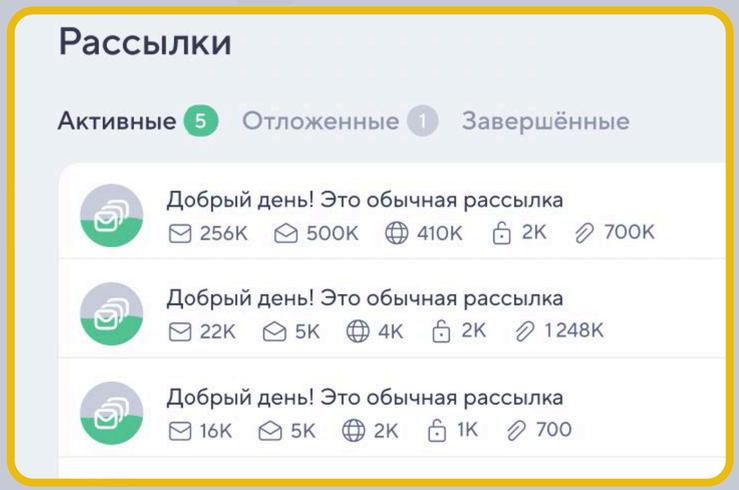


Как работает имитация фишинга?



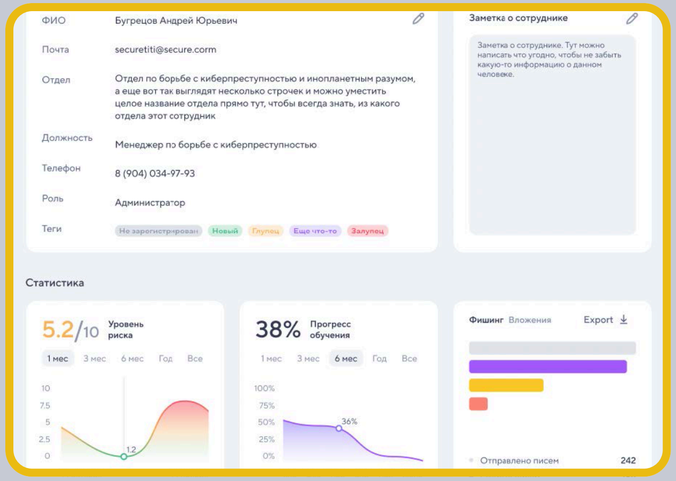
Мониторинг статистики расссылки

Во время рассылки можно следить за её аналитикой, не дожидаясь окончания. С помощью подробной статистики выявляются потенциально уязвимые сотрудники вашей компании, а также общий уровень опасности.



Множество рассылок

На платформе можно создавать сразу несколько рассылок с разными параметрами, это позволяет настраивать и запускать рассылки для разных отделов, которые по-разному реагируют на письма.



Отдельная карточка сотрудника

У каждого сотрудника есть отдельная страница с его данными и подробной статистикой. С её помощью можно следить за прогрессом отдельного сотрудника в компании.

Функциональность системы дистанционного обучения

Добавление собственных курсов

Контроль процесса прохождения курса

Автоматизация процесса обучения при помощи гибкой системы настроек

Соответствие законодательству

Федеральный закон «О персональных данных» от 27.07.2006 № 152-ФЗ

п.6 ч.1 ст.18.1 ФЗ-152: ознакомление работников оператора, непосредственно осуществляющих обработку персональных данных, с положениями законодательства Российской Федерации о персональных данных, в том числе требованиями к защите персональных данных, документами, определяющими политику оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников.

Положение Банка России от 20 апреля 2021 г. № 757-П + ГОСТ Р 57580.1-2017

п. 8.3.1 ГОСТ Р 57580.1-2017: обучение, практическая подготовка (переподготовка) работников финансовой организации, ответственных за применение мер защиты информации; повышение осведомлённости (инструктаж) работников финансовой организации в области защиты информации.

Приказ ФСТЭК России от 25 декабря 2017 г. № 239 КИИ

Состав мер по обеспечению безопасности для значимого объекта соответствующей категории значимости:
— Информирование и обучение персонала (ИПО).

Мы — эксперты в области информационной безопасности

- Наша команда состоит из профессионалов с многолетним стажем в области аудита информационной безопасности, тестирования на проникновение и проектирования систем защиты информации.
  Мы ориентируемся на частные и государственные компании, которые заботятся о безопасности своей информации и защищённости IT инфраструктуры.

- Используя накопленные знания и опыт проведения обучающих тренингов, мы создали платформу для повышения уровня осведомлённости сотрудников в области информационной безопасности.

Нам доверяют

Ростех
РТ-Энергоэффективность
РТ
Развитие бизнеса
Ростех
Техприемка
Ростех
KAMAZ
ОАК
Объединенная авиастроительная корпорация
ОДК
КБП
СИБЕР
Нацимбио
Высокоточные комплексы
УВЗ
НОВИКОМБАНК

Контакты

Адрес: 117587, г. Москва,
Варшавское шоссе,
дом 118, корпус 1

Tel.: +7 (499) 390-79-05

E-mail: info@rt-ib.ru

Сайт: rt-ib.ru

РТ
Информационная безопасность