Security Awareness: Защити свой бизнес изнутри

Платформа для развития сотрудников в области кибербезопасности

Проблема

1

Неосведомленность

Недостаточная осведомленность пользователей о рисках кибербезопасности, основах цифровой гигиены и необходимых мерах защиты

2

Отсутствие контроля

Нехватка ресурсов или отсутствие возможности контроля знаний сотрудников

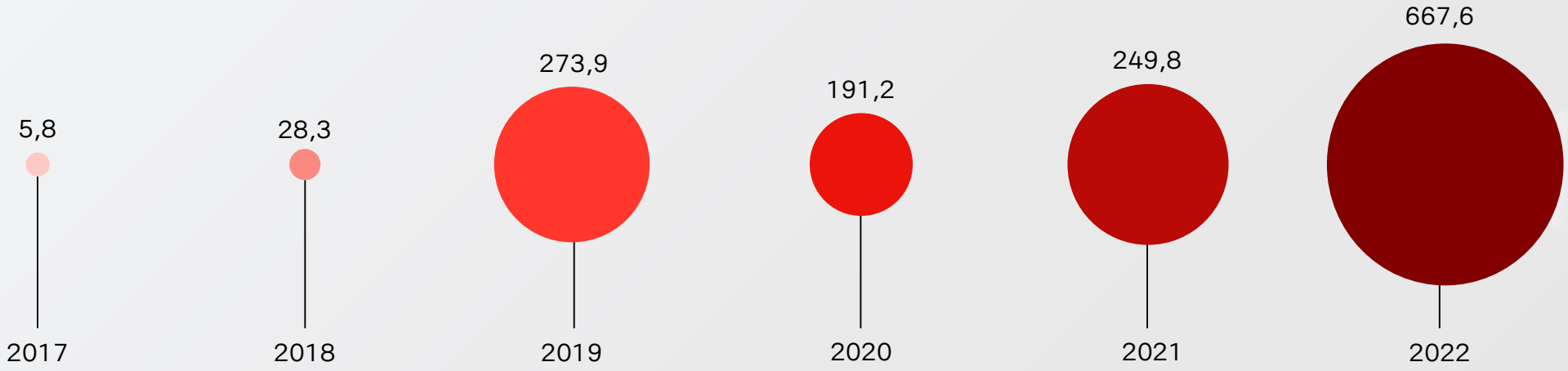
3

Нехватка аналитики

Отсутствие подробной аналитики по уровню подготовки сотрудников и степени их уязвимости

Статистика

93 %
утечек данных
произошли из-за
фишинговых атак



количество утекших записей ПДн и платежной информации. Млн записей, 2017–2022 гг.

Источники: https://www.computerweekly.com/news/365532100/Nine-in-10-enterprises-fell-victim-to-successful-phishing-in-2022

InfoWatch. Утечки данных организаций по вине или неосторожности внутреннего нарушителя

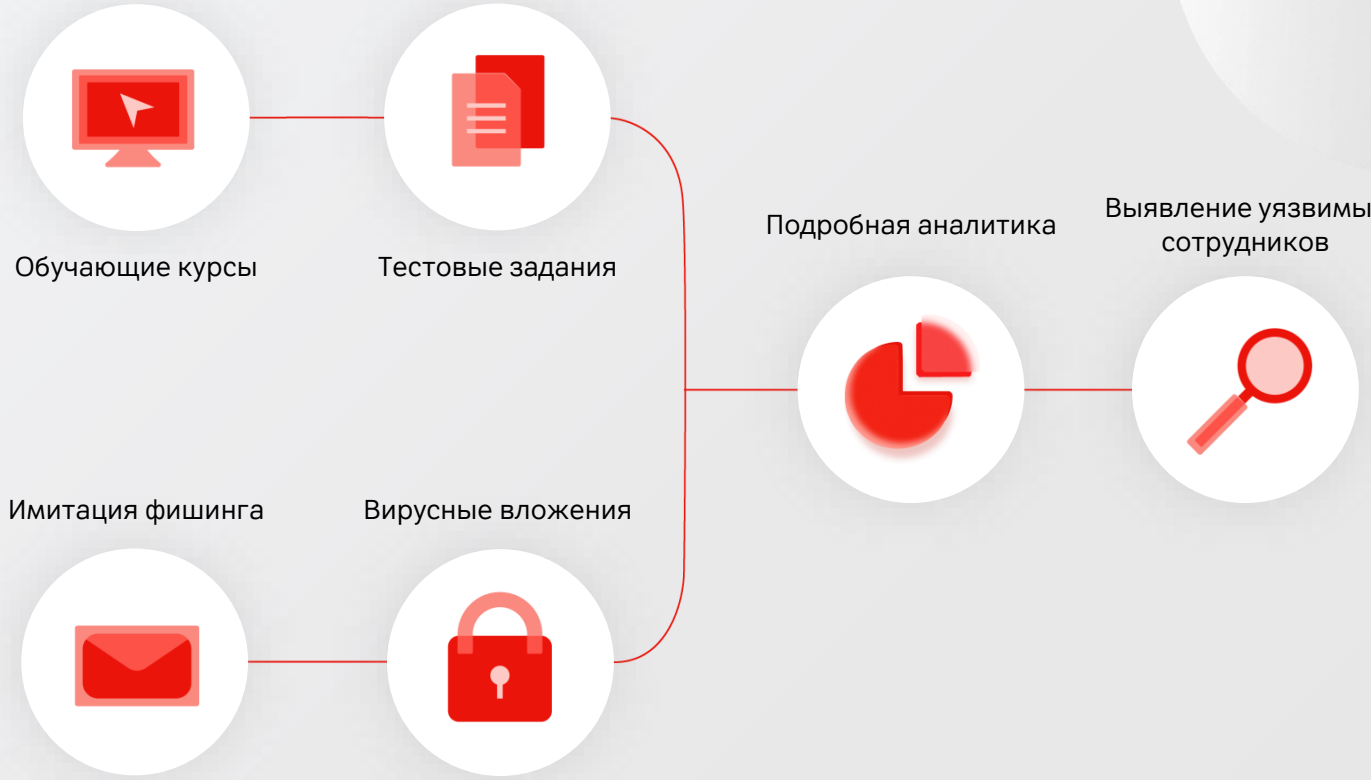
Как защититься

Регулярное обучение

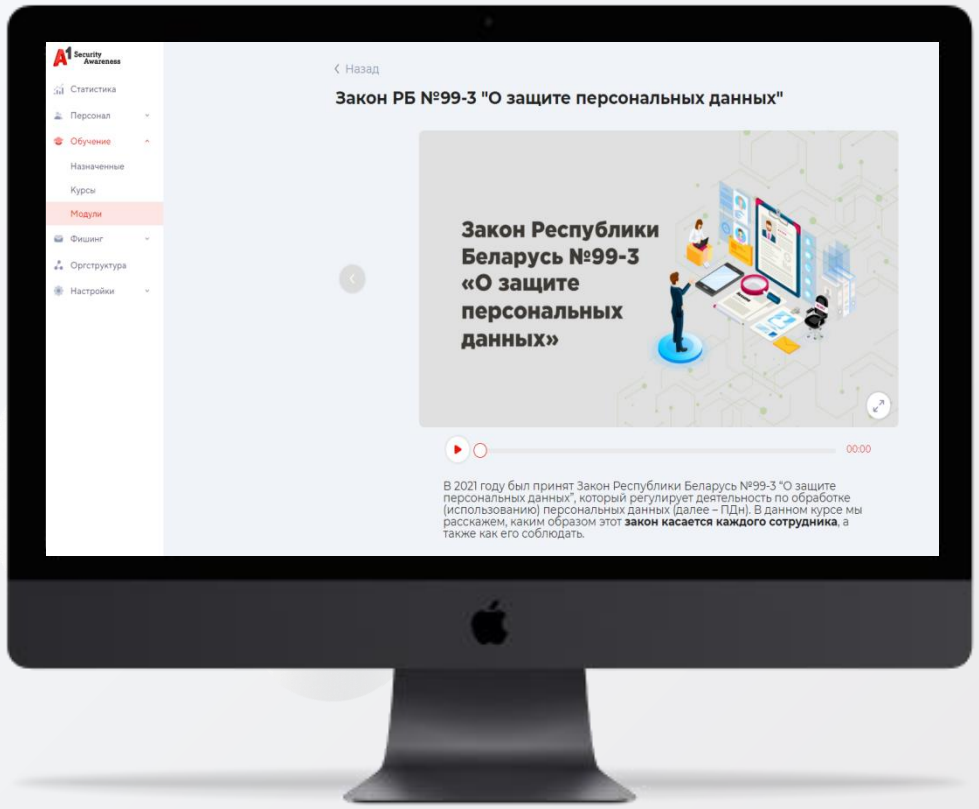
Повышение осведомленности сотрудников в области ИБ

Имитированные атаки

Проверка сотрудников, как они реагируют на потенциальную угрозу со стороны мошенников

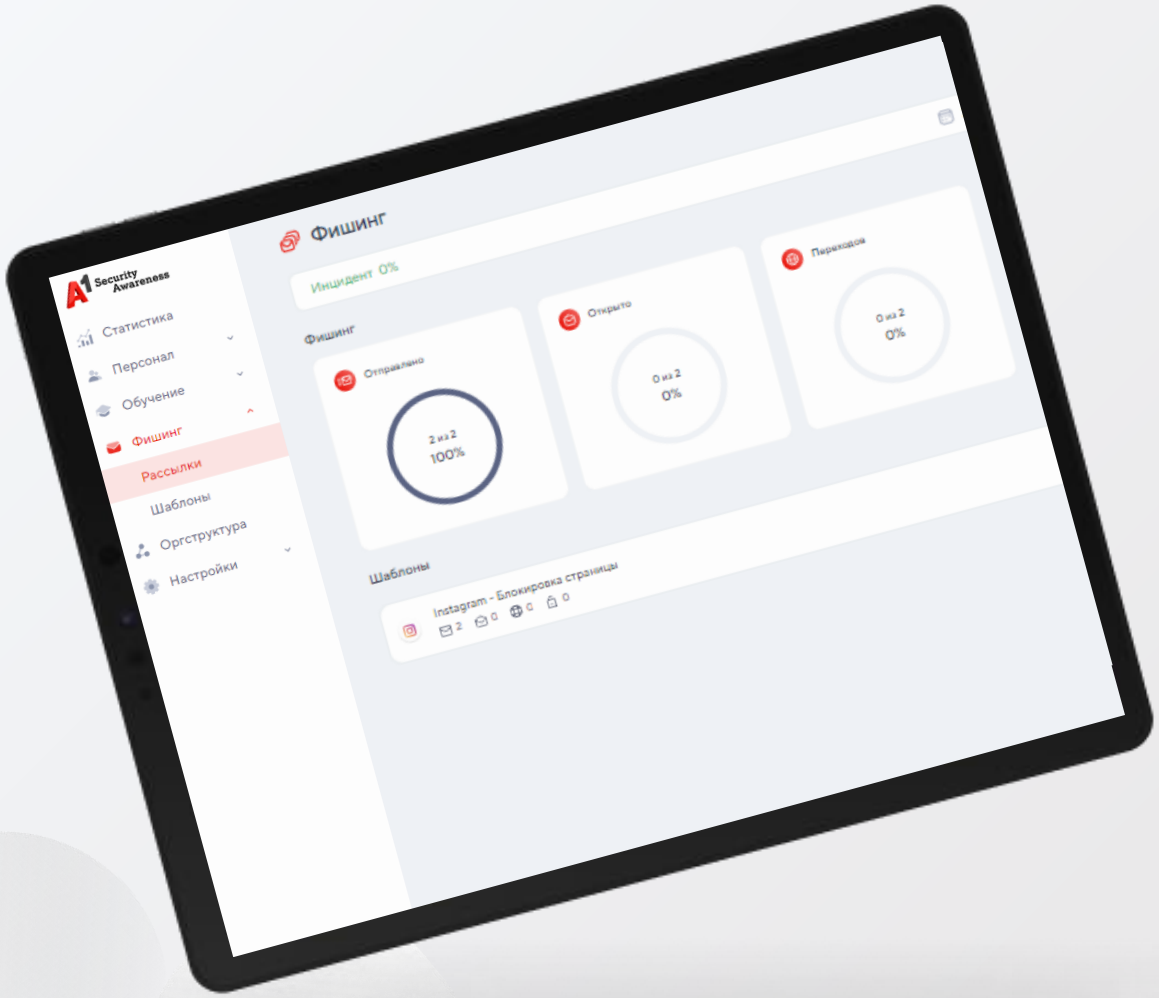


Security Awareness – это



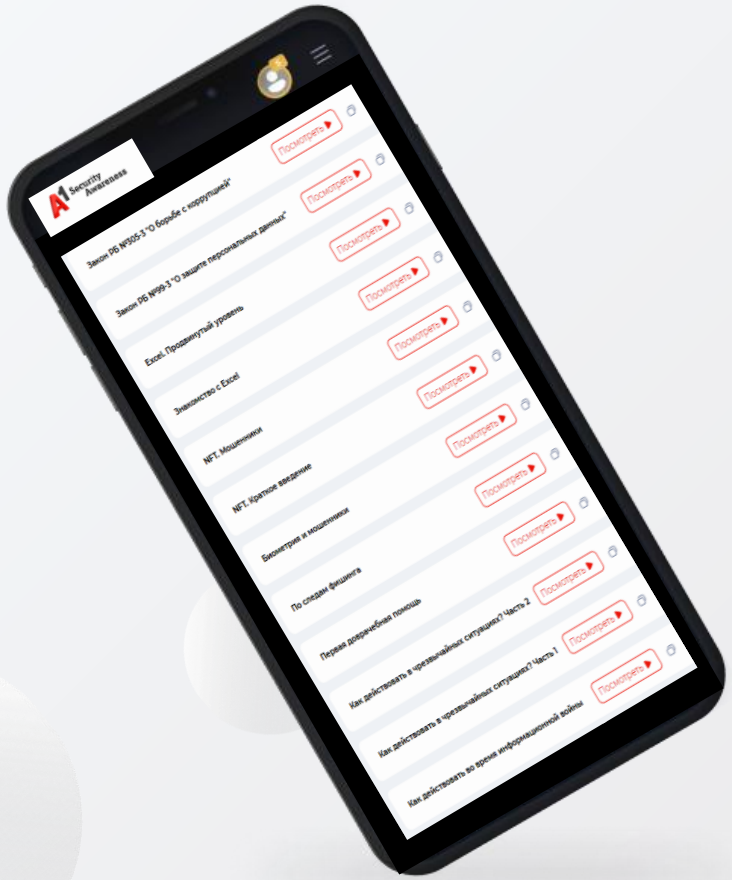
- Базовые курсы по кибербезопасности
- Тесты после прохождения курсов
- Имитация фишинга

Имитация фишинга



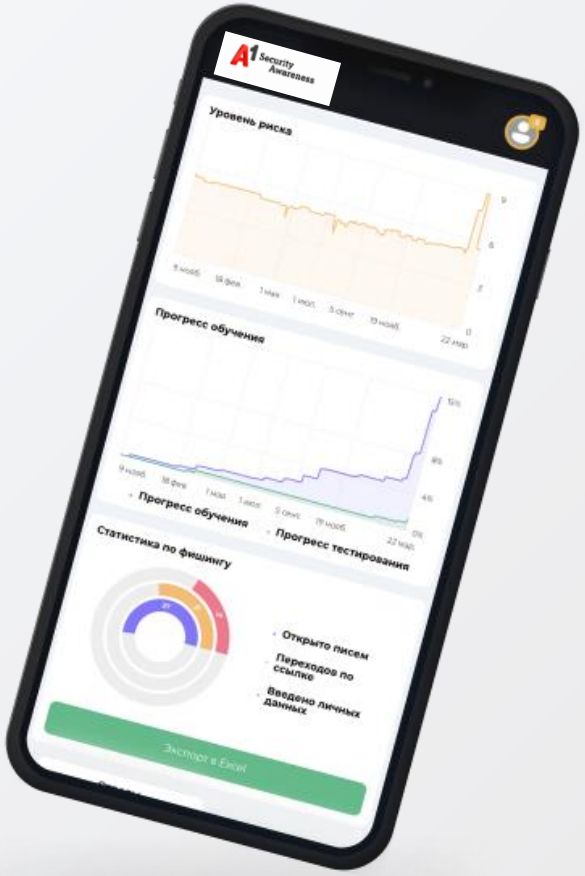
Встроенный в систему фишинговый модуль позволяет проверить, как поведут себя сотрудники компании при реальной атаке, и выявить, кто из них наиболее уязвим к этому виду социальной инженерии.

Авторские курсы



Возможность самостоятельного создания курсов либо редактирование действующих под цели компании.

Гибкость

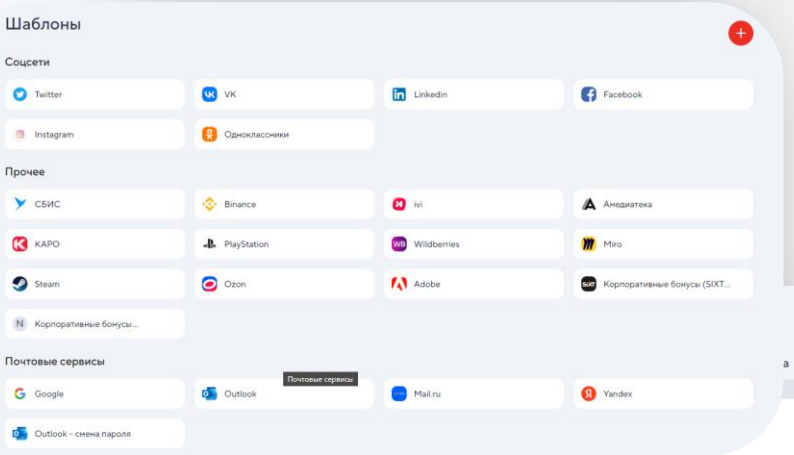


Каждый заказчик может настроить периодичность обучения по выбранным курсам и частоту фишинговых рассылок для соответствия внутренней политике безопасности компании

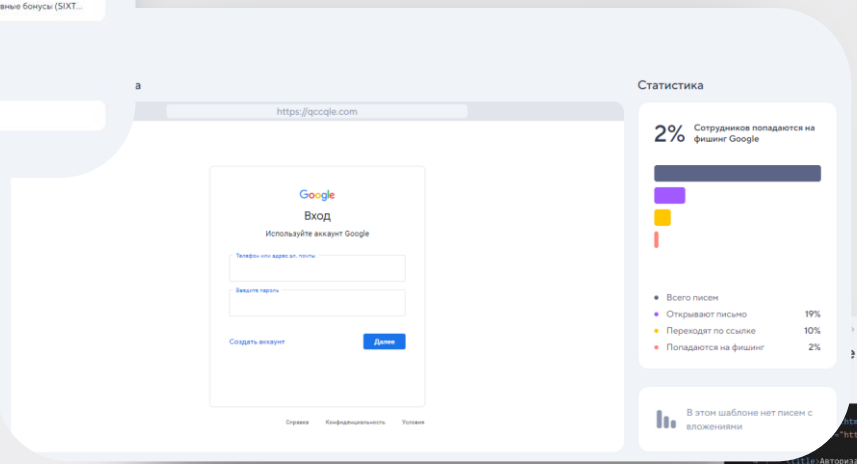
Редактор шаблонов

Используйте готовые

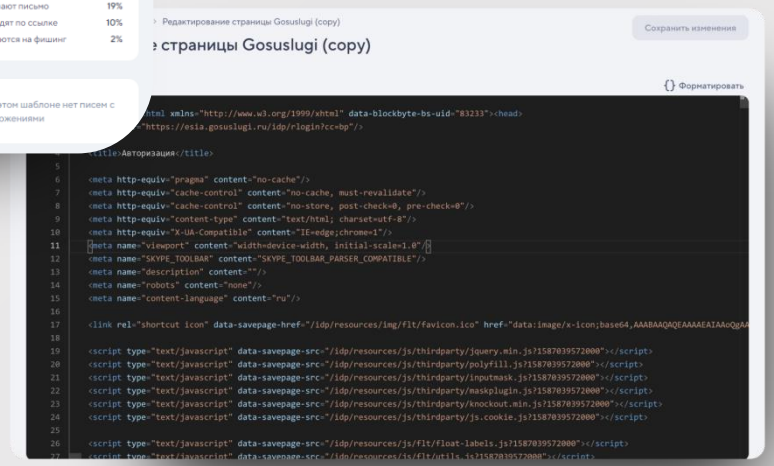
Возможность редактировать готовые и создавать собственные фишинговые шаблоны прямо в системе при помощи пары кликов



Создавайте свои



Редактируйте

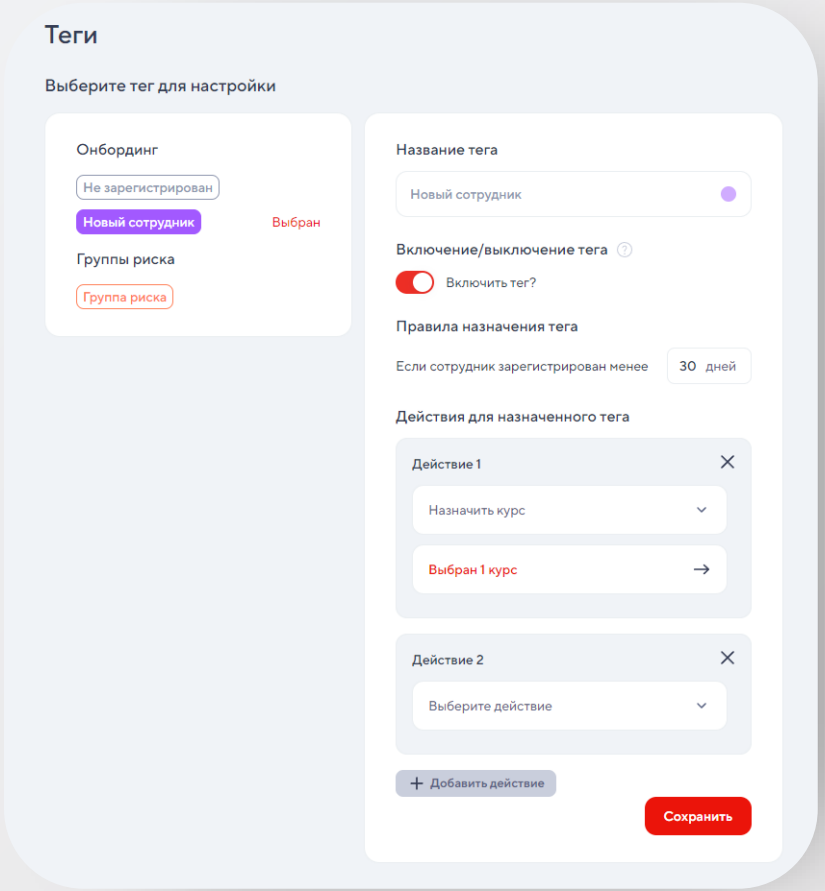


Система тегирования

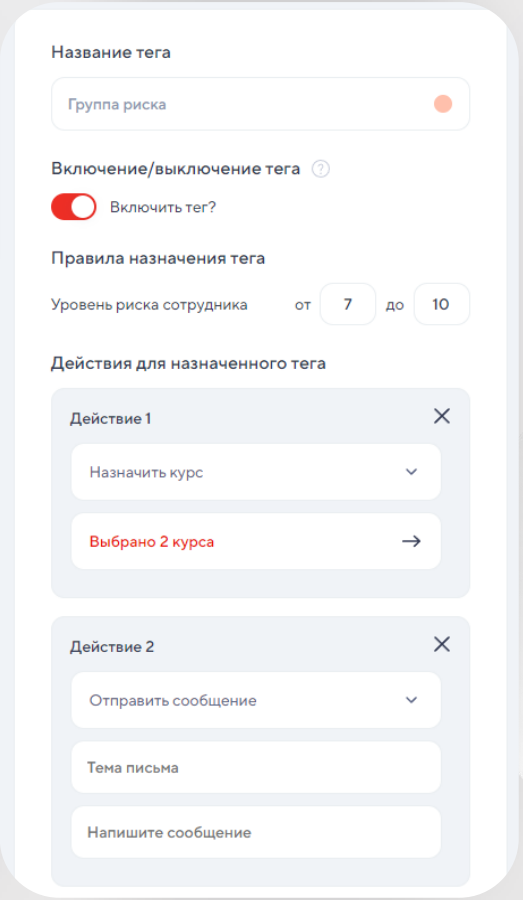
Создание произвольных групп пользователей и назначение им индивидуальных правил

- **Гибко, удобно и просто**

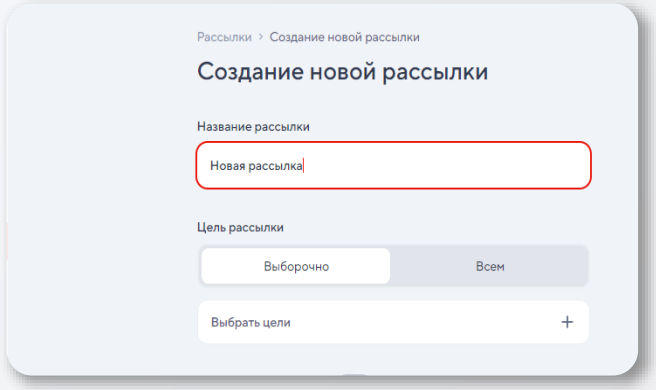
Автоматическое назначение курса для новых сотрудников



Автоматическое назначение курса для группы риска

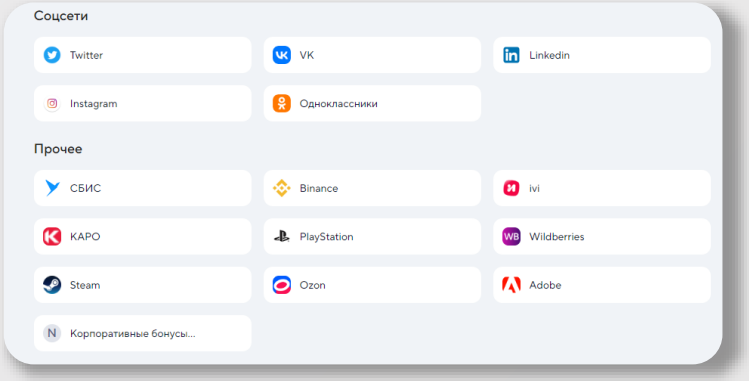


Как работает имитация фишинга?



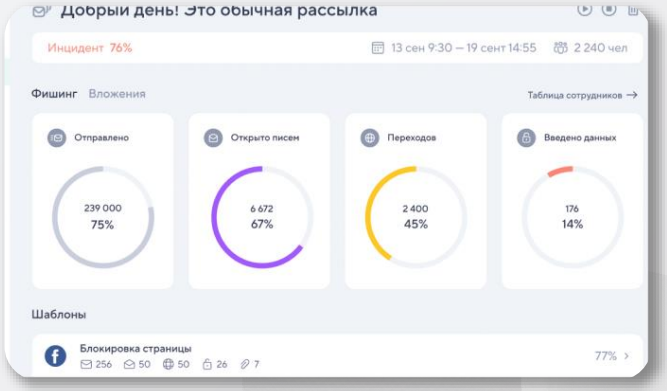
Создание рассылки

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



Шаблоны писем

На платформе есть готовые шаблоны для рассылки фишинговых писем, которые можно редактировать или создавать собственные.

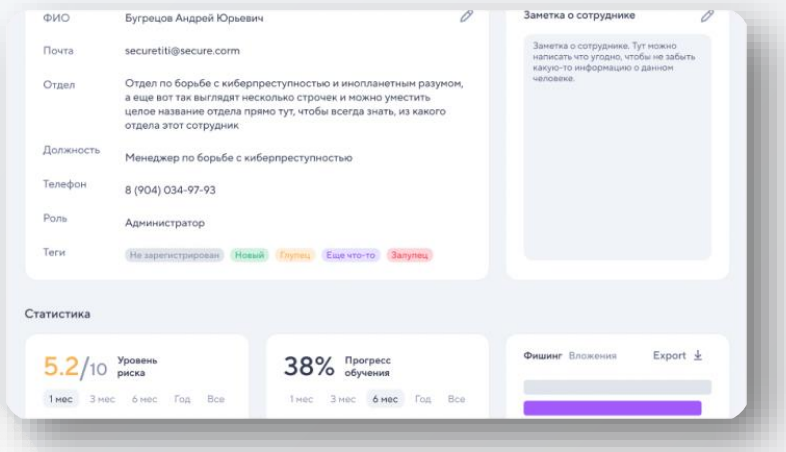


Мониторинг статистики рассылки

Следить за аналитикой можно в процессе рассылки, не дожидаясь её окончания.

Подробная статистика показывает уязвимых сотрудников, а также общий уровень опасности вашей компании.

Как работает имитация фишинга?

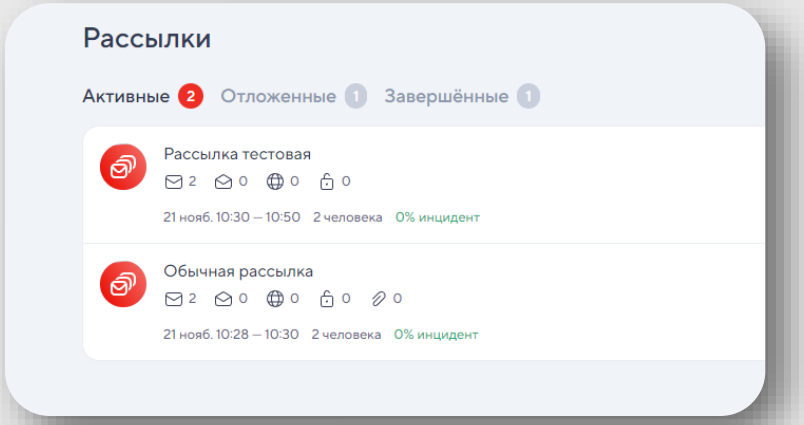


Карточка сотрудника

У каждого сотрудника есть своя отдельная страница с его данными и подробной статистикой, позволяющей отслеживать прогресс.

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.



Мы предлагаем

Доступ к платформе: обучение и фишинг

Разовая фишинговая атака

Самостоятельное управление

- Базовые курсы, тестирование, регулярный фишинг, статистика, степень защищённости вашей компании
- Выявление уязвимых сотрудников, итоговый отчёт по результатам атаки
- Гибкое управление платформой, назначение собственных групп и правил.

Последствия фишинговых атак

3 млрд

фишинговых писем ежедневно злоумышленники отправляют Компаниям*

85%

утечек данных происходят из-за «человеческого фактора»**

$4,24 млн

составляет средняя стоимость утечки данных в 2022 году***

* 2021 Data Breach Investigation Report

** Cost of a Data Breach Report 2021, Ponemon Institute и IBM Security)

*** Email Fraud Landscape: Spring 2021

Спасибо

sales@a1data.by
+375296000225