

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

Теоритическая 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.

The screenshot displays the SECURE-T platform interface. On the left is a dark sidebar menu with icons and labels for 'Statistics', 'Education', 'Employees', 'Phishing', 'Course base', 'Learning management', 'My statistics', and 'Organizational structure'. The main content area is white and features a course titled 'The basics of using mobile devices safely'. At the top of the course page, there is a 'Back' link and a 'Get tested' button. The course content is presented as a video player with a progress bar at the bottom. The video frame shows three numbered steps: 1. 'Методы защиты информации постоянно совершенствуются' (Information protection methods are constantly improving), 2. 'Обновляйте приложения и операционную систему' (Update applications and the operating system), and 3. 'Новые версии имеют улучшенную систему безопасности' (New versions have an improved security system). Below the video, there is a text block: 'Try to update your applications and operating system as often as possible, as these updates are often related to security improvements. As cybercriminals are constantly improving their methods of scanning information, you need to be sure that your mobile phone has the latest protection.' The bottom left of the interface shows license information: 'License: Used: 218/1000, Status: active, Date of creation: 09.11.2020, End date: 09.11.2022' and the user profile 'Bugretsov Andrey, No department / Product designer'.

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

SECURE-T

Statistics

Education

Employees

Phishing

Course base

Learning management

My stats

Organizational structure

License:
Used: 218/1000
Status: active
Date of creation: 09.11.2020
End date: 09.11.2022

Bugretsov Andrey
No department / Product Designer

< Back

The basics of surfing the Internet safely

Get tested

https://www.yourwebsite.ru

https://www.google.com

http://www.yourwebsite.ru

www.google.com

Избегайте сомнительных сайтов без надежного шифрования

The basics of surfing the Internet safely

Question 1 of 10 60 minutes left

Your colleague on one site has a notification about an urgent browser update. What do you advise him to do?

Choose the correct answer:

- We urgently need to update the browser. This message just wouldn't appear
- Ignore the message and stay on the site
- Do not click on the link for the proposed update. It is better to check the relevance of the version in the settings of the browser itself.

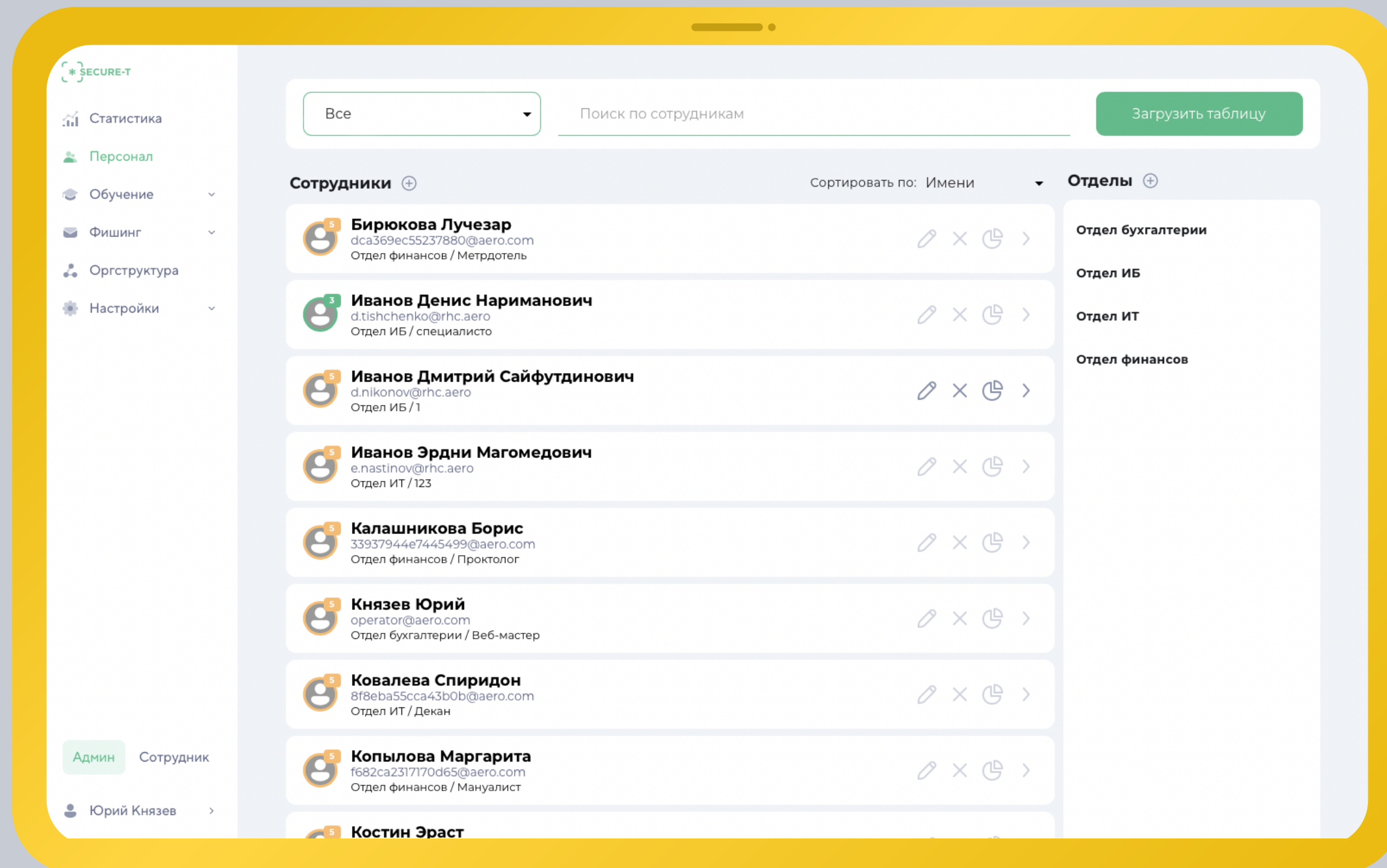
Further

Finish testing

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.

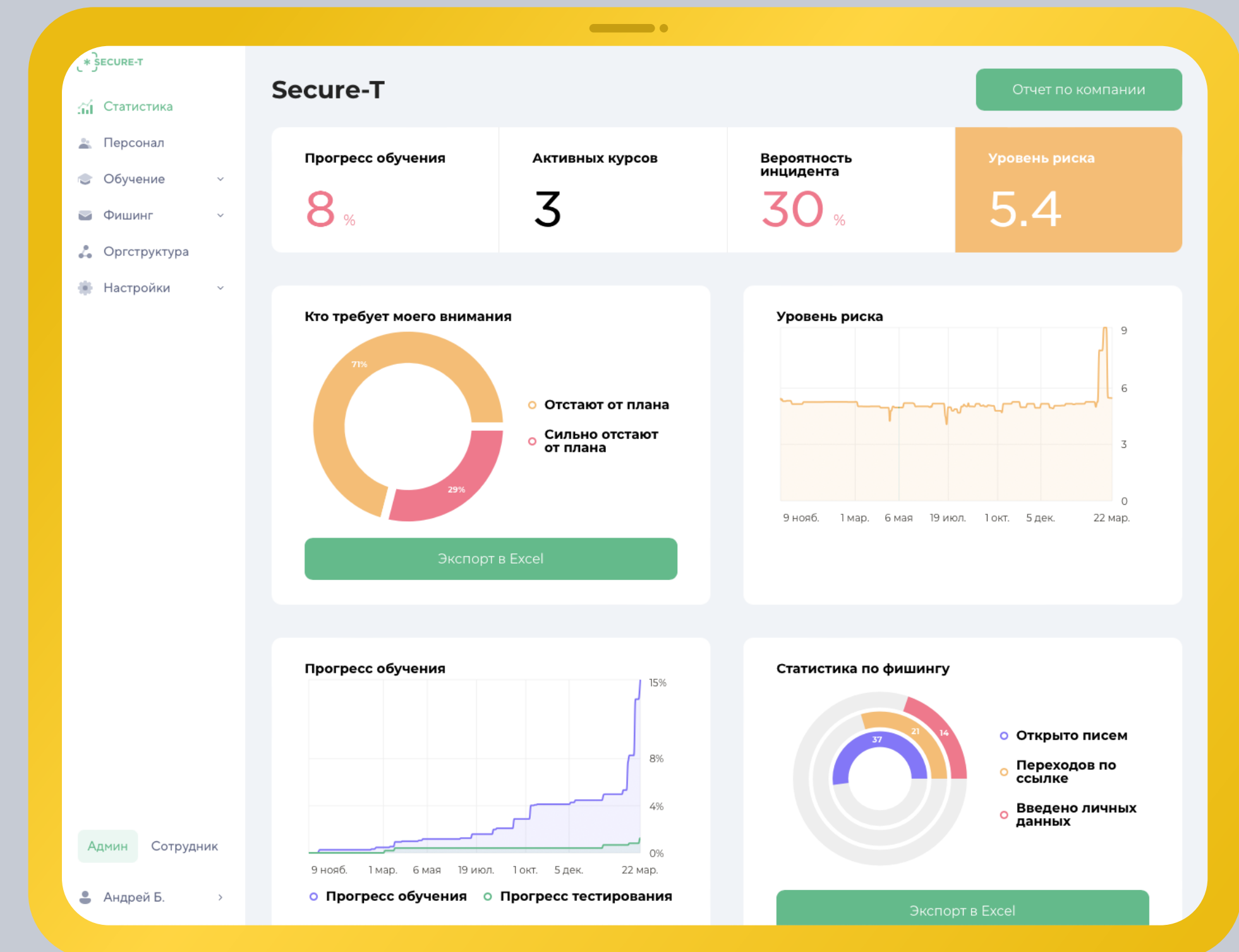
Преимущества

Простая интеграция



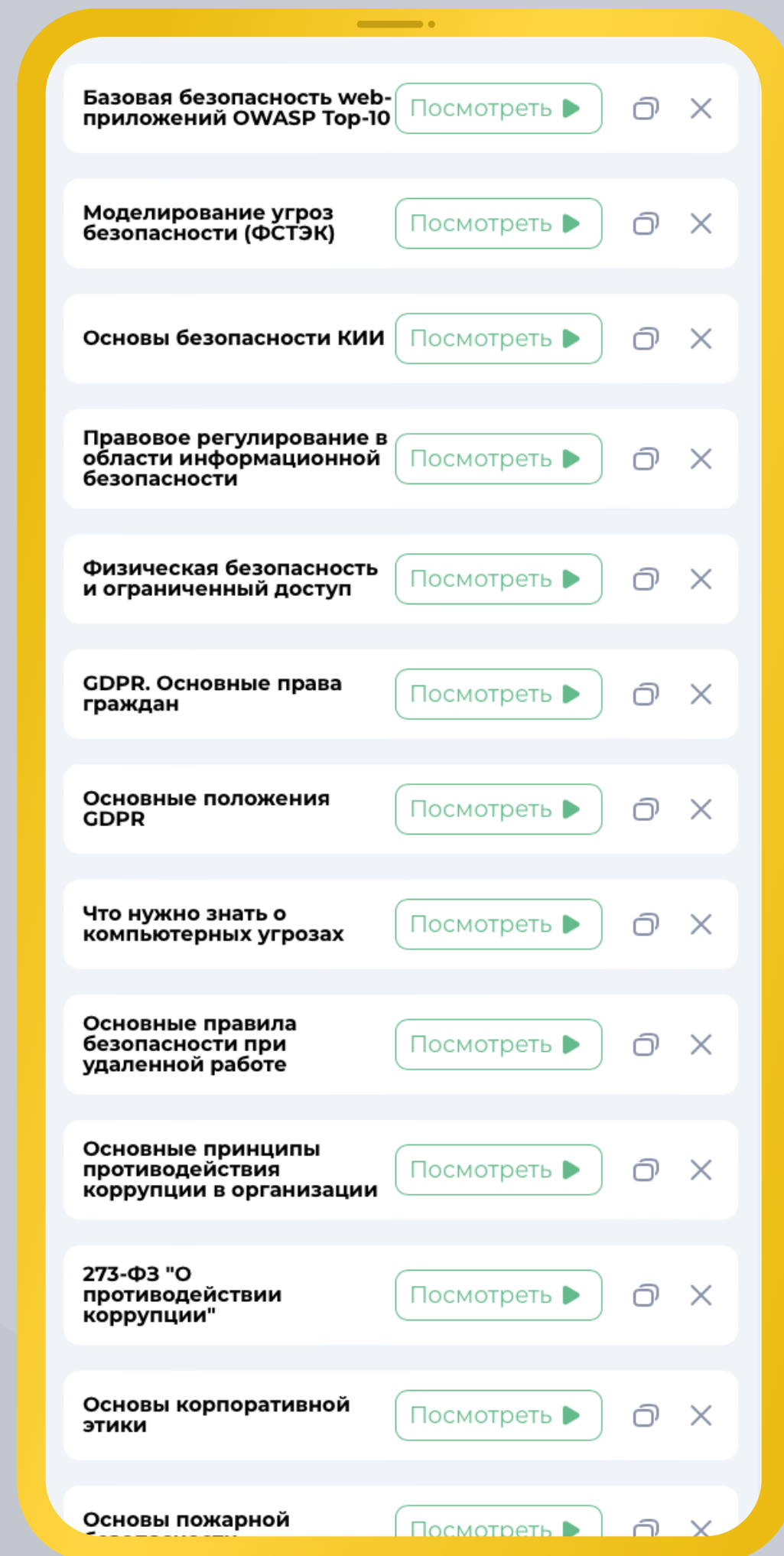
Интеграция платформы очень проста: загрузите список пользователей с минимальным набором информации — можно начинать работать. Внедрение системы не требует большого количества трудозатрат.

Аналитический шаблон



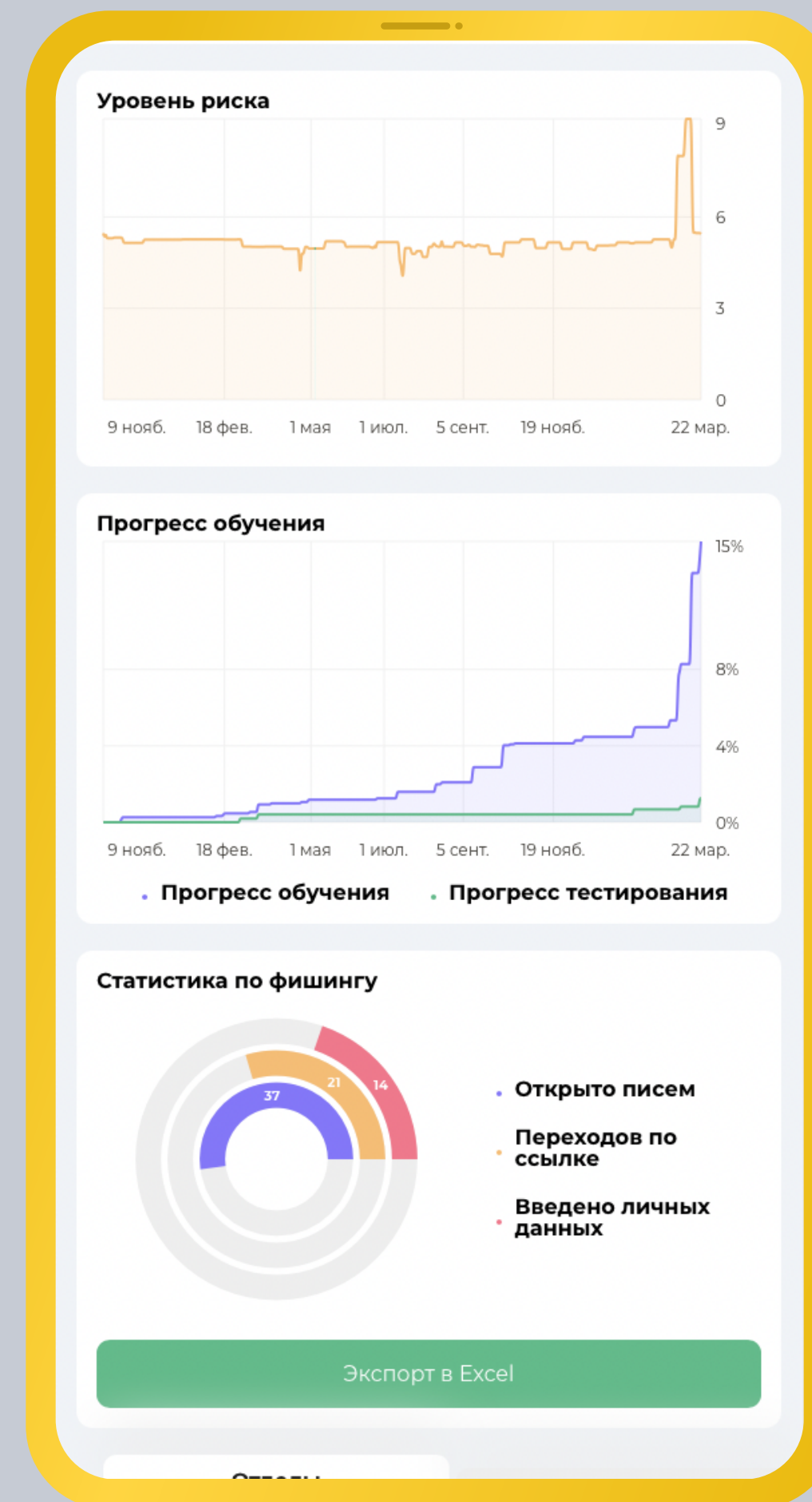
Встроенный в систему фишинговый модуль проверяет, как поведут себя сотрудники компании при реальной атаке, и вычисляет, кто из них наиболее уязвим к этому виду социальной инженерии.

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 политике безопасности компании.

Редактор шаблонов



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

Шаблоны

Прочее

СБИС

Банки

Сбербанк Альфабанк ВТБ

Соцсети

Twitter VK LinkedIn Instagram

Гос структуры

Gosuslugi Gosuslugi (copy)

Почтовые сервисы

Google Outlook Mail.ru Google (copy)

Шаблоны > Gosuslugi

Gosuslugi

Фишинговая страница

gcsuslugi.ru

Вход для портала Госуслуг

Мобильный телефон или почта

Пароль

Войти

Я не знаю пароль

Куда ещё можно войти с паролем от Госуслуг?

Помощь и поддержка Условия использования Политика конфиденциальности

Русский

Официальный интернет-портал государственных услуг. 2021 г.

Письма

Статистика

20% Сотрудников попадают на фишинг Gosuslugi

Шаблоны > Gosuslugi (copy) > Редактирование страницы Gosuslugi (copy)

Сохранить изменения

Просмотр HTML

```
1 <!DOCTYPE html><html xmlns="http://www.w3.org/1999/xhtml" data-blockbyte-bs-uid="83233"><head>
2 <base href="https://esia.gosuslugi.ru/idp/rlogin?cc=bp"/>
3
4 <title>Авторизация</title>
5
6 <meta http-equiv="pragma" content="no-cache"/>
7 <meta http-equiv="cache-control" content="no-cache, must-revalidate"/>
8 <meta http-equiv="cache-control" content="no-store, post-check=0, pre-check=0"/>
9 <meta http-equiv="content-type" content="text/html; charset=utf-8"/>
10 <meta http-equiv="X-UA-Compatible" content="IE=edge;chrome=1"/>
11 <meta name="viewport" content="width=device-width, initial-scale=1.0"/>
12 <meta name="SKYPE_TOOLBAR" content="SKYPE_TOOLBAR_PARSER_COMPATIBLE"/>
13 <meta name="description" content="" />
14 <meta name="robots" content="none"/>
15 <meta name="content-language" content="ru"/>
16
17 <link rel="shortcut icon" data-savepage-href="/idp/resources/img/flt/favicon.ico" href="data:image/x-icon;base64,AAABAAQAEAAAAEIAA0QgAA
18
19 <script type="text/javascript" data-savepage-src="/idp/resources/js/thirdparty/jquery.min.js?1587039572000"></script>
20 <script type="text/javascript" data-savepage-src="/idp/resources/js/thirdparty/polyfill.js?1587039572000"></script>
21 <script type="text/javascript" data-savepage-src="/idp/resources/js/thirdparty/inputmask.js?1587039572000"></script>
22 <script type="text/javascript" data-savepage-src="/idp/resources/js/thirdparty/maskplugin.js?1587039572000"></script>
23 <script type="text/javascript" data-savepage-src="/idp/resources/js/thirdparty/knockout.min.js?1587039572000"></script>
24 <script type="text/javascript" data-savepage-src="/idp/resources/js/thirdparty/js.cookie.js?1587039572000"></script>
25
26 <script type="text/javascript" data-savepage-src="/idp/resources/js/flt/float-labels.js?1587039572000"></script>
27 <script type="text/javascript" data-savepage-src="/idp/resources/js/flt/utils.js?1587039572000"></script>
```

Используйте готовые

Создавайте свои

Редактируйте

Система тегирования

Онбординг — обучение для
новых пользователей

Группа риска —
отслеживай уязвимых

Теги

Выберите тег для настройки

Онбординг

Новый сотрудник **Выбран**

Не зарегистрирован

Еще что-то

Группы риска

Группа риска

Название тега

Новый сотрудник

Правила назначения тега

Если сотрудник зарегистрирован менее 30 дней

Действия для назначенного тега

Действие 1

Назначить курс

Назначить 2 курса

Действие 2

Отправить сообщение

Тема письма

Напишите сообщение

+ Добавить действие

Сохранить

Название тега

Группа риска

Правила назначения тега

Уровень риска сотрудника больше или равен 7

Действия для назначенного тега

Действие 1

Назначить курс

Назначить 2 курса

+ Добавить действие

Сохранить

Собственные теги

Настраивай свои правила

Гибко, удобно и просто

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

Как работает имитация фишинга?

Фишинг > Создание новой рассылки

Создание новой рассылки

Название рассылки

Новая рассылка

Цели рассылки

Выборочно Всем

Выбрать цели +

Отложенная рассылка

Выбрать дату начала рассылки

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.

Банки

Сбербанк Альфабанк ВТБ

Альфабанк - копия

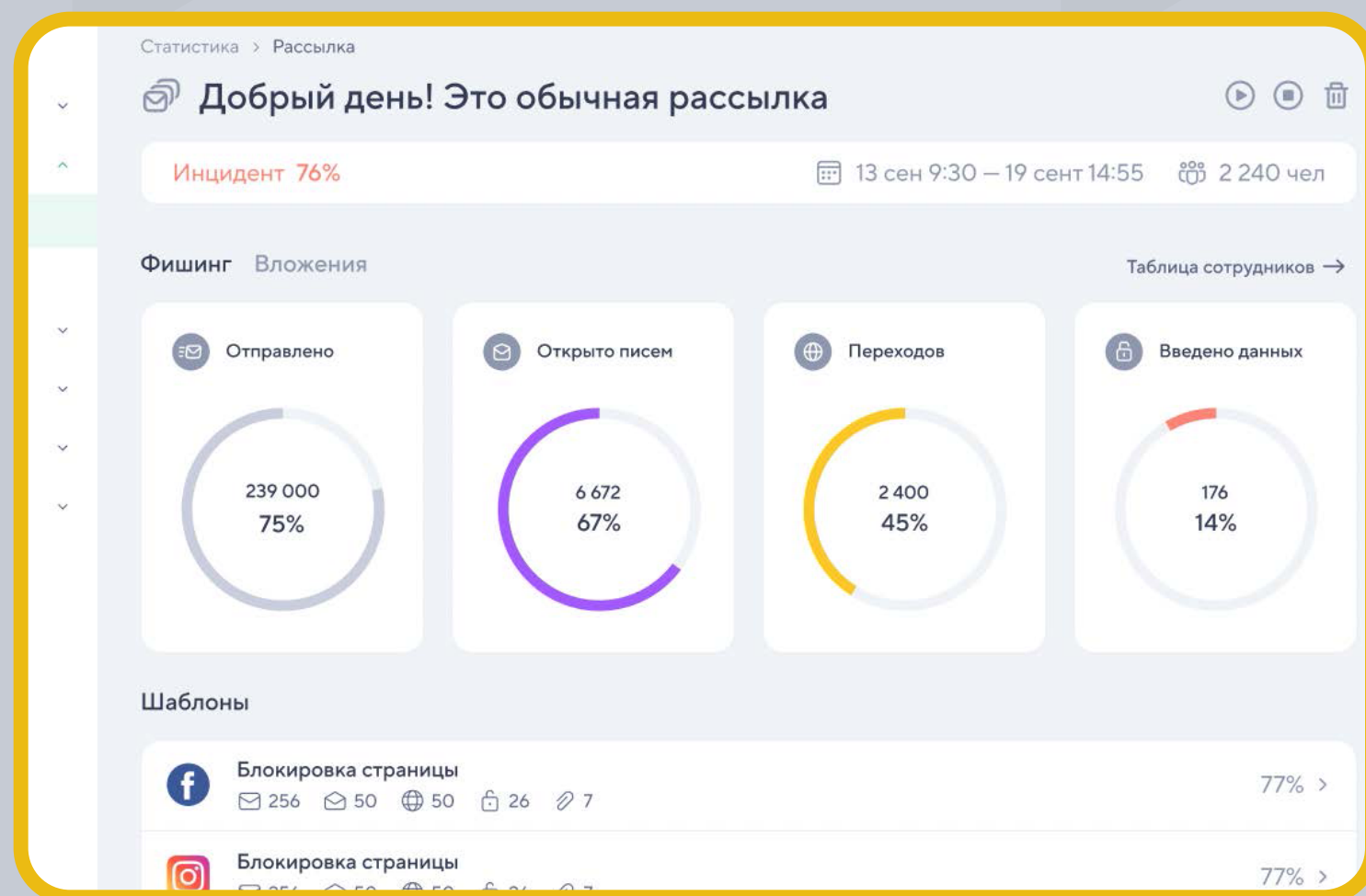
Соцсети

Twitter VK LinkedIn

Instagram

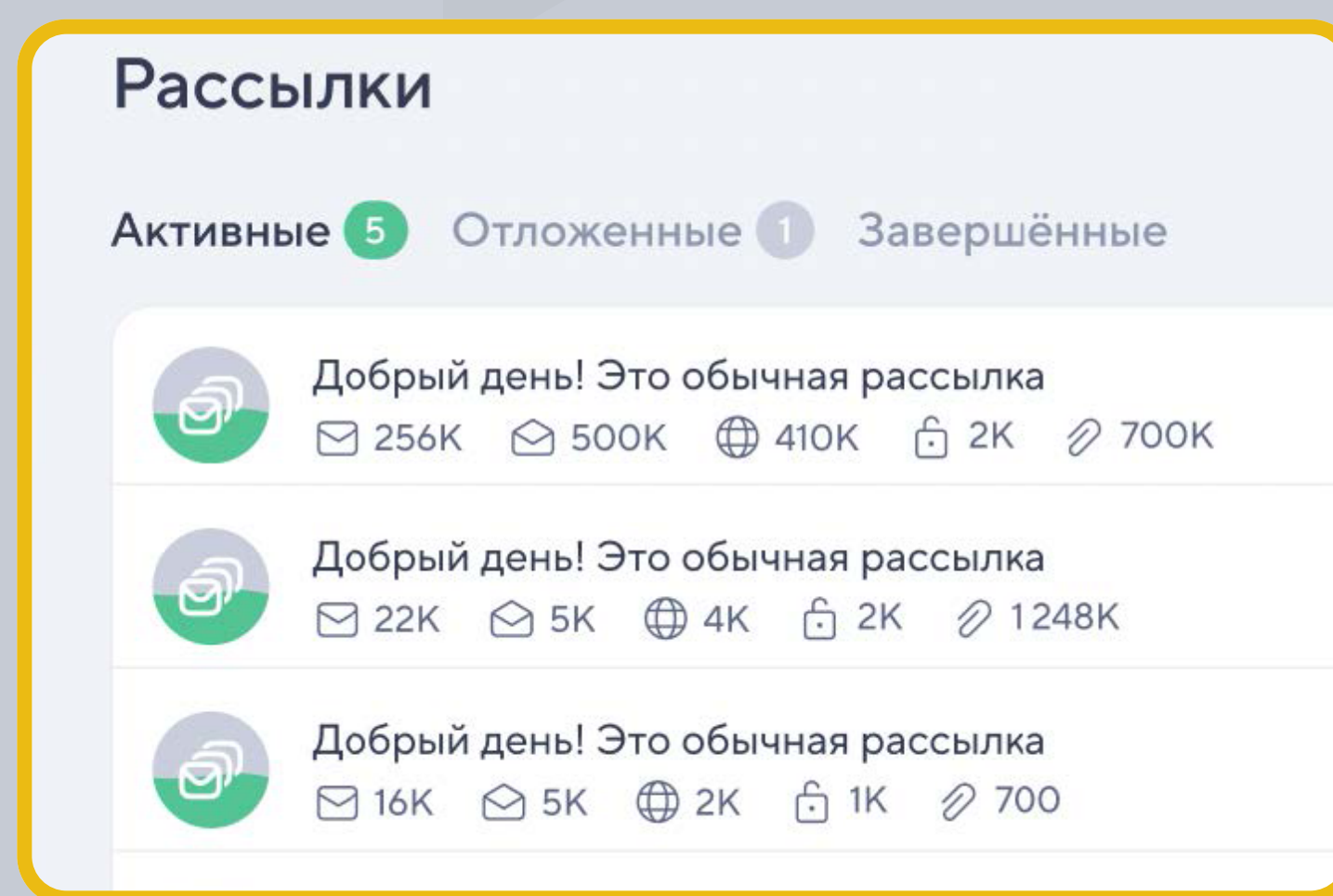
Гос структуры

Как работает имитация фишинга?



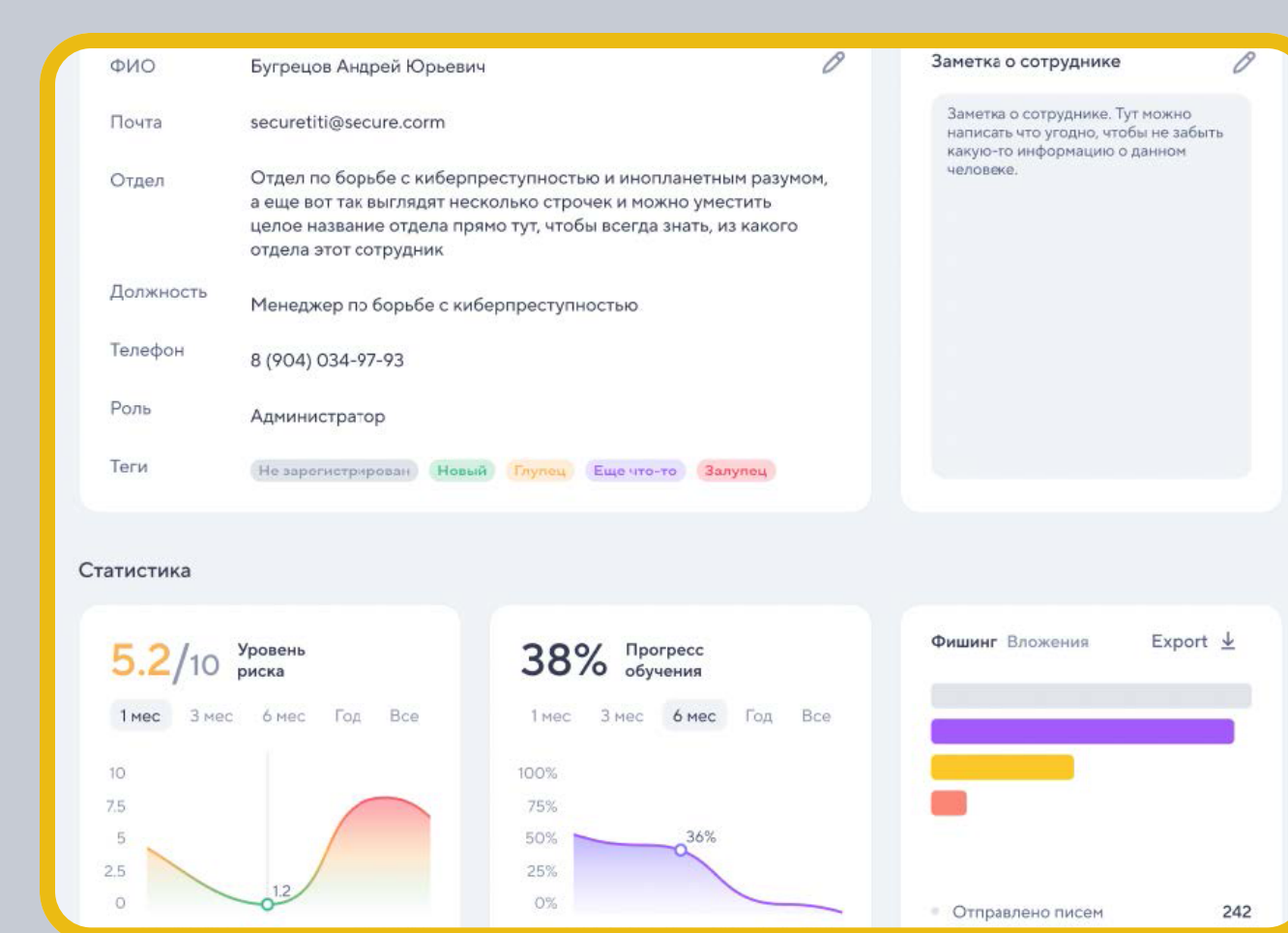
Мониторинг статистики рассылки

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



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

