Киберкультура для всех организаций:

Как контролировать влияние человеческого фактора на периметр информационной безопасности

Спикер: Бугаев Руслан

SECURE-T

Цель: изучение влияния человеческого фактора на периметр информационной безопасности

Первый шаг

Построение процесса повышения осведомленности

Второй шаг

Переход к состоянию киберкультуры внутри организации

Проблема

Неосведомленность

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

Отсутствие контроля

Нехватка ресурсов или отсутствие возможности контроля знаний сотрудников

Нехватка аналитики

Отсутствие подробной аналитики по уровню подготовки сотрудников и степени их уязвимости

Низкий уровень вовлеченности

Низкая мотивация сотрудников участвовать в программах по кибербезопасности, что затрудняет формирование устойчивых навыков

Быстро меняющиеся угрозы

Непрерывное появление новых киберугроз и тактик злоумышленников, что требует постоянного обновления знаний сотрудников и адаптации мер защиты

Законодательство

SECURE-T

Федеральный закон № 152-ФЗ

О персональных данных: Меры по защите персональных данных.

Федеральный закон № 98-ФЗ

О коммерческой тайне.

Федеральный закон № 187-ФЗ

О безопасности критической информационной инфраструктуры Российской Федерации.

ГОСТ Р ИСО/МЭК 27002-2012

Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности.

Указ Президента РФ от 01.05.2022 № 250

О дополнительных мерах по обеспечению информационной безопасности Российской Федерации.

Приказ ФСТЭК России № 17

Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах.

Приказ ФСТЭК России № 31

Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессах на критически важных объектах.

Приказ ФСТЭК России № 239 КИИ

Состав мер по обеспечению безопасности и обучению персонала.

Положение Банка России № 382-П

О требованиях к обеспечению защиты информации при осуществлении переводов денежных средств.

Положение Банка России № 683-П, № 757-П

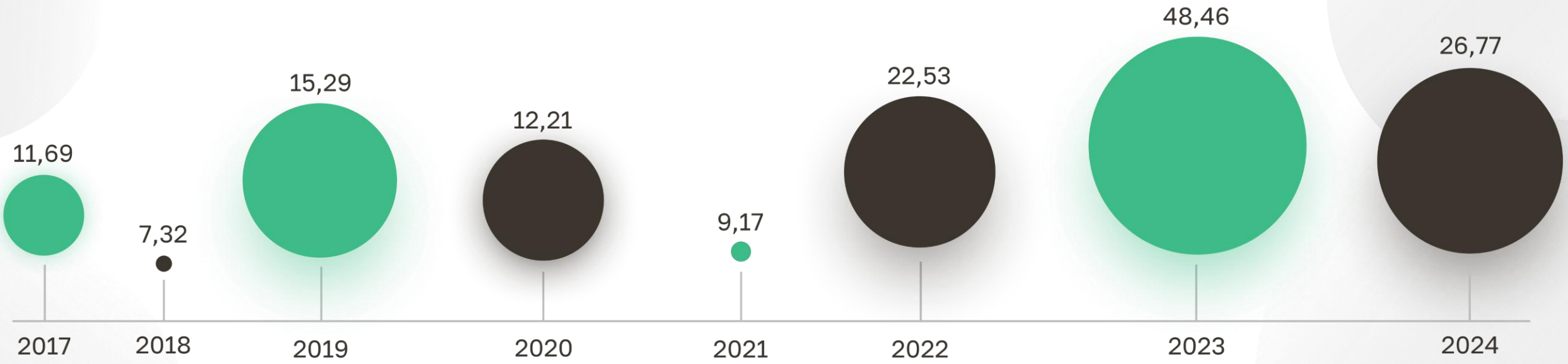
Описание обязательного обучения работников финансовых организаций.

ГОСТ Р 56939-2024

Защита информации. Разработка безопасного программного обеспечения. Общие требования.

Статистика

Совокупное количество персональных данных, скомпрометированных в результате внешних и внутренних утечек, в 2024 году составило **26,77 млрд записей**

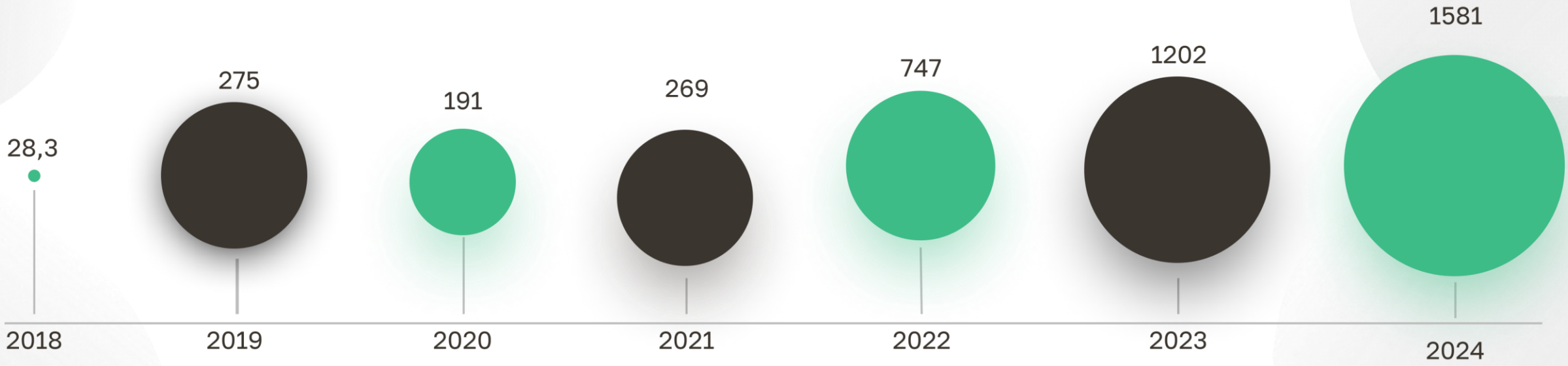


Количество утечек информации и количество утекших записей ПДн в мире, 2017-2024 гг

Источник: InfoWatch. Утечки информации в мире, 2023-2024 годы

Статистика

Совокупное количество ПДН и платежной информации,
скомпрометированных в результате утечки данных,
в 2024 году составило **1581** млн записей



Количество утекших записей ПДн и платежной информации в России. Млн записей, 2018–2024 гг.

Источник: InfoWatch. Росиия: Утечки информации ограниченного доступа 2023-2024

Последствия

SECURE-T

Компания:

Snowflake

Происшествие:

В апреле 2024 года произошла утечка данных, затронувшая около 165 клиентов американской компании Snowflake. Утечки произошли из-за недостаточной защиты учётных записей клиентов и их подрядчиков, в частности из-за отсутствия многофакторной аутентификации и использования слабых паролей.

Результат:

Среди пострадавших клиентов оказались Ticketmaster и AT&T. У Ticketmaster хакеры похитили данные 560 млн пользователей, включая историю покупок и реквизиты карт. У AT&T были украдены записи телефонных звонков и SMS-сообщений.

Источник:
https://falcongaze.com/ru/pressroom/publications/incidenty-ib/samye-gromkie-utechki-dannyh-2024-goda.html#3

Последствия

Компания:

Компании малого и среднего бизнеса

Происшествие:

В мае 2025 года компании малого и среднего бизнеса, использующие CRM «Мегаплан» и Bitrix24, подверглись волне фишинговых атак. Мошенники рассылали персонализированные письма, которые имитировали запросы на согласование документов или стандартные уведомления от CRM. Основной мишенью становились руководители, обладающие расширенными правами доступа.

Результат:

Злоумышленники смогли похитить внутренние документы, базы данных клиентов и сотрудников, а также конфиденциальные сведения о контрактах. В наиболее серьёзных случаях происходила полная выгрузка файлов из облачного хранилища. От атаки пострадали как минимум 25 компаний.

Источник: https://www.anti-malware.ru/news/2025-05-14-111332/46027

Как защититься

Регулярное обучение

Повышение осведомленности сотрудников в области ИБ

Имитированные атаки

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

С чего начать?

Повышение осведомленности пользователей

Регулярное обучение

Повышение осведомленности сотрудников в области ИБ

Имитированные атаки

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

Документальное сопровождение

Обеспечения прозрачности процессов, систематизации обучения и фиксации результатов

Данные элементы необходимо систематизировать на уровне процессов в организации для формирования целостного подхода к информационной безопасности

Как обучать

SECURE-T

Регламенты

Тренинги

Курсы в СДО

Программы обучения

Проверки с помощью фишинга

Приказы

+

Законодательство

могут помочь организации соблюдать требования законодательства

Установка стандартов

стандарты и правила для обеспечения ИБ в организации

Управление рисками

идентификация и управление рисками, связанными с ИБ

—

Бюрократия

повышение административной нагрузки в организации

Соблюдение актуальности

нет возможности часто менять документы

Затраты

финансовые и временные ресурсы на разработку, внедрение и поддержание

Как обучать

SECURE-T

Тренинги

Программы обучения

Курсы в СДО

Проверки с помощью фишинга

Приказы

+

Погружение

очные тренинги обычно более глубоко погружают в материал

Персонализация

программа обучения может быть построена на основе уровня знаний и потребностей участников

Обратная связь

участники могут задавать вопросы по ходу обучения

—

Затраты

большие финансовые затраты на организацию и проведение

Время

ограниченное время на посещения тренинга

Доступность

на рынке сложно найти квалифированных инструкторов

Как обучать

SECURE-T

Курсы в СДО

+

Гибкость

пользователи могут пройти обучение в любое время

Доступность

большое количество курсов можно найти в интернете без дополнительной платы

Разнообразие

разные форматы подачи материала, включая видео, интерактив и прочее

—

Затраты

большие финансовые затраты на интеграцию СДО

Самодисциплина

не все пользователи способны эффективно управлять временем

Обратная связь

не всегда есть возможность получить обратную связь от экспертов курса

Программы обучения

Проверки с помощью фишинга

Приказы

Как обучать

Проверки с помощью фишинга

Программы обучения

Приказы

+

Реалистичность

создание максимально приближенных ситуаций

Практический опыт

помогает развивать навыки распознавания подозрительных сообщений и действий

Сознательность

пользователи могут стать более осторожными и бдительными

–

Доступность

контракт с подрядчиками (большие финансовые затраты) или бесплатные версии (GoPhish)

Как обучать

SECURE-T

Программы обучения

\+

Структурированность

чёткая и логичная структура, которая позволяет последовательно изучать материалы

Регулярность и системность

чёткая и логичная структура, которая позволяет последовательно изучать материалы

\–

Требует времени и ресурсов

для регулярного обновления программ необходимы значительные затраты

Требует согласования

требует внедрения процессов на уровне организаций

Приказы

Как обучать

Приказы

+

Обязательность выполнения

делает обучение обязательным для всех сотрудников, что предотвращает уклонение от обучения

Четкие сроки и ответственность

упрощает контроль за выполнением и помогает избежать задержек

Основание для контроля

юридическая база для мониторинга и наказания за невыполнение обязательств

–

Формализм

Риск формального прохождения обучения

Риск низкой мотивации

негативное восприятие обучения по принуждению

Необходимость постоянного контроля

без надлежащего контроля исполнение приказа может оставаться на бумаге

Как обучать

Метрики знаний:
- результаты тестов
- количество назначенных курсов
- количество сотрудников, прошедших курс

Метрики поведения:
- количество переходов по ссылке
- количество ввода личных данных
- количество открытий вложений
- количество проведенных атак
- количество открытий писем
- количество отправленных писем

Метрика уязвимости:
- уровень риска пользователя

Метрики вовлеченности:
- процент сотрудников, прошедших курсы

Решение

secure-t asap

Теория

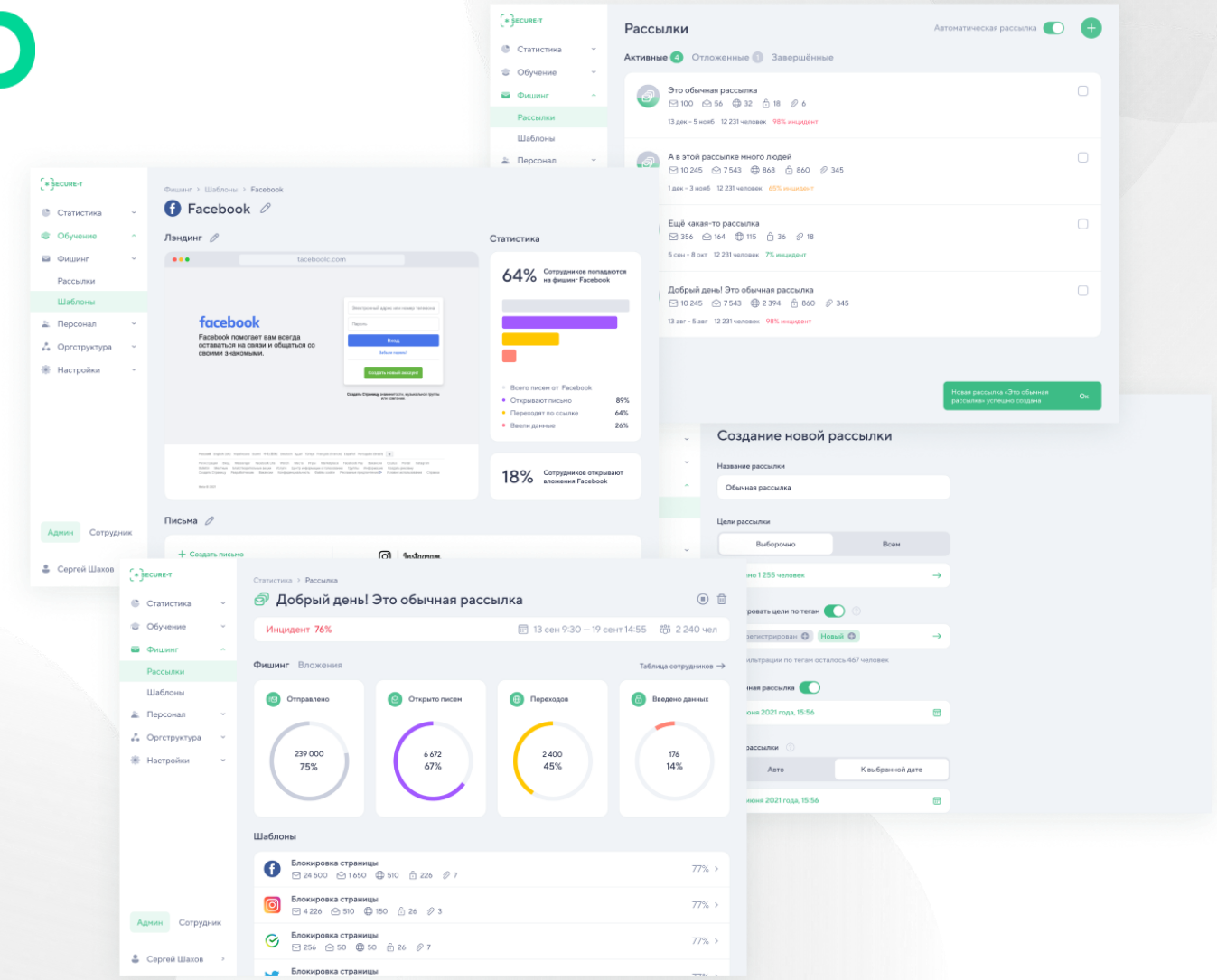
Обучающие курсы и тесты

Практика

Имитация фишинга и вирусные вложения

Аналитика

Подробная статистика
и выявление уязвимых сотрудников



Все возможности

secure-t asap

Курсы

Объем обучающих курсов не менее 60 модулей

Фишинг

Персонализированные письма, а также вложения

Конструктор

Создание поддельных писем и лэндингов

Интеграция

Интеграция с системами СДО (WebTutor)

СДО

Возможность загружать свои собственные курсы

Логирование

Фиксирование всех действий пользователей

Редактор курсов

Возможность вносить изменения в наши курсы

Онбординг

Автоматическое назначение по группам

Настройка тестов

Гибкая настройка тестовых вопросов

Этап 1

обучение

Выбор курса

Правовое регулирование в ИБ

1 модуль

Основы безопасности КИИ

1 модуль

Всё, что нужно знать о GDPR

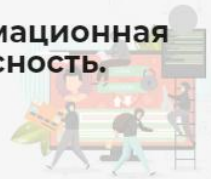
2 модуля

Противодействие коррупции в РФ

2 модуля

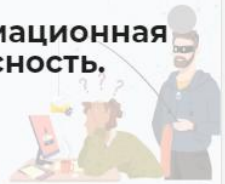
Информационная безопасность. Часть 2

8 модулей



Информационная безопасность. Часть 1

8 модулей

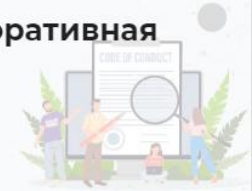


ФЗ-152 "О персональных данных"

1 модуль

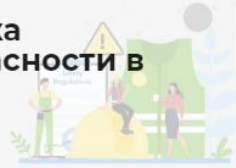
Корпоративная этика

1 модуль



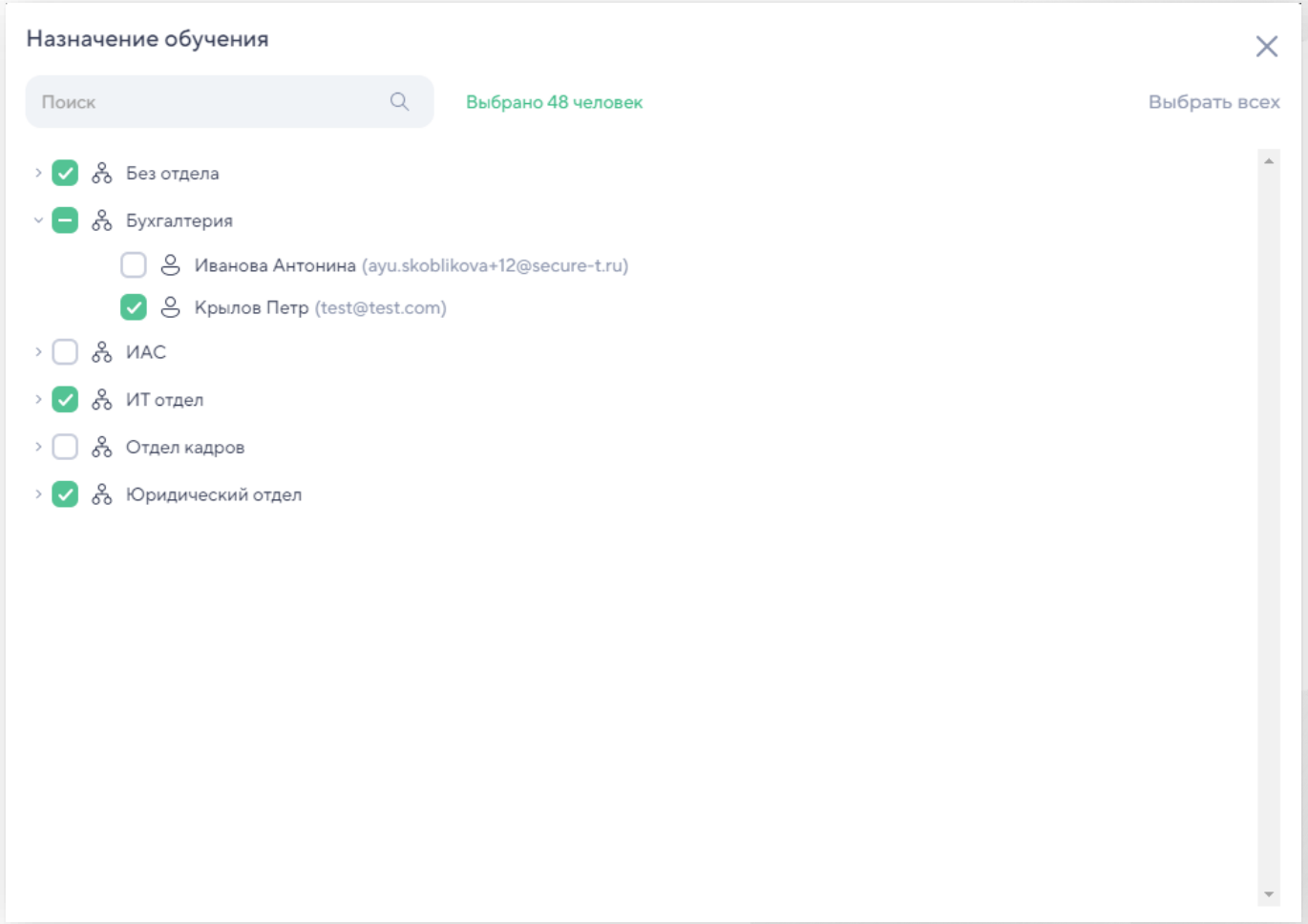
Техника безопасности в офисе

2 модуля



Этап 1

обучение



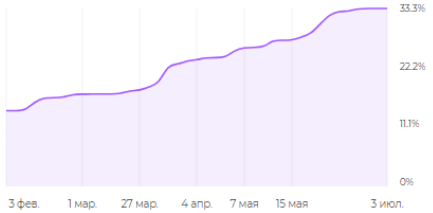
Этап 1

обучение

Информационная безопасность. Часть 1

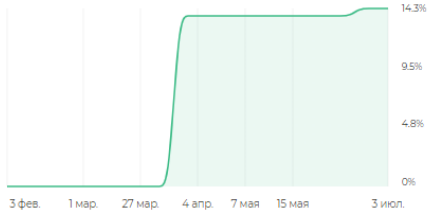
осталось 26 дней

Прогресс обучения



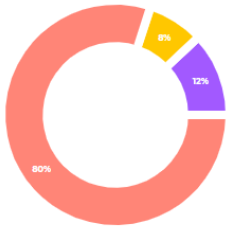
Прогресс обучения

Прогресс тестирования



Прогресс тестирования

Кто требует моего внимания



Опережают план

Отстают от плана

Сильно отстают от плана

дата старта
03.02.2023

дата окончания
30.07.2023

курс пройден
3/30 сотрудников

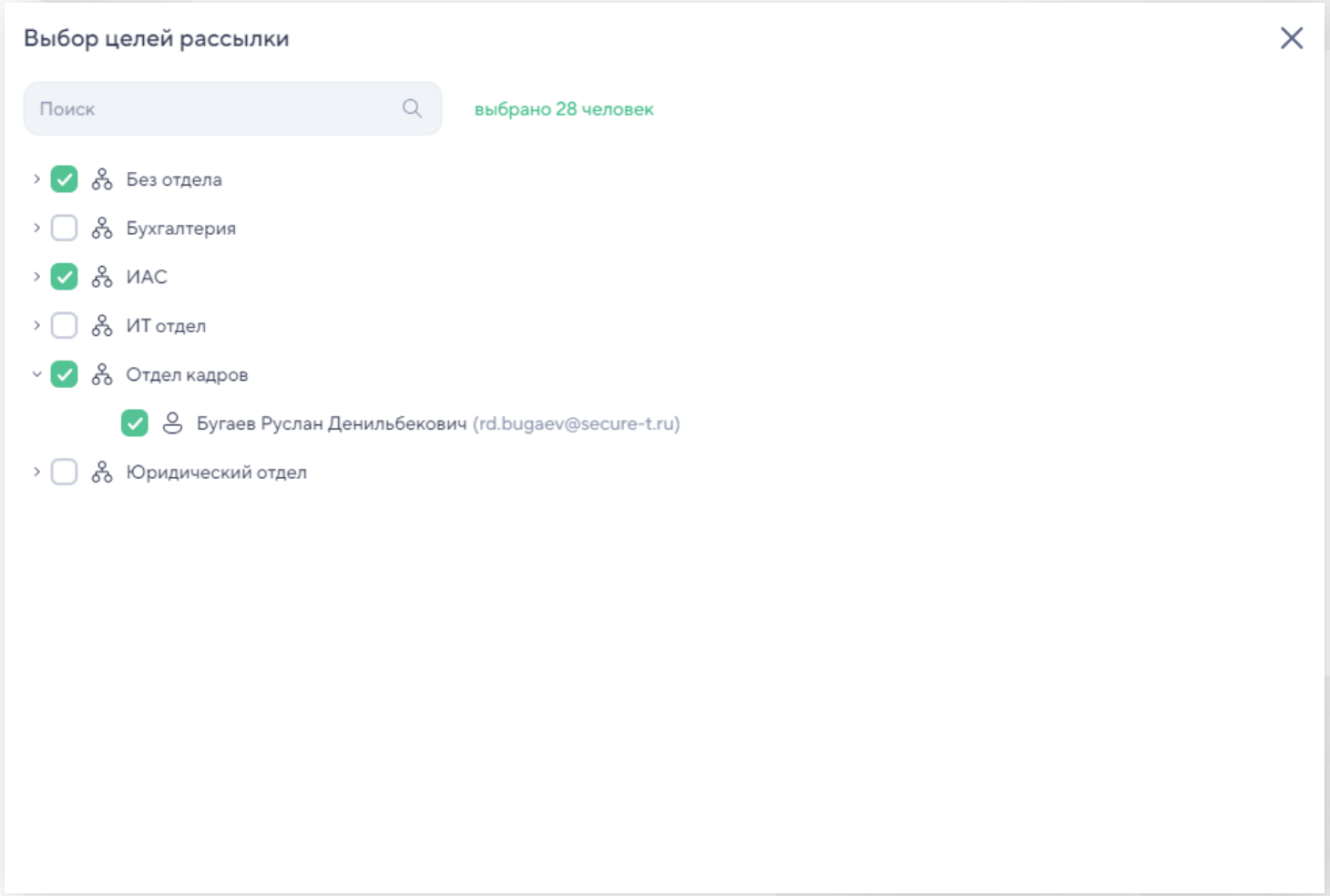
описание
Многие считают, что корпоративной системы безопасности достаточно для предотвращения утечек конфиденциальных данных. Тем не менее статистика показывает, что основной причиной утечек данных происходит “благодаря” халатности сотрудников. Узнайте, какие привычки должны войти в вашу жизнь, чтобы вы смогли обезопасить личную и корпоративную информацию.

Экспорт в Excel

завершить обучение

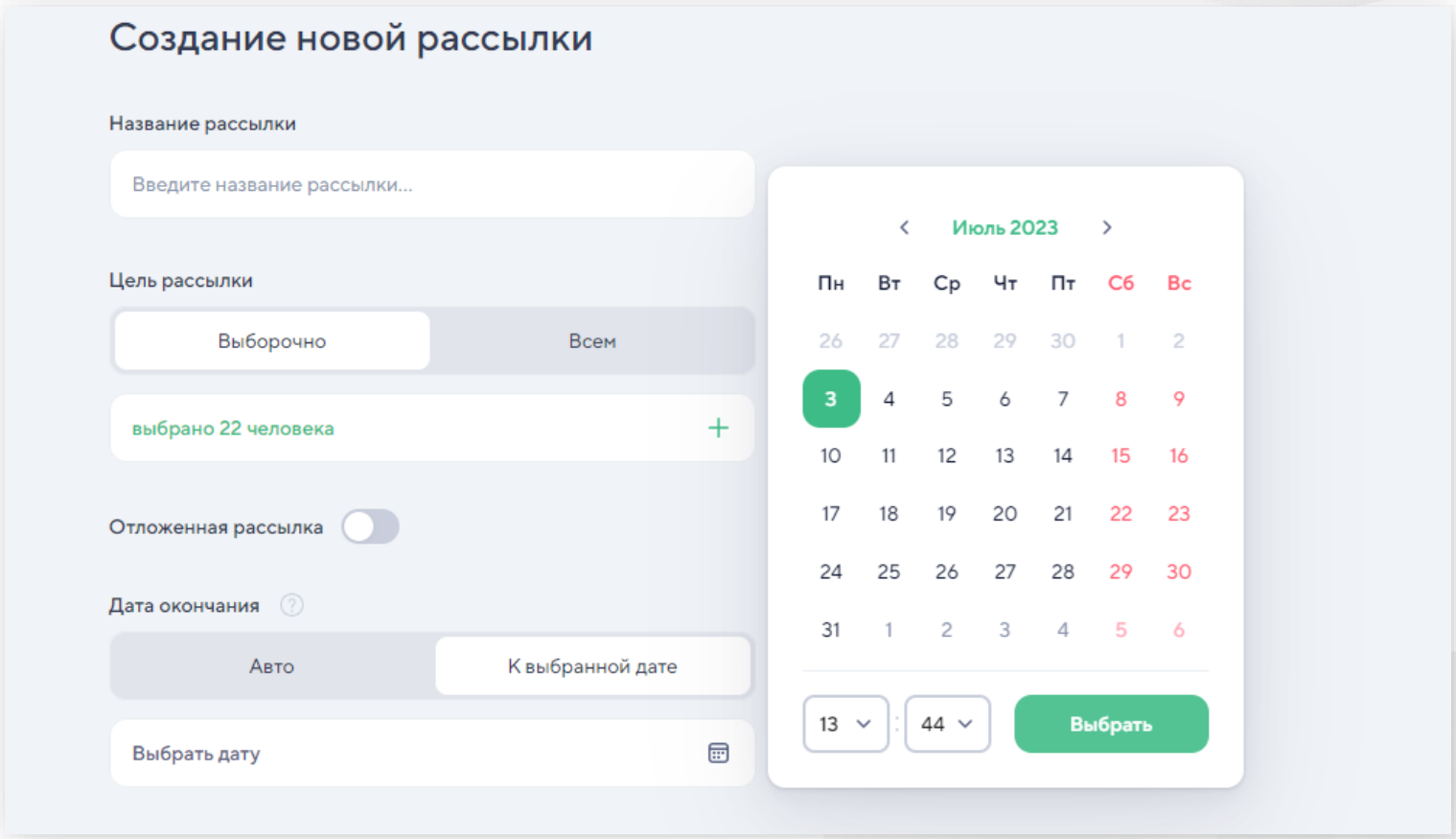
Этап 2

проверка



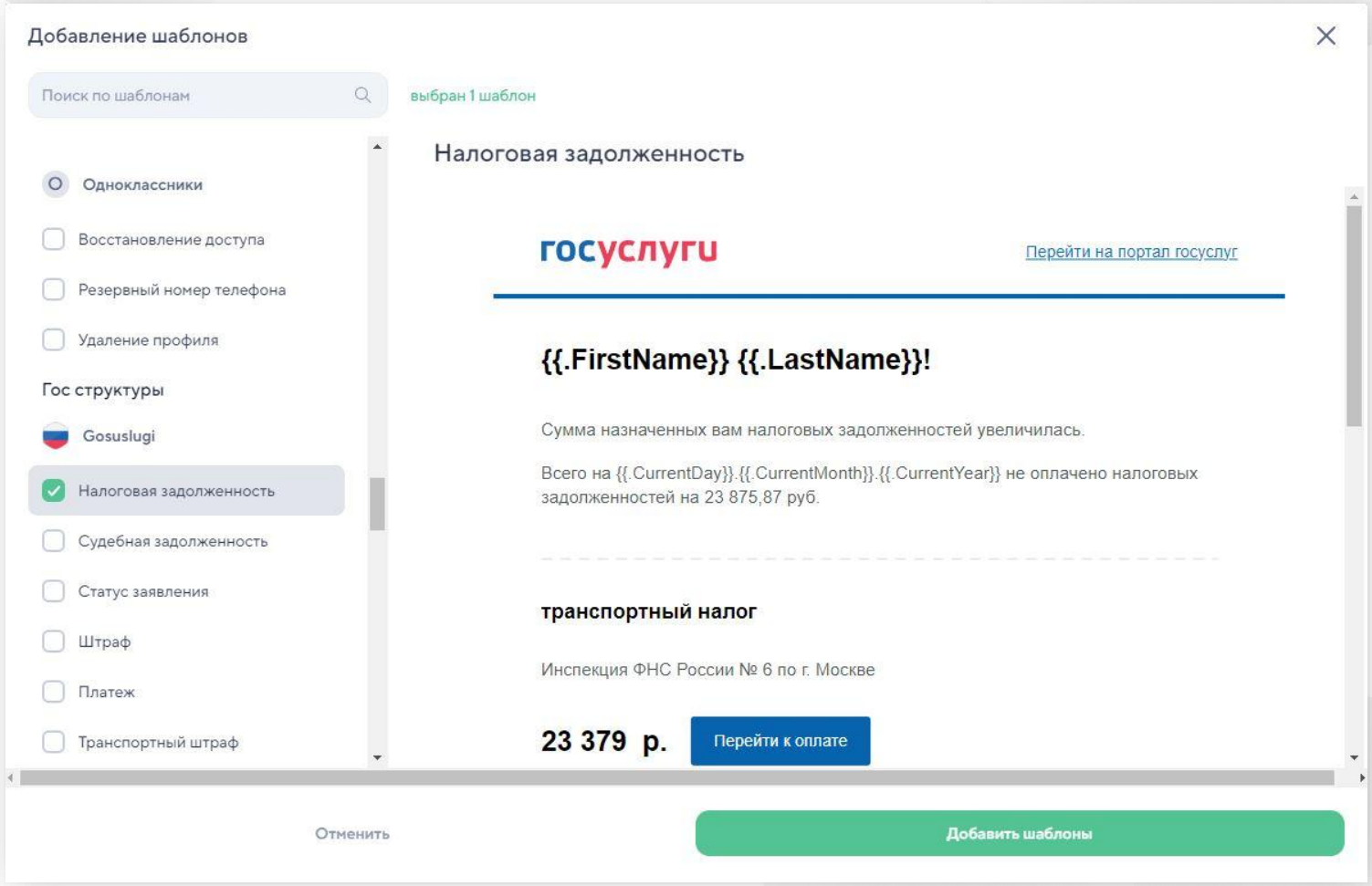
Этап 2

проверка



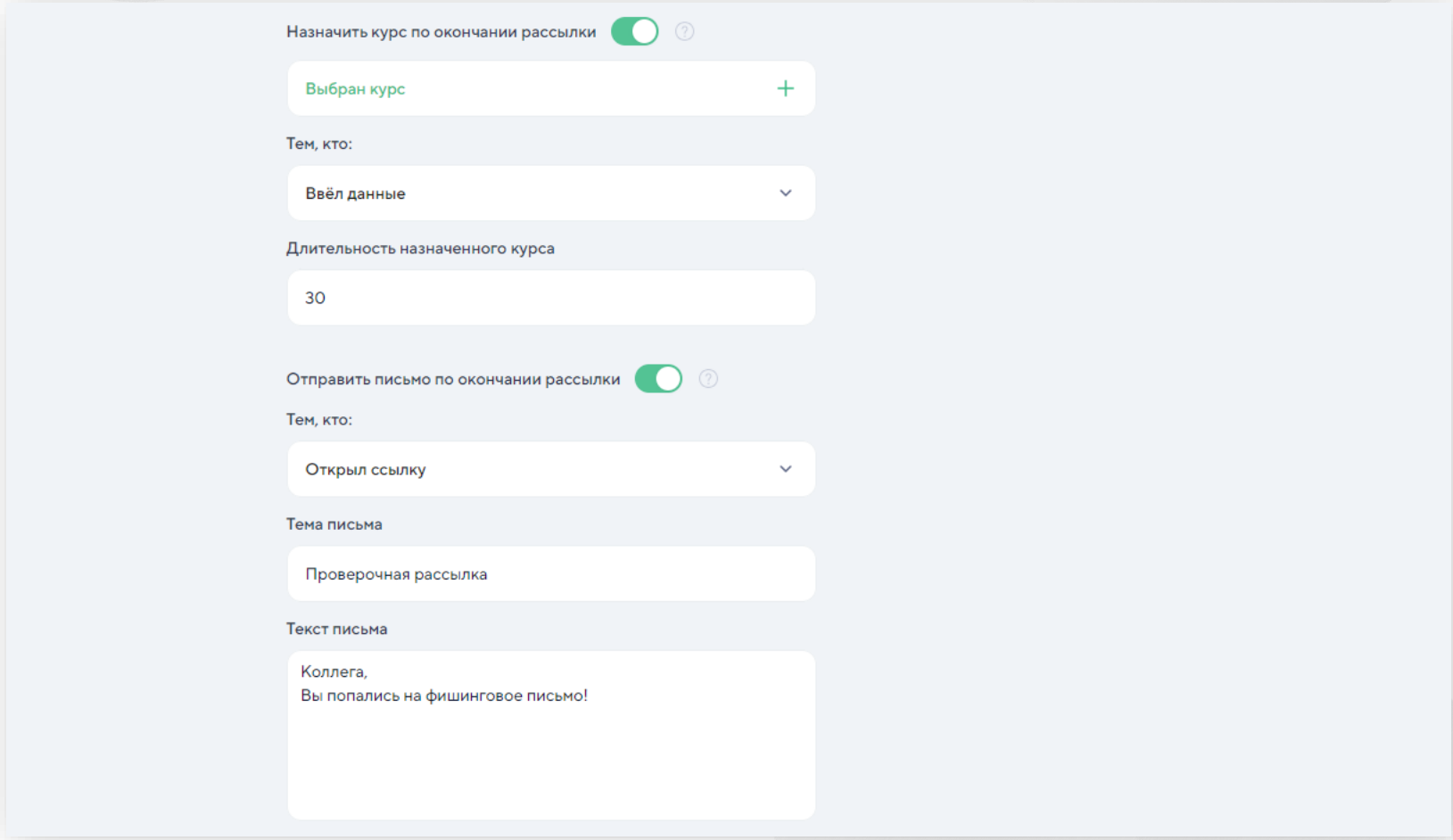
Этап 2

проверка



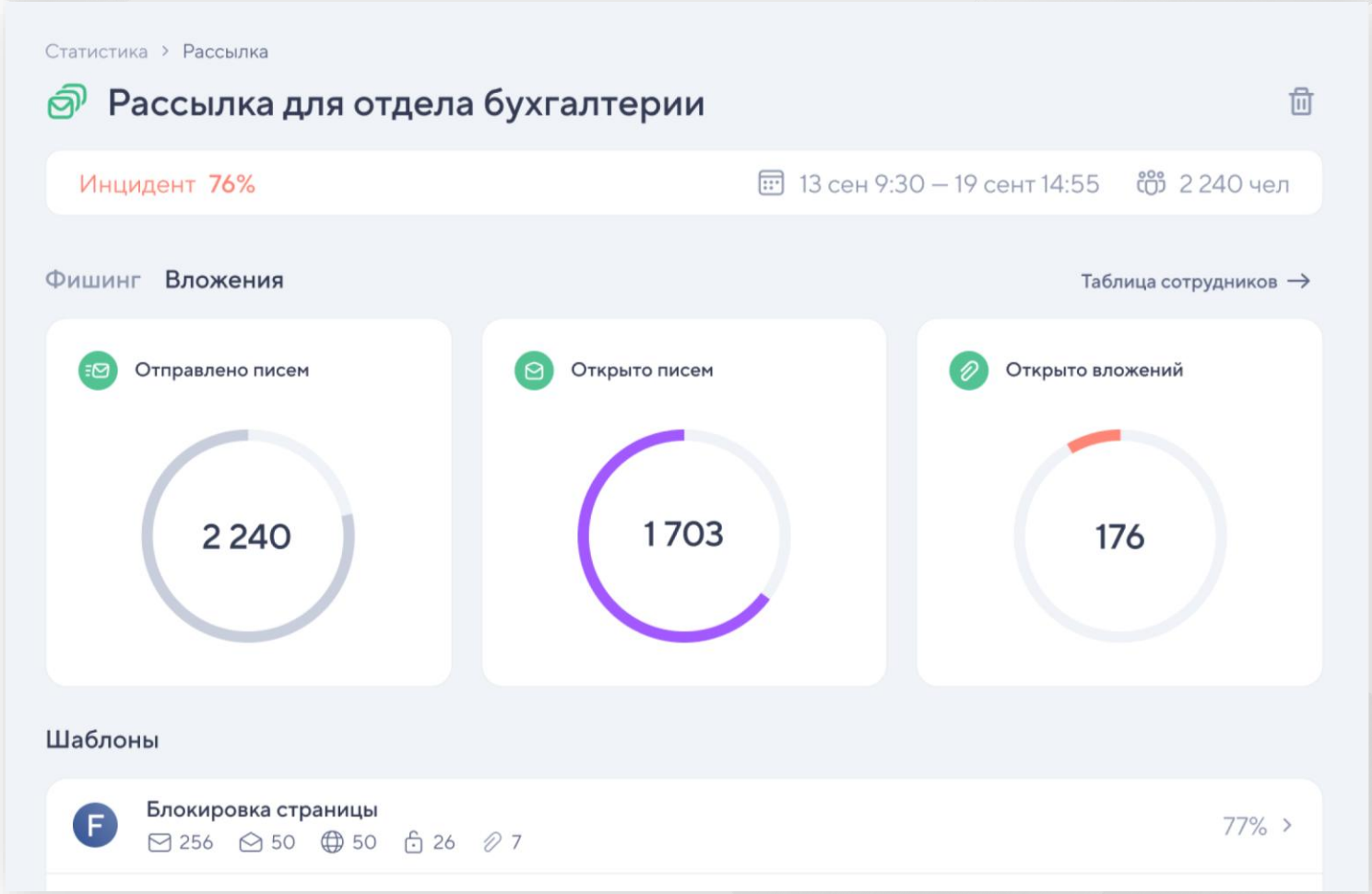
Этап 2

проверка



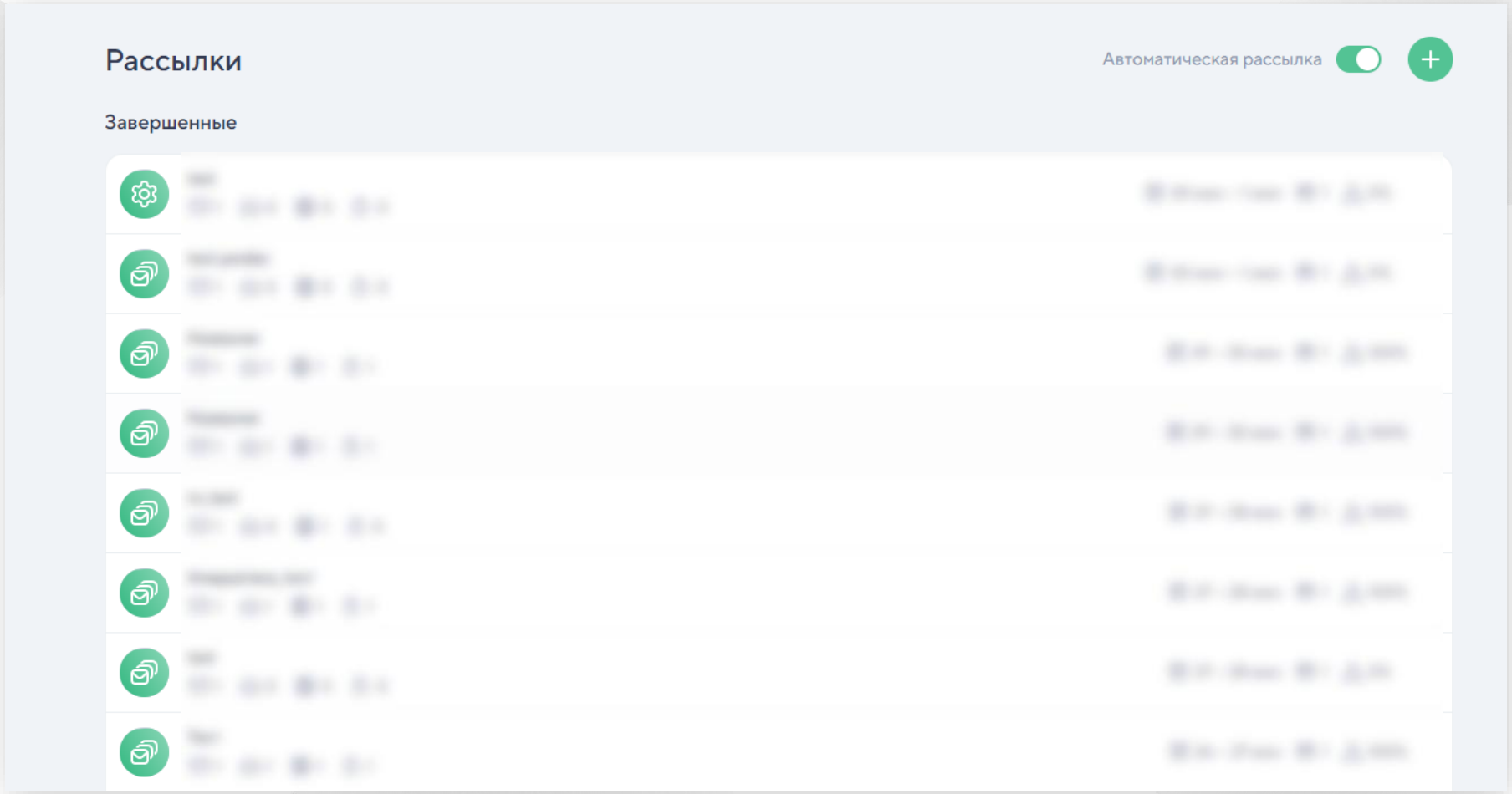
Этап 2

проверка



Этап 3

закрепление



Этап 3

закрепление

Как действовали мошенники

Адресаты
отобрали заранее

Домены
зарегистрировали более 30 похожих

Приманка
письма с зараженными вложениями

00:00

Мошенники **хорошо подготовились перед атакой**: тщательно отобрали адресатов, зарегистрировали более 30 похожих доменов, создали электронные письма. Жертва получила **письмо с заражённым архивом** в формате ISO, который позволяет обходить проверку безопасности. В то время как пользователь просматривал документ из письма, **в фоновом режиме выполнялся вредоносный код** для сбора информации.

Внедрение системы приносит ощутимые результаты

Кейс 1

Дано

Поставщик инженерных услуг
(150 лицензий)

Проблема

При проверке сотрудников было выявлено, что 27% персонала подвержены фишинговым атакам

После годового использования secure-t asap

Процент снижения количества сотрудников, подверженных фишингу

68%

Внедрение системы приносит ощутимые результаты

Кейс 2

Дано

Компания по разработке и внедрении различных решений (500 лицензий)

Проблема

Компания столкнулась с утечкой конфиденциальных данных из-за человеческого фактора

После годового использования secure-t asap

Улучшение реакции на инциденты безопасности, в частности на фишинг

87%

Внедрение системы приносит ощутимые результаты

Кейс 3

Дано

Российский коммерческий банк
(1500 лицензий)

Проблема

Нехватка практических знаний о цифровой гигиене способствовала утечке персональных данных

После годового использования secure-t asap

Общее сокращение ошибок и нарушений со стороны персонала

73%

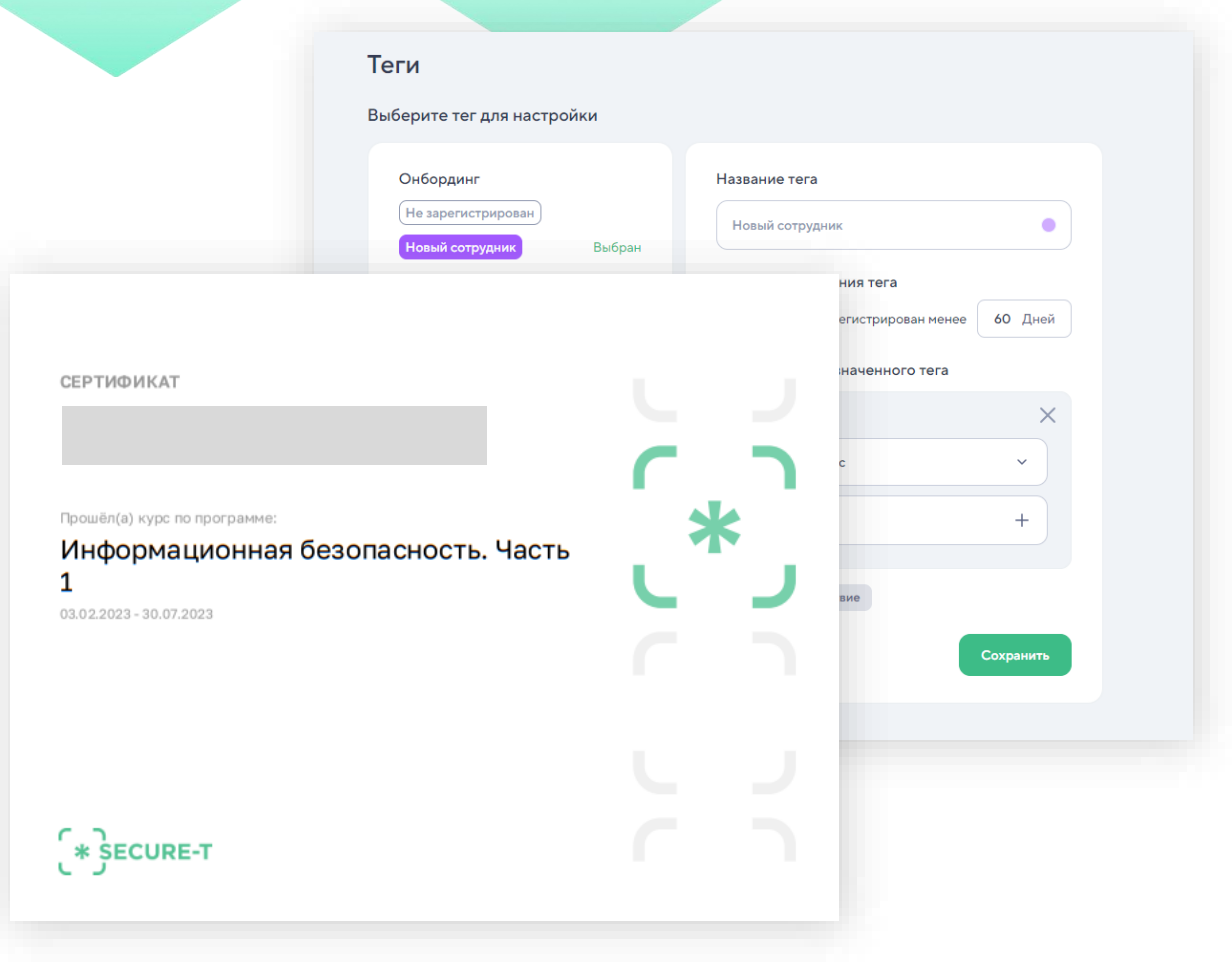
План обучения*

Онбординг

Введение в основы информационной безопасности для новых сотрудников

Сертификаты

Возможность скачать сертификаты после успешного прохождения любого курса



Наши контакты

Телефон

+7 (495) 105-54-85

Почта

info@secure-t.ru

Secure-T Insights

SECURE-T

Получи решение

Телефон

+7 (495) 105-54-85

Почта

info@secure-t.ru

Сканируй QR и оставь заявку

SECURE-T