

Культура кибербезопасности для всех компаний

Спикер: Бугаев Руслан



Проблема

Неосведомленность

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

Отсутствие контроля

Нехватка ресурсов или отсутствие возможности контроля знаний сотрудников

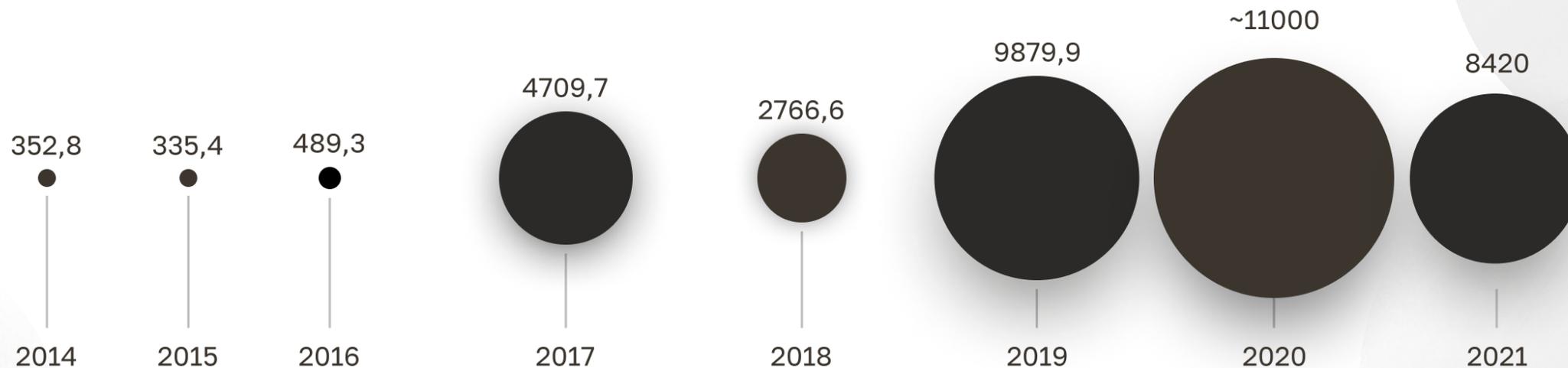
Нехватка аналитики

Отсутствие подробной аналитики по уровню подготовки сотрудников и степени их уязвимости

Статистика

8,4 %
записей было
скомпрометировано
в 2021 г.

80 %
утечек данных имеют
гибридный вектор
воздействия



Объём данных, скомпрометированных в результате внутренних утечек. Млн записей, 2014–2021 гг.

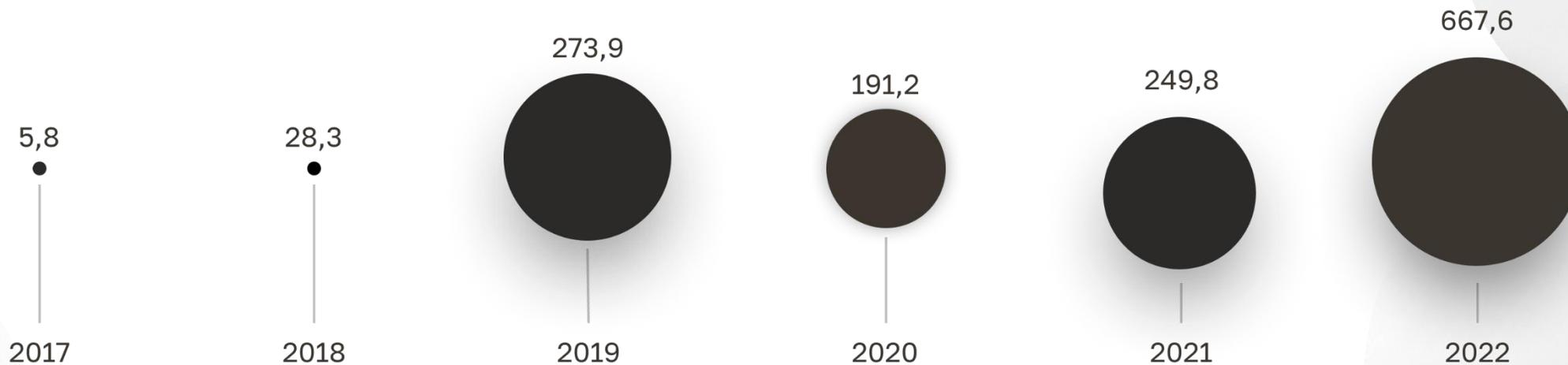
Источники:

Источник: InfoWatch. Утечки данных организаций по вине или неосторожности внутреннего нарушителя

Статистика

92 % компаний стали жертвами фишинговых атак в 2022 году

93 % утечек данных произошли из-за фишинговых атак



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

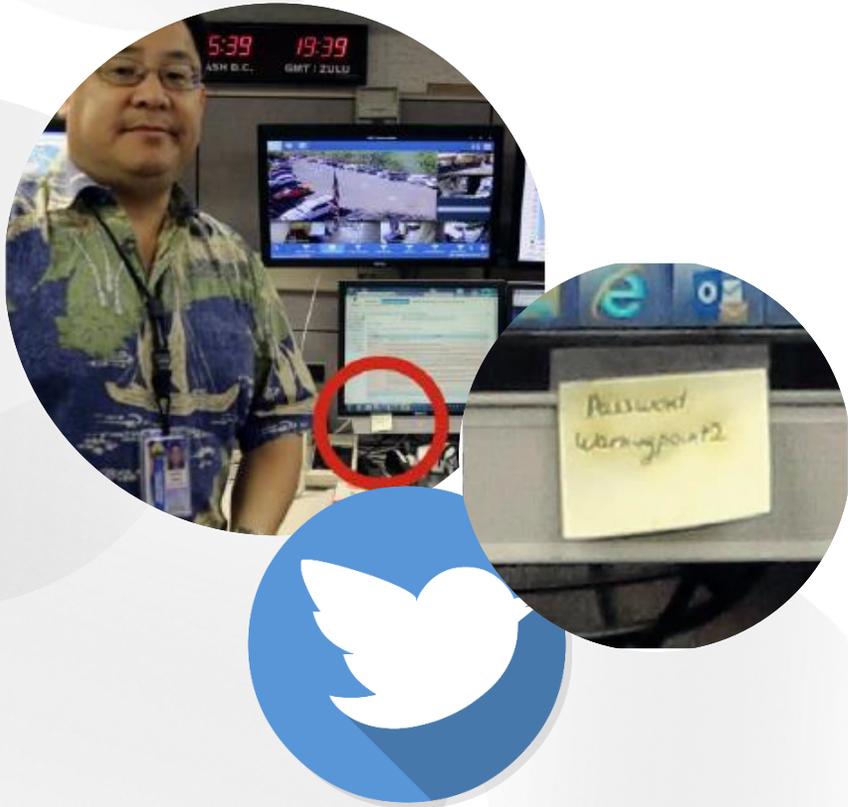
Источники:

<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

Кейс 1

Последствия



Компания

Управление по ЧС на Гавайях

Происшествие

Сотрудник выложил фото, где на фоне был виден пароль на стикере

Результат

Была объявлена ложная тревога на территории штата

Кейс 2

Последствия



Компания

крупный производитель пищевой продукции

Происшествие

Брутфорс учебной записи с правами администратора

Результат

Был загружен вирус шифровальщик, из-за которого работа предприятия была парализована на 3 часа

Кейс 3

Последствия



Crelan

Компания

крупный бельгийский банк

Происшествие

Многим сотрудникам были разосланы письма якобы от высокопоставленных руководителей

Результат

Банк потерял более 70 миллионов евро

Как защититься

Регулярное обучение

Повышение осведомленности сотрудников в области ИБ

Имитированные атаки

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

Тренинги

Курсы
в СДО

Плакаты

Контроль
обучения

Проверки
с помощью
фишинга

Регламенты

Как обучать

Тренинги



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 квалифицированных инструкторов

Курсы
в СР

Регламенты

Плакаты

Проверки
с помощью
фишинга

Как обучать

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

Регламенты

Плакаты

Проверки
с помощью
фишинга

Как обучать

Плакаты



Стоимость

небольшие финансовые затраты на размещение в офисе

Доступность

большое количество плакатов можно найти в интернете

Повторение

постоянно привлекают внимание сотрудников в офисе, что служит напоминанием о важных аспектах



Не вся информация

плакаты ограничены по размеру и объему информации

Неинтерактивность

нет возможности проверить усвоение материала

Обновление

нет возможности часто актуализировать информацию

Регламенты

Проверки с помощью фишинга

Как обучать

Регламенты

Проверки
с помощью
фишинга



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

Регламенты



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

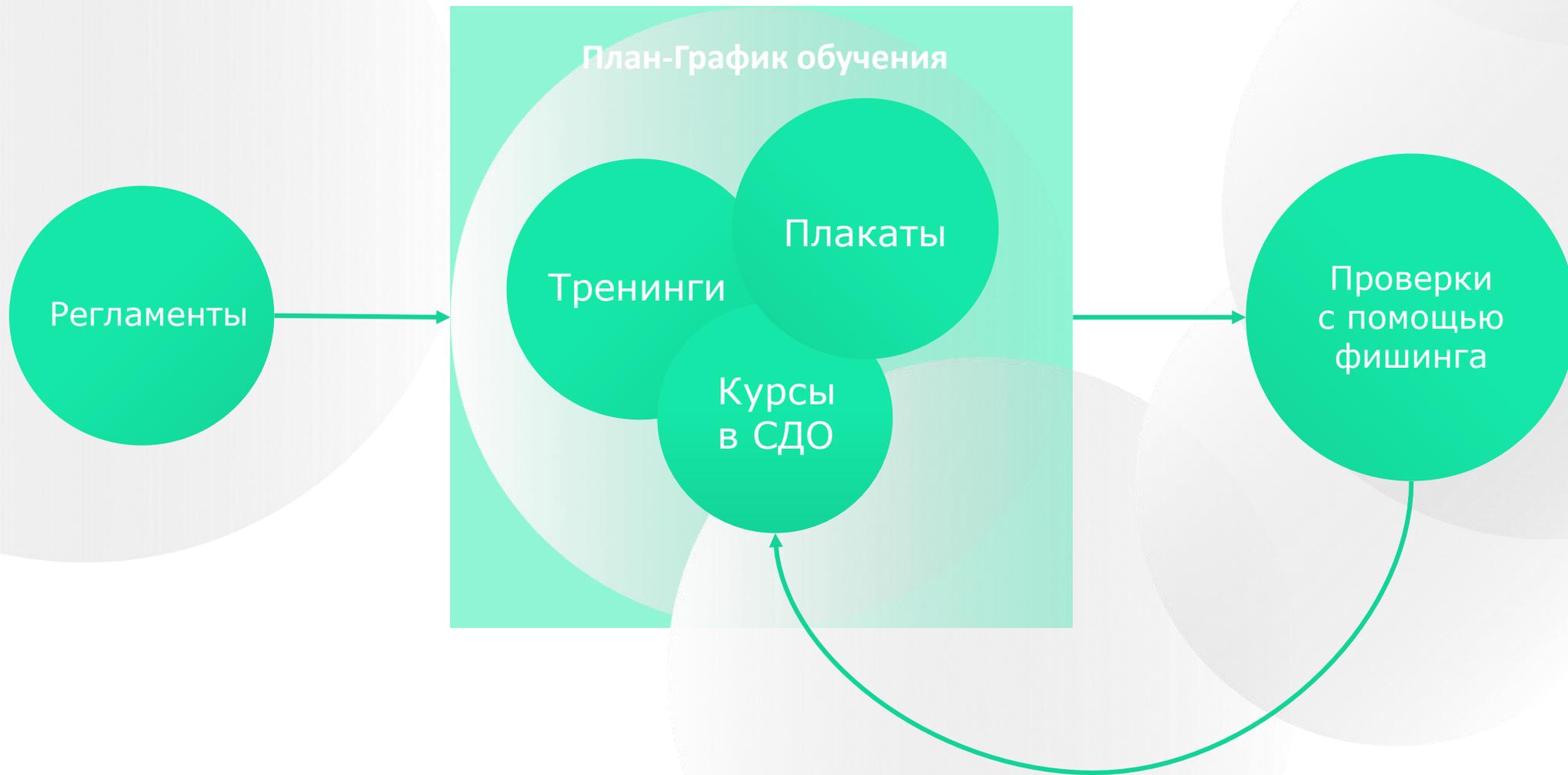
Соблюдение актуальности

нет возможности часто менять документы

Затраты

финансовые и временные ресурсы на разработку, внедрение и поддержание

Как обучать



План обучения

I квартал

Фишинговая рассылка

Первая массовая рассылка начинается параллельно с обучением (несколько шаблонов в течение двух недель)

Обучение

Курсы по информационной безопасности (часть 1, часть 2, часть 3) продолжительностью примерно 4-5 часов

Формирование отчета с результатами по итогам периода I



План обучения

II квартал

Фишинговая рассылка

Фишинговые письма будут направляться в течение всего периода обучения (1 письмо / 2 недели)

Обучение

ФЗ-152 «О персональных данных», а также другие курсы по необходимости

Формирование отчета с результатами по итогам периода II

Выстраивание процесса повышения осведомленности сотрудников в области ИБ

3 млрд

фишинговых писем ежедневно
злоумышленники отправляют
КОМПАНИЯМ

2021 Data Breach Investigations Report

85%

утечек данных происходят
из-за «человеческого фактора»

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

\$4,24 млн

составляет средняя стоимость
утечки данных в 2022 году

Email Fraud Landscape: Spring 2021

Решение



secure-t asap

Решение **secure-t asap**

Теория

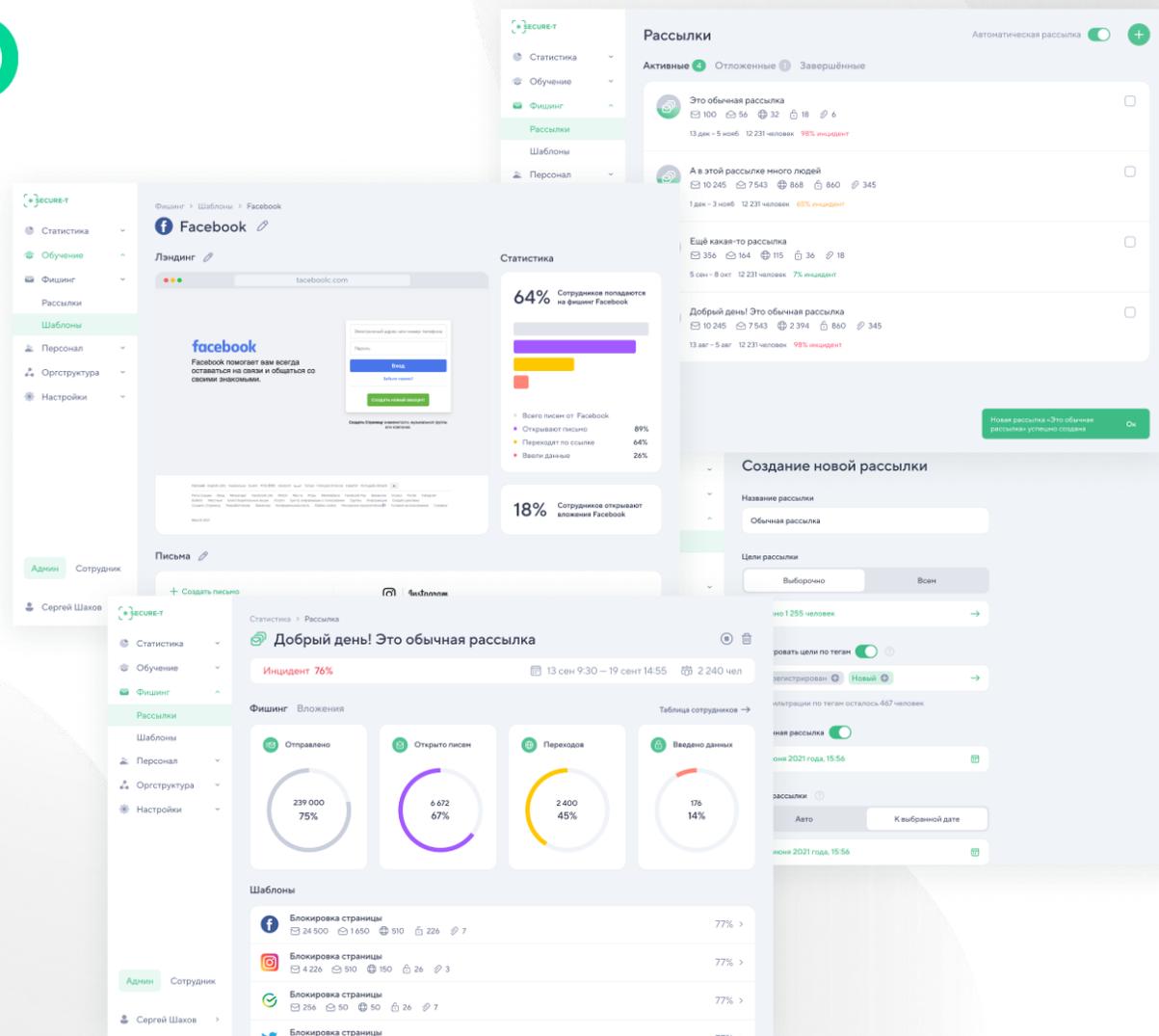
Обучающие курсы и тесты

Практика

Имитация фишинга и вирусные вложения

Аналитика

Подробная статистика
и выявление уязвимых сотрудников



Все возможности

secure-t asap

Курсы

Объем обучающих курсов не менее 40 модулей

Интеграция

Интеграция с системами СДО (WebTutor)

Редактор курсов

Возможность вносить изменения в наши курсы

Фишинг

Персонализированные письма, а также вложения

СДО

Возможность загружать свои собственные курсы

Онбординг

Автоматическое назначение по группам

Конструктор

Создание поддельных писем и лендингов

Логирование

Фиксирование всех действий пользователей

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



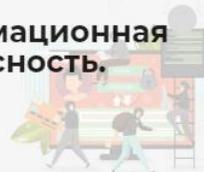
Противодействие коррупции в РФ

2 модуля



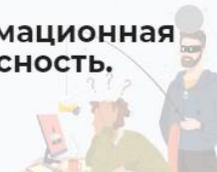
Информационная безопасность. Часть 2

8 модулей



Информационная безопасность. Часть 1

8 модулей



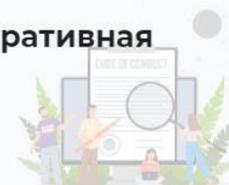
ФЗ-152 "О персональных данных"

1 модуль



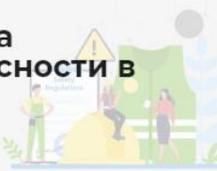
Корпоративная этика

1 модуль



Техника безопасности в офисе

2 модуля



Этап 1

обучение

Назначение обучения

Поиск Выбрано 48 человек Выбрать всех

- >  Без отдела
- >  Бухгалтерия
 -  Иванова Антонина (ayu.skoblikova+12@secure-t.ru)
 -  Крылов Петр (test@test.com)
- >  ИАС
- >  ИТ отдел
- >  Отдел кадров
- >  Юридический отдел

Этап 1

обучение

Информационная безопасность. Часть 1

осталось 26 дней

Прогресс обучения



Прогресс тестирования



Кто требует моего внимания



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

Выбор целей рассылки



Поиск



выбрано 28 человек

- >  Без отдела
- >  Бухгалтерия
- >  ИАС
- >  ИТ отдел
- ▼  Отдел кадров
 -  Бугаев Руслан Денильбекович (rd.bugaev@secure-t.ru)
- >  Юридический отдел

Этап 2

проверка

Создание новой рассылки

Название рассылки

Введите название рассылки...

Цель рассылки

Выборочно

Всем

выбрано 22 человека



Отложенная рассылка



Дата окончания ?

Авто

К выбранной дате

Выбрать дату



< Июль 2023 >

Пн	Вт	Ср	Чт	Пт	Сб	Вс
26	27	28	29	30	1	2
3	4	5	6	7	8	9
10	11	12	13	14	15	16
17	18	19	20	21	22	23
24	25	26	27	28	29	30
31	1	2	3	4	5	6

13

44

Выбрать

Этап 2

проверка

Добавление шаблонов

Поиск по шаблонам выбран 1 шаблон

- Одноклассники
- Восстановление доступа
- Резервный номер телефона
- Удаление профиля

Гос структуры

-  Gosuslugi
- Налоговая задолженность**
- Судебная задолженность
- Статус заявления
- Штраф
- Платеж
- Транспортный штраф

Налоговая задолженность

госуслуги [Перейти на портал госуслуг](#)

{{.FirstName}} {{.LastName}}!

Сумма назначенных вам налоговых задолженностей увеличилась.

Всего на {{.CurrentDay}}.{{.CurrentMonth}}.{{.CurrentYear}} не оплачено налоговых задолженностей на 23 875,87 руб.

транспортный налог

Инспекция ФНС России № 6 по г. Москве

23 379 р. [Перейти к оплате](#)

[Отменить](#) [Добавить шаблоны](#)

Этап 2

проверка

Назначить курс по окончании рассылки ?

Выбран курс +

Тем, кто:

Ввёл данные ▾

Длительность назначенного курса

30

Отправить письмо по окончании рассылки ?

Тем, кто:

Открыл ссылку ▾

Тема письма

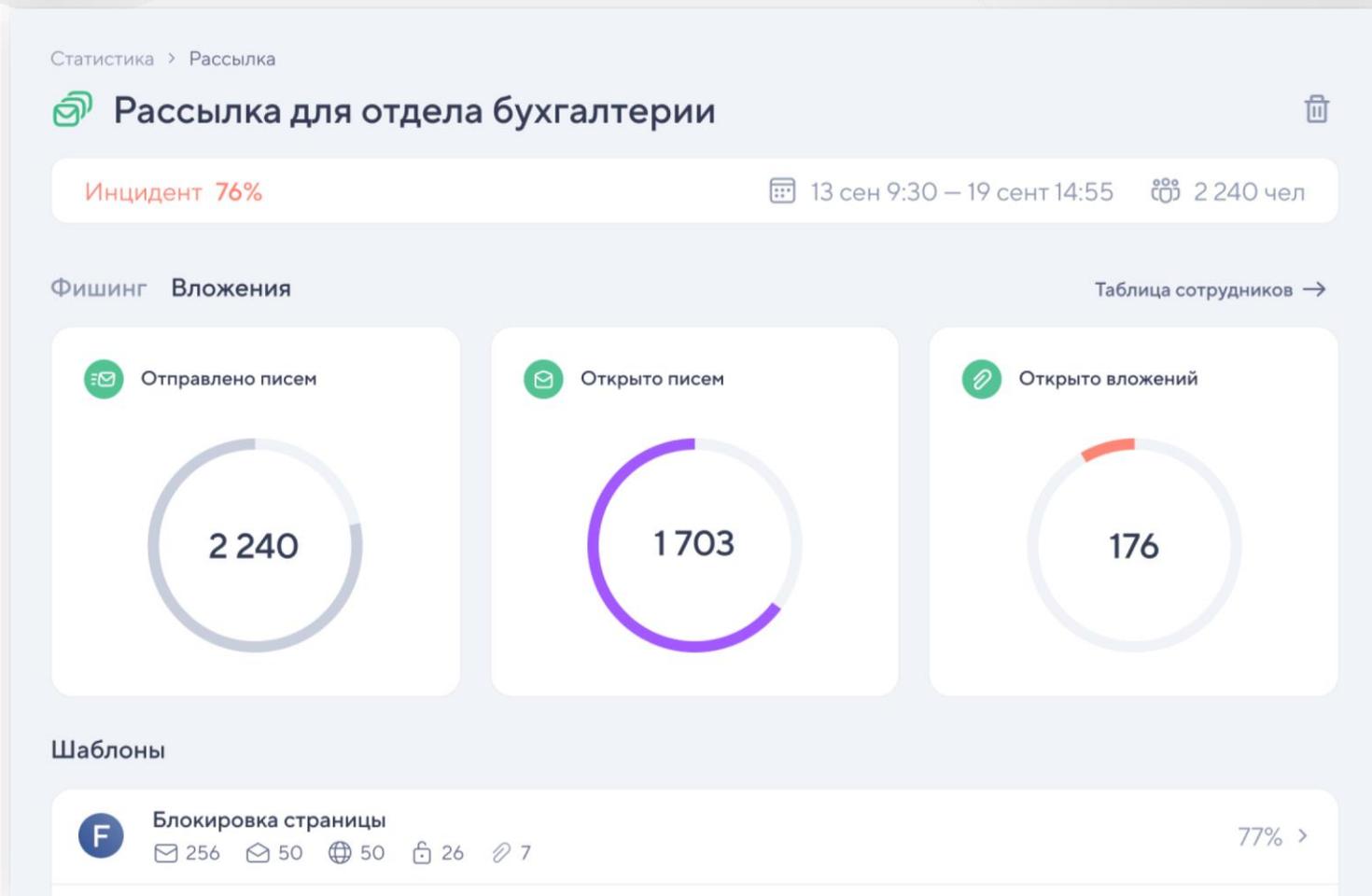
Проверочная рассылка

Текст письма

Коллега,
Вы попались на фишинговое письмо!

Этап 2

проверка



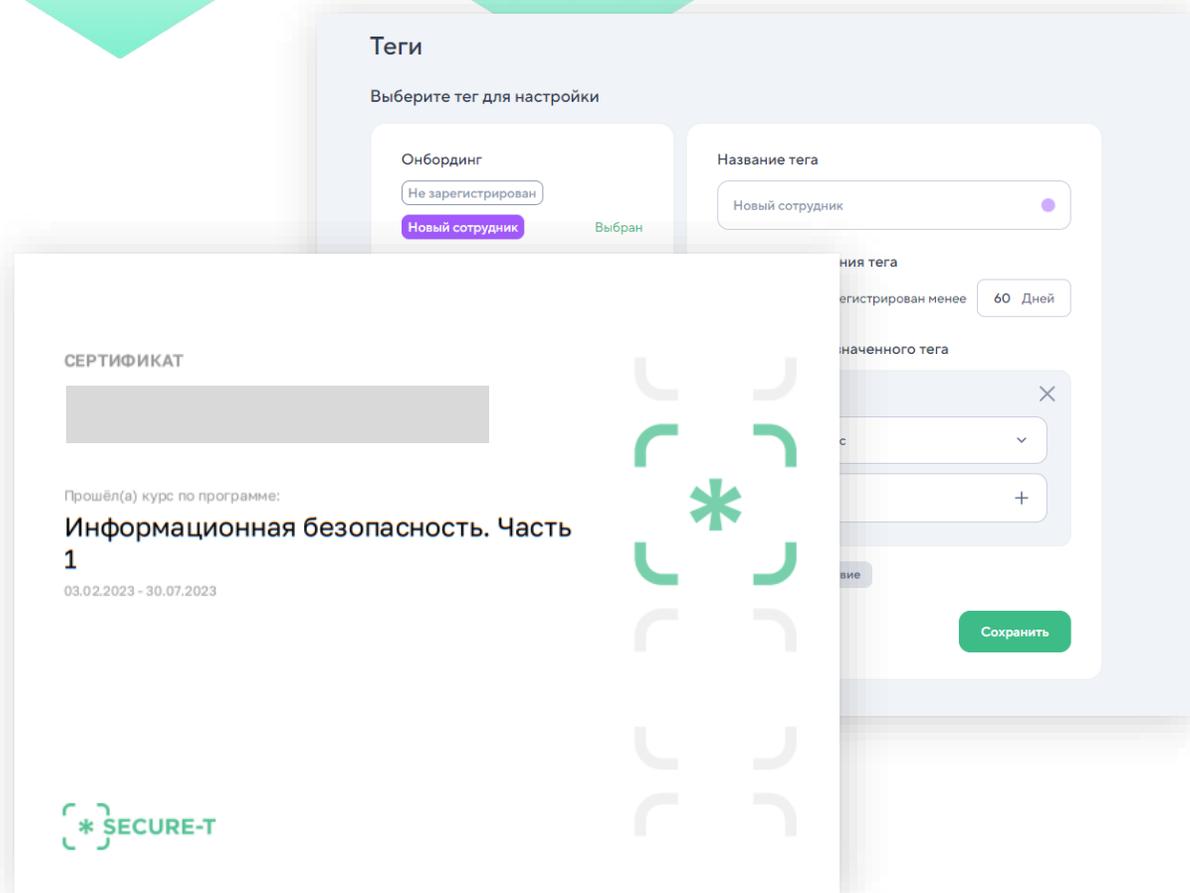
План обучения*

Онбординг

Введение в основы информационной безопасности для новых сотрудников

Сертификаты

Возможность скачать сертификаты после успешного прохождения любого курса



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%

Получить доступ
к демо версии



Получить бесплатные материалы

В конце конференции мы разыграем наш костюм*



*будет направлен победителю по почте

Ссылка на платформу [secure-t asap](https://secure-t.asap)

edu.secure-t.ru

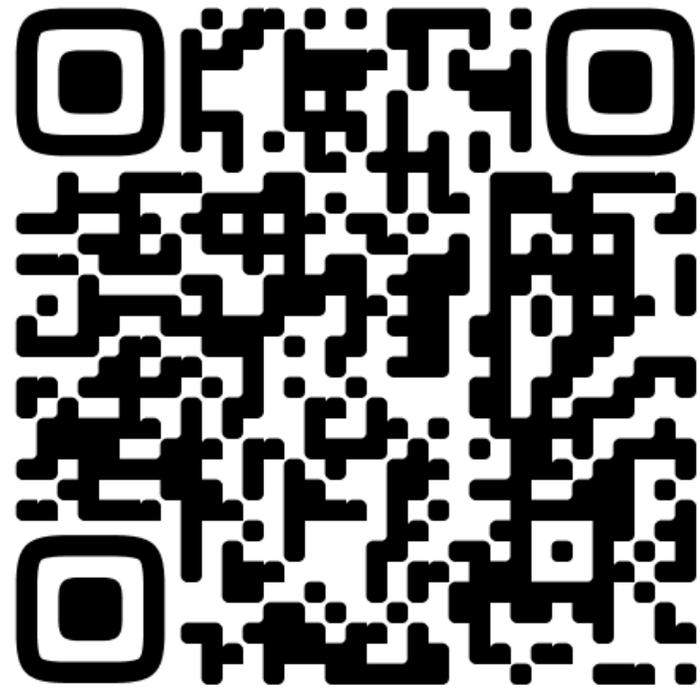
Наши контакты

Телефон

+7 (495) 105-54-85

Почта

info@secure-t.ru



Secure-T Insights

