КИБЕРБЕЗОПАСНОСТЬ

SECURITY AWARENESS

Повышение уровня осведомленности: базовый процесс



Бугаев Руслан

Руководитель развития бизнеса

Статистика цифровых атак

Атаки на организации

50% социальная инженерия

Атаки на частных лиц

88% социальная инженерия

По итогам IV квартала 2024 года **социальная инженерия** продолжает оставаться одним из наиболее популярных методов для цифровых атак.

Основные каналы социальной инженерии

84%	44%	22%	18%
Email	Сайты	Соцсети	Мессенджеры
для организаций	для частных лиц	увеличилась доля использования	

Социальные сети и мессенджеры дают злоумышленникам массу возможностей для обмана пользователей

Законодательное регулирование

152-ФЗ
О персональных данных: принципы и правила обработки

98-ФЗ
О коммерческой тайне

187-ФЗ
О безопасности критической информационной инфраструктуры РФ

ГОСТ Р ИСО/МЭК 27002-2021
Информационная технология. Методы и средства обеспечения безопасности. Свод практических рекомендаций по выбору и внедрению мер защиты информации)

Указ Президента РФ от 01.05.2022 № 250
О дополнительных мерах по обеспечению информационной безопасности РФ

Приказ ФСТЭК России № 117
Об утверждении требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий

Приказ ФСТЭК России № 239
Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры РФ

ГОСТ Р 56939-2024
Защита информации. Разработка безопасного программного обеспечения. Общие требования

Приказ ФСТЭК России от 11.04.2025 №117

Об утверждении Требований о защите информации, содержащейся в государственных информационных системах

Иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений

Зарегистрирован 16.06.2025, № 82619

Дата вступления в силу

1 марта 2026 года

Приказ ФСТЭК России от 11.04.2025 №117

56. Мероприятия по повышению уровня знаний и информированности пользователей информационных систем по вопросам защиты информации должны включать:

- Доведение до пользователей информационных материалов, в том числе в форме памяток, баннеров, буклетов, по актуальным вопросам защиты информации;
- Проведение лекций, семинаров, обучающих игр по вопросам защиты информации;
- Проведение имитационных рассылок электронных писем на служебные адреса электронной почты, иные служебные средства коммуникаций с целью оценки устойчивости пользователей к методам социальной инженерии;
- Проведение тренировок с пользователями по практической отработке мероприятий по защите информации, предусмотренных внутренними регламентами по защите информации, и формированию навыков по защите информации.

57. Применяемые оператором (обладателем информации) способы повышения уровня знаний пользователей по вопросам защиты информации, периодичность и формы оценки уровня знаний должны определяться во внутренних регламентах по защите информации.

Оценка уровня знаний должна проводиться не реже одного раза в три года или после компьютерного инцидента, произошедшего у оператора (обладателя информации).

Для пользователей, у которых отсутствуют знания по вопросам защиты информации, должно быть организовано повторное прохождение обучающих курсов по вопросам защиты информации.

Приказ ФСТЭК №117

Оценка уровня зрелости киберкультуры



БУМАЖНОЕ КОРОЛЕВСТВО

Мы закрываемся бумажками – чтобы соответствовать требованию законодательства



БАЗОВЫЙ ПРОЦЕСС ПОВЫШЕНИЯ УРОВНЯ ОСВЕДОМЛЕННОСТИ

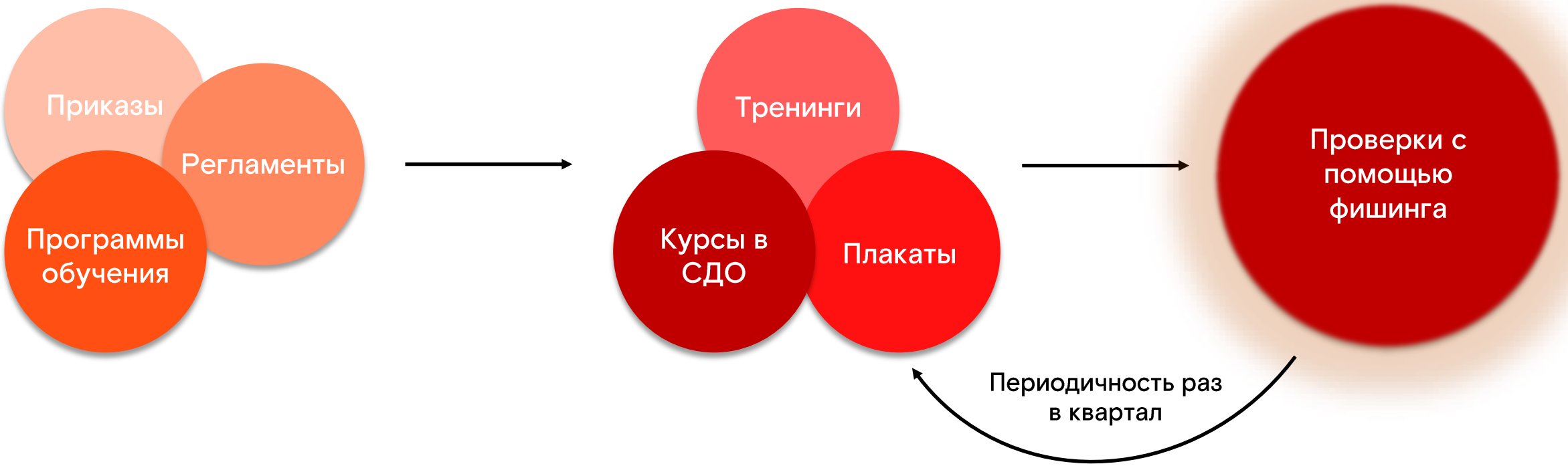
Мы обучаем сотрудников, проводим тренировочные мероприятия и отслеживаем основные метрики, чтобы оценить эффективность



ВАУ, ЭТО КИБЕРКУЛЬТУРА

Помимо базового процесса, мы сегментируем обучение по группам и у нас есть коммуникационный план. С метриками, конечно же

Базовый процесс – как построить?



Метрики знаний

- Результаты тестов
- Количество назначенных курсов
- Количество сотрудников, прошедших курс

Метрики поведения

- Количество переходов по ссылке
- Количество ввода личных данных
- Количество открытых вложений
- Количество проведенных атак
- Количество открытых писем
- Количество отправленных писем

Метрика уязвимости

- Уровень риска пользователя

Метрики вовлеченности

- Процент сотрудников, прошедших курсы

Хорошая новость – есть мануал!

SECURE-T

2025

Киберкультура для всех организаций

Фреймворк по повышению осведомленности рядовых сотрудников

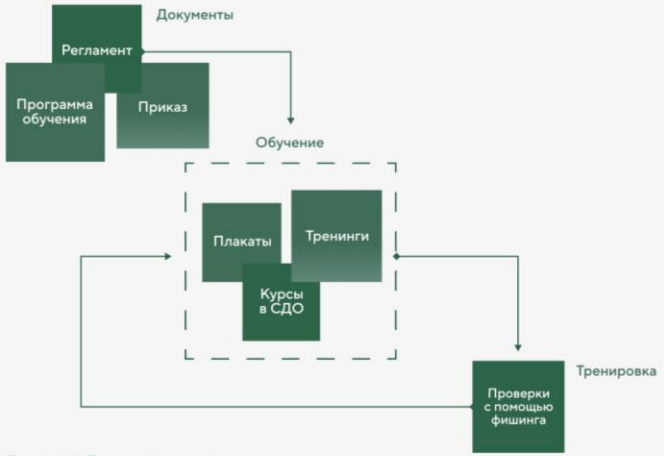


Версия 1.0

Чек-лист стратегии по повышению осведомленности в области ИБ: общий трек

Современные угрозы информационной безопасности требуют системного подхода к обучению сотрудников. Данный фреймворк описывает процесс организации и контроля обучения для повышения осведомленности рядовых сотрудников, минимизации рисков и повышения устойчивости к киберугрозам для всех организаций.

Верхнеуровнево процесс выглядит следующим образом:



Раздел 1. Документация

- Утвердить приказ о проведении обучения сотрудников (Приложение 1)
- Утвердить регламент по обучению и проверке знаний (Приложение 2)
- Разработать программу обучения (опционально)
- Обеспечить доступ сотрудников к документам

Раздел 2. Перечень тем для обучения:

Строгих требований к темам нет — каждая организация определяет их самостоятельно, исходя из своей специфики. До 2024 года NIST рекомендовал следующий перечень тем для повышения осведомленности сотрудников:

- Использование паролей;
- Защита от вредоносного ПО;
- Последствия несоблюдения политики ИБ;
- Появление электронных писем от незнакомых людей и открытие вложений;
- Использование сети Интернет;
- Спам;
- Резервное копирование и восстановление информации;
- Вопросы социальной инженерии;
- Управление инцидентами (кому звонить, что делать);
- Защита от просмотра информации посторонними;
- Безопасность оборудования от окружающей среды;
- Передача информации и оборудования третьим лицам;
- Работа из дома и использование корпоративных систем для личных целей;
- Использование портативных устройств;
- Передача конфиденциальной информации по сети Интернет;
- Безопасность ноутбуков вне территории организации;
- Использование персонального ПО и АО;
- Использование корпоративных систем;
- Регулярное обновление корпоративных систем и ПО;
- Использование лицензионного ПО;
- Вопросы контроля доступа;
- Персональная ответственность пользователей и соглашение о неразглашении;
- Контроль доступа на территорию и правила взаимодействия с посетителями;
- Безопасность рабочих мест;
- Защита конфиденциальной информации;
- Правила использования электронной почты.

В связи с актуальными киберугрозами также настоятельно рекомендуем включить обучение по следующим темам:

- Распознавание дипфейков;
- Защита от вишинга;
- Актуальные угрозы в мессенджерах;
- Правила обработки персональных данных;
- Охрана коммерческой тайны.

*NIST SP 800-50 Building an Information Technology Security Awareness and Training Program

Хорошая новость – есть мануал!

Полезные материалы

SECURE-T

strategy@secure-t.ru

+ 7 (495) 105-54-85

Полезный канал по киберкультуре

Памятка по ИБ для сотрудников

Стратегия: киберкультура для коммерческих организаций



12

НУ ЛАДНО, ВОТ КЬЮАР НА ФРЕЙМ

Бери и делай

Что такое Secure-T Security Awareness?

Обучающий модуль

110+

профильных курсов

Фишинговый модуль

Имитация фишинговых атак

Модуль статистики

Сбор аналитики на личном и корпоративном уровне

Secure-T Security Awareness

Современная образовательная платформа для обучения специалистов данного профиля

Открывает целый спектр надежных методов защиты от цифровых атак и тренирует эффективное реагирование в случае угрозы. Платформа направлена на **повышение и контроль уровня киберграмотности сотрудников.**

Более **90%** кибератак происходят из-за недостатка знаний в области цифровой безопасности

Обучайте

По современным программам

Проверяйте

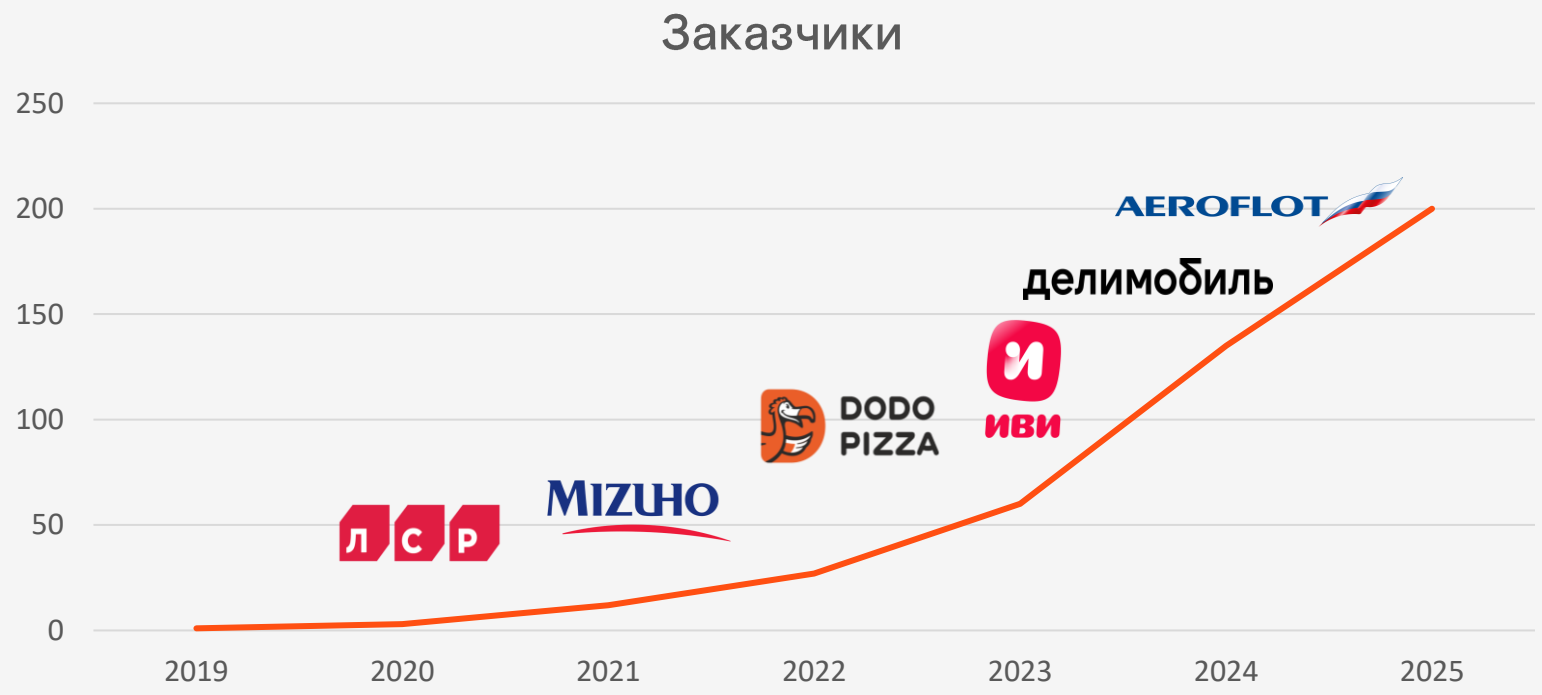
Результаты и прогресс

Выявляйте

Уязвимости персонала

О нас

Динамика роста заказчиков



Действующие заказчики

200+

по 2025 год

Retention

90%+

удержание клиентов

Решение secure-t asap

Теория

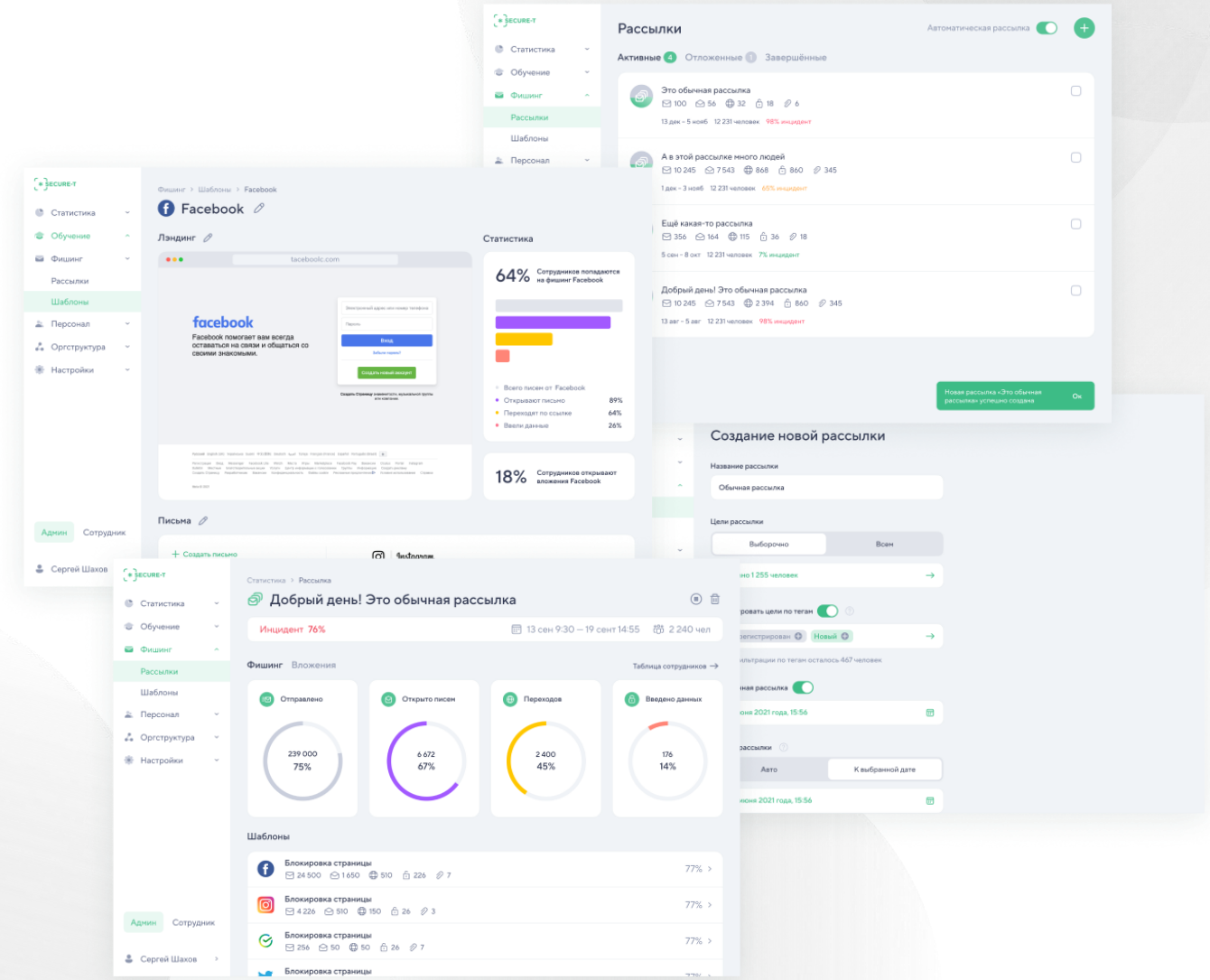
Обучающие курсы и тесты

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



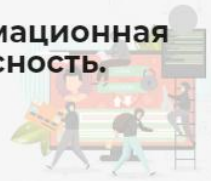
Всё, что нужно знать о GDPR
2 модуля



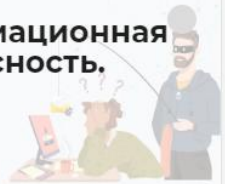
Противодействие коррупции в РФ
2 модуля



Информационная безопасность. Часть 2
8 модулей



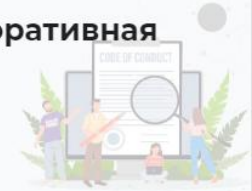
Информационная безопасность. Часть 1
8 модулей



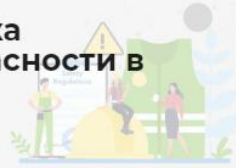
ФЗ-152 "О персональных данных"
1 модуль



Корпоративная этика
1 модуль

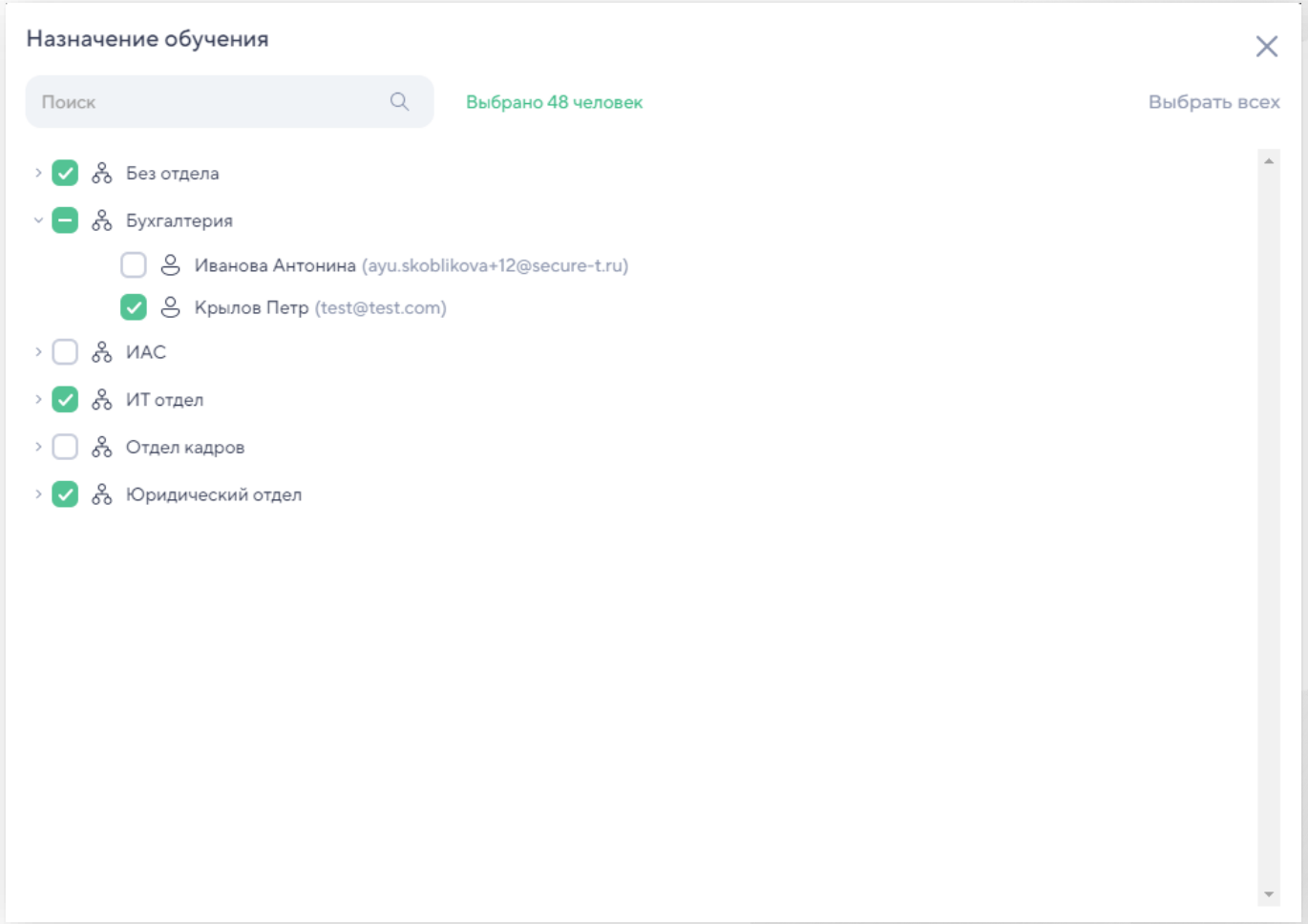


Техника безопасности в офисе
2 модуля



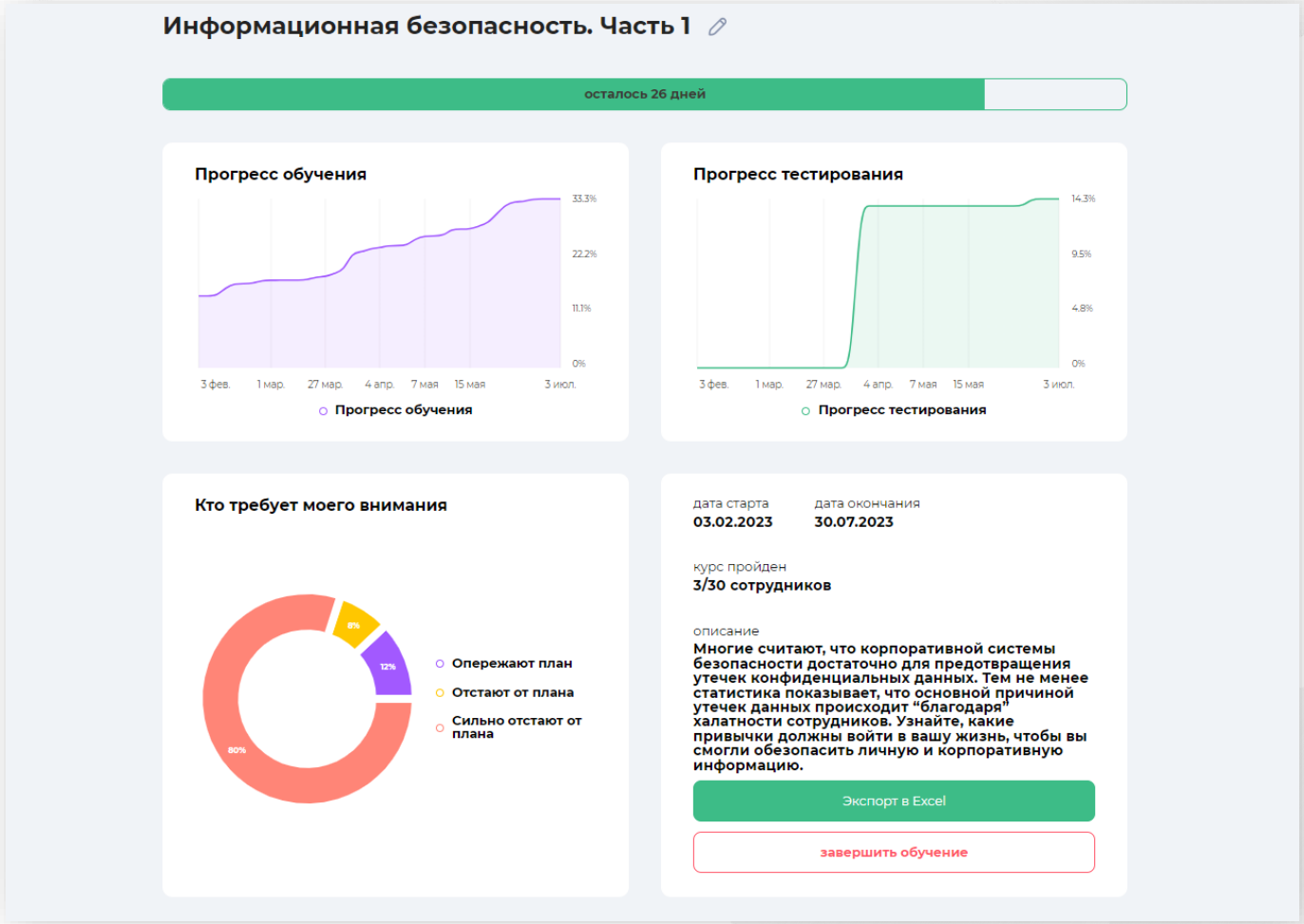
Этап 1

Обучение



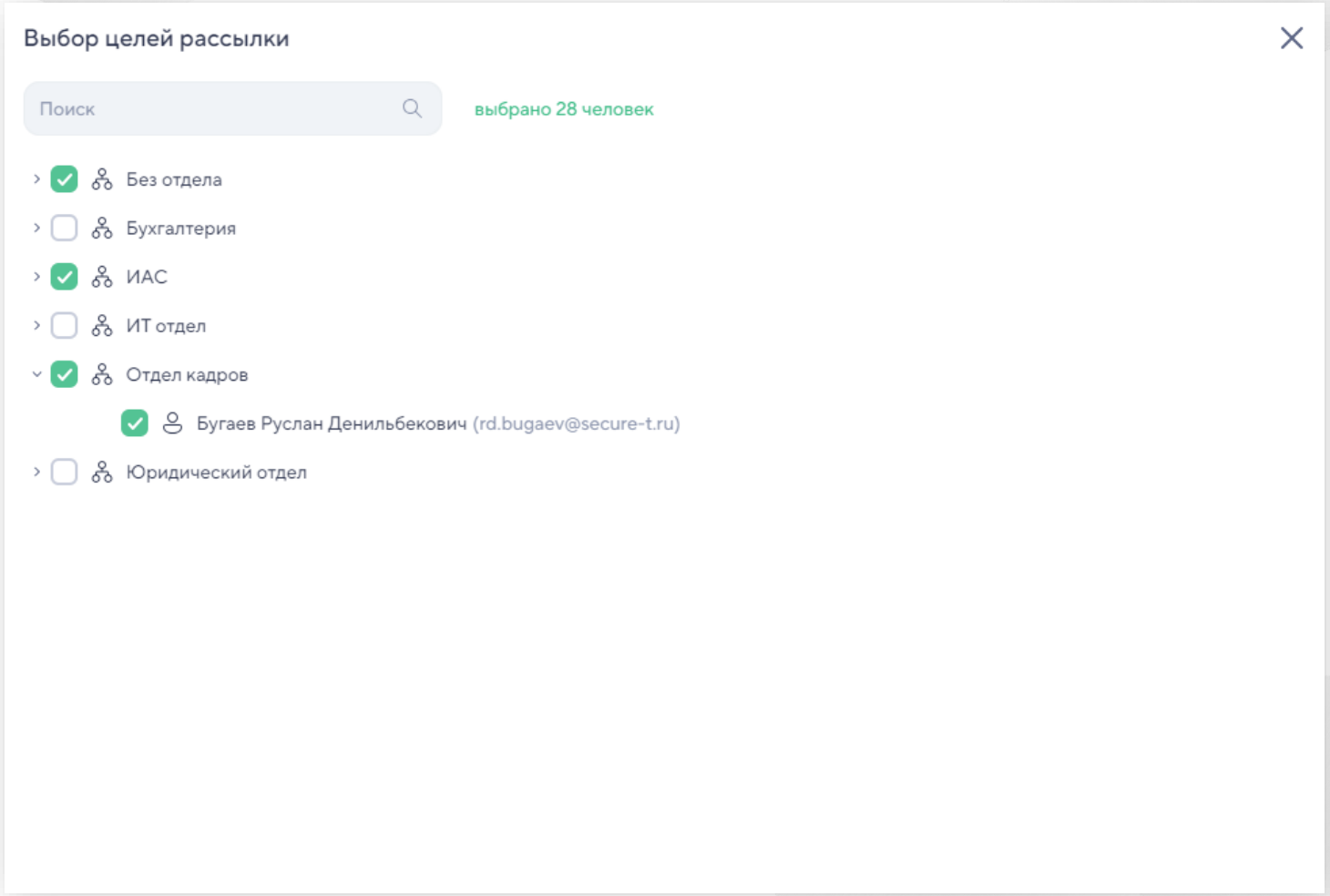
Этап 1

Обучение



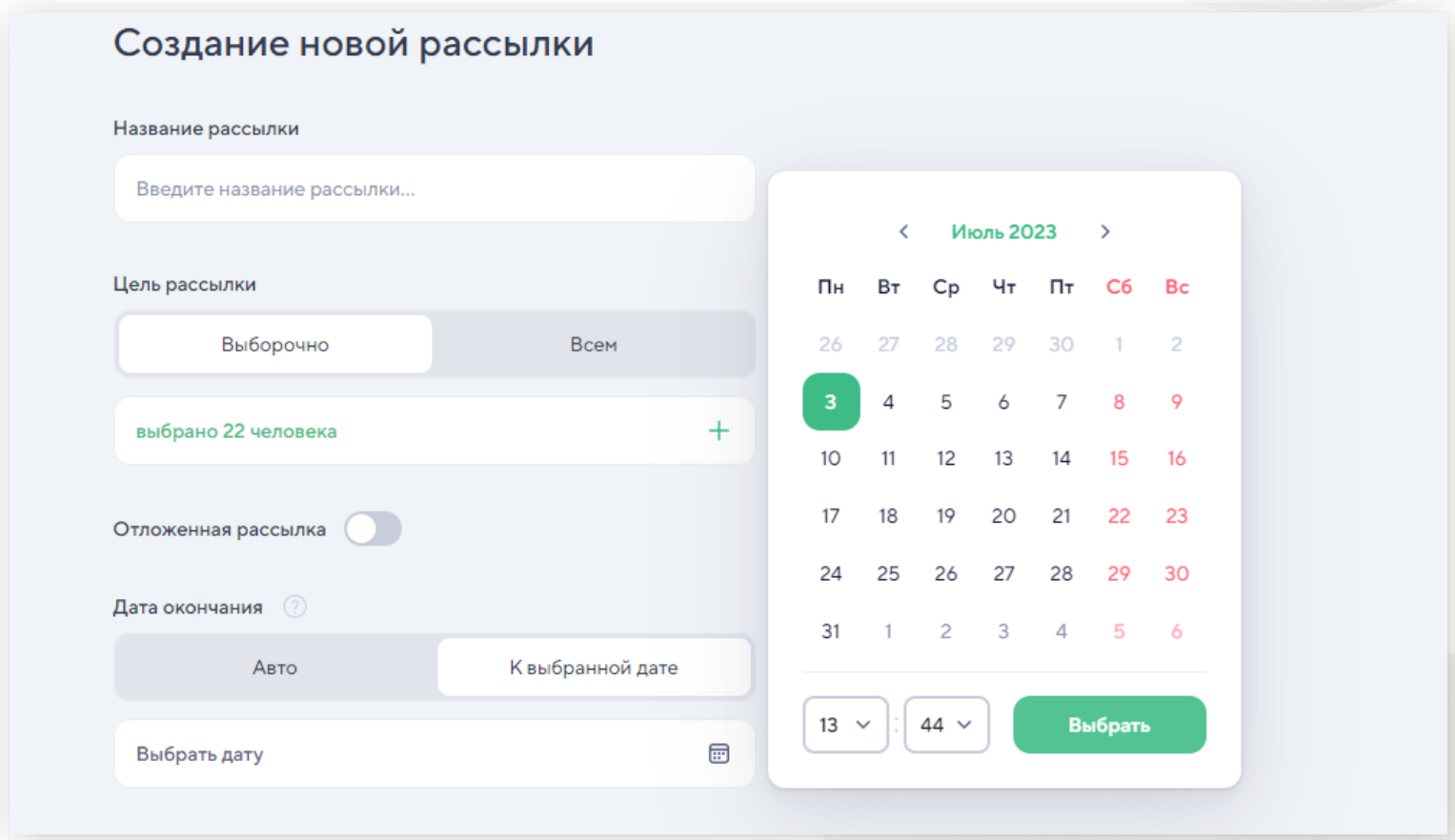
Этап 2

проверка



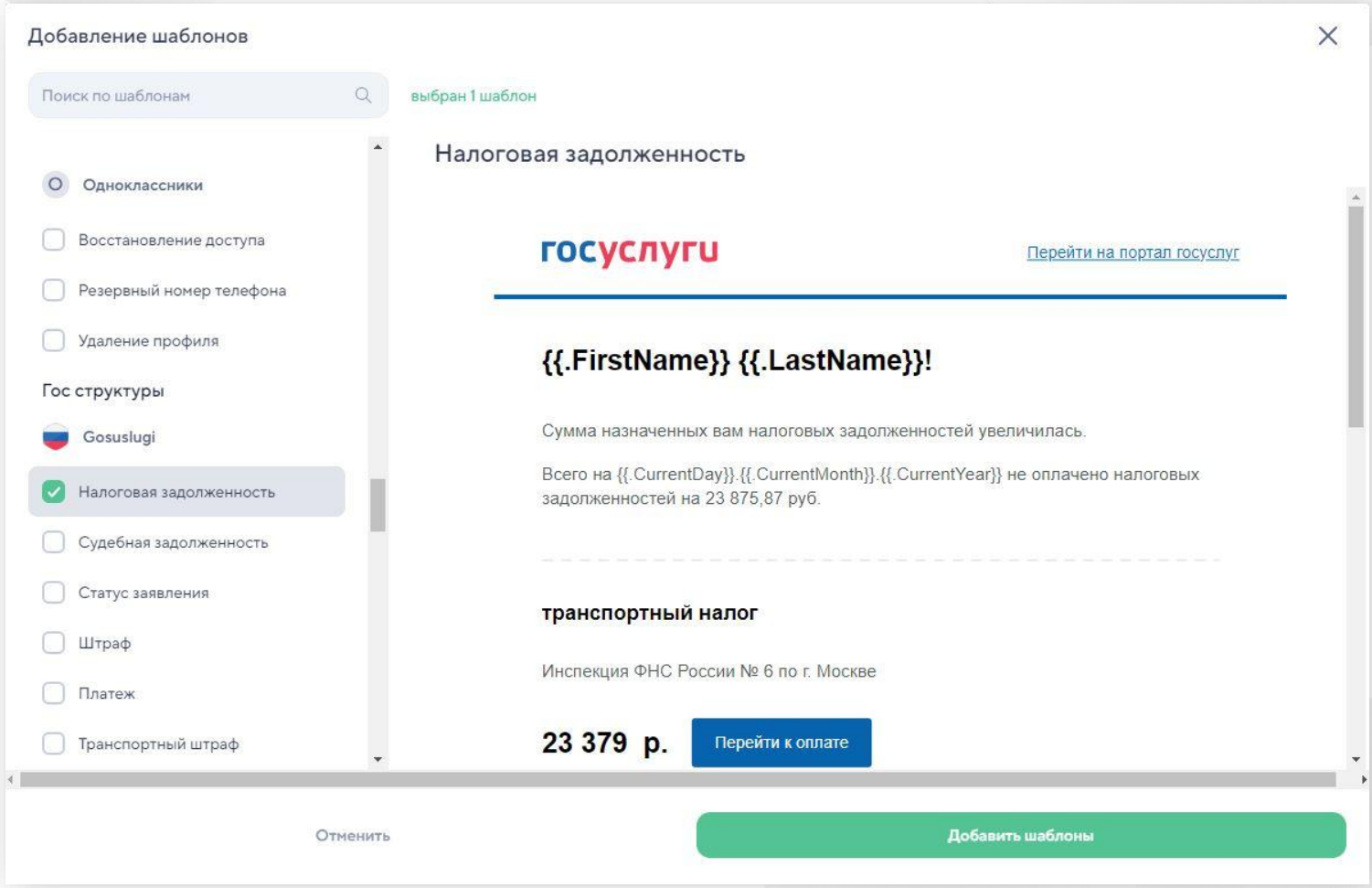
Этап 2

проверка



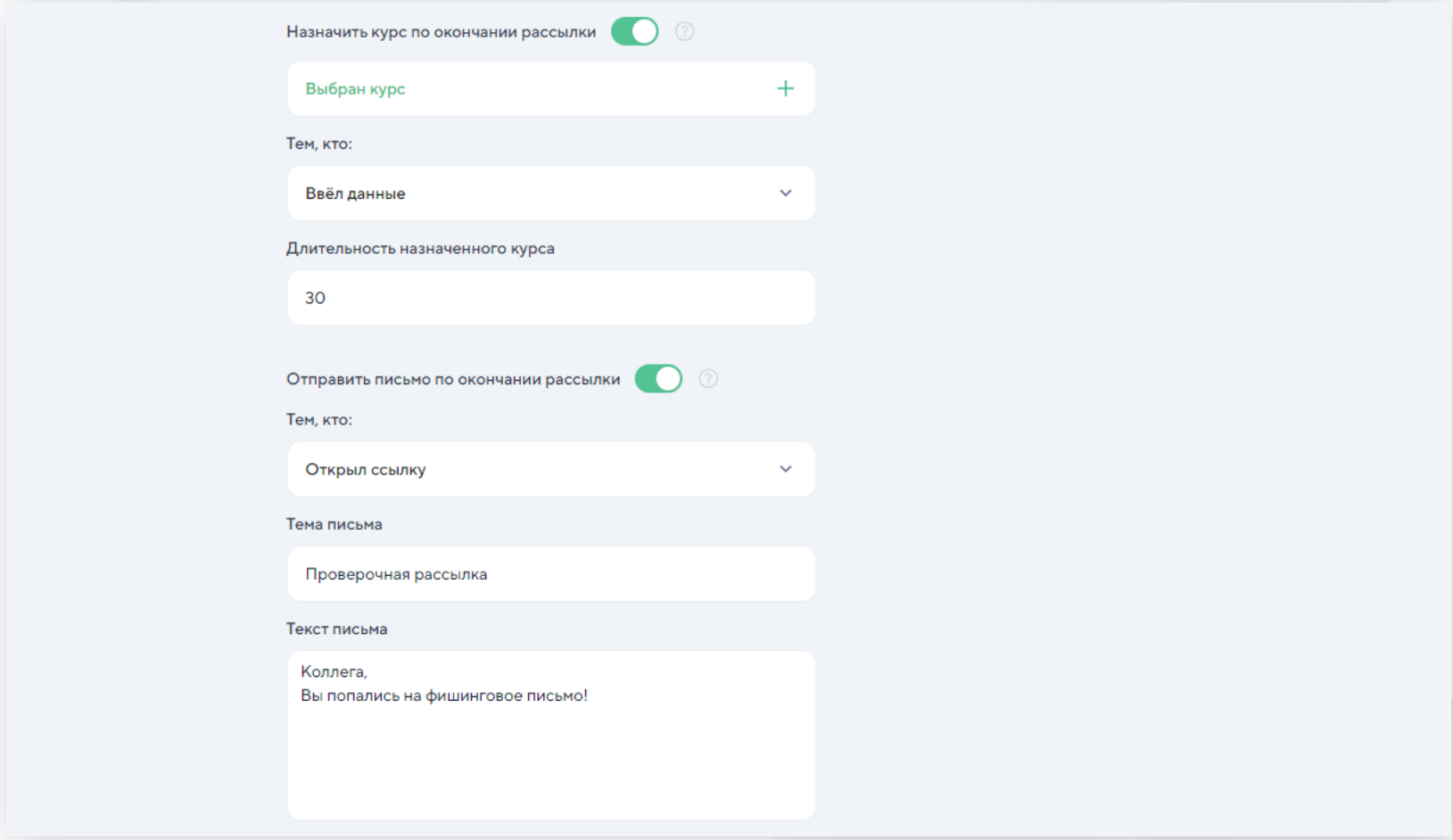
Этап 2

проверка



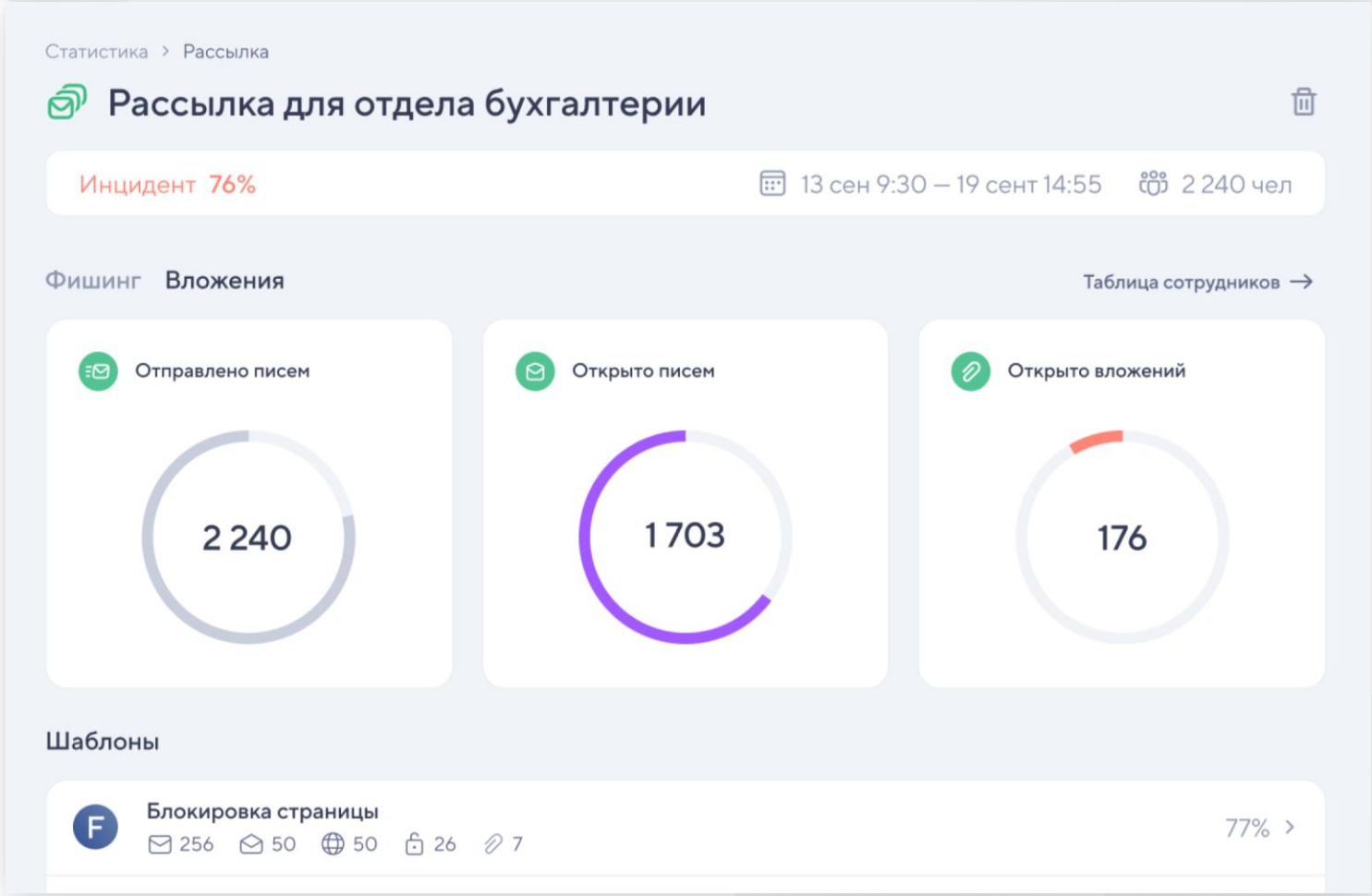
Этап 2

проверка



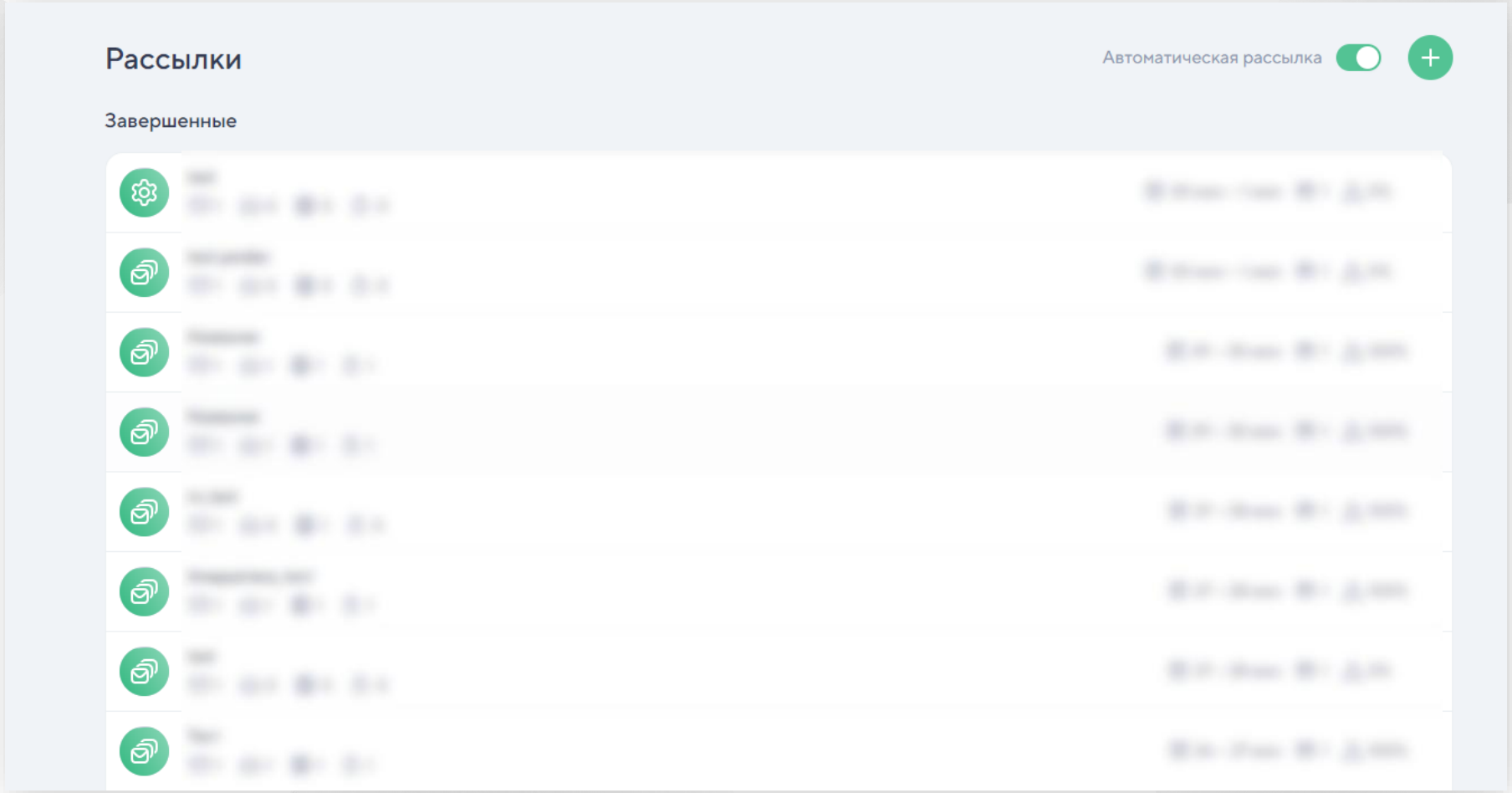
Этап 2

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.

КИБЕРБЕЗОПАСНОСТЬ

SECURITY AWARENESS

Повышение уровня осведомленности: киберкультура для зрелых организаций



Бугаев Руслан

Руководитель развития бизнеса

Ладно, ну а киберкультура-то что

Это только общий трек



А по SANS у нас еще

- Технические специалисты
- Топ - менеджмент
- Безопасники

А еще, тут нет никакой коммуникации – процесс-то односторонний!

В общем, выглядит это как-то так

ТОП - МЕНЕДЖЕРЫ

Тренинг

Обучение со спикером + тестирование

Опрос

Проведение опроса для определения уровня удовлетворенности

Коммуникация

Телеграм-канал с новостями и ОС

ОБЩИЙ ТРЕК

Тест-опрос

Проведение тест-опроса и проверочная фишинговая рассылка для определения уровня знаний на текущий период

Вебинар-знакомство

Первый вебинар с отделом ИБ для ознакомления с программой и мотивационной составляющей + телеграм-канал

Обучение и фишинг

Изучение модулей сотрудниками + фишинговая рассылка + тестирование

ВОТ НАШ БАЗОВЫЙ ПРОЦЕСС

Итоговый вебинар

Вебинар-тренинг, включающий в себя: вопросы-ответы, анализ ошибок в тесте и кейс-сессия

Итоговый опрос

Сбор показателей удовлетворенности, отзывы и предложения по улучшению

И так

СПЕЦИАЛИСТЫ ИБ

- Обучение
- Фишинг
- Отраслевые мероприятия
  - Вовлечение сотрудников ИБ в мероприятия по киберкультуре
- Коммуникация
  - Телеграм-канал

ТЕХНИЧЕСКИЙ ТРЕК

- Обучение и фишинг
  - Обучение по безопасной разработке, изучение основных уязвимостей, фишинг-рассылка
- Внутренние мероприятия
  - Площадки для внутренних докладов по ИБ, форумы по вопросам ИТ и ИБ
- Тренинг
  - Участие в тренингах и открытых турнирах CTF
- Внутренняя баг-баунти
  - Участие в программе поиска и устранения уязвимостей в системах
- Коммуникация
  - Телеграм-канал

Элементы киберкультуры

ОБУЧЕНИЕ И ПРАКТИКА

КУРСЫ СДО
С брендированием компании

ПЛАКАТЫ
Индивидуальный дизайн

ФИШИНГ
Письма и вложения

ФЛЕШКИ
Проверка пользователей

ТЕСТЫ
Уникальные и разнообразные вопросы

ТРЕНИНГИ
Со специалистами области

Подрядчик | Компания | Совместно

Периодичность обучения и практики: Раз в квартал

МЕТРИКИ:

Метрики знаний:
- Результаты тестов
- Количество назначенных курсов
- Количество сотрудников, прошедших курс

Метрики поведения:
- Количество проведенных атак
- Количество открытых писем
- Количество отправленных писем
- Количество переходов по ссылке
- Количество ввода личных данных
- Количество открытых вложений
- Индекс изменения поведения (снижение инцидентов безопасности, вызванных человеческим фактором)*
- Процент подключенных флешек

Метрика уязвимости:
- Уровень риска пользователя

Метрики вовлеченности:
- Процент сотрудников, прошедших курсы

* Количество инцидентов может быть низким, поэтому корреляция не всегда наглядна

Элементы киберкультуры

СТРАТЕГИЯ КОММУНИКАЦИИ

ОЧНЫЕ ВСТРЕЧИ

Включая кейс-сессии с разбором вопросов и тестов

ТЕЛЕГРАМ

Для размещения актуальной информации

МОТИВАЦИЯ

Программа поощрения сотрудников

ПОЧТА

Отдельный сервис для связи с ИБ

ОПРОС

Метрики вовлеченности, осведомленности, удовлетворенности

ВЕБИНАРЫ

Организация вебинаров вне учебного процесса

Подрядчик | Компания | Совместно

Периодичность проведения очных встреч, опросов, мероприятий: Минимум раз в квартал

МЕТРИКИ:

Метрики удовлетворенности:

- Оценка уровня удовлетворенности сотрудников курсами по киберкультуре с помощью опросов (индивидуальные мероприятия для каждой целевой группы)

Метрика осведомленности:

- Оценка через опросы уровня осведомленности сотрудников о новых типах киберугроз и атаках, возникающих в цифровом пространстве

Метрики вовлеченности:

- Процент сотрудников, посетивших вебинары
- Процент сотрудников, посетивших очные встречи
- Количество обращений в службу ИБ за советами

Метрика успешности информационных материалов:

- Количество скачиваний или просмотров размещенных материалов
- Количество подписанных на канал

Элементы киберкультуры



Периодичность обновления регламентов, приказов, планов обучения: **Ежегодно** или при изменениях в нормативной базе, техниках угроз, а также после проведения крупных аудитов или инцидентов

Использование системы для обучения и повышения уровня осведомленности в части фишинга: **Минимум раз в квартал**

МЕТРИКИ AWARENESS:

Метрики знаний:	• Результаты тестов • Количество назначенных курсов • Количество сотрудников, прошедших курс
Метрики поведения:	• Количество переходов по ссылке • Количество ввода личных данных • Количество открытых вложений • Количество проведенных атак • Количество открытых писем • Количество отправленных писем
Метрика уязвимости	• Уровень риска пользователя
Метрики вовлеченности:	• Процент сотрудников, прошедших курсы
Метрики плагина для почты:	• Количество пересланных тренировочных писем • Количество обнаруженных пользователями фишинговых атак

Как разводить функции обучения и контроля HR & ИБ

ФУНКЦИИ HR

ОБУЧЕНИЕ

Департамент HR отвечает за два основных процесса обучения посредством LMS:

- Обучение новых сотрудников
- Регулярное обучение

ТРЕНИНГИ

Проведение совместных мероприятий со спикерами на тематику ИБ

КОММУНИКАЦИЯ

Взаимная поддержка коммуникационных планов и каналов

ФУНКЦИИ ИБ

ИМИТАЦИЯ АТАК

Департамент ИБ занимается проведением учений по социальной инженерии при помощи SA

ПОДГОТОВКА МАТЕРИАЛОВ

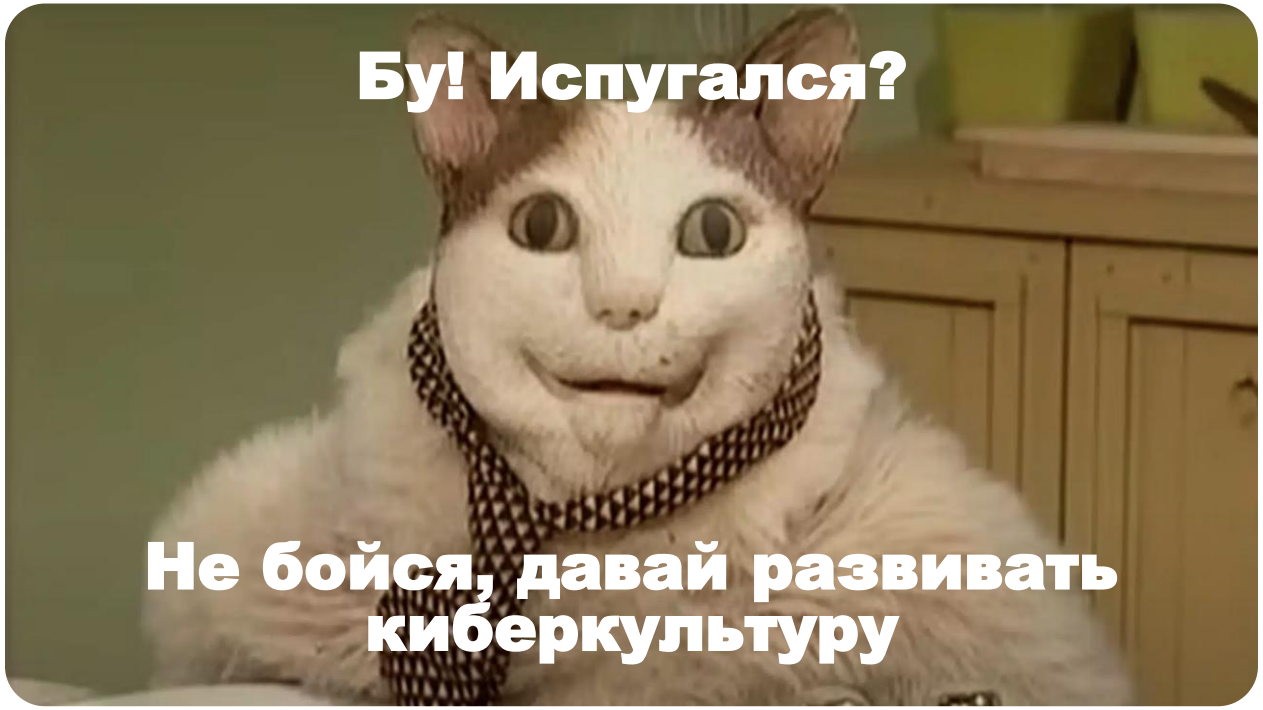
В связи с динамичным развитием угроз, а также появлением новых мошеннических схем, департамент ИБ должен предоставлять материалы с актуальной информацией и методах защиты

ОБУЧЕНИЕ

На своей платформе, ИБ обучает 3 группы:

- Безопасная разработка
- КУД пользователи
- Пользователи, не прошедшие проверку

Стратегия киберкультуры



Ответы на вопросы

Готовы обсудить внедрение Security Awareness?

Наша команда поможет подобрать оптимальное решение для вашей организации

Телефон

+7 (495) 105-54-85

Email

info@secure-t.ru