

The background of the slide is a high-quality image of the Earth as seen from space. The right side of the frame is dominated by the curved horizon of the planet, showing the blue of the oceans and the white of the clouds. The left side is a deep, dark blue space filled with numerous small, distant stars. A thin, bright white line of light stretches horizontally across the middle of the image, adding a sense of depth and focus.

КИБЕРБЕЗОПАСНОСТЬ

SECURITY AWARENESS

Повышение уровня осведомленности:
базовый процесс

Шевченко Константин

Менеджер по развитию 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%

Email

для организаций



44%

Сайты

для частных лиц



22%

Соцсети

увеличилась доля использования



18%

Мессенджеры

Социальные сети и мессенджеры дают злоумышленникам массу возможностей для обмана пользователей

Законодательное регулирование

152-ФЗ

О персональных данных: принципы и правила обработки

Указ Президента РФ от 01.05.2022 № 250

О дополнительных мерах по обеспечению информационной безопасности РФ

98-ФЗ

О коммерческой тайне

Приказ ФСТЭК России № 117

Об утверждении требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий

187-ФЗ

О безопасности критической информационной инфраструктуры РФ

Приказ ФСТЭК России № 239

Об утверждении требований по обеспечению безопасности значимых объектов 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)

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

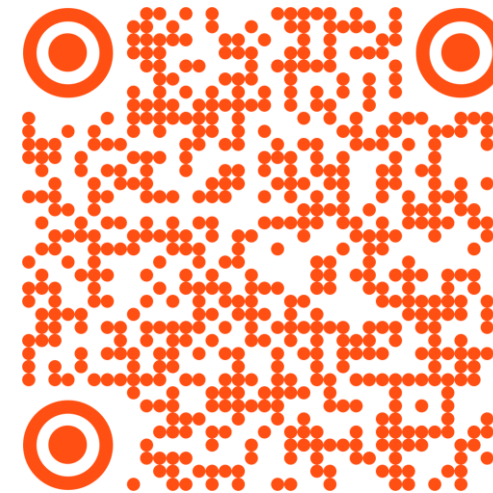
56. Мероприятия по повышению уровня знаний и информированности пользователей информационных систем по вопросам защиты информации должны включать:

- 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.

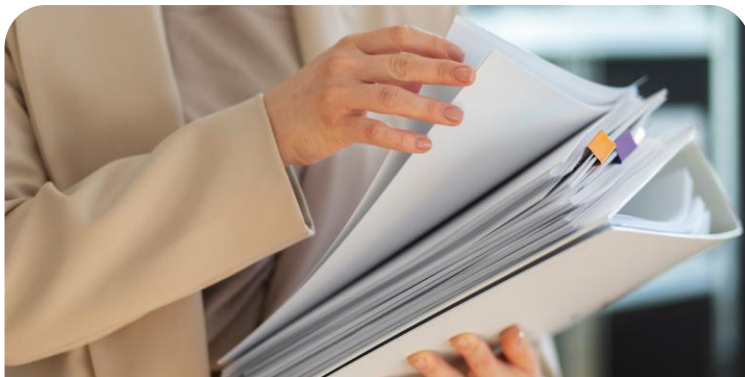
Оценка уровня знаний должна проводиться не реже одного раза в три года или после компьютерного инцидента, произошедшего у оператора (обладателя информации).

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

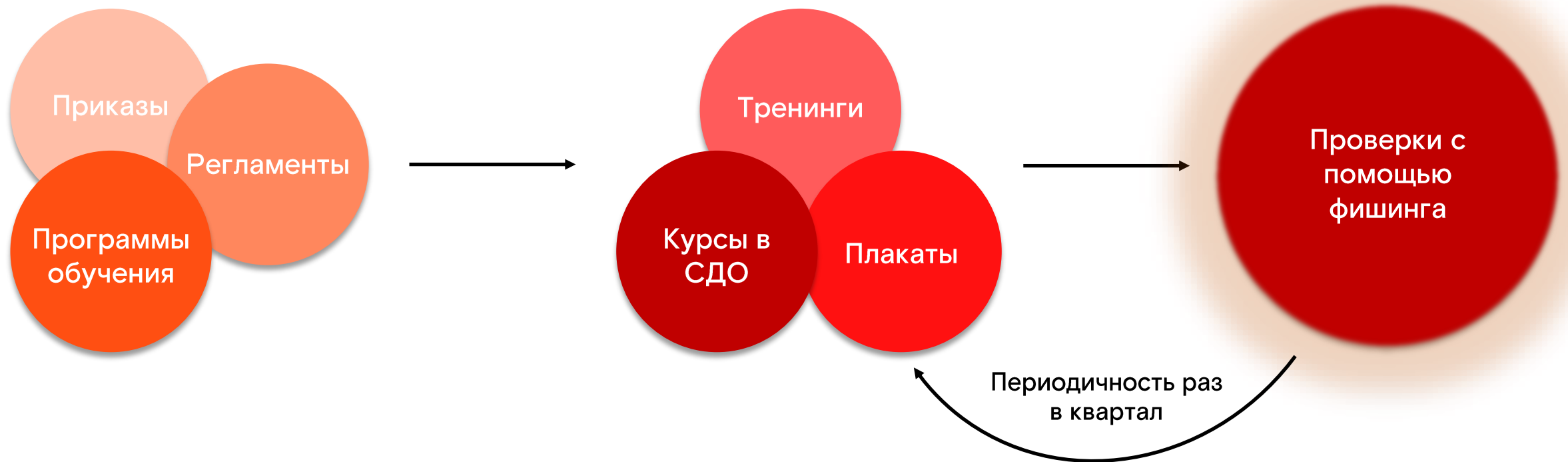
Мы обучаем сотрудников, проводим тренировочные мероприятия и отслеживаем основные метрики, чтобы оценить эффективность



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!

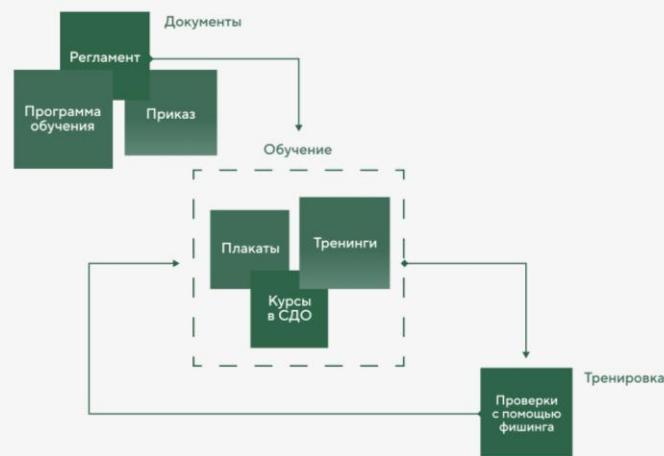
* SECURE-T		2025
Киберкультура для всех организаций	Фреймворк по повышению осведомленности рядовых сотрудников	
		
Версия 1.0		

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!

НУ ЛАДНО, ВОТ КЬЮАР НА ФРЕЙМ

Полезные материалы			 strategy@secure-t.ru + 7 (495) 105-54-85
Полезный канал по киберкультуре			
			
Памятка по ИБ для сотрудников			
			
Стратегия: киберкультура для коммерческих организаций			



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



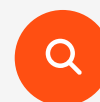
Обучайте

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

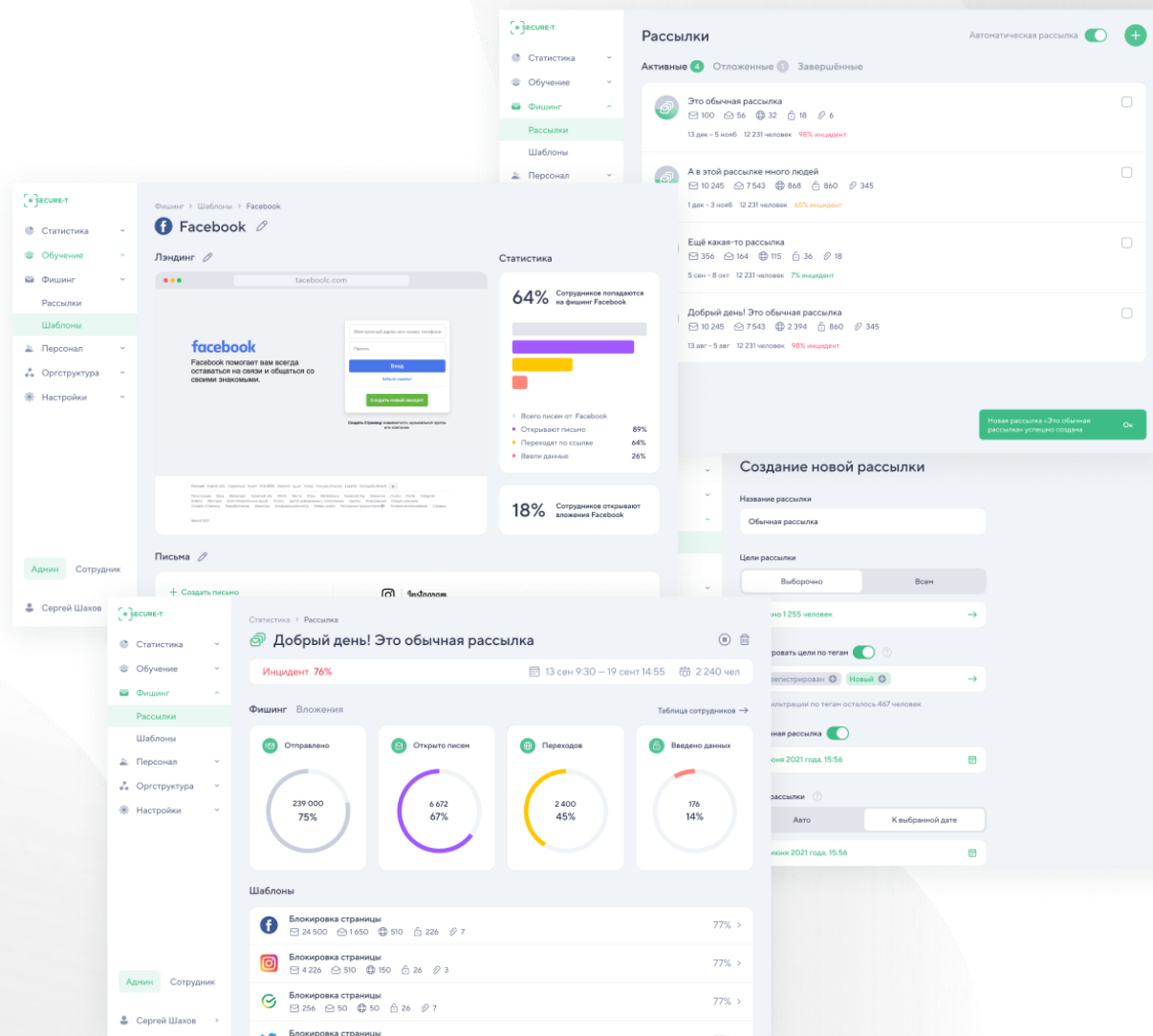
Обучающие курсы и тесты

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 лендингов

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



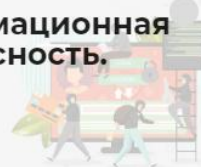
**Противодействие
коррупции в РФ**

2 модуля



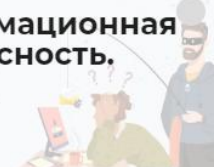
**Информационная
безопасность.
Часть 2**

8 модулей



**Информационная
безопасность.
Часть 1**

8 модулей



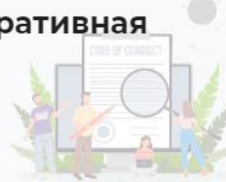
**ФЗ-152 "О
персональных
данных"**

1 модуль



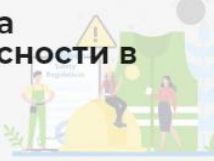
**Корпоративная
этика**

1 модуль



**Техника
безопасности в
офисе**

2 модуля



| Этап 1

Обучение

Назначение обучения

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

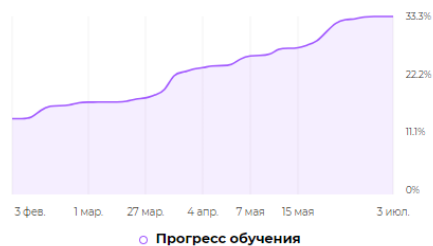
| Этап 1

Обучение

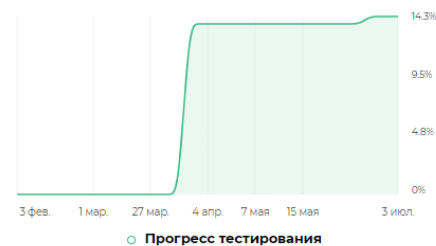
Информационная безопасность. Часть 1

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

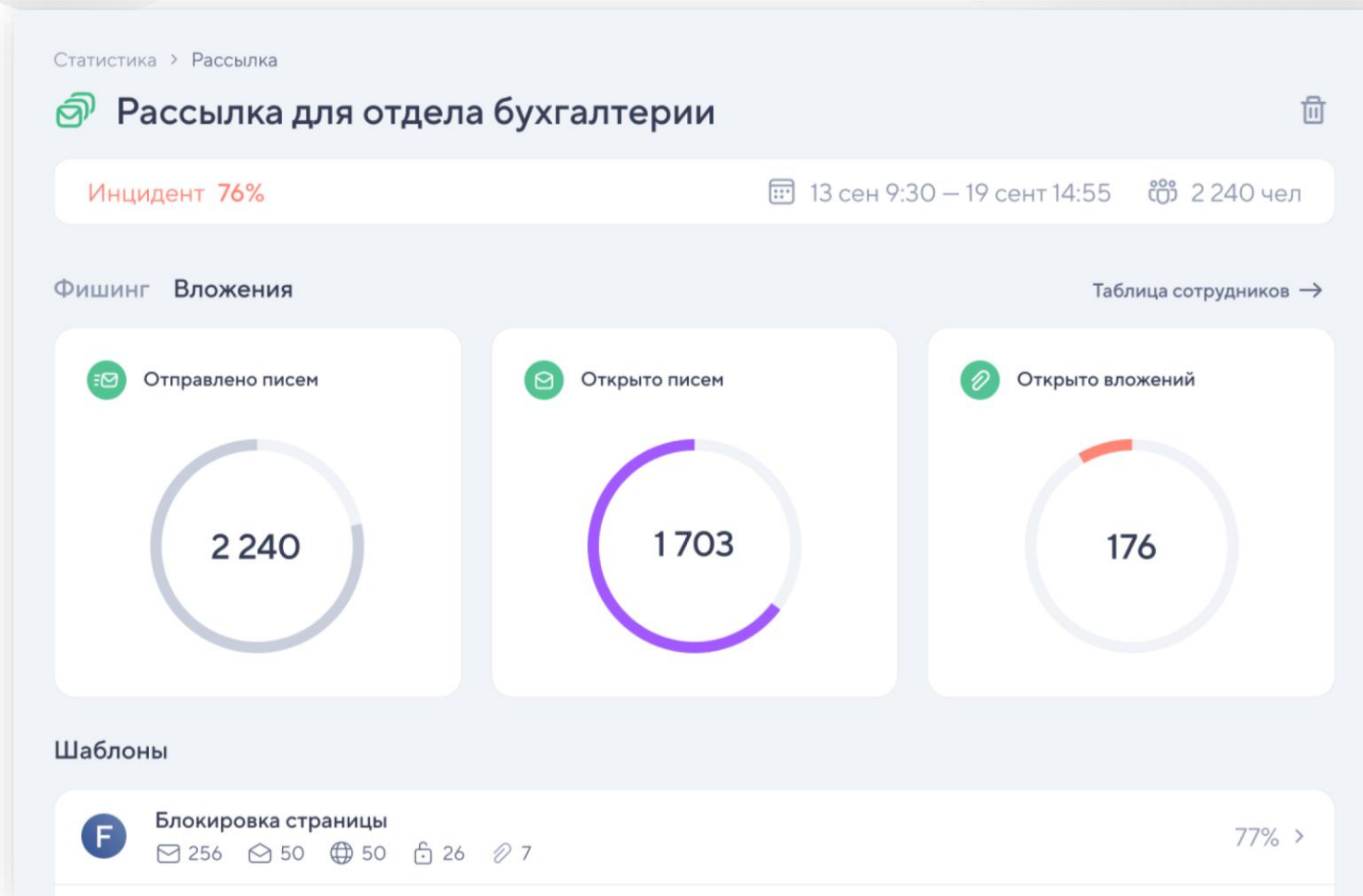
Проверочная рассылка

Текст письма

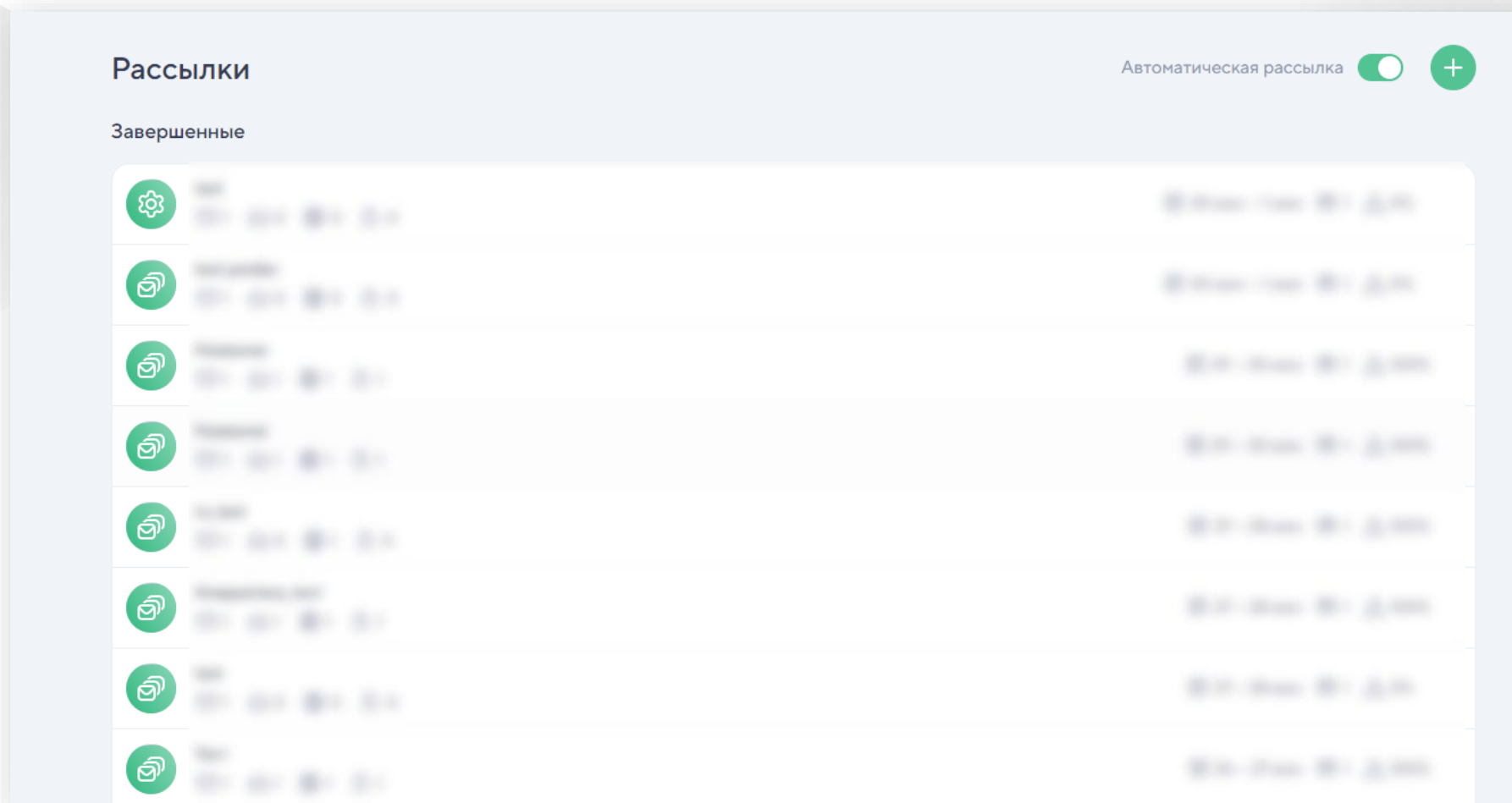
Коллега,
Вы попались на фишинговое письмо!

| Этап 2

проверка



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.

The background of the slide is a high-quality image of the Earth as seen from space. The right side of the image shows the curved horizon of the planet, with blue oceans and dark landmasses. The left side is a deep blue gradient. The overall composition is clean and professional, with a focus on the title and the speaker's information.

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

| Базовый процесс – как построить?



А по SANS у нас еще



Технические
специалисты



Безопасники

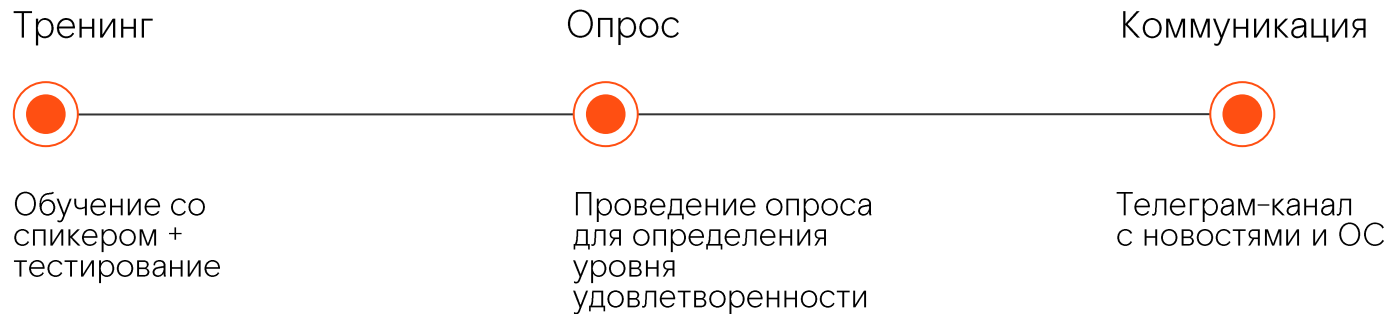


Топ –
менеджмент

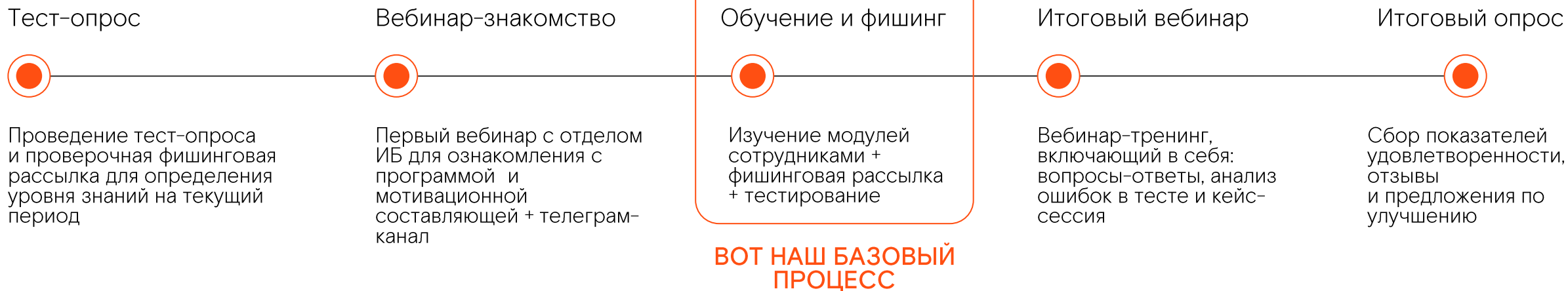
А еще, тут нет никакой коммуникации – процесс-то односторонний!

| В общем, выглядит это как-то так

ТОП – МЕНЕДЖЕРЫ



ОБЩИЙ ТРЕК



| И так

СПЕЦИАЛИСТЫ ИБ

Обучение



Фишинг



Отраслевые мероприятия



Коммуникация



Вовлечение сотрудников ИБ в мероприятия по киберкультуре

Telegram-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



Telegram-канал

| Элементы киберкультуры

ОБУЧЕНИЕ И ПРАКТИКА

КУРСЫ СДО

С брендингом
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

ТЕХНОЛОГИЧЕСКИЙ ПРОГРЕСС

Paperwork

РЕГЛАМЕНТ

Обучения сотрудников

ПЛАН ОБУЧЕНИЯ

Сроки и порядок проведения мероприятий

ПРИКАЗ

Основание для проведения обучения

Программное обеспечение

AWARENESS

Система повышения уровня осведомленности пользователей

ПЛАГИН ДЛЯ ПОЧТЫ

Контроль обратной связи и предотвращения инцидентов



Подрядчик



Компания



Совместно

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

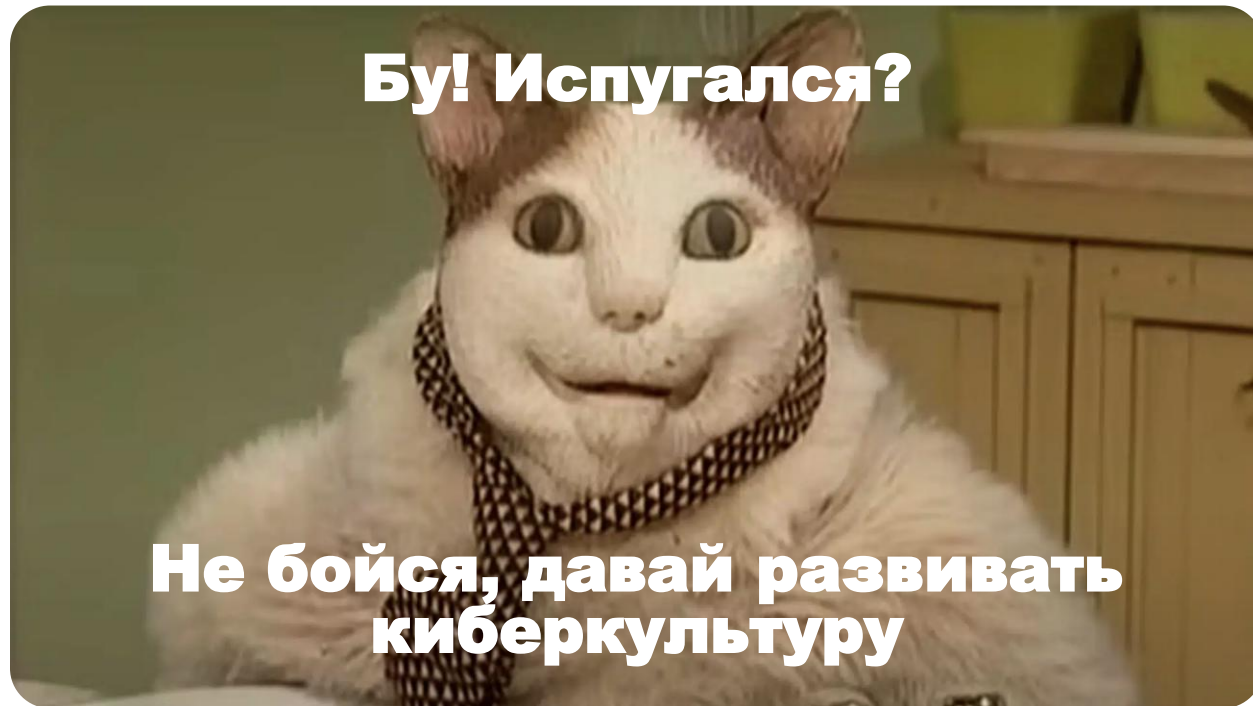
В связи с динамичным развитием угроз, а также появлением новых мошеннических схем, департамент ИБ должен предоставлять материалы с актуальной информацией и методах защиты

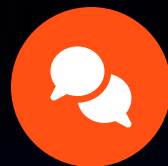
ОБУЧЕНИЕ

На своей платформе, ИБ обучает 3 группы:

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

| Стратегия киберкультуры





Отвeты 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