Киберкультура для всех организаций:

Как контролировать влияние человеческого фактора на периметр информационной безопасности

Спикер: Никишкин Харитон Григорьевич
Генеральный директор Secure-T

Тезисы

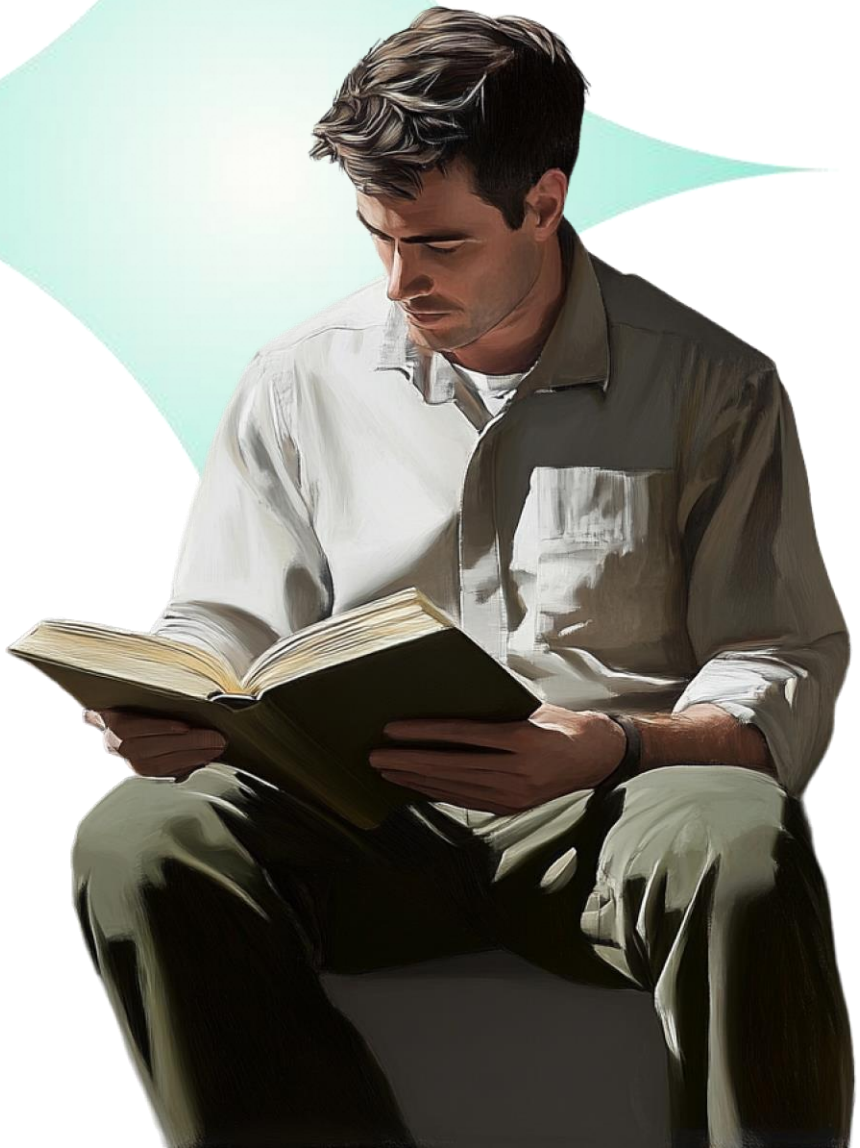
SECURE-T

Периметр информационной безопасности

это концепция, которая описывает границы, в рамках которых осуществляется защита информационных активов организации.

Контроль влияния на периметр информационной безопасности

это комплексный подход, который позволяет организациям эффективно управлять рисками и обеспечивать защиту своих информационных активов. Он требует постоянного внимания и адаптации к изменяющимся условиям внешней среды и технологическим тенденциям.



Проблема

Неосведомленность

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

Нехватка аналитики

Отсутствие подробной аналитики по уровню подготовки сотрудников и степени их уязвимости

Отсутствие контроля

Нехватка ресурсов или отсутствие возможности контроля знаний сотрудников

Низкий уровень вовлеченности

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

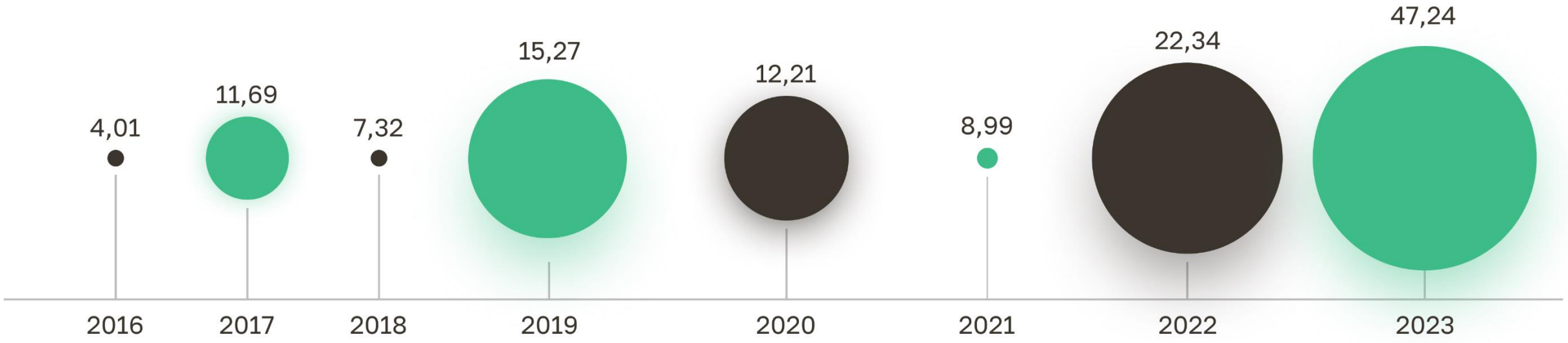
Быстро меняющиеся угрозы

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

Статистика

SECURE-T

Совокупное количество персональных данных, скомпрометированных в результате внешних и внутренних утечек, в 2023 году составило **42,24 млрд записей**



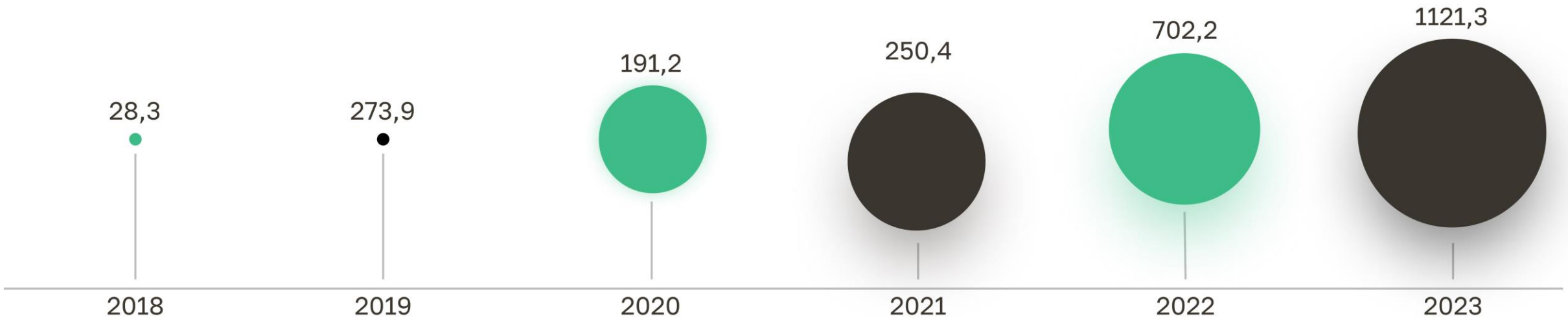
Количество утечек информации и количество утекших записей ПДн в мире, 2016-2023 гг

Источник: InfoWatch. Утечки информации в мире, 2022-2023 годы

Статистика

SECURE-T

Совокупное количество ПДН и платежной информации,
скомпрометированных в результате утечки данных,
в 2023 составило **1121,3 млн записей**



Количество утекших записей ПДн и платежной информации в России. Млн записей, 2018–2023 гг.

Источник: InfoWatch. Утечки информации ограниченного доступа в России за 2022-2023

Последствия

Компания:

Uber

Происшествие:

Хакеры получили доступ к внутренним системам Uber через социальную инженерию. Они обманом убедили сотрудника предоставить свои учетные данные через фишинговую атаку, что позволило злоумышленникам проникнуть в критические системы компании, включая Slack и другие внутренние ресурсы

Результат:

Утечка внутренних данных, включая финансовую информацию, привела к репутационным потерям, замедлению работы компании и проведению расследования

Последствия

Компания:

Microsoft 365

Происшествие:

В начале 2023 была совершена фишинговая атака на более чем 56 000 корпоративных учетных записей Microsoft 365 и скомпрометировала по меньшей мере 8000 из них. Пользователям приходили фишинговые письма с разными сценариями социальной инженерии и ссылками. Атака была направлена на миллионы пользователей Office 365 в 62 странах.

Результат:

Мошенникам удалось получить незаконную прибыль в размере 500 000 долларов, прежде чем специалисты компании смогли взять ситуацию под контроль.

Законодательство

152-ФЗ

«О персональных данных»
Меры по защите персональных данных

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»

Положение Банка России

(№ 683-П, № 757-П)
Описание обязательного обучения работников финансовых организаций

Приказ ФСТЭК России от 25.12.2017г. №239 КИИ

Состав мер по обеспечению безопасности и обучению Персонала

Сегодня мы рассмотрим как базовые, так и более сложные процессы

SECURE-T

Как
стратегии и методы реализации

Где
подходящие форматы и платформы

Кого обучать
определение целевой аудитории

Что
основные элементы и содержание программ

Когда
оптимальные сроки и частота мероприятий

Какие метрики
оценка эффективности программ

Цель: изучение влияния человеческого фактора на периметр информационной безопасности

Первый шаг

Построение процесса повышения осведомленности

Второй шаг

Переход к состоянию киберкультуры внутри организации

Шаг первый. Повышение осведомленности

Контроль
влияния человеческого фактора на периметр ИБ

Обеспечение
цифровой гигиены и безопасности

Развитие
навыков реагирования на угрозы

Информирование
сотрудников об актуальных угрозах

Шаг второй. Повышение киберкультуры

Снижение

уязвимости организаций

Повышение

доверия к отделу ИБ

Предупреждение

цифровых угроз

Формирование

ответственного поведения в сети

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

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

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

+

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

Программы обучения

Курсы в СДО

Проверки с помощью фишинга

Приказы

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

SECURE-T

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

Киберкультура

SECURE-T

Как понять насколько зрелый процесс в организации?

Киберкультура — это совокупность социальных норм, ценностей и практик, которые формируются в процессе взаимодействия людей с цифровыми технологиями и информационными системами

Цели

01. Обеспечение цифровой гигиены и безопасности
02. Развитие навыков реагирования на угрозы
03. Снижение уязвимости организаций
04. Формирование ответственного поведения в сети
05. Предупреждение цифровых угроз
06. Повышение доверия к отделу ИБ

Решение

Развитие культуры кибербезопасности

Развитие киберкультуры обеспечивает устойчивость компании в условиях быстро меняющейся цифровой среды и является основой для создания надежной цифровой экосистемы.

01.
Обеспечивает цифровую гигиену и безопасность
Способствует созданию безопасной рабочей среды и снижению риска утечек данных

02.
Развивает навыки реагирования на угрозы
Помогает сотрудникам уверенно действовать в случае инцидентов, минимизируя последствия

03.
Снижает уязвимость организаций
Уменьшает вероятность атак за счет повышения осведомленности о киберугрозах

04.
Формирует ответственное поведение в сети
Способствует соблюдению правил безопасности и снижению числа инцидентов, связанных с ошибками сотрудников

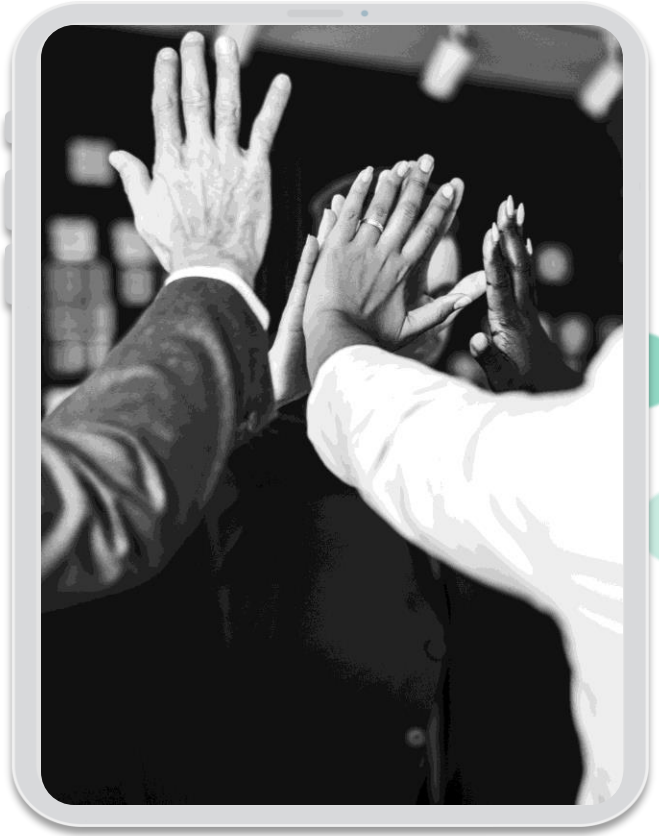
05.
Предупреждает цифровые угрозы
Позволяет проактивно выявлять и устранять риски, прежде чем они станут проблемой

06.
Повышает доверие к отделу ИБ
Укрепляет сотрудничество между сотрудниками и специалистами по безопасности, что способствует лучшему соблюдению политик ИБ

Индивидуальное решение для каждого

Мы подготовили решение, направленное на индивидуальный подход к каждой категории сотрудников:

- Топ-менеджеры
- Технический трек
- Общий трек
- Специалисты ИБ



План обучения

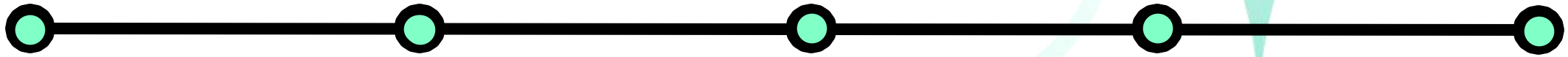
Топ-менеджеры

Обучение со спикером + тестирование

Проведение опроса для определения уровня удовлетворённости

Телеграмм канал с новостями и ОС

Общий трек



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

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

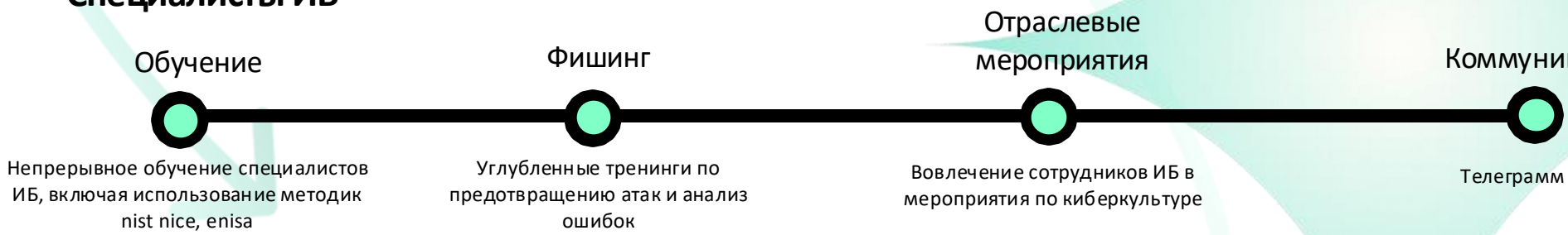
Изучение модулей сотрудниками + фишинг рассылка + тестирование

Вебинар-тренинг, включающий в себя: вопрос-ответ, анализ ошибок в тесте и кейс-сессия

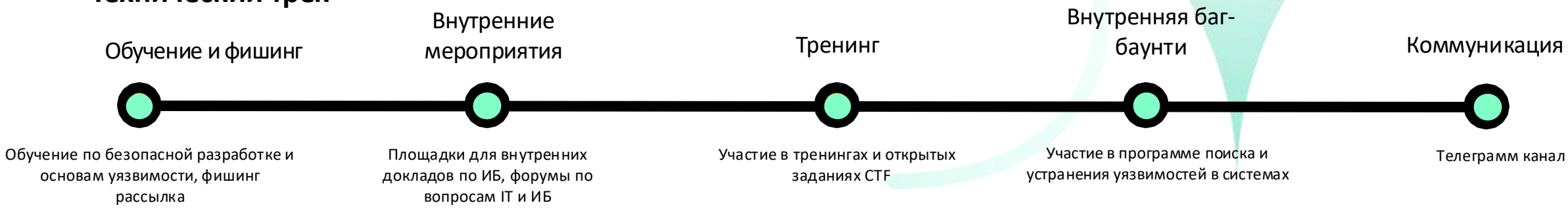
Сбор показателей удовлетворённости, отзывы и предложения по улучшению

План обучения

Специалисты ИБ



Технический трек



Элементы киберкультуры

Подрядчик | Компания | Совместно

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 в области

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, осведомлённости, удовлетворённости

Вебинары
Создание вебинаров вне учебного процесса

Технологический процесс

Paperwork

Регламент
Обучения сотрудников

План обучения
Сроки и порядок проведения мероприятий

Приказ
Основание для проведения обучения

Программное обеспечение

Awareness
Система повышения осведомленности пользователей

Плагин для почты
Для контроля обратной связи и предотвращения инцидентов

Элементы киберкультуры

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 открытий писем
- количество отправленных писем
- количество переходов по ссылке
- количество ввода личных данных
- количество открытий 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

Периодичность проведения очных встреч, опросов, мероприятий: минимум раз в квартал
Остальные активности проводятся на постоянной основе

Метрики:

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

Метрика осведомленности:
- оценка уровень осведомленности сотрудников о новых типах киберугроз и атаках, возникающих в цифровом пространстве через опросы

Метрики вовлеченности:
- процент сотрудников, посетивших вебинары
- процент сотрудников, посетивших очные встречи
- количество обращений в службу ИБ за советами

Метрика успешности информационных материалов:
- успешность 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, технологии угроз, а также после проведения крупных аудитов или инцидентов
Использование системы для повышения осведомленности в части фишинга и обучения: минимум раз 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 открытий вложений
- количество проведенных атак
- количество открытий писем
- количество отправленных писем

Метрика уязвимости:
- уровень риска пользователя

Метрики вовлеченности:
- процент сотрудников, прошедших курсы

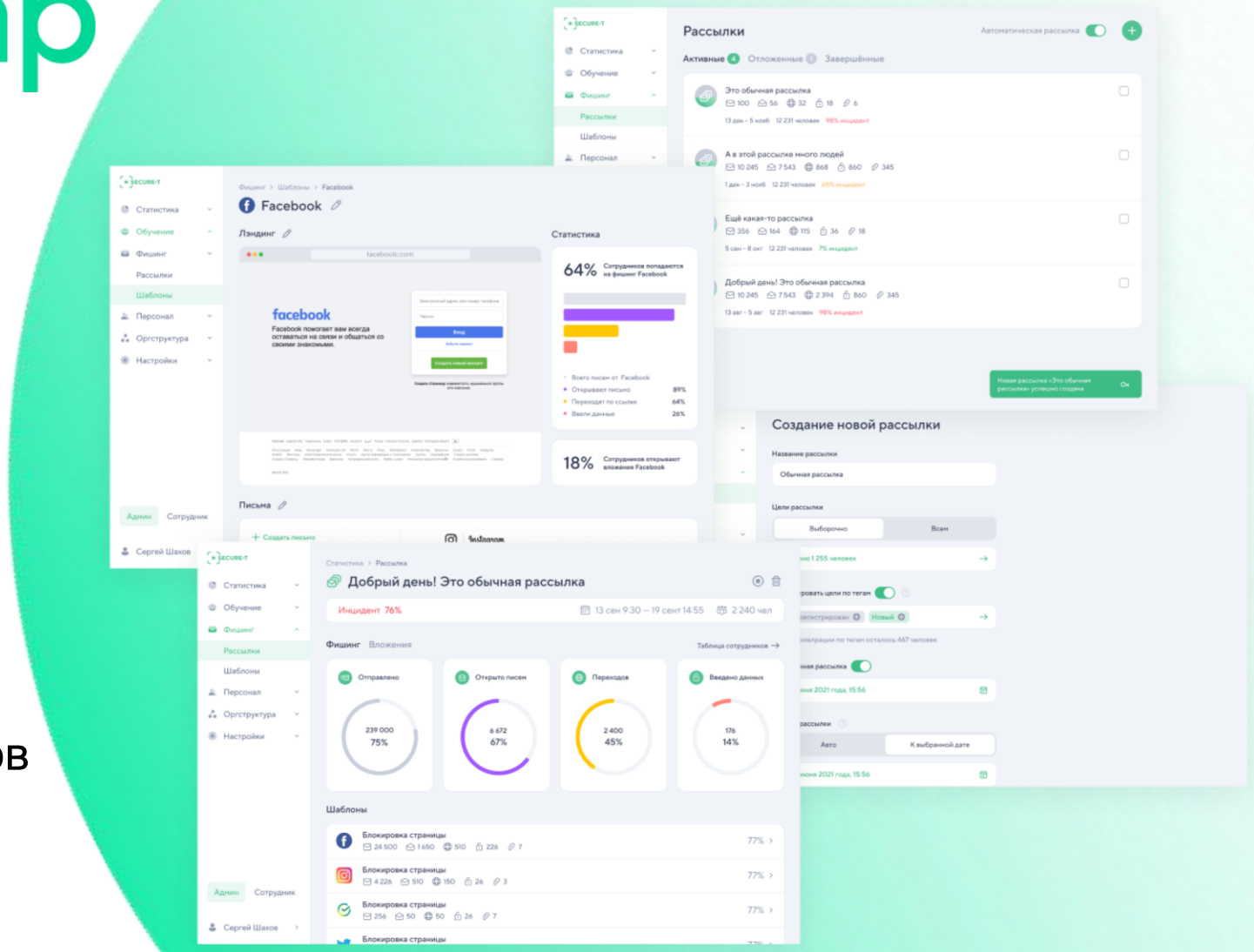
Метрики плагина для почты:
- количество пересланных тренировочных писе
- количество обнаруженных пользователями фишинговых атак

Решение
secure-t asap

Теория
Обучающие курсы и тесты

Практика
Имитация фишинга и вирусных вложения

Аналитика
Подробная статистика
и выявление уязвимых сотрудников

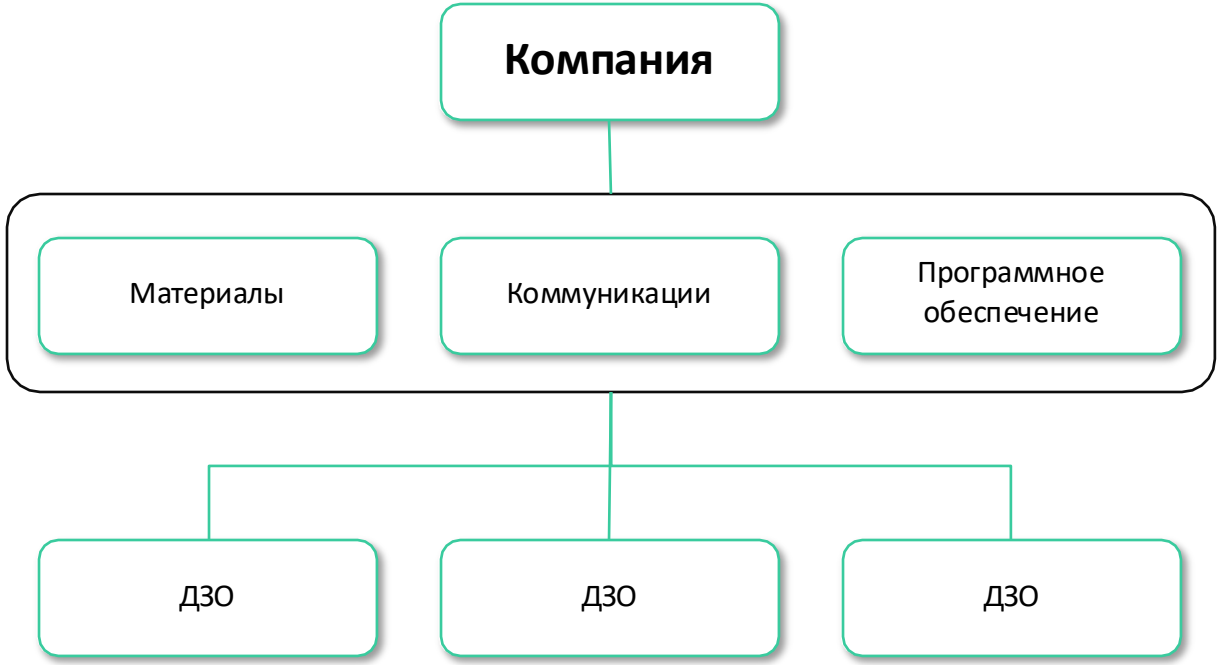


Киберкультура и группа компаний

SECURE-T

Общая политика

- Унифицированные обучающие материалы
- Общий канал коммуникаций
- Единое брендирование под группу компаний
- Единая система для всех ДЗО

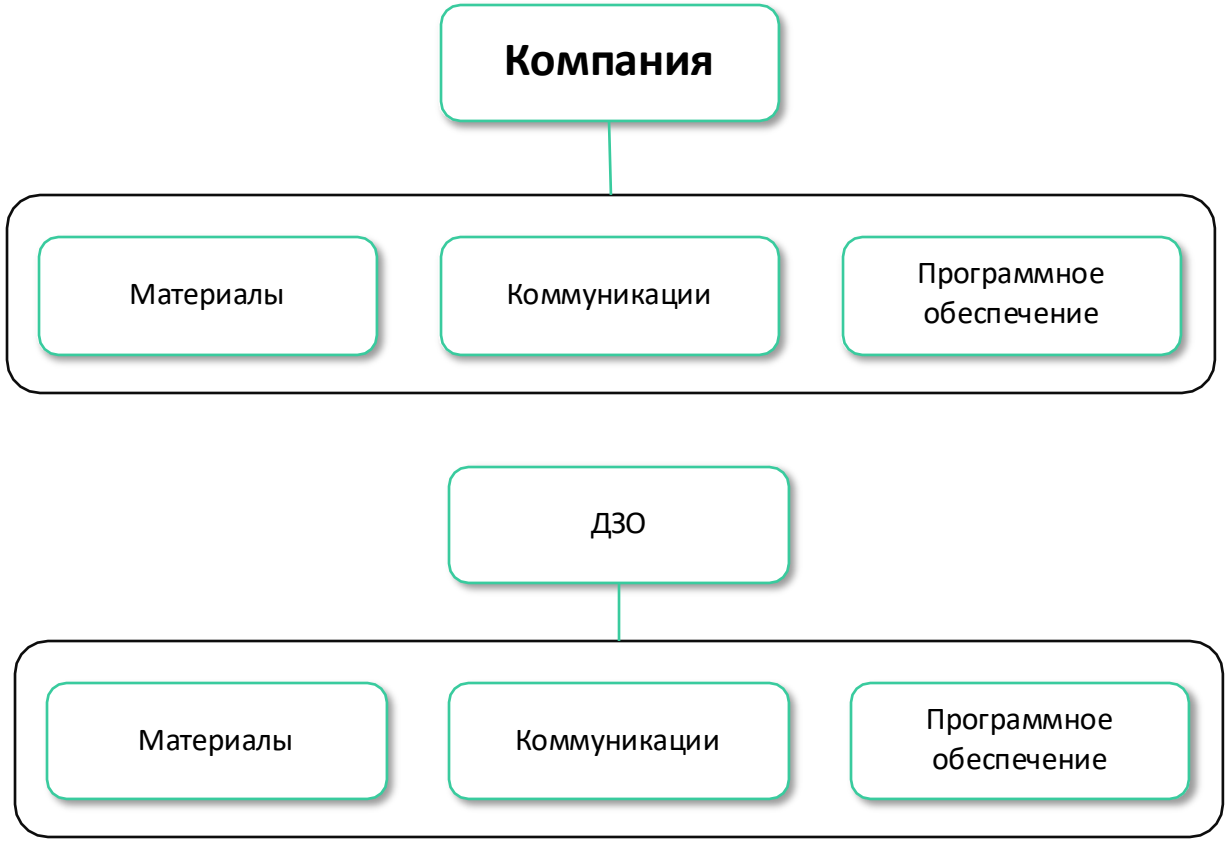


Киберкультура и группа компаний

SECURE-T

Индивидуальная политика

- Адаптированные обучающие материалы с учетом отраслевой специфики
- Узконаправленная коммуникация с пользователями и администраторами
- Индивидуальное брендирование
- Собственное ПО



Наши контакты

Телефон

+7 (495) 105-54-85

Почта

info@secure-t.ru

Secure-T Insights

SECURE-T