Культура кибербезопасности

От политики к практике: как превратить сотрудников из слабого звена в сильную защиту компании

ОБЗОР

Структура презентации

01

Современный ландшафт угроз

Реальная картина киберугроз 2024-2025: статистика, тренды, новые методы атак

02

Политика vs Культура

Ключевое отличие двух подходов и почему документов недостаточно

03

Барьеры на пути

Три главных препятствия при построении культуры безопасности

04

Сила обучения

Доказательная база эффективности: научные данные и реальные кейсы

05

Практические инструменты

Решения для каждого сценария: пароли, фишинг, социальная инженерия

06

Дорожная карта

Пошаговый план внедрения культуры безопасности в компании

ГЛАВА 01

Современный ландшафт угроз

Реальная картина киберугроз 2025: статистика, тренды, новые методы атак

Цифры, которые нельзя игнорировать

Согласно исследованию Threat Zone 2026 от BI.ZONE Threat Intelligence, в 2025 году фишинг стал основным способом первоначального проникновения в инфраструктуру компаний России и СНГ.

64%

Атак через фишинг

18%

Через удалённый доступ

9%

Компрометация подрядчиков

7%

Эксплуатация уязвимостей

Уроки на миллионы

Крупнейшие финансовые потери из-за человеческого фактора. Общий ущерб: **Более $160 млн** потеряно из-за ошибок сотрудников

1

2021 • Банк ОАЭ • $35 млн

Метод: Голосовой дипфейк генерального директора. Злоумышленники создали реалистичный голосовой клон руководителя. Сотрудник перевел $35 млн на счета мошенников.

Урок: Даже голос руководителя нужно верифицировать

2

2016 • Crelan Bank • €75,6 млн

Метод: BEC-атака (Business Email Compromise). Взломана почта генерального директора. Мошенники отправили поддельные платежные поручения.

Урок: Верифицируйте платежи через альтернативные каналы

3

2015/16 • FACC • $50 млн

Метод: Социальная инженерия. Атака на австрийского производителя авиакомпонентов. Финансовый директор перевел средства мошенникам.

Урок: Обучение сотрудников критически важно

НОВЫЕ УГРОЗЫ

Эволюция угроз: дипфейки и ИИ

Как искусственный интеллект меняет правила игры в кибербезопасности

Дипфейк-атаки

62%

компаний столкнулись с атаками с использованием дипфейков за последние 12 месяцев

↑ Рост на 19% за год

ИИ-фишинг

179

случаев использования дипфейков зафиксировано только в I квартале 2025 года

Больше, чем за весь 2024 год

Реальные кейсы 2025

- **Криптовалютная компания:** Злоумышленники организовали видеоконференцию в Zoom с дипфейками топ-менеджеров и убедили сотрудника установить вредоносное «расширение»
- **Атака на госучреждения США:** Преступники выдавали себя за высокопоставленных чиновников, используя AI-генерацию голосовых сообщений
- **Министр обороны Италии:** AI клонировал голос министра и других чиновников для обмана предпринимателей с целью хищения средств

ГЛАВА 02

Политика vs Культура

Почему документов недостаточно для настоящей защиты

Два подхода к безопасности

Политика

Нормативные требования

Создает четкие ожидания и формальную ответственность для всех уровней

Управление рисками

Определяет процедуры и регламенты реагирования на инциденты

Реагирование на инциденты

Устанавливает алгоритмы действий при нарушениях

Политика — это фундамент, но не гарантия безопасности

Культура

Лидерство

Руководство личным примером демонстрирует приоритет безопасности

Вовлеченность сотрудников

Люди понимают «зачем» и сами хотят защищать компанию

Открытость и коммуникация

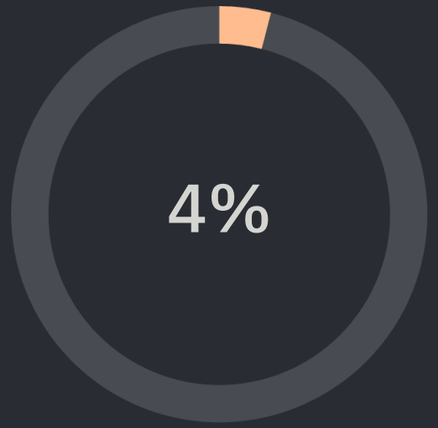
Сотрудники не боятся сообщать о проблемах, нет культуры страха

Непрерывное обучение

Постоянное развитие навыков и адаптация к новым угрозам

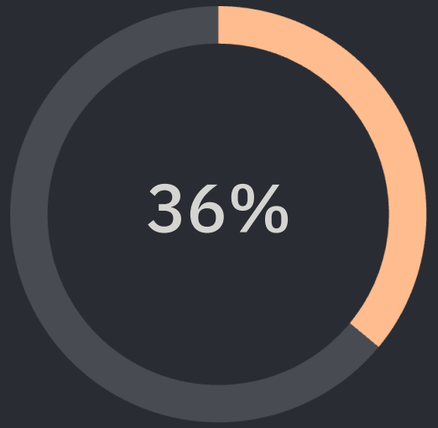
Культура формирует доверие и мотивирует соблюдать правила

Технологии бессильны без людей



Сотрудников

создают 80% инцидентов. Исследование Qualcomm показало, что небольшая группа «риск-сотрудников» генерирует большинство проблем безопасности



Сотрудников

выполняют опасные команды. Даже после обучения треть сотрудников доверяется мошенникам в тестовых атаках

Почему культура важнее

Технологии не достаточны

Антивирусы, файерволы и SOC не спасают, если сотрудник добровольно передает данные мошеннику

Человеческий фактор

Люди остаются самым слабым звеном, но при правильной культуре становятся сильнейшей защитой

Постоянная адаптация

Угрозы эволюционируют быстрее, чем обновляются технологии. Только обученные сотрудники могут адаптироваться

Раннее обнаружение

Вовлеченные сотрудники сообщают о подозрительной активности, предотвращая крупные инциденты

ГЛАВА 03

Барьеры на пути

Что мешает построить культуру безопасности в компании

Три главных барьера

Почему программы безопасности часто проваливаются

Руководитель не подает пример

Проблема: Руководитель говорит о важности безопасности, но сам нарушает правила. Просит отправить финансовый отчет через мессенджер вместо защищенного канала.

Последствие: Сотрудники видят противоречие и перестают соблюдать правила

Нет вовлеченности

Проблема: Меры безопасности воспринимаются как неудобство в работе. 2FA воспринимается как «лишние клики», сложные пароли — как «головная боль».

Последствие: Сотрудники ищут обходные пути, создавая уязвимости

Страх коммуникации

Проблема: Сотрудники боятся сообщать о нарушениях из-за страха наказания. Кликнул на фишинг — молчу, чтобы не получить выговор.

Последствие: Инциденты скрываются до тех пор, пока не станут катастрофой

ГЛАВА 04

Сила обучения

Доказательная база эффективности: научные данные и реальные кейсы

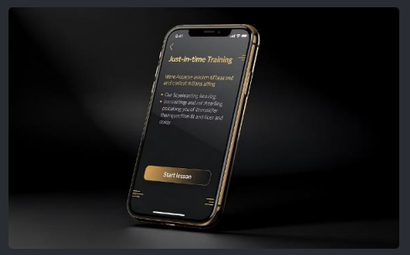
Что работает: проверенные методы

Эффективные подходы к обучению сотрудников

Персонализация

Адаптация сценариев под отделы и роли сотрудников. Бухгалтерия — письма о повышении зарплаты, IT — уведомления об обновлении VPN, HR — изменения корпоративной политики.

↑ Повышает узнаваемость угроз



Микрообучение

Обучение в момент ошибки (Just-in-time). Сразу после клика на фишинг — короткий урок. Объяснение признаков атаки и правильных действий.

↓ Снижает повторные ошибки на 40-60%

Поведенческие метрики

Измеряемые показатели эффективности: Phish-prone % — доля кликов по фишингу, Time-to-report — время до сообщения в SOC.

Регулярность

Постоянное обучение, а не разовые тренинги. Минимум один тренинг в месяц. Принцип интервального обучения (spaced learning).

ГЛАВА 05

Практические инструменты

Решения для каждого сценария: пароли, фишинг, социальная инженерия

Защита паролей

Менеджеры паролей, 2FA, принцип минимальных привилегий

Распознавание фишинга

Красные флаги, правило трех проверок, кнопка «Сообщить в ИБ»

Защита от манипуляций

Fake-Boss атаки, фишинговые сайты, дипфейк-атаки

Как распознать фишинг: красные флаги

1 **Срочность и давление**

«Срочно!», «Только сегодня!», «Аккаунт будет заблокирован!»

2 **Незнакомые отправители**

Подозрительные email-адреса, опечатки в домене

3 **Запросы конфиденциальных данных**

Никто не должен просить пароли или коды по email

4 **Подозрительные ссылки**

Наведите курсор — проверьте куда ведет ссылка

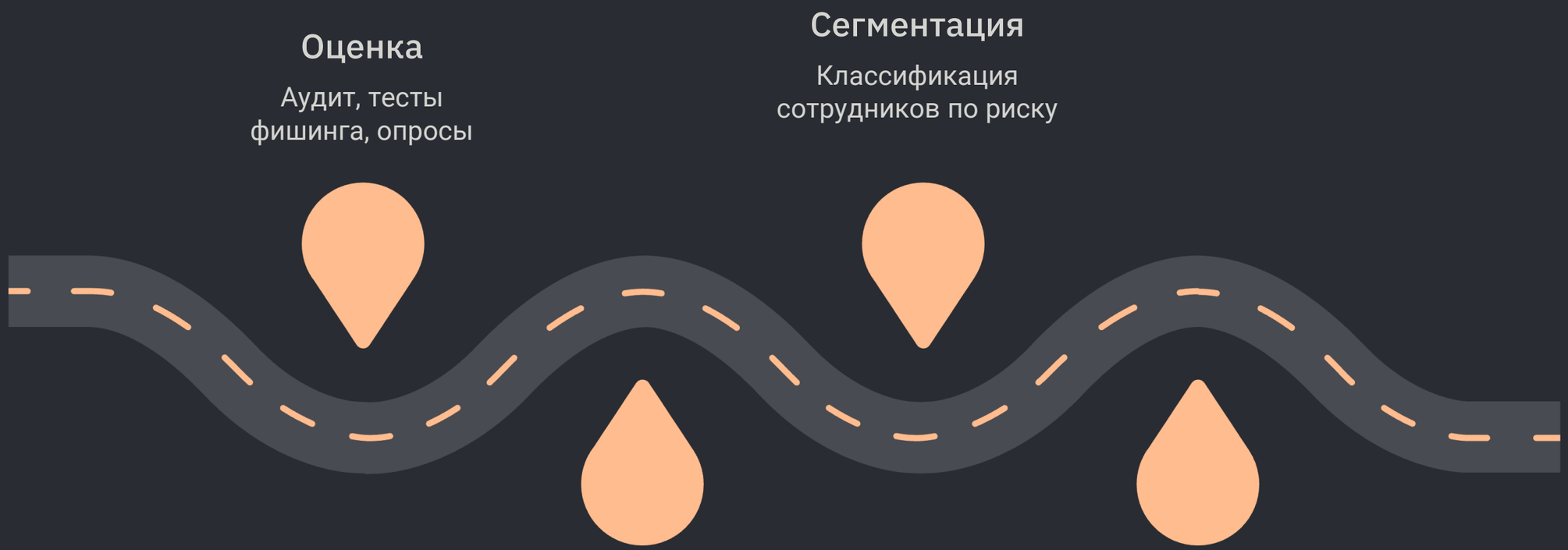
5 **Грамматические ошибки**

Нестандартные формулировки, опечатки

ГЛАВА 06

Дорожная карта

Как внедрить культуру безопасности в компании



Этап 1: Оценка текущего состояния

Аудит политик безопасности

- Проверка существующих регламентов
- Выявление пробелов в документации

Тестовые фишинг-атаки

- Базовая оценка уязвимости сотрудников
- Определение phish-prone percentage

Опрос сотрудников

- Понимание текущего уровня осведомленности
- Выявление проблемных зон

Анализ инцидентов

- Изучение прошлых нарушений безопасности
- Определение паттернов и рисков

Этап 2: Вовлечение руководства

Презентация для топ-менеджмента

- Демонстрация рисков и потенциальных потерь
- Обоснование ROI программы безопасности

Личный пример руководства

- Участие в тренингах наравне с сотрудниками
- Публичная поддержка инициатив безопасности

Выделение бюджета

- Финансирование программы обучения
- Инвестиции в технологии и инструменты

Назначение ответственных

- Формирование команды по безопасности
- Распределение ролей и обязанностей

Этап 3: Сегментация сотрудников

Группа высокого риска

- Финансовый отдел, бухгалтерия
- Руководители с доступом к критичным данным
- Усиленное обучение и мониторинг

Группа среднего риска

- HR, маркетинг, продажи
- Регулярный контакт с внешними лицами
- Стандартная программа обучения

Группа низкого риска

- Технические специалисты
- Сотрудники с ограниченным доступом
- Базовое обучение

Персонализация сценариев под каждую группу повышает эффективность обучения на 40%

Этап 4: Программа обучения

Непрерывный процесс

Реалистичные фишинг-симуляции

- Имитация реальных атак
- Адаптация под специфику отделов
- Минимум 1 раз в месяц

Микрообучение в момент ошибки

- Мгновенная обратная связь
- Короткие уроки (2-3 минуты)
- Объяснение признаков угрозы

Регулярные тренинги

- Новые угрозы и методы защиты
- Практические кейсы
- Интерактивные форматы

Геймификация

- Рейтинги и достижения
- Соревнования между отделами
- Мотивация через игровые механики

ЭТАП 5

Технологии

Внедрение технологий

Усиление защиты

Двухфакторная аутентификация (2FA)

- Обязательна для всех критичных систем
- Защита от компрометации паролей

Менеджеры паролей

- Корпоративное решение для всех сотрудников
- Генерация и хранение сложных паролей

Мониторинг и аналитика

- Отслеживание подозрительной активности
- Анализ поведенческих паттернов
- Раннее обнаружение угроз

Кнопка «Сообщить в ИБ»

- Интеграция в почтовый клиент
- Быстрое реагирование на угрозы
- Вовлечение сотрудников в защиту

ЗАКЛЮЧЕНИЕ

Культура безопасности — инвестиция в будущее

Только комплексный подход, включающий обучение, технологии и правильную корпоративную культуру, может обеспечить надежную защиту от современных киберугроз

Обучение

Регулярное и персонализированное

Технологии

2FA, менеджеры паролей, мониторинг

Культура

Лидерство, вовлеченность, открытость

Сотрудники — не слабое звено, а сильная защита компании

Остались вопросы?

Бондарев Владимир Михайлович