КУЛЬТУРА КИБЕРБЕЗОПАСНОСТИ

Как сотрудники помогают защищать компанию

Регламенты работают, когда сотрудники следуют им каждый день



Как меняются атаки

Verizon DBIR 2026 · глобальные данные за 2025 год

31%

Через уязвимости

48%

Связаны с вымогательством

45%

Используют рабочий ИИ без согласования

Ошибка сотрудника может стоить миллионы

Три случая, когда доверие без проверки обернулось потерями

01

ARUP · 2024 · ≈$25 млн

Мошенники провели видеоконференцию с дипфейками руководителей. Сотрудник сделал 15 переводов на сумму около $25 млн.

Крупный платёж стоит подтвердить по другому каналу

02

ORION · 2024 · ≈$60 млн

Сотруднику направили поддельные поручения от руководства. Он перевёл деньги на счета третьих лиц; потери составили около $60 млн.

Платёж стоит подтвердить напрямую у отправителя запроса

03

MGM RESORTS · 2023 · >$100 млн

В атаке на MGM злоумышленники получили доступ через социальную инженерию. Компания отключила часть систем: бронирование, платежи и доступ в номера; восстановление заняло около 10 дней.

IT-служба должна проверять личность звонящего



Регламенты работают, когда им следуют каждый день

РЕГЛАМЕНТЫ

Фиксируют обязательные действия
Помогают понять, что важно
Подсказывают, что делать при инциденте

ПОВЕДЕНИЕ

Руководители соблюдают регламенты
Сотрудники понимают, зачем они нужны
О подозрительном сообщают сразу

Регламент полезен только тогда, когда им пользуются.

Технологии не заменяют внимательность сотрудников

41%

Руководителей по ИБ сообщили об инциденте с дипфейком в аудиозвонке

36%

Руководителей по ИБ сообщили об инциденте с дипфейком в видеозвонке

Знакомые признаки обмана работают хуже — поэтому сомнительный звонок нужно проверять по другому каналу.

Культура нужна, чтобы сотрудник заметил обман, остановился и быстро сообщил о проблеме.

Что обычно мешает

Руководитель обходит регламенты

Когда руководители обходят регламенты, сотрудники понимают: правила можно не соблюдать.

Регламенты неудобны

Если 2FA и пароли слишком мешают работе, люди начинают искать небезопасный обход.

Страх сообщить

Когда сотрудник боится наказания, о проблеме узнают слишком поздно.



Обучение должно быть связано с реальной работой

01

ПРИМЕРЫ ИЗ РАБОТЫ

Бухгалтерия — платежи и реквизиты; закупки — поставщики; HR — персональные данные; IT — доступы и MFA.

02

СРАЗУ ПОСЛЕ ОШИБКИ

После инцидента разберите цепочку действий: что заметили, где нужно было остановиться и кому сообщить.

03

ПОВТОРЯТЬ РЕГУЛЯРНО

Проводите короткие тренировки по ролям несколько раз в год, а не один обязательный курс.



Оценивайте не только клики: важны сообщения о подозрительных письмах, звонках и запросах, а также время реакции.

Сначала оценить риск, затем закрепить регламенты в работе

01

Понять риск

Проверить регламенты и привычки

02

Личный пример

Руководители проходят обучение первыми

03

Выбрать нужные темы

Учесть задачи и уровень доступа

04

Повторять регулярно

Короткие упражнения и понятные показатели



С ЧЕГО НАЧАТЬ

Два шага для старта

01 Показать цену ошибки

Показать, как инцидент влияет на деньги и работу компании.

02 Руководители проходят обучение первыми

Руководители учатся вместе с сотрудниками.

Обучение зависит от задач и доступа

ВЫСОКИЙ РИСК	Финансы, казначейство, IT-администраторы и руководители, утверждающие платежи
СРЕДНИЙ РИСК	Закупки, продажи, HR и сотрудники, которые часто общаются с внешними контрагентами
БАЗОВЫЙ РИСК	Большинство офисных ролей с ограниченным доступом к системам и данным

Уровень обучения определяют задачи, доступ и типичные рабочие сценарии, а не должность сама по себе.

Безопасность — часть нормальной работы

Сотрудники знают, что делать по регламенту, используют защитные инструменты и проверяют просьбы срочно перевести деньги, сообщить код, открыть доступ или отправить файл.

ОБУЧЕНИЕ

Короткое обучение по ролям

ТЕХНОЛОГИИ

2FA, менеджеры паролей, мониторинг

КУЛЬТУРА

Личный пример и готовность сообщить

Главный навык — остановиться и проверить просьбу независимым способом.



ОСТАЛИСЬ ВОПРОСЫ?

Владимир Бондарев

Telegram: @vbondarev
Мобильный: +7 (925) 868 2646

vbondarev.ru

vbondarev.ru