# Год киберкультуры

Как мы строим позитивные
отношения ИБ с сотрудниками

Анастасия Иванова

И.О. руководителя отдела Киберкультуры

Культура — это то,
что ты делаешь, если
на тебя никто не смотрит

# Развитая киберкультура

## Цифровой иммунитет компании растет

### Сотрудники работают безопасно и не создают инцидентов ИБ

Все сотрудники мотивированы проходить обучение вовремя и главное — проходят его

Сотрудники тренируются на имитированных атаках «из дикой среды»

Результаты и эффективность обучения понятны, измерены, оценены

Учебные материалы актуальны и регу-лярно обновляются

DevOps поддерживают инфраструктуру в безопасном состоянии

Число выявленных уязвимостей после VM непрерывно уменьшается

Разработчики пишут безопасный код — все задачи реали-зуются безопасно by design

Бэклог на доработку после AppSec непрерывно уменьшается

### Сотрудники проактивны и вовлечены в вопросы ИБ

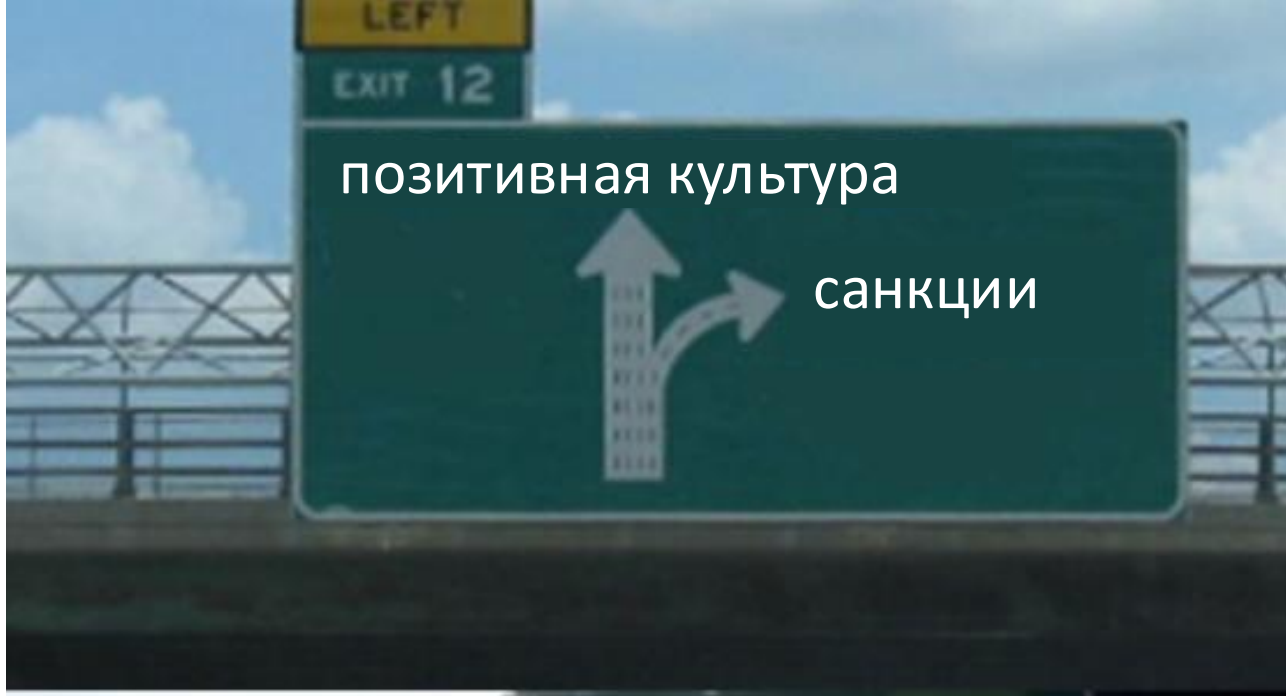
Сотрудники принимают безопасные решения даже в новых ситуациях, которые возникают каждый день

Сотрудники ретранслируют знания и навыки коллегам

Сотрудники не боятся «перестраховаться» и обратиться в ИБ, если сталкиваются с чем-то подозрительным

ИБ имеет высокий авто-ритет среди сотрудни-ков и руководства, знает как повышать лояльность и выстраивать отношения с руководителями других БЮ

Какую культуру безопсности выбрать?




# С какими вопросами работаем сейчас

## объективные

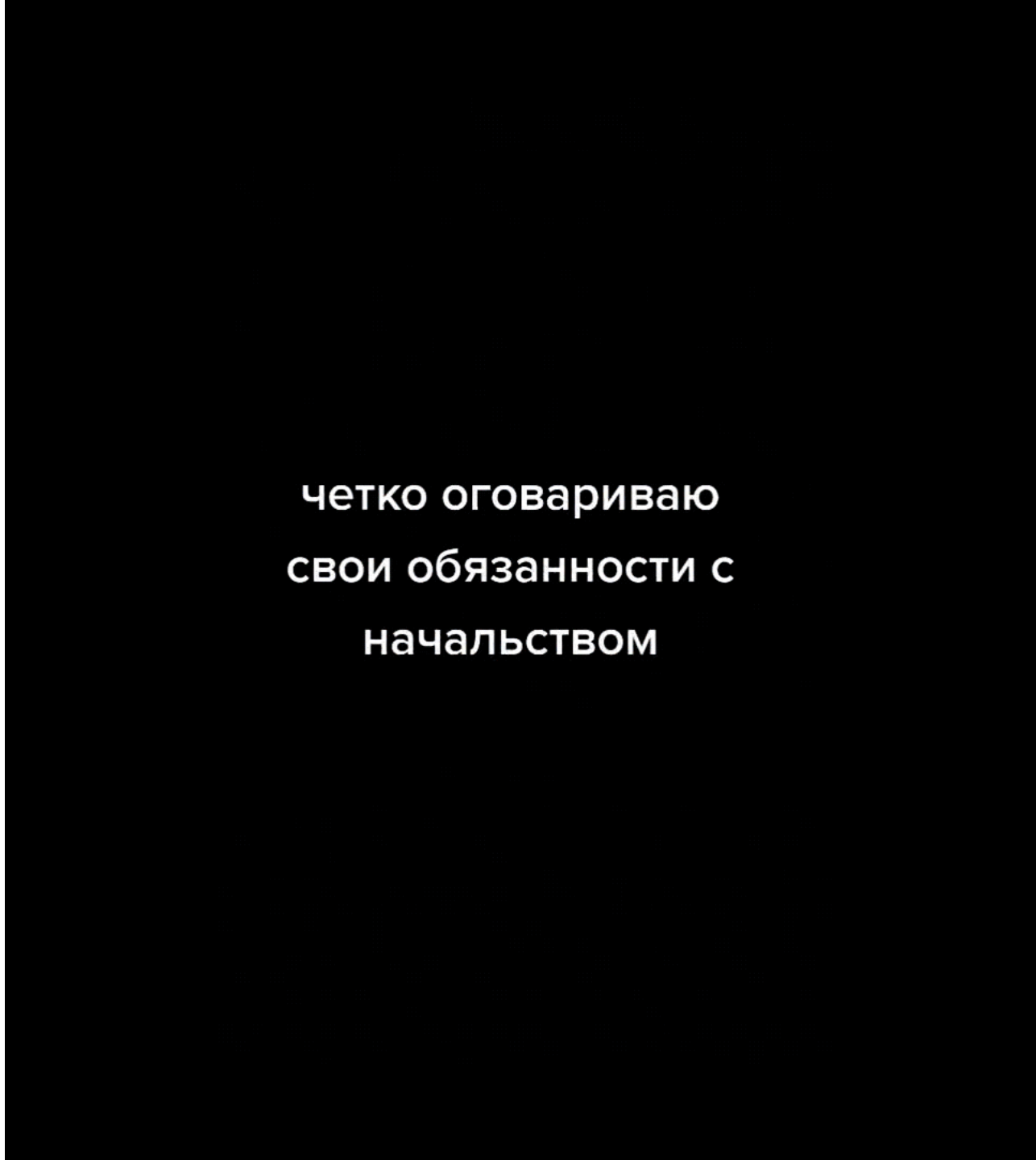
- переходный период
- объём разнообразного обучения
- большая и очень неоднородная аудитория
- набор инструментов

## коммуникационные

- как встроиться в огромный информационный поток
- как сменить вектор отношений с ИБ на «важный»
- как работать с фундаментальными убеждениями

# Наши подходы и инструменты

- Грамотная, проработанная методология обучения
- Высокая степень погружения в техническую специфику
- Подходы behavioral science
- Инструменты PR — это про внутреннюю репутацию и внутренние коммуникации
- Инструменты маркетинга — это про call to action
- Безграничное терпение



# Фундамент культуры безопасности

Обучение

Коммуникации

Вовлечение

**Очень много мотивации**

# Что из этого работает

# Обучение

## Из чего состоит?

1. Выявление проблем
2. Обязательный онбординг и базовое обучение
3. Профилирование
4. Безопасная разработка
5. Фишинговые тренировки

## Что мы сделали

1. Провели фундаментальное исследование всей компании.
2. Обновили и запустили новые материалы:
   - Памятка новичку
   - Базовый курс
   - Живые онбординг-встречи
   - Памятка по настройке личных устройств
   - Памятка по данным
3. Запустили подготовку микромодулей для разных профилей специалистов
4. Реализовали два подхода: интерактивная платформа и интерактивные вебинары. Лучше — систематическая работа с платформой

# Курс и памятка

1 Ответить

[redacted] 23.09.2024, 14:16

Годно!

1 Ответить

[redacted] 19.09.2024, 16:10

Курс правда супер, тем кто делал - предайте спасибо большущее!

2 Ответить

[redacted] 16.09.2024, 13:52

Курс хороший, необходимость проходить его несколько раз - угнетающая.

1 Ответить

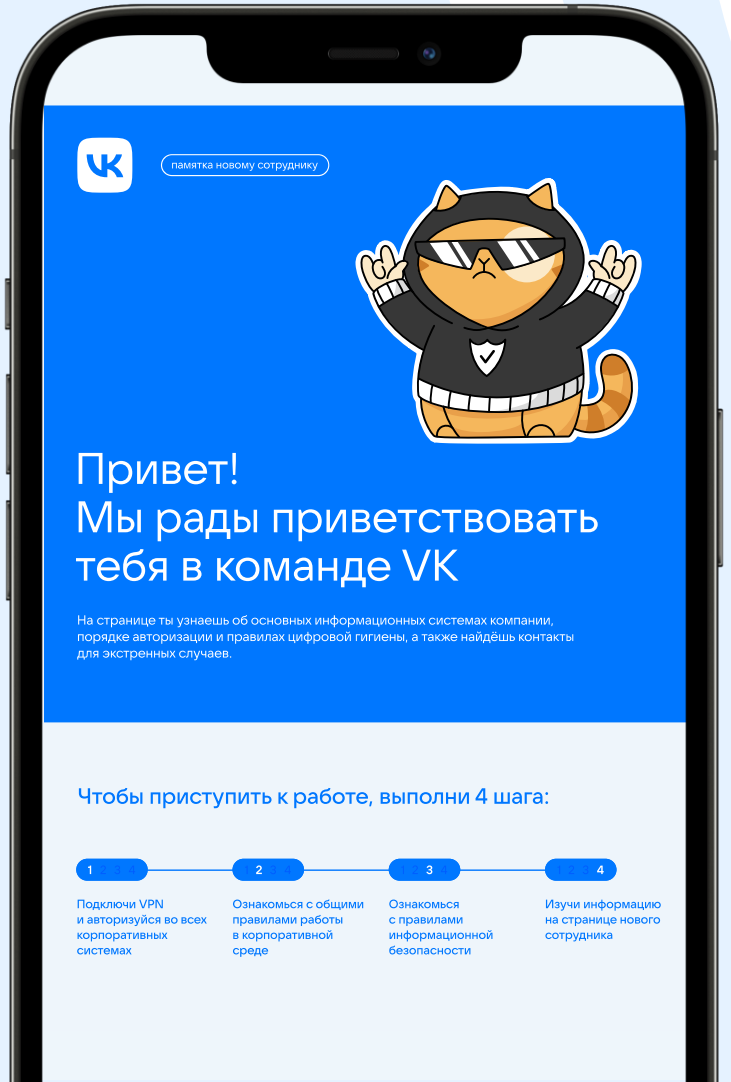
[redacted] 13.09.2024, 16:36

отличный курс

1 Ответить

[redacted] 13.09.2024, 15:17

Супер, рекомендую. Чтобы освежить знания и познакомится с внутренними правилами ВК связанными с обменом информации!



# Коммуникации

## Из чего состоит?

1. Выстраивание постоянной коммуникации с сотрудниками
2. Информирование о работе ИБ (самое важное про инциденты, внедрение новых технологий)
3. Формирование позитивного имиджа: ИБ не надзиратель, а, в первую очередь, партнер и защитник
4. Повышение уровня осведомлён-ности и киберграмотности
5. Креативный подход к базовым темам

## Что мы сделали

1. Создали хелпдеск по ИБ
2. Выработали систему постинга и дайджесты важнейших событий.
3. Об изменениях сообщаем заранее, постепенно, обсуждаем со стейк-холдерами, открыто, публично.
4. Самое популярное — делаем регулярные разборы атак как учебных, так и реальных, с которыми сталкиваются сотрудники
5. Сделали много митапов для разных групп

# Вовлечение

Из чего состоит?

1. Практическая отработка знаний
2. Внедрение геймификации
3. Формирование сообщества
4. Повышаем значение обратной связи
5. Работа с эмоциями

## Что мы сделали

1. Переформатировали  CTF
2. Создали игру «У нас инцидееент»
3. Сделали коллаборацию с художниками
4. Обновили систему вознаграждений и мерча
5. Провели исследование CSI

ежегодный CTF

## Главное

1. Ввели лиги
2. Сделали много более простых задач
3. Добавили интересные категории
4. Собираем обратную связь персонально
5. Добавили ценные призы

детектив

игра

Главное

1. В основе — реальные инциденты
2. Добавили пасхалки для отрасли
3. Играли с сотрудниками и разбирали
4. Можно получить за активность

# Cybersecurity Awareness Week 2024

совместно с простор

# Выводы о взаимодействии с ИБ в целом

**90%**

Общая удовлетворенность опытом обращения в ИБ по остальным каналам

## Какие это каналы

- Личная переписка со специалистом. Часть опрошенных радуется проактивности специалистов ИБ;
- Чат «Спроси у безопасности»;
- Электронная почта.

# Подписывайтесь на наши сообщества

ВКонтакте

Мой канал

Telegram