Что-то на кибер-культурном

Как строить 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

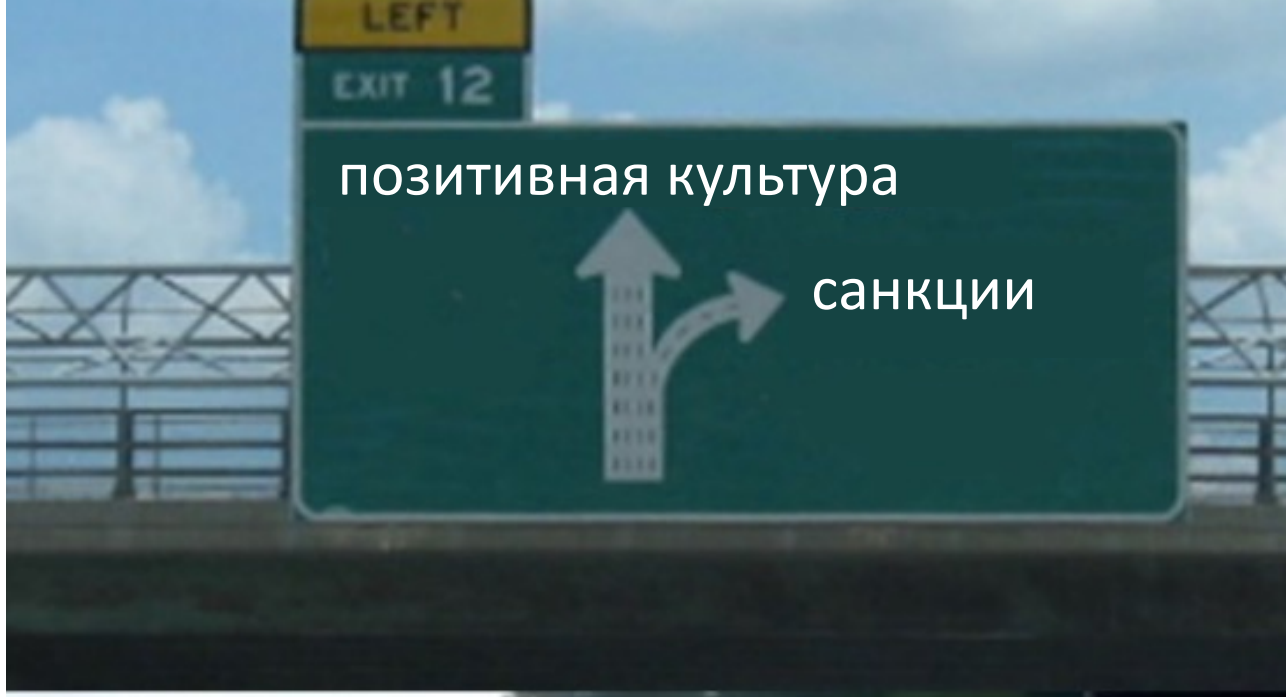
Сотрудники принимают безопасные решения даже в новых ситуациях, которые возникают каждый день

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 проблемами мы столкнулись на старте

объективные

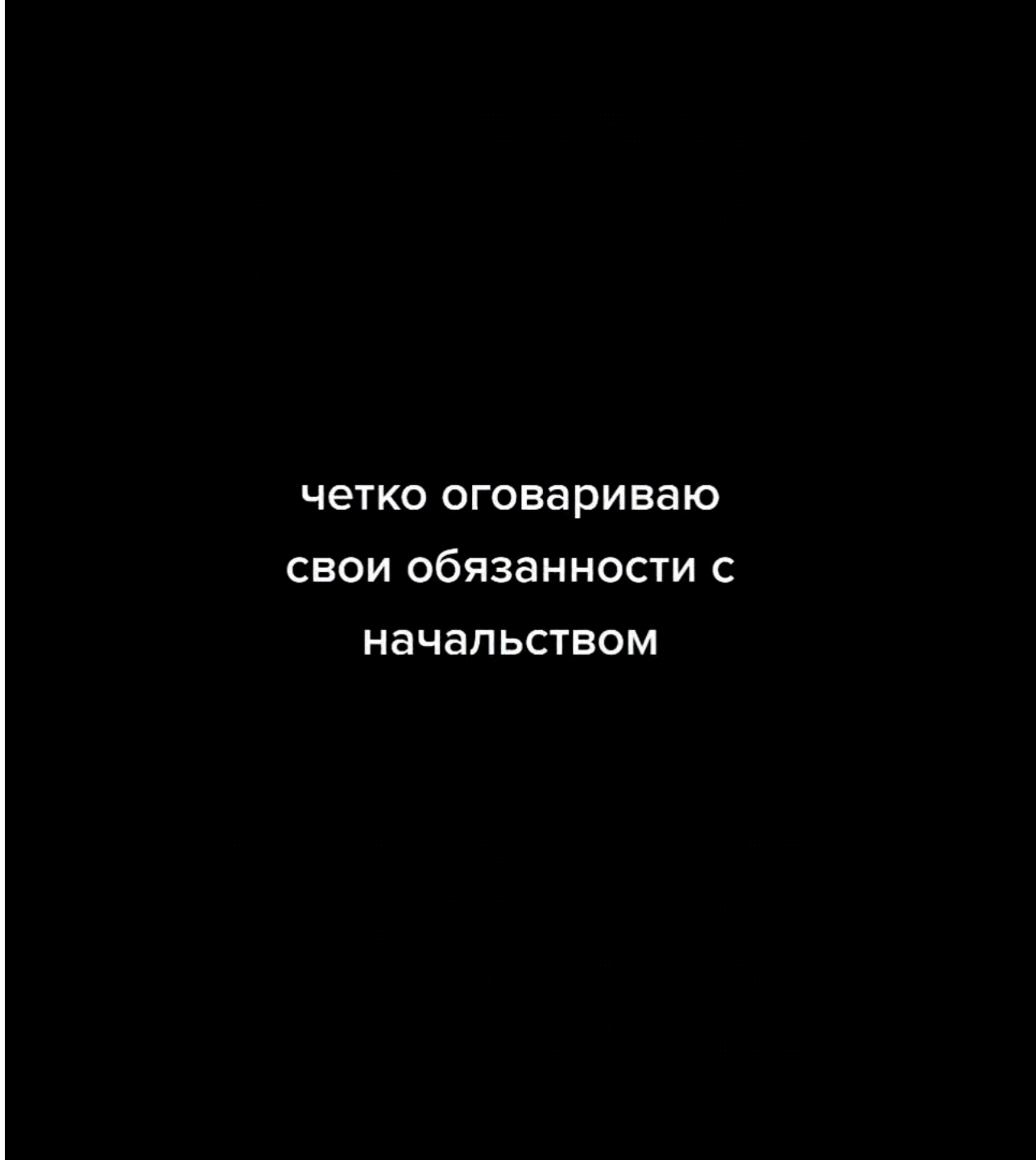
- не было отлаженного процесса взаимодействия ИБ и сотрудников
- переходный период
- неактуальное обучение
- не было объективной картины проблем
- большая и очень неоднородная аудитория

коммуникационные

- ИБ воспринимался как ограничитель
- недостаточная информированность сотрудников про ИБ в целом
- сотрудники боялись сообщать об ошибках

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

Мотивация

Фундамент культуры безопасности

Обучение	Коммуникации	Вовлечение

Очень много мотивации

Обучение

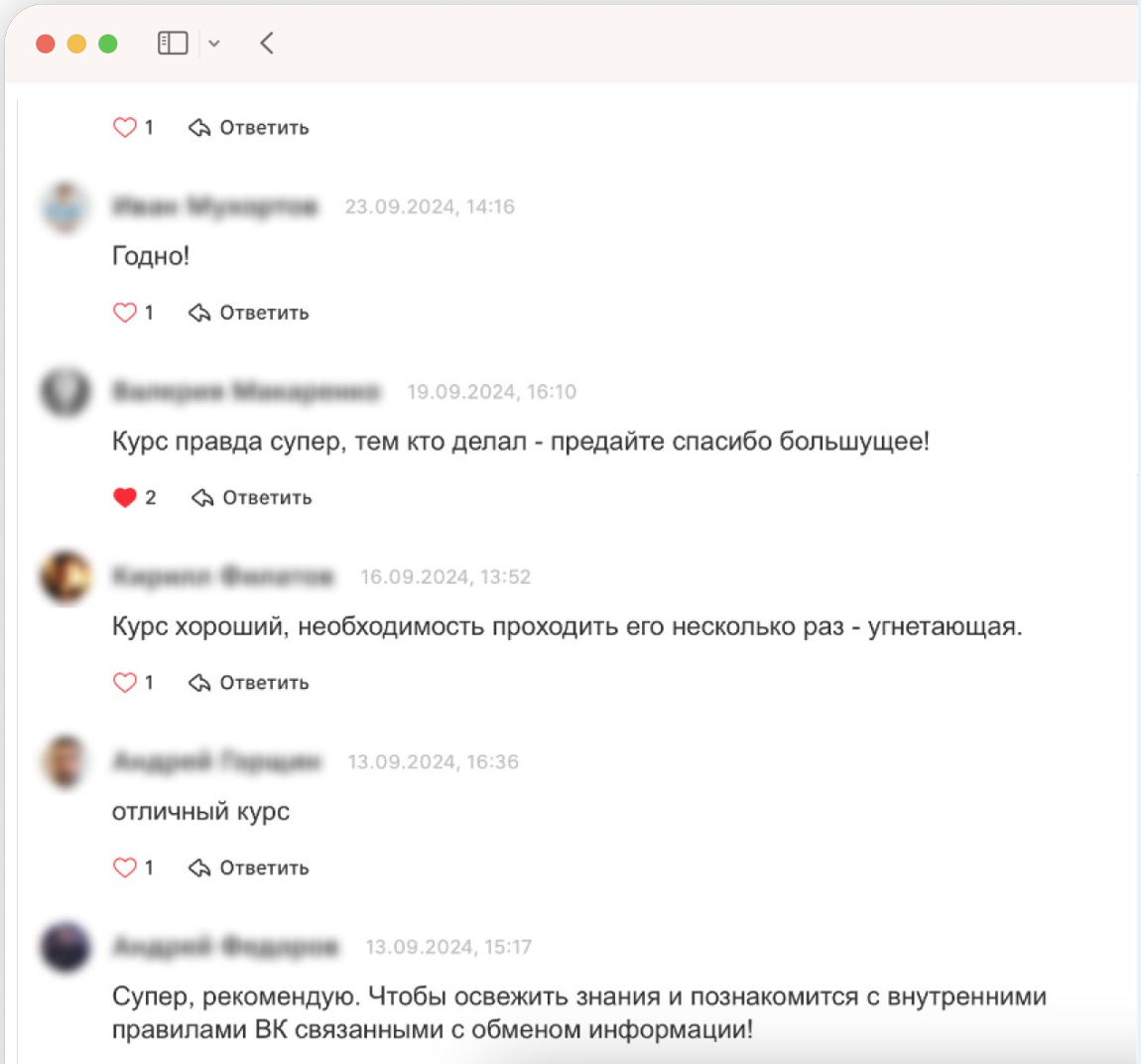
Из чего состоит?

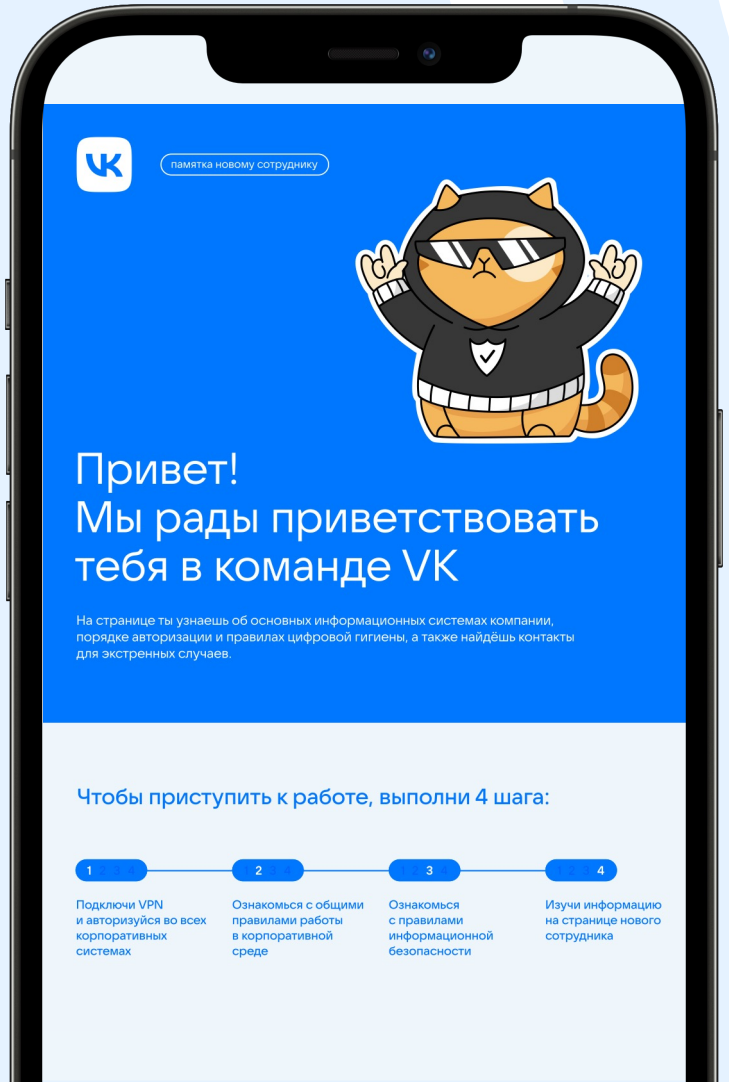
1. Выявление проблем
2. Обязательный онбординг и базовое обучение
3. Профилирование
4. Безопасная разработка
5. Фишинговые тренировки

Что мы делаем

1. В основе — фундаментальное исследование всей компании.
2. Регулярно обновляем все материалы:
   - Памятка новичку
   - Базовый курс
   - Живые онбординг-встречи
   - Постоянный контакт с HR
3. Микромодули для разных профилей специалистов
4. Два подхода: интерактивная платформа и интерактивные вебинары.
5. Поставили в приоритет не «классические» метрики

Курс и памятка





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 делаем

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. Делаем регулярные разборы атак как учебных, так и реальных, с которыми сталкиваются сотрудники
5. Эксперименты с форматами подачи информации

Вовлечение

Из чего состоит?

1. Практическая отработка знаний
2. Внедряем геймификацию, где это нужно
3. Формируем сообщество
4. Открываем возможность сотрудникам ретранслировать свои знания
5. Повышаем значение обратной связи

Что мы делаем

1. Проводим не только фишинговые тренировки, но и регулярные CTF
2. Проводим квесты и игры в дополнение к обучению
3. Чаты по CTF, вознаграждения и мерч за помощь ИБ
4. Митапы со смежными командами
5. Проводим исследования CSI и корректируем планы в зависимости от обратной связи

Выводы о взаимодействии с ИБ в целом

90%

Общая удовлетворенность опытом обращения в ИБ по остальным каналам

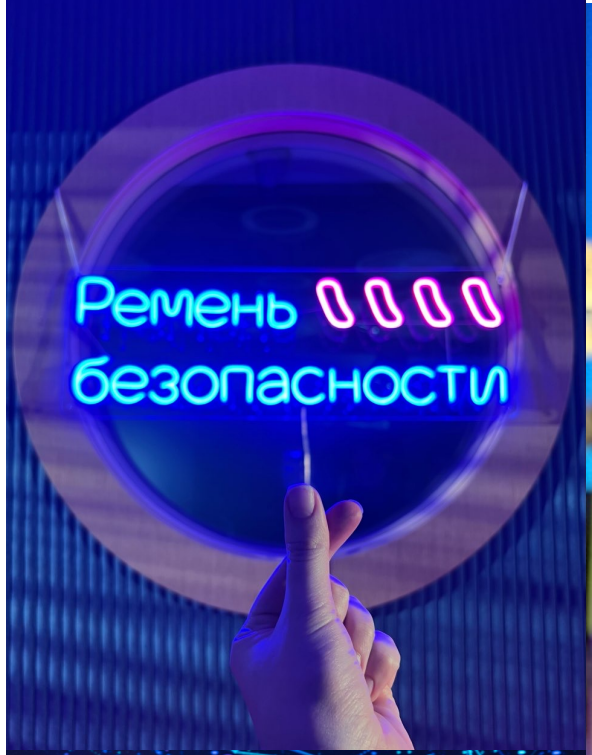
Какие это каналы

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

ежегодный CTF

Участники знают, за что борются!

Ежегодная Security Awareness week



Как мотивируем

- Система внутренних вознаграждений
- Внутренняя программа Bug Bounty
- Система построения комьюнити. Быть безопасным — круто!
- Призы и мерч

ИБ значки 5/10

BB-самурай

Вручается за нахождение **уязвимости.**
Ведь BB — это не цель, а путь.
Вес уязвимостей будут оценивать эксперты

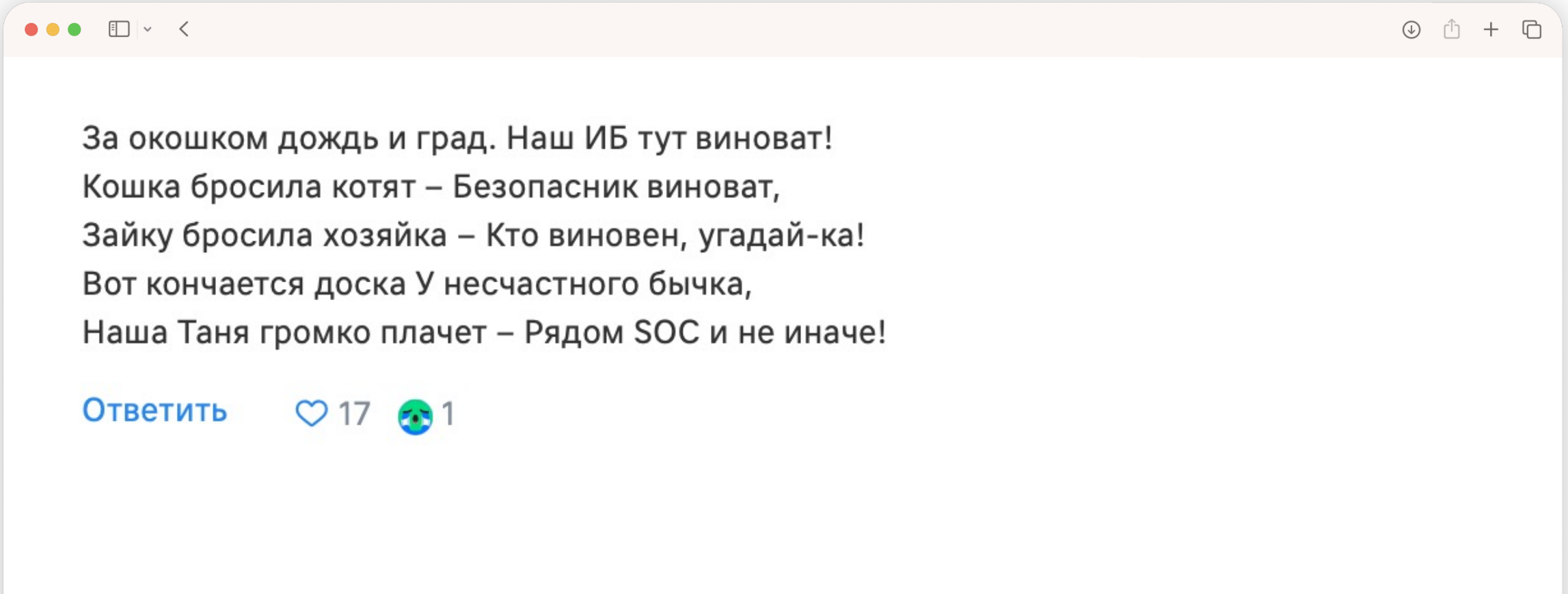
ИБ значки 1/10

Амбассадор ИБ

Вручается за **продвижение принципов информационной безопасности** в своих БЮ и подразделениях, а также за продвижение принципов киберкультуры

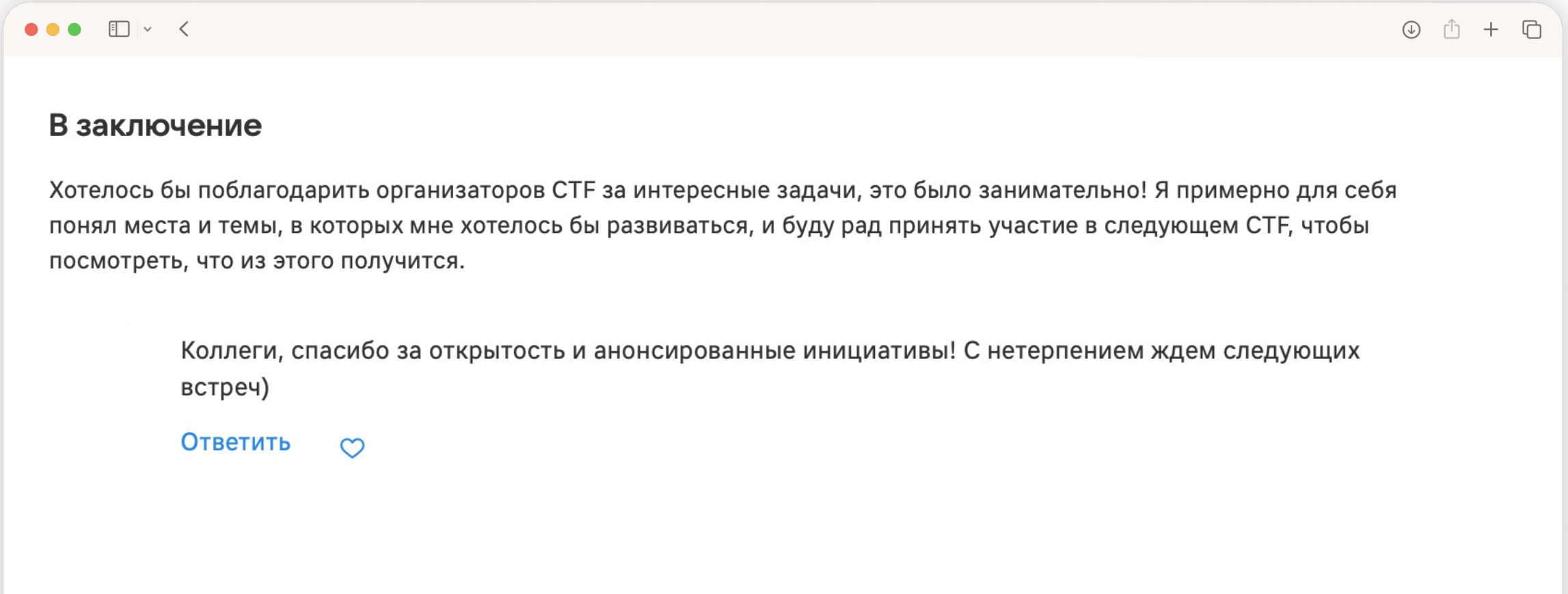
Главное изменение

было так



Главное изменение

стало так



В заключение

Хотелось бы поблагодарить организаторов CTF за интересные задачи, это было занимательно! Я примерно для себя понял места и темы, в которых мне хотелось бы развиваться, и буду рад принять участие в следующем CTF, чтобы посмотреть, что из этого получится.

Коллеги, спасибо за открытость и анонсированные инициативы! С нетерпением ждем следующих встреч)

Ответить

Подписывайтесь на наши сообщества

ВКонтакте

Мой канал

Telegram