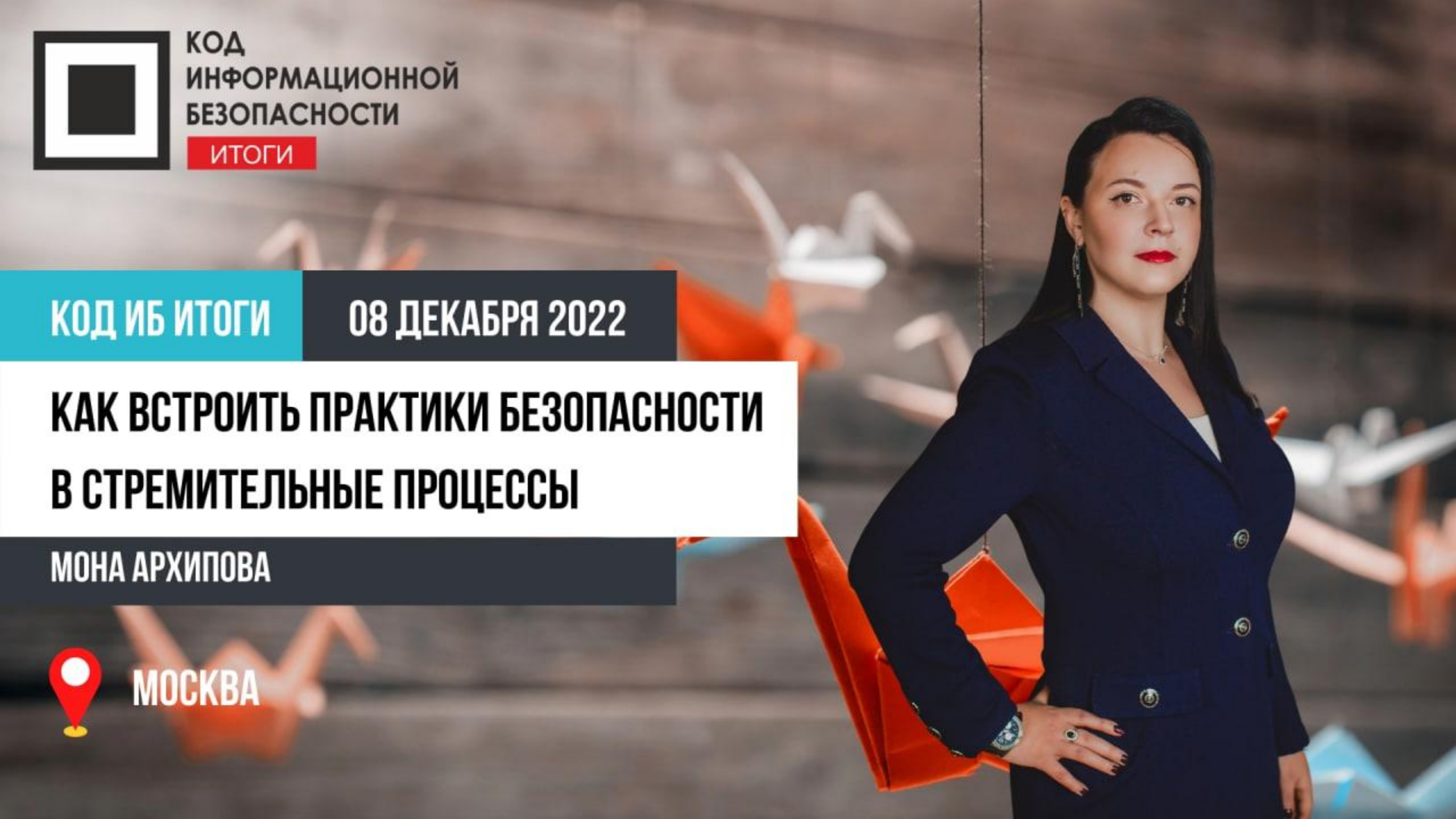
КОД
ИНФОРМАЦИОННОЙ
БЕЗОПАСНОСТИ
ИТОГИ

КОД ИБ ИТОГИ | 08 ДЕКАБРЯ 2022

КАК ВСТРОИТЬ ПРАКТИКИ БЕЗОПАСНОСТИ В СТРЕМИТЕЛЬНЫЕ ПРОЦЕССЫ

МОНА АРХИПОВА

МОСКВА



Обо мне

- Независимый эксперт по ИТ и безопасности
- Совладелица нескольких бизнесов
- Стала vCISO, когда это еще не было мейнстримом

Ключевые компетенции:

- IT-мониторинг и эксплуатация;
- кризисное управление;
- менеджмент инцидентов ИБ — SOC, CERT;
- системы обнаружения аномалий от дизайна до администрирования и аналитики;
- форензика

Бэкграунд

- Системное администрирование - *nix, сети
- Более 16 лет в ИТ, из них более 10 - в ИБ. От junior до C-level.
- Окончила Российский Государственный Социальный Университет в 2010 году по специальности “Комплексная защита объектов информатизации“.

Что происходит?

Бизнес-истории

Business

- Больше продуктов
- Больше внутренних и внешних заказчиков
- TTM vs Continuity vs Security
- Кто быстрее тот и выиграл

Tech

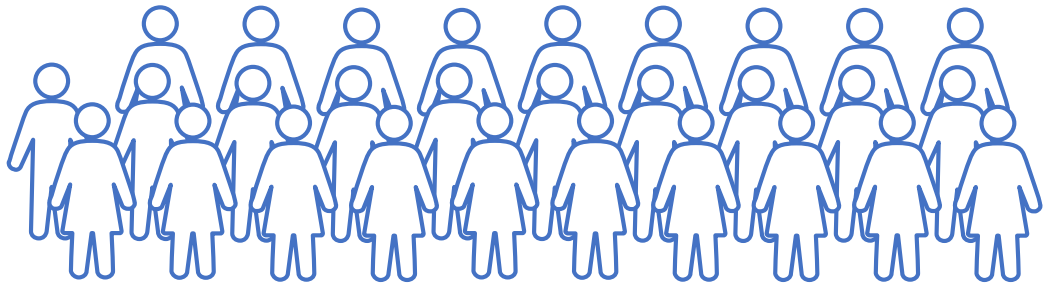
- Fast to start ~~fast to fail~~
- Agile, agile и в продакшн
- Архитектурные особенности
- Распределенные команды

Security

- Техдолг по багам
- False-positive
- Ручное управление
- Кадровый дефицит

Кадровая гонка

Developers

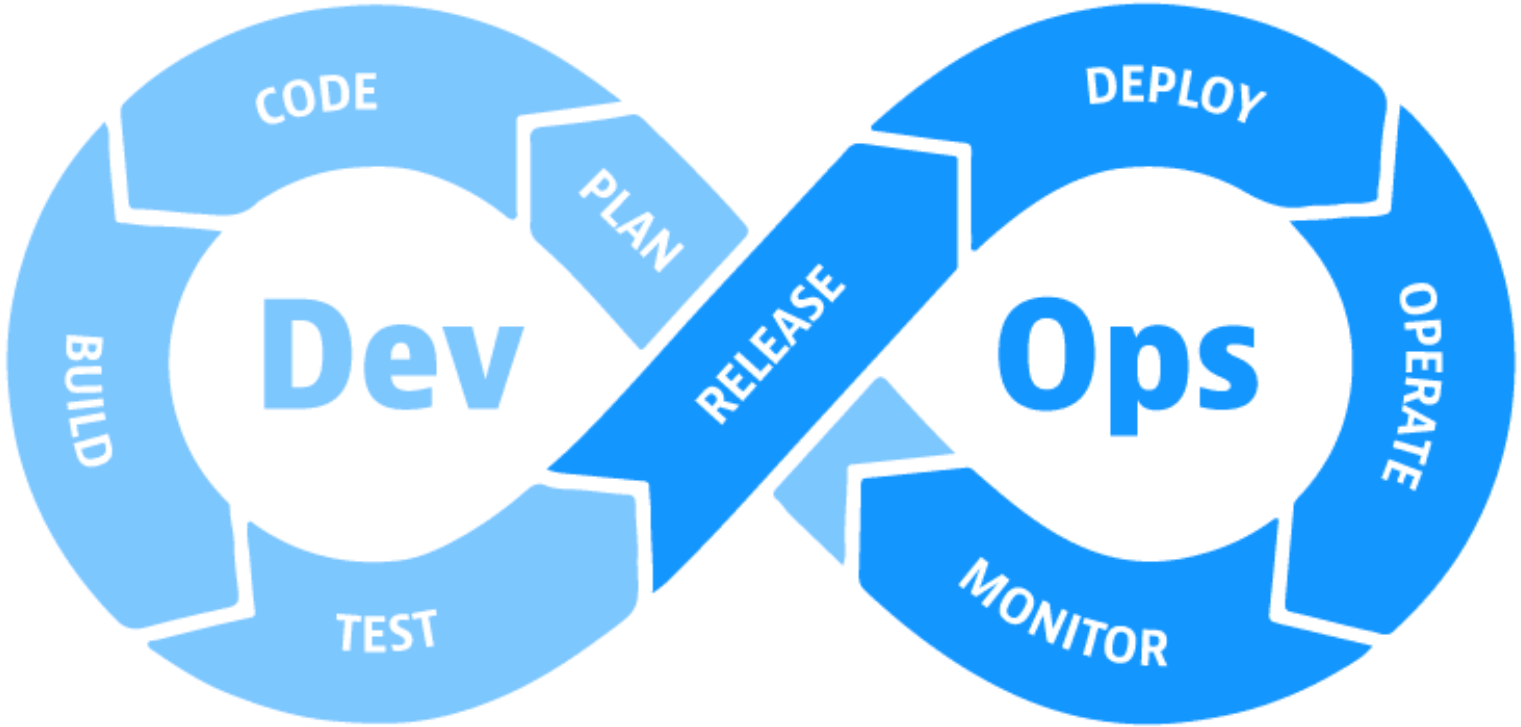


Operations

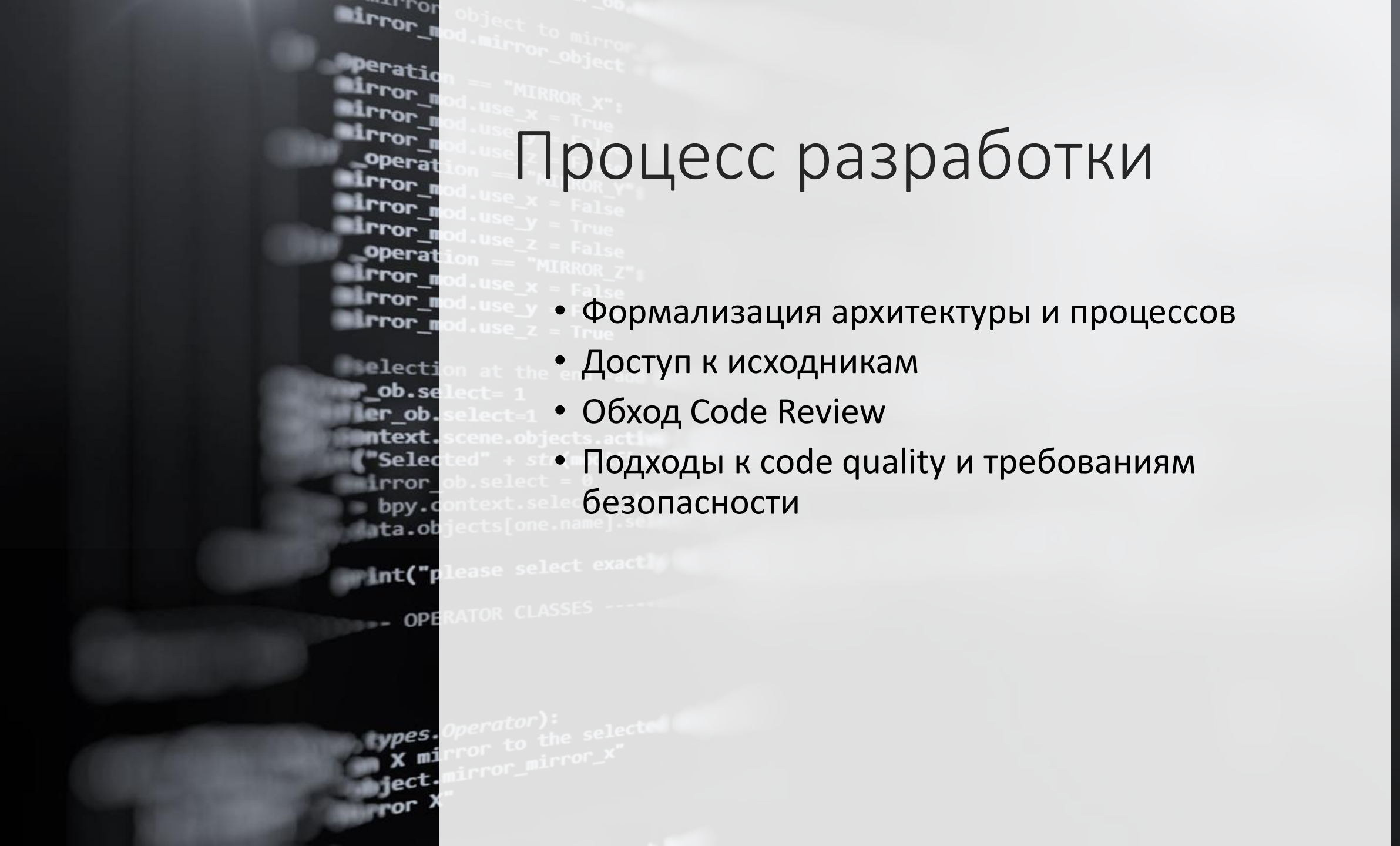
Security

Внутри разработки

DevOps процессы



А где Security?

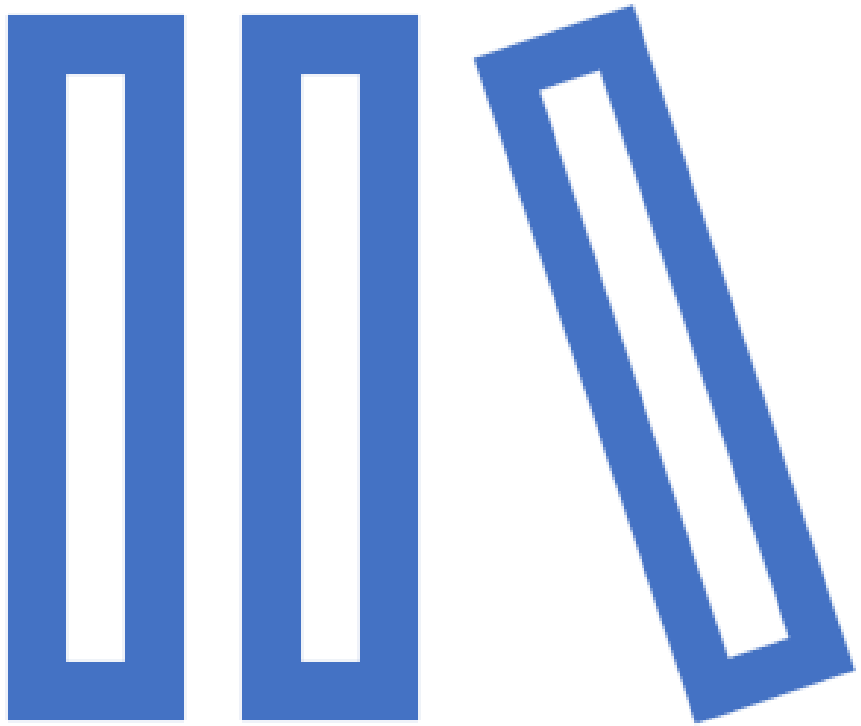


Процесс разработки

- Формализация архитектуры и процессов
- Доступ к исходникам
- Обход Code Review
- Подходы к code quality и требованиям безопасности

Continuous Integration (CI)

- Модификация кода на сборке
- Уязвимые библиотеки/пакеты
- Инфраструктура: система сборки, репозитории, внешние библиотеки
- Обход автоматизированных проверок



Continuous Deployment (CD)

- Безопасность контейнеров
- Система доставки и контроля
- Лишние интерфейсы
- Инфраструктурное окружение

Встраиваем безопасность

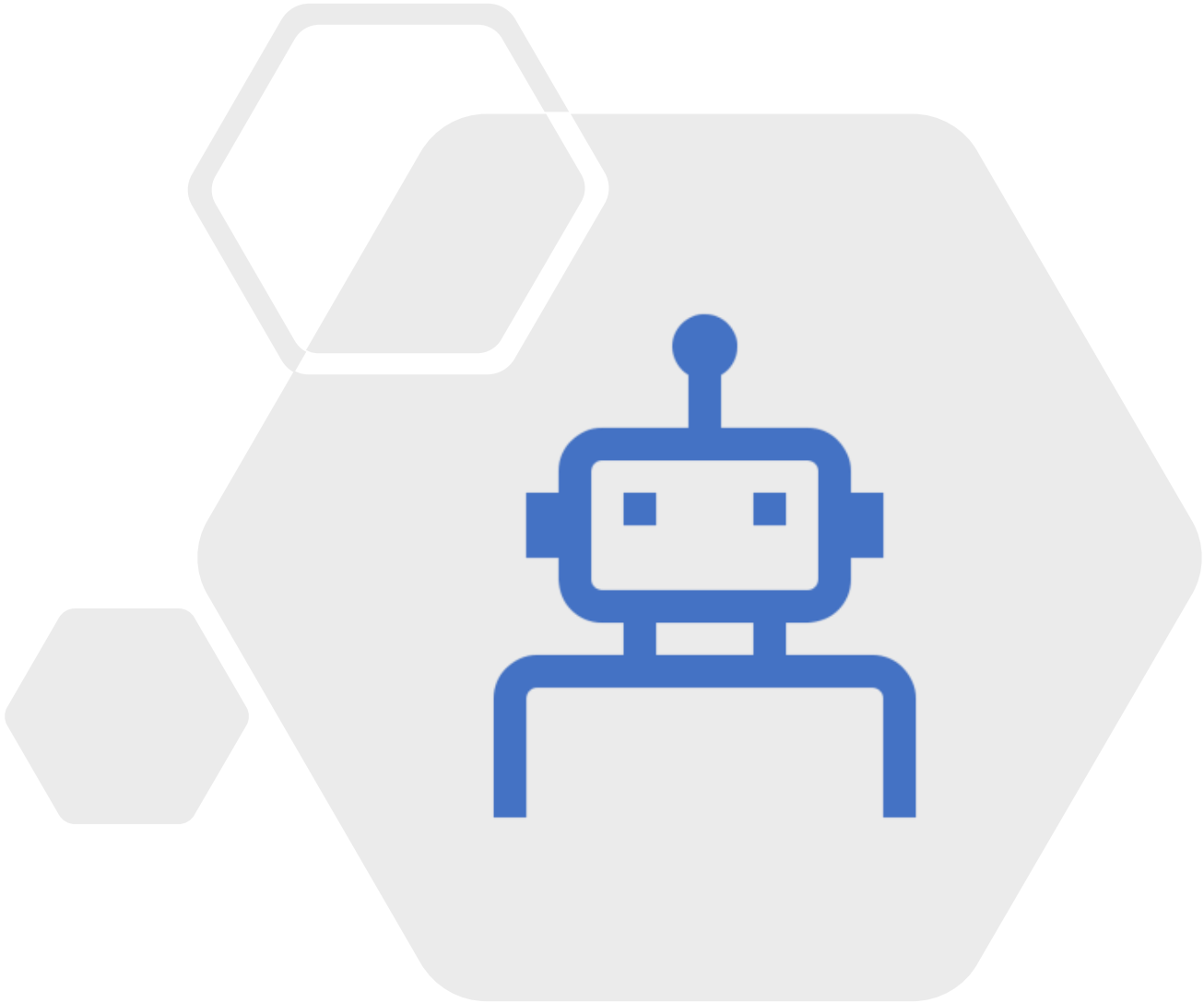
С чего начать?

Люди и взаимодействие важнее процессов и инструментов
Работающий продукт важнее исчерпывающей документации
Сотрудничество с заказчиком важнее согласования условий контракта
Готовность к изменениям важнее следования первоначальному плану

Agile Manifest
(и страшный сон безопасности)

DevSecOps (формально)

- Требования регуляторов
- Лицензионная чистота (3rd party)
- Меньше уязвимостей и техдолга
- Стабильность работы
- Симбиоз процессов и инструментов



Инструментарий: Dev

- Linters
- Методички от ИБ
- Формализация стека
- Open-Source Analysis
- Анализ open-source компонентов
- Не можешь предотвратить - возглавь

Инструментарий: CI

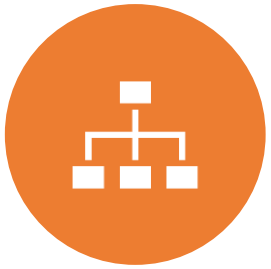
- SAST
- Open-Source Analysis (automated)
- 3rd party зависимости (component analysis)
- Традиционная обвязка уровня инфраструктуры (мониторинг, контроль целостности, подписи кода и пр)

Инструментарий: CD

Сканирование контейнеров
DAST
Observability (и иные подходы к мониторингу)
AppSec Orchestration/Correlation
Тандем с процессами QA

Люди и процессы

Процессная боль



РАЗНЫЕ КОМАНДЫ – РАЗНЫЕ ПРОЦЕССЫ. ИНСТРУМЕНТЫ ПОРОЙ ТОЖЕ.

КАЧЕСТВО? КАКОЕ КАЧЕСТВО?

ИНСТРУМЕНТЫ ОБНАРУЖИЛИ ПРОБЛЕМЫ. С МОМЕНТА ОБНАРУЖЕНИЯ УЖЕ ВЫКАТИЛИ N НОВЫХ РЕЛИЗОВ

MVP КАК ОТДЕЛЬНЫЙ МИР

DevSecOps (а теперь неформально)

- Диалог вместо требований (не отменяет формализации)
- Польза от решений безопасности
- Observability – это интересно
- Учиться нужно в обе стороны
- Security champions

Security champions

- Внутренняя экспертиза
- Менторский подход
- То, что не видит автоматизация
- Адаптивность под типы команд
- База знаний

Готова ответить

на ваши вопросы

E-mail

mona@sudo.su

Telegram

@Mona_Sax