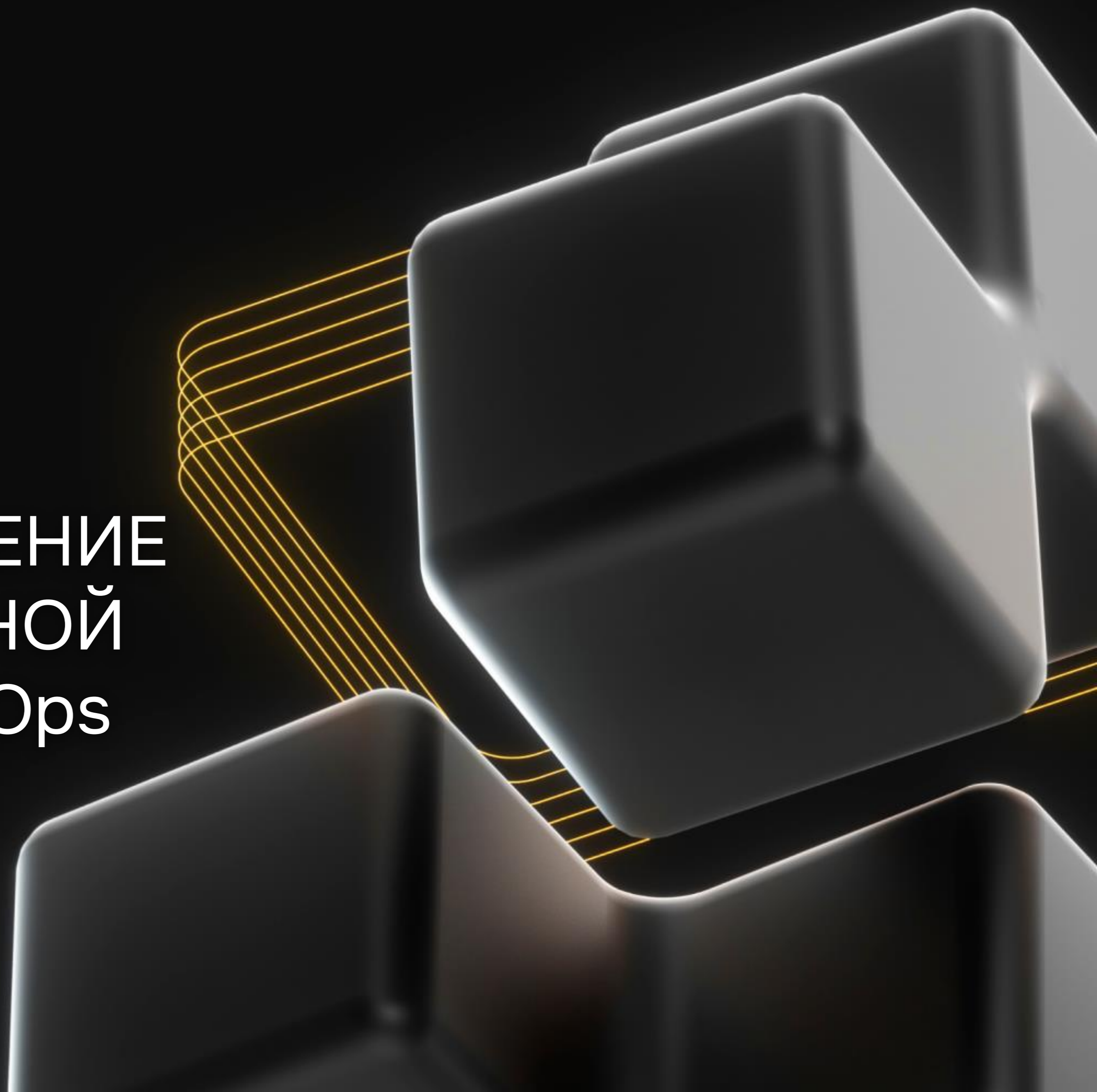


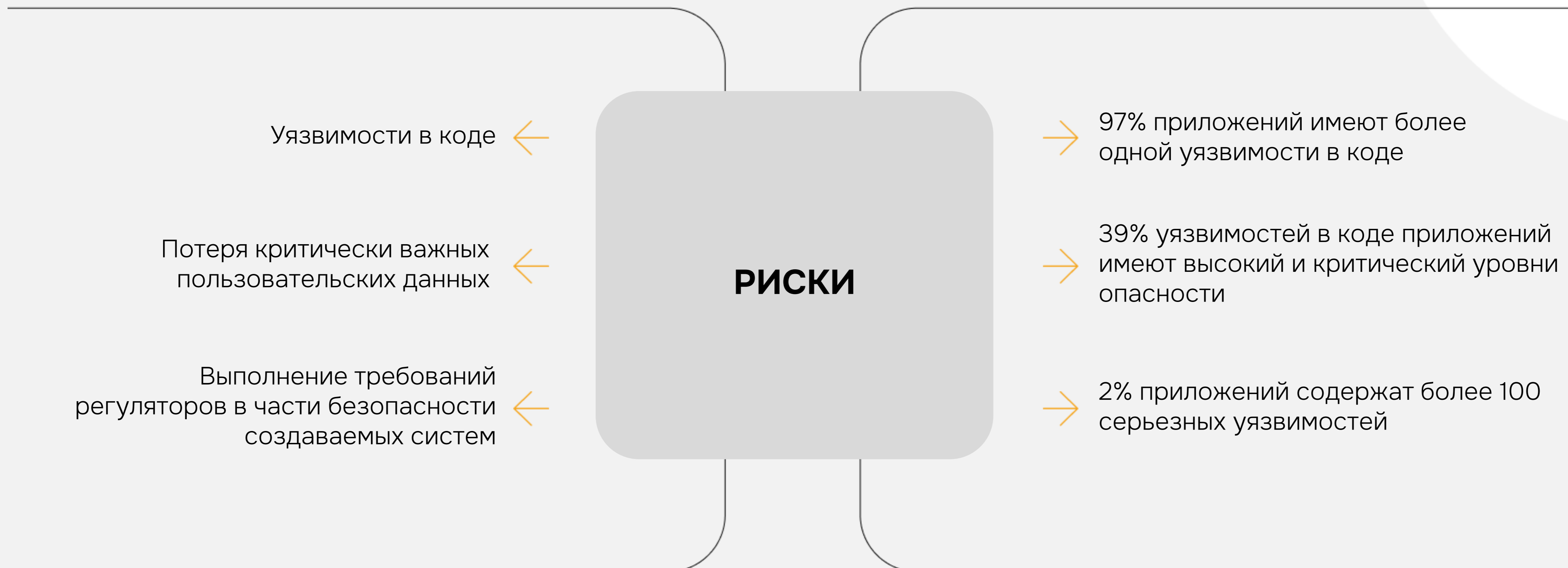


ЦЕНТР
КИБЕРБЕЗОПАСНОСТИ

ПОСТАНОВКА И ВНЕДРЕНИЕ ПРОЦЕССОВ БЕЗОПАСНОЙ РАЗРАБОТКИ – DevSecOps



РИСКИ В СФЕРЕ ИБ ПРИ РАЗРАБОТКЕ СОБСТВЕННОГО ИЛИ ИСПОЛЬЗОВАНИИ ЗАКАЗНОГО ПО



* По результатам исследования компании Contrast Security

ИНСТРУМЕНТ МИНИМИЗАЦИИ РИСКОВ



DevSecOps

предполагает внедрение принципов информационной безопасности на всех этапах непрерывного цикла создания программного обеспечения – от сборки до интеграции и развертывания.

Снижается количество уязвимостей в исходном коде

Выявленные недостатки безопасности устраняются быстрее и эффективнее

Уменьшается ущерб от возможных инцидентов



ЦЕНТР КИБЕРБЕЗОПАСНОСТИ УЦСБ – СИСТЕМНЫЙ ПОДХОД К ПОСТАНОВКЕ ПРОЦЕССОВ DevSecOps



Аудит процессов разработки



Разработка дорожной карты внедрения DevSecOps



Сопровождение в процессе перехода от DevOps к DevSecOps



Обучение разработчиков



Подбор и внедрение необходимых инструментов



Помощь в сертификации разработок

В ОДНОМ МЕСТЕ – ВСЕ НУЖНОЕ: ПРОФЕССИОНАЛЬНАЯ ЭКСПЕРТИЗА, ПРОВЕРЕННЫЕ ИНСТРУМЕНТЫ, ГОТОВЫЕ СЕРВИСЫ

АУДИТ ПРОЦЕССОВ РАЗРАБОТКИ



Изучение и подробное описание процессов разработки



Составление перечня используемых инструментов



Определение бизнес-логики процессов разработки



Формирование отчета о состоянии DevOps или DevSecOps



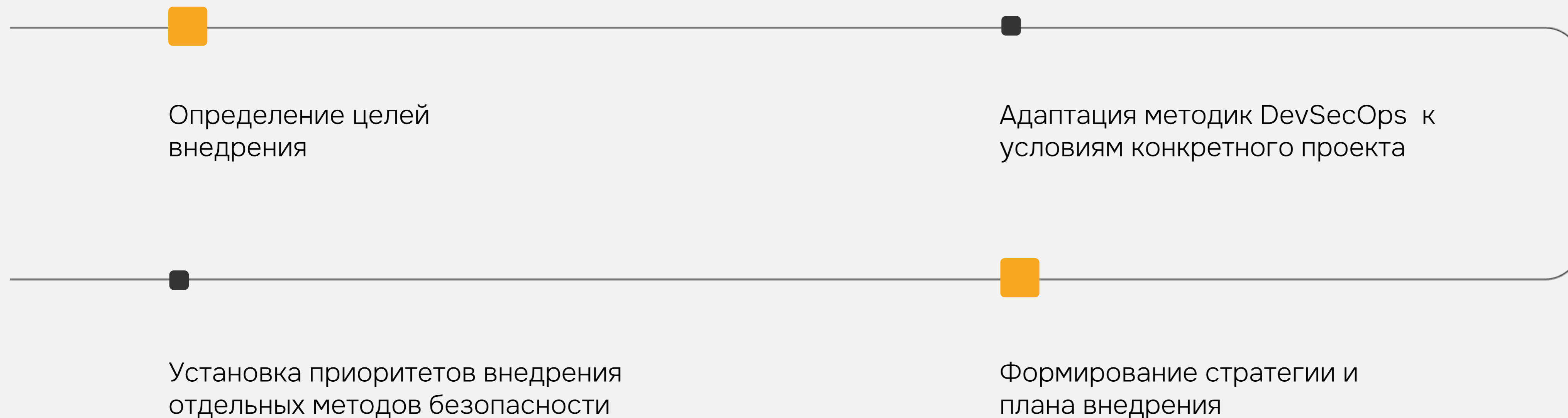
Консультирование по потенциальным угрозам и недостаткам с точки зрения ИБ



РЕЗУЛЬТАТ

Определены проблемы и «узкие места», зафиксировано состояние «как есть», команда проекта и руководство компании понимает текущее положение дел. Есть возможность планировать изменения.

РАЗРАБОТКА ДОРОЖНОЙ КАРТЫ ВНЕДРЕНИЯ DevSecOps



РЕЗУЛЬТАТ

Поставлены цели внедрения, описан желаемый результат, разработан подробный план внедрения DevSecOps



СОПРОВОЖДЕНИЕ ПРОЦЕССА ПЕРЕХОДА от DevOps к DevSecOps



Реализация «нашей» части мероприятий
плана внедрения DevSecOps



При необходимости – поиск и
приглашение внешних специалистов



Общий мониторинг выполнения плана



Консультирование специалистов заказчика,
решение возникающих вопросов

РЕЗУЛЬТАТ

Максимально комфортное и безболезненное внедрение инструментов безопасности в цикл разработки под руководством опытных кураторов. Достижение поставленных целей проекта.



ОБУЧЕНИЕ РАЗРАБОТЧИКОВ

- Обучение методикам постановки ИБ-задач в разработке
- Подготовка Security Champions
- Повышение компетентности участников команды проекта в сфере ИБ
- Консультации по практическому применению инструментов безопасности

РЕЗУЛЬТАТ

Разработчики обладают актуальными знаниями об инструментах и методах информационной безопасности в цикле DevOps, а также умеют применять их на практике



ПОДБОР И ВНЕДРЕНИЕ НЕОБХОДИМЫХ ИНСТРУМЕНТОВ

Находим и внедряем наиболее подходящие для конкретного проекта инструменты безопасности

Системы статического и динамического анализа кода

Решения Software Composition Analysis (SCA)

Средства анализа защищенности и мониторинга инцидентов

Аппаратные платформы и облачные сервисы

РЕЗУЛЬТАТ

Процесс разработки обеспечен наиболее эффективными средствами безопасности.

ПОДДЕРЖКА ПРОЦЕССА СЕРТИФИКАЦИИ



Проверка продукта на соответствие требованиям регуляторов



Подготовка перечня рекомендаций для устранения расхождений



Разработка полного комплекта необходимой документации



Сопровождение процесса сертификации до результата

РЕЗУЛЬТАТ

Разработанный продукт соответствует требованиям законодательства с точки зрения информационной безопасности и имеет подтверждающие документы от регулирующих органов.



ПОЛНЫЙ СПЕКТР УСЛУГ В СФЕРЕ DevSecOps

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ РАБОТЫ ВАШЕЙ СИСТЕМЫ

- Подключение к собственному SOC
- Круглосуточный мониторинг безопасности
- Быстрое реагирование на инциденты и блокировка атак
- Регулярное тестирование на уязвимости (пентест)

ПРОВЕРКА БЕЗОПАСНОСТИ СТОРОННЕГО ПО

- Оценка исходного кода с точки зрения ИБ
- Выявление уязвимостей, тестирование на проникновение
- Исследование критических функциональных блоков
- Разработка рекомендаций по повышению безопасности



ЦЕНТР КИБЕРБЕЗОПАСНОСТИ УЦСБ

Системный подход к
защите процессов
разработки

01

Многолетний опыт
успешных внедрений
DevSecOps

02

Команда
сертифицированных
экспертов

03

Все компетенции по
соответствию
требованиям
законодательства

04

Поставка и внедрение
необходимых инструментов

05

Обучение
сотрудников

06

Возможность
подключения к
собственным сервисам
безопасности

07

ОПЫТ УЦСБ В СФЕРЕ DEVSECOPS



Построили с нуля процессы безопасной разработки в региональном банке для продуктов дистанционного банковского обслуживания



Сделали анализ защищенности кластеров управления контейнерами, реализовали требования мировых стандартов



Настроили и сопровождали продукты класса Container Security



Выполнили работы по всем направлениям анализа защищенности приложения – от статического анализа до тестирования на проникновение



Интегрировали процессы DevSecOps в существующие CI/CD процессы и pipeline разработки



Внедрили процессы безопасности в публичных облаках, выстроили безопасность процессов Infrastructure as code



Провели аудит существующих процессов безопасной разработки, сформировали рекомендации по их развитию





ЦЕНТР КИБЕРБЕЗОПАСНОСТИ



sec.ussc.ru



cybersec@ussc.ru

