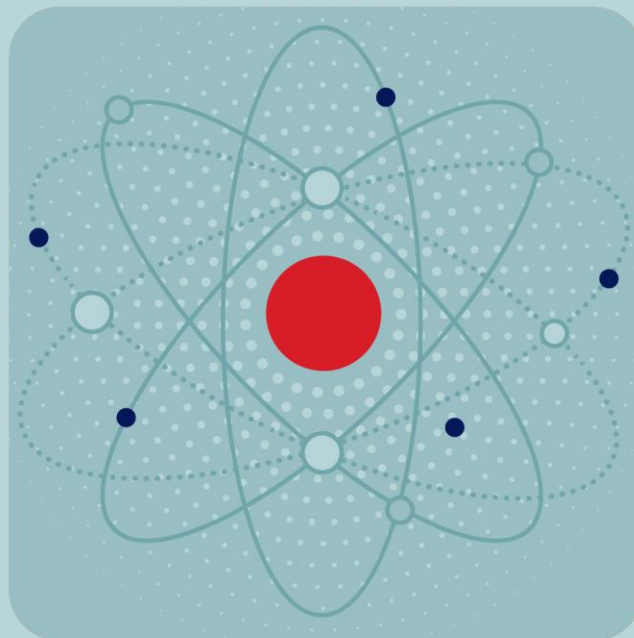


ТЕХНОЛОГИЧЕСКАЯ
ПАРТНЕРСКАЯ КОНФЕРЕНЦИЯ

РУТОКЕН ЦНЧ ТЕХНОЛОГИИ ДОВЕРИЯ



КОМПАНИЯ
ПРАКТИВ



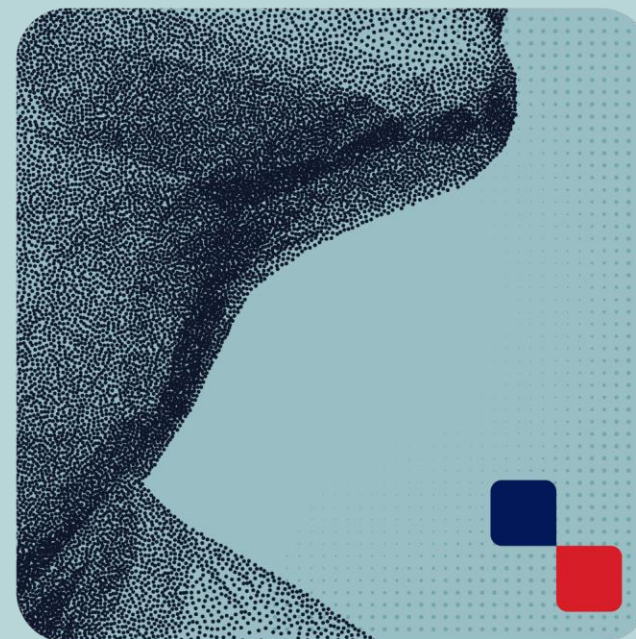
Внедрение безопасной разработки: путь к сертификации ФСТЭК и повышению качества продуктов

**Владислав
Крылов**

Консультант по информационной
безопасности AKTIV CONSULTING,
Компания «Актив»

**Дмитрий
Мешков**

Руководитель отдела десктопной
разработки,
Компания «Актив»



Кто я?



- ✓ 30 лет, Весы
- ✓ 11 лет в сфере ИБ, погружен в безопасную разработку с 2023
- ✓ Болею за ФК «Ливерпуль», люблю мопсов

Где я тружусь?

- ✓ АКТИВ.CONSULTING — бизнес-направление Компании «Актив»
- ✓ Обладаем экспертизой от анализа угроз, внедрения security by design (SAST, DAST, fuzzing) до пентестинга

Хокку-девиз наших проектов:

**«Строки кода –
уязвимости прячутся.
Сканеры ищут»**



На что опираться при внедрении безопасной разработки?



ГОСТ Р 56939–2024

«Защита информации. Разработка безопасного программного обеспечения» — ключевой стандарт, регламентирующий процессы безопасной разработки

Определяет требования к:

- ✓ управлению уязвимостями
- ✓ контролю целостности кода
- ✓ автоматизации тестирования безопасности
- ✓ документированию и верификации процессов

А еще...

Приказ ФСТЭК России № 239

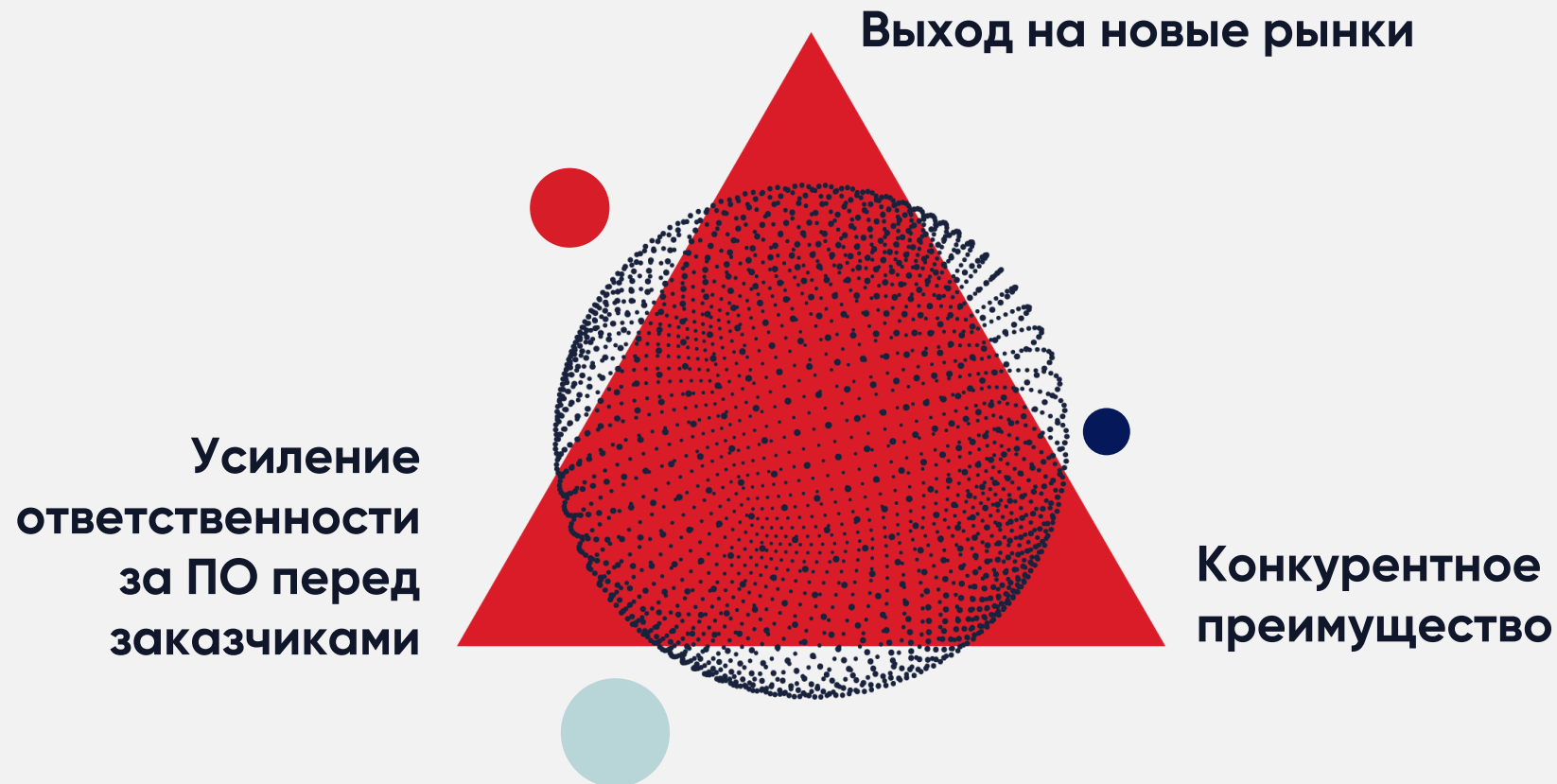
устанавливает требования к защите информации при разработке ПО для ЗО КИИ

ГОСТ Р 71207–2024

регламентирует методы статического анализа кода для выявления уязвимостей



Внедрение БРПО открывает перед компаниями значительные возможности для развития



Почему нужно было внедрить в Компании «Актив»?



✓ Соответствие
обязательным
требованиям

✓ Работа
с субъектами
КИИ

✓ Защита интересов
компании и клиентов



Внедрение процессов безопасной разработки ПО согласно **ГОСТ Р 56939–2024**

Шаг 1.

Оценка текущего состояния
и планирование

Шаг 2.

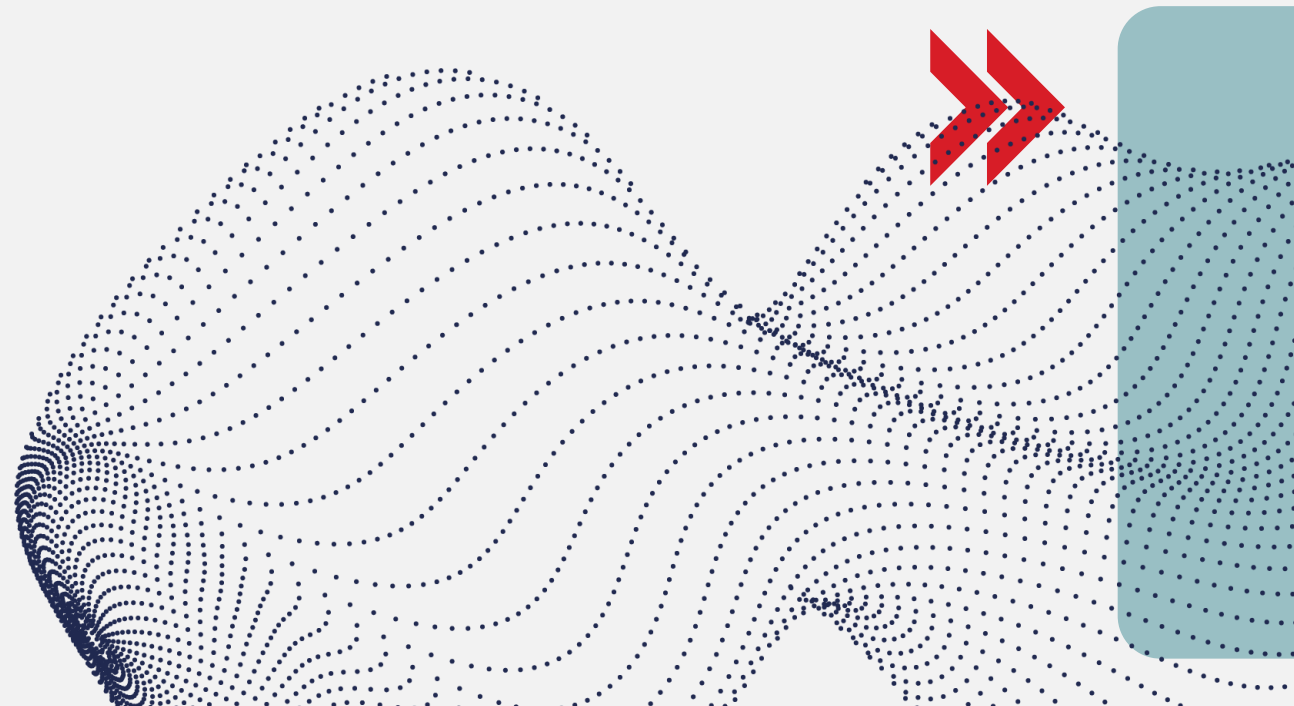
Выбор инструментов

Шаг 3.

Адаптация инфраструктуры

Шаг 4.

Документирование процессов



Внедрение процессов безопасной разработки ПО согласно **ГОСТ Р 56939–2024**

Шаг 5.

Внедрение организационных мер

Шаг 6.

Верификация и тестирование

Шаг 7.

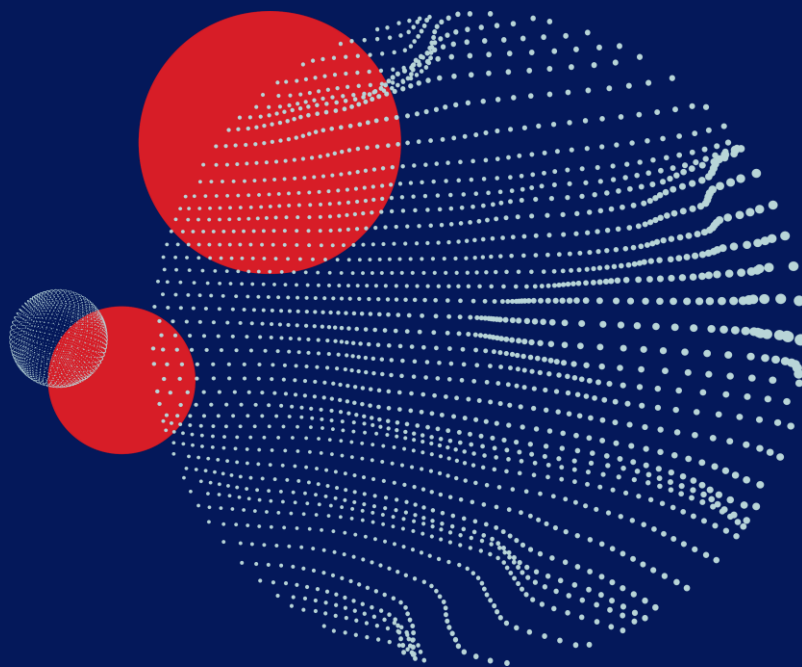
Поддержка и сопровождение

Шаг 8.

Сертификация (при необходимости)



В теории все звучит хорошо.
А как на практике?



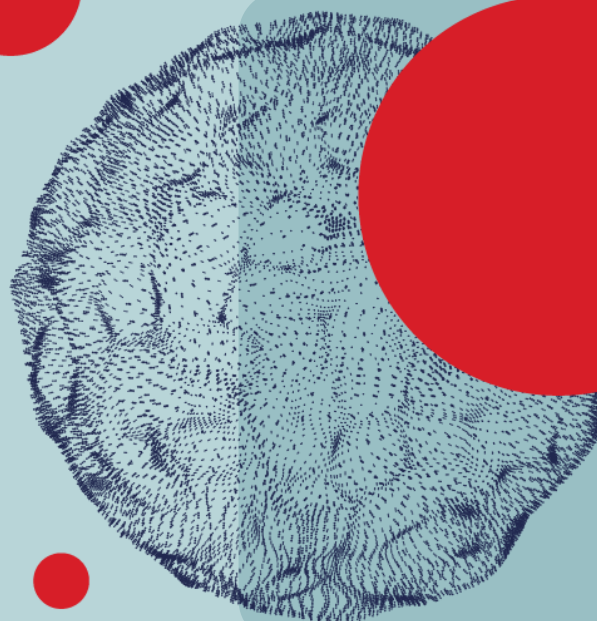
Кто я?



- ✓ 29 лет, Дева (это же важно?..)
- ✓ 13 лет в сфере ИБ (если с ВУЗом)
- ✓ Не болею, люблю кошек

Где я тружусь?

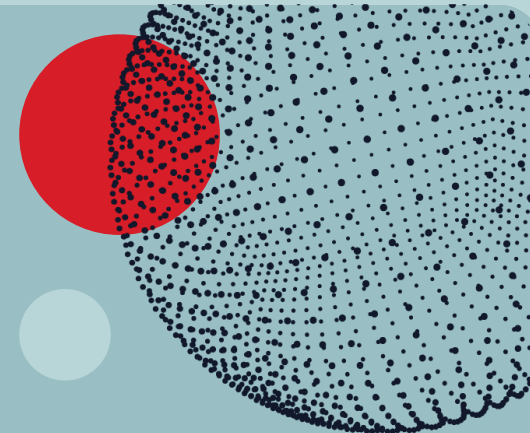
- ✓ Руткен — руководитель отдела десктопной разработки
- ✓ Пьем чай, разрабатываем средства защиты информации



Взгляд на БРПО со стороны разработки



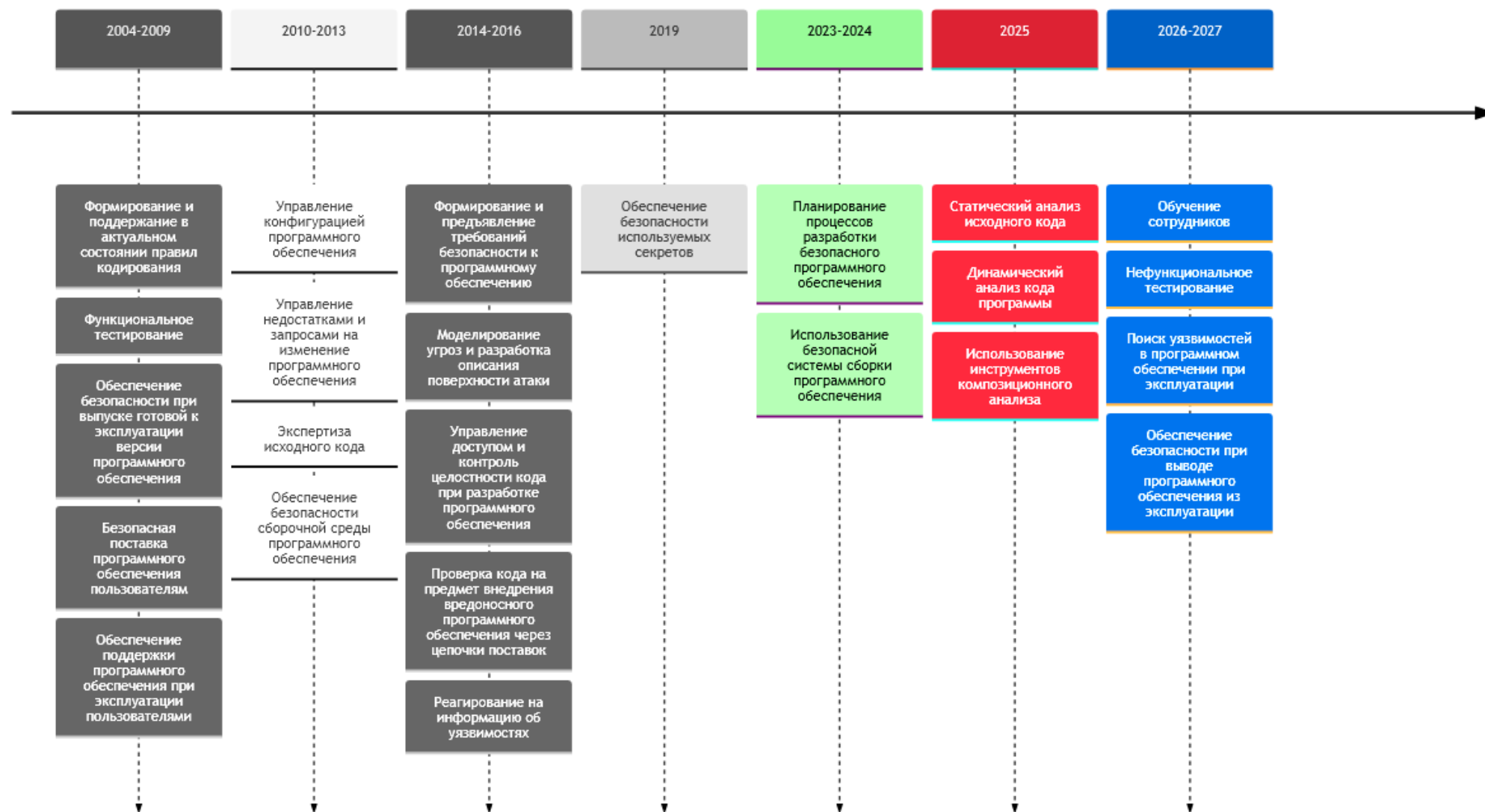
- ✓ Сертификация
- ✓ Конкурентное преимущество



- ✓ Автоматические проверки новыми инструментами
- ✓ Осознанность в разработке
- ✓ Культура написания кода



Развитие процессов БРПО Рутокен



Статический анализ



- ✓ Похож на остальные инструменты автоматической обработки кода
- ✓ Понятен разработчикам
- ✓ Много инструментов для анализа C/C++
- ✓ Хорошие инструменты платные =(

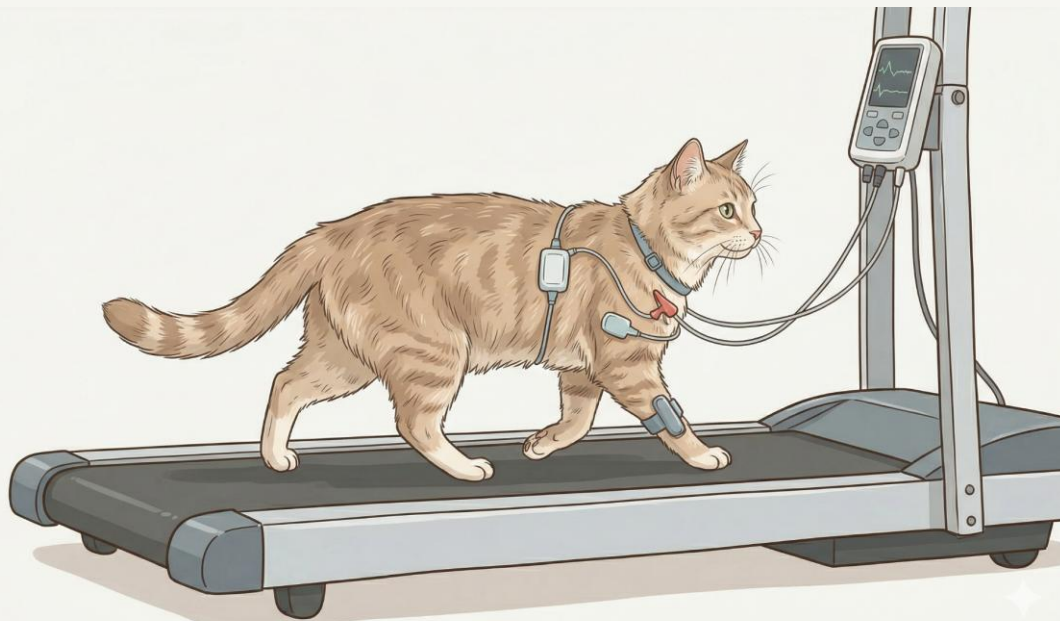
Композиционный анализ



- ✓ Нет универсального рецепта для C/C++
- ✓ Необходим новый инструмент накопления и обработки уязвимостей
- ✓ Непривычные работы для разработчика
- ✓ Помогает по-новому взглянуть на работу с заимствованным кодом



Динамический анализ



- ✓ Качество анализа зависит от экспертизы разработчика фаззинг-целей
- ✓ Требуется большое число ресурсов, нельзя просто скопировать из другого проекта
- ✓ Требуется лучше понять, как собирается проект, и изменить процесс сборки

Дальнейшее **развитие**

- ✓ Сертификация процессов разработки
- ✓ Построение универсального «безопасного» конвейера разработки для всех наших продуктов
- ✓ Обучение сотрудников





Владислав **Крылов**

Консультант по информационной безопасности АКТИВ.CONSULTING, Компания «Актив»



Дмитрий **Мешков**

Руководитель отдела десктопной разработки, Компания «Актив»



krylov@aktiv.consulting
www.aktiv.consulting
+7 906 720-87-25



Meshkov@rutoken.ru
www.rutoken.ru
+7 926 586-90-96