AKTIV.
CONSULTING

Бизнес-завтрак

Безопасная разработка ПО в субъектах КИИ
Типовые сложности и пути решения

Александр Моисеев

Ведущий консультант по информационной безопасности AKTIV.CONSULTING

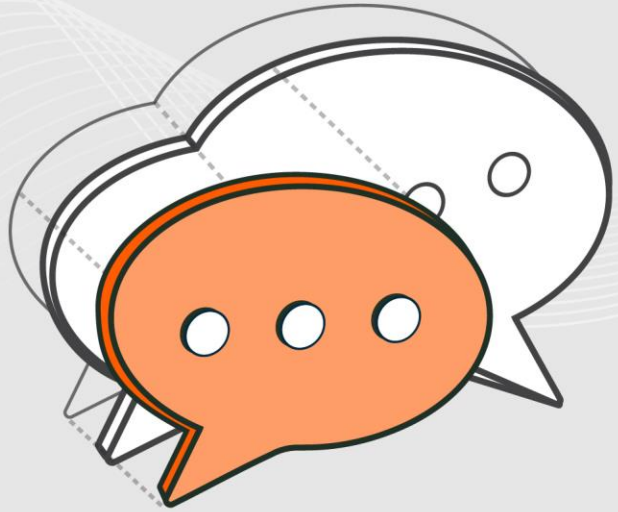
О чем сегодня пойдет речь:

№1

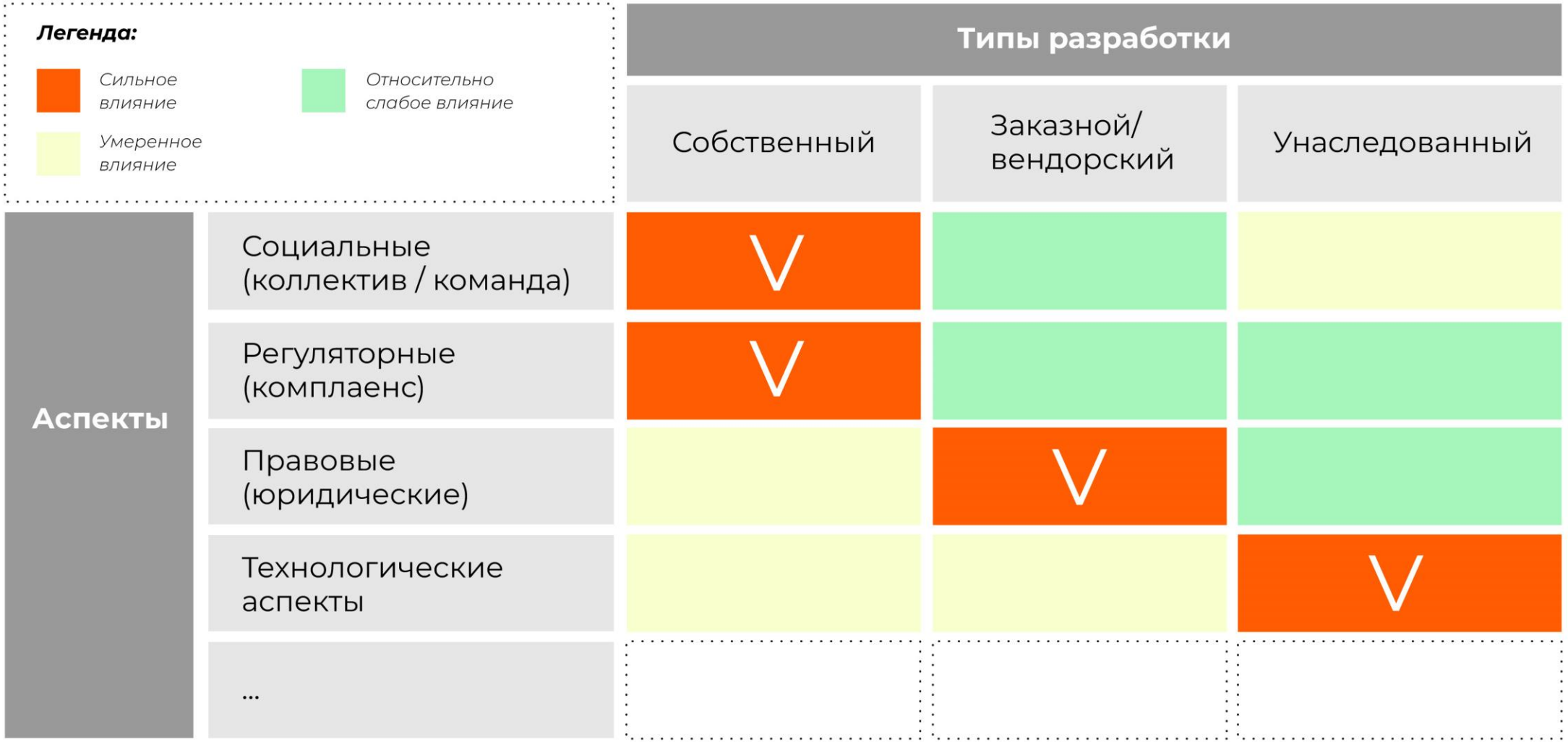
Сложности
при внутренней разработке ПО

№2

Сложности
унаследованного ПО



Классификация сложностей



№1 Сложности при внутренней разработке

1.1

Сопротивление сотрудников

1.2

Отсутствие референса и готового фреймворка

1.1 Сопротивление сотрудников

Ценности	Причины сопротивления	Пути решения
Непрерывность бизнеса	Неопределенность	Принятие взвешенного решения
Обеспечение безопасности	Понимания предметной области	Работа с возражениями на разных уровнях
Развитие	Работает – не трогай	Выделение роли security champion
Автоматизация	Низкая осведомленность	Повышение осведомленности

1.2 Отсутствие референса и готового фреймворка

Не существует единого универсального фреймворка, учитывающего:

Актуальные **отраслевые требования**

Влияние **на технологические и производственные** процессы

Специфику **применяемого стека** IT / OT-технологий

Специфику **ЖЦ ПО и самого ЗО КИИ**

Разработка такого фреймворка требует ресурсов кроссфункциональной команды

Пути решения

МЕТОДЫ

- Структурные методы *(CORE, JSD, ...)*
- Прослеживаемость *(прямая и обратная)*
- Стандарты кодирования
- Программирование с защитой
- Формальное доказательство *(методы CCS, CSP, VDM, Z)*

СРЕДСТВА

- Универсальный язык программирования *(UML)*
- Статический и динамический анализ
- Доверенные инструментальные средства
- Функциональное тестирование и тестирование методом «черного ящика»
- Стресс-тестирование

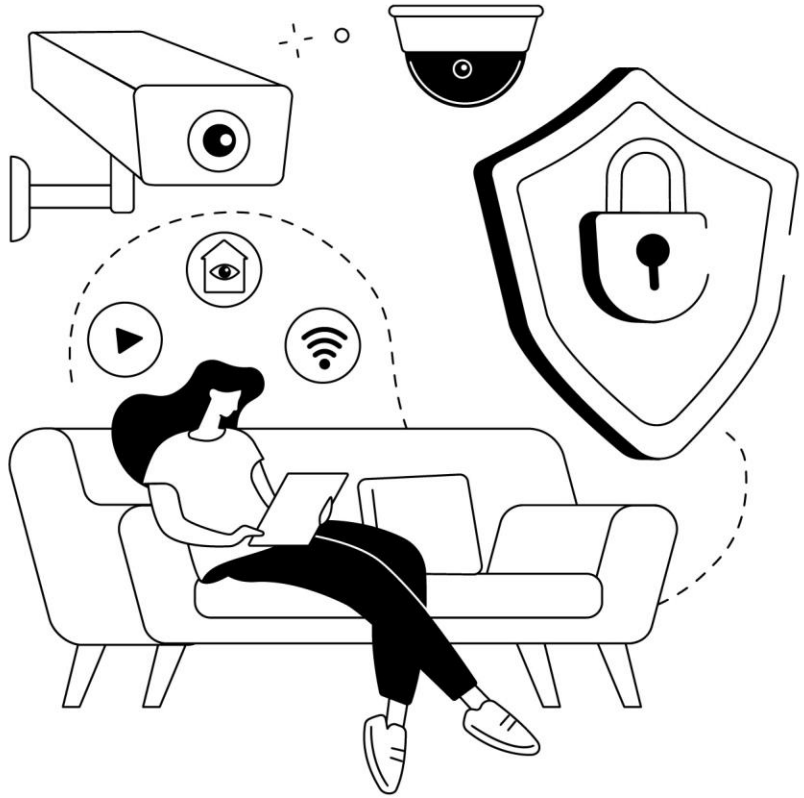
Рекомендуемый набор мер для обеспечения безопасности при разработке

Управление доступом к среде разработки

Фаззинг

Управление уязвимостями в сегменте разработки и продуктовой среде

Тестирование на проникновение



№2 Сложности унаследованного ПО

2.1

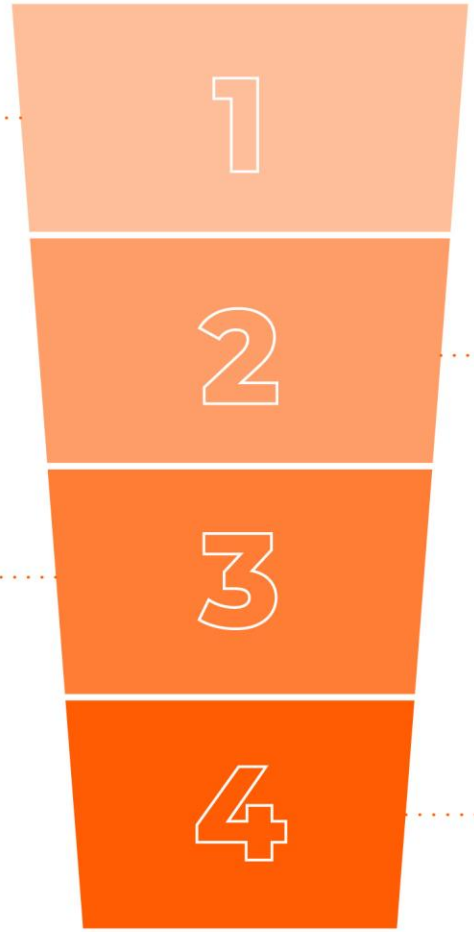
Полное отсутствие исходного кода

2.2

Исходный код доступен частично

2.1 Полное отсутствие исходного кода

Неподдерживаемый код
(нет патчей и обновлений безопасности)



Нет документации к ПО
(проектной, эксплуатационной)

Используются устаревшие версии ЯП, библиотек

Не используются технологии защиты кода
(DEP, ASLR, safe stack и т.п.)

Пути решения

Проверки безопасности методом серого ящика

Разработка **эксплуатационной документации**

Налаживание канала **обратной связи с пользователем**

Сканирование

Применение **компенсирующих мер**

Преимущество:

Повышение защищенности и компленс

Исследование исполняемого файла
методом «серого ящика»

1	**Статический анализ «1/2»** **Динамический анализ «1/2»**	Поиск нетипичных артефактов или поведения
2	**Фаззинг**	Локализация ошибок
3	**Статический анализ «2/2»** **Динамический анализ «2/2»**	Декомпиляция, дизассемблирование и отладка

2.2 Исходный код доступен частично

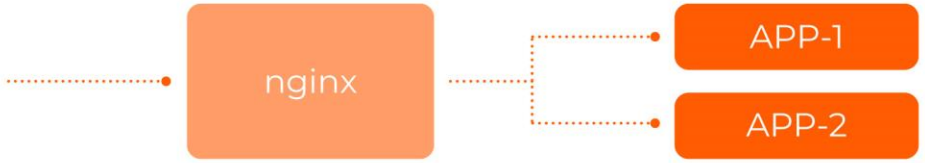
1. Поддержка кода и разработка новых фич **затруднена**
2. **Небезопасное** хранение кода в директориях
3. Код **не документирован** *(нет проектной, эксплуатационной, тестовой документации)*
4. Используются **устаревшие** фреймворки, версии ЯП
5. Код написан **в старом стиле,** по устаревшим архитектурным паттернам

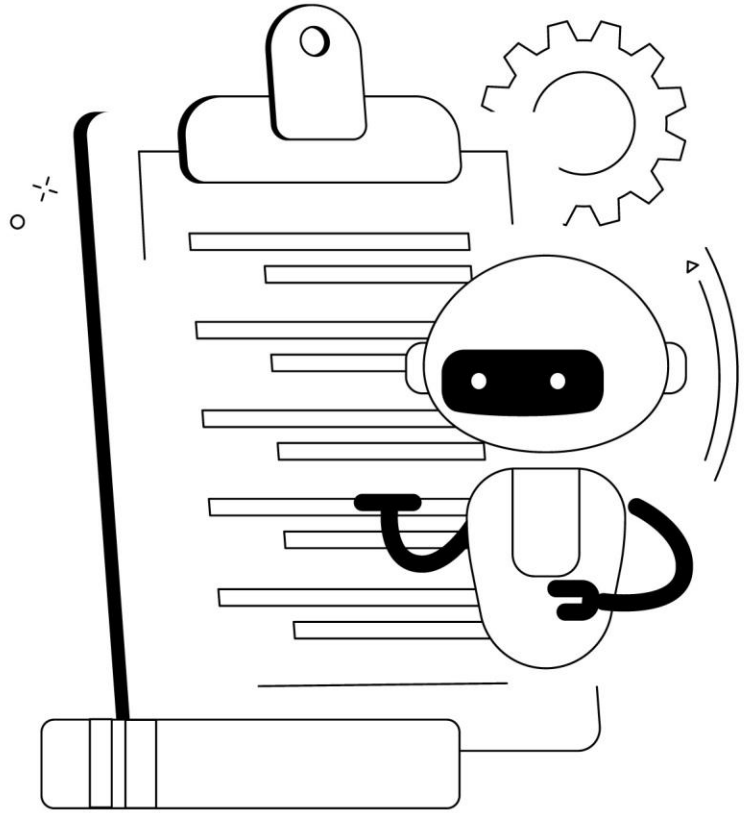
Пути решения

1. **Разработать новый проект *(долго, дорого, сложно)***

2. ***Переписать существующий проект (не менее, а то и более долго, дорого, сложно)***
   - Обновить зависимости
   - Удалить мертвые зависимости
   - Перенастроить сборку и развертывание приложения

3. **Поддержка нескольких приложжений через роутинг *(быстро, дешево, но узкая применимость)***





Преимущество:

Организация поддержки ЖЦ ПО

В качестве резюме

01

Повышение роли ИБ в компании и создание центра компетенций

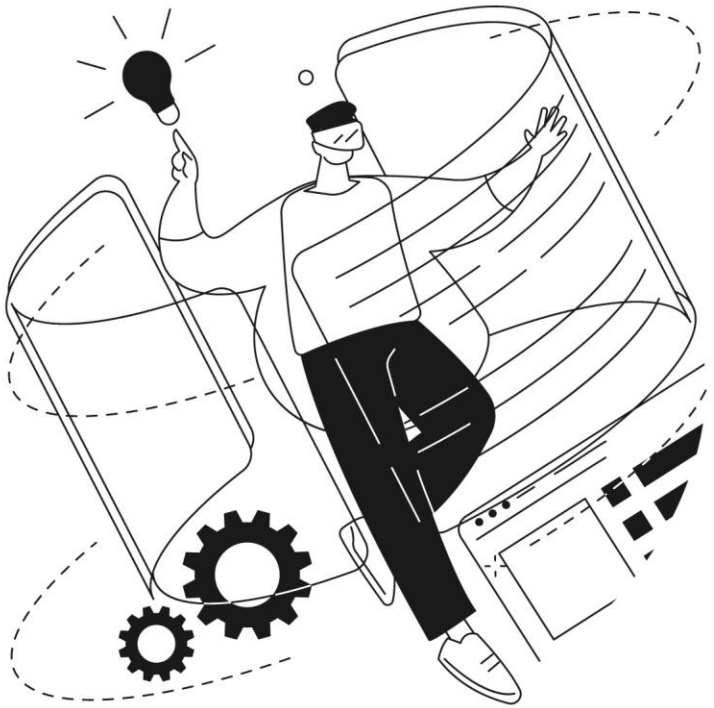
02

Повышение защищенности организации за счет безопасности прикладного ПО

03

Соответствие регуляторике – это инструмент обоснования инвестиций

Рекомендуем начать с оценки соответствия требованиям 239 приказа



AKTIV.
CONSULTING

Александр Моисеев

Ведущий консультант по информационной безопасности AKTIV.CONSULTING

moiseev@aktiv.consulting