

М

Т

АБИСС 10.10.23

DevSecOps:

почему он должен Вас волновать и откуда начать



Илья Шаров

Руководитель направления DevSecOps
МТС — связь и экосистема цифровых сервисов

С

Структура

01. Призма требований

- Обзорный матч по безопасной разработке: ГОСТ 56939, Профиль защиты ЦБ, Приказ N 239 ФСТЭК
- Лучшие практики DevSecOps vs РБПО

02. Стратегии внедрения

- Что должно быть по умолчанию для внедрения практик безопасной разработки
- Подходы к стратегии внедрения безопасной разработки
- Личный опыт внедрения
- Аргументация

03. Грабли Story

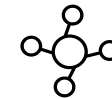
- Грабли #1 - опыт внедрения OSA Firewall (как не нужно)
- Грабли #2 – «бизнес принимает риски»



**Призма
требований**



**Стратегии
внедрения**

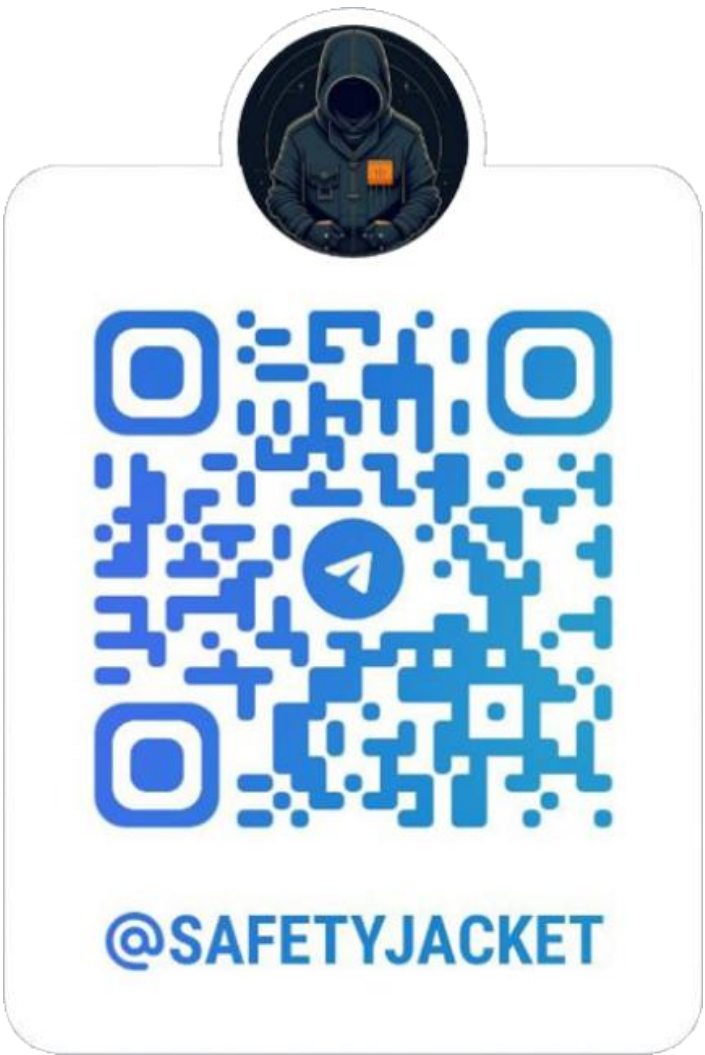
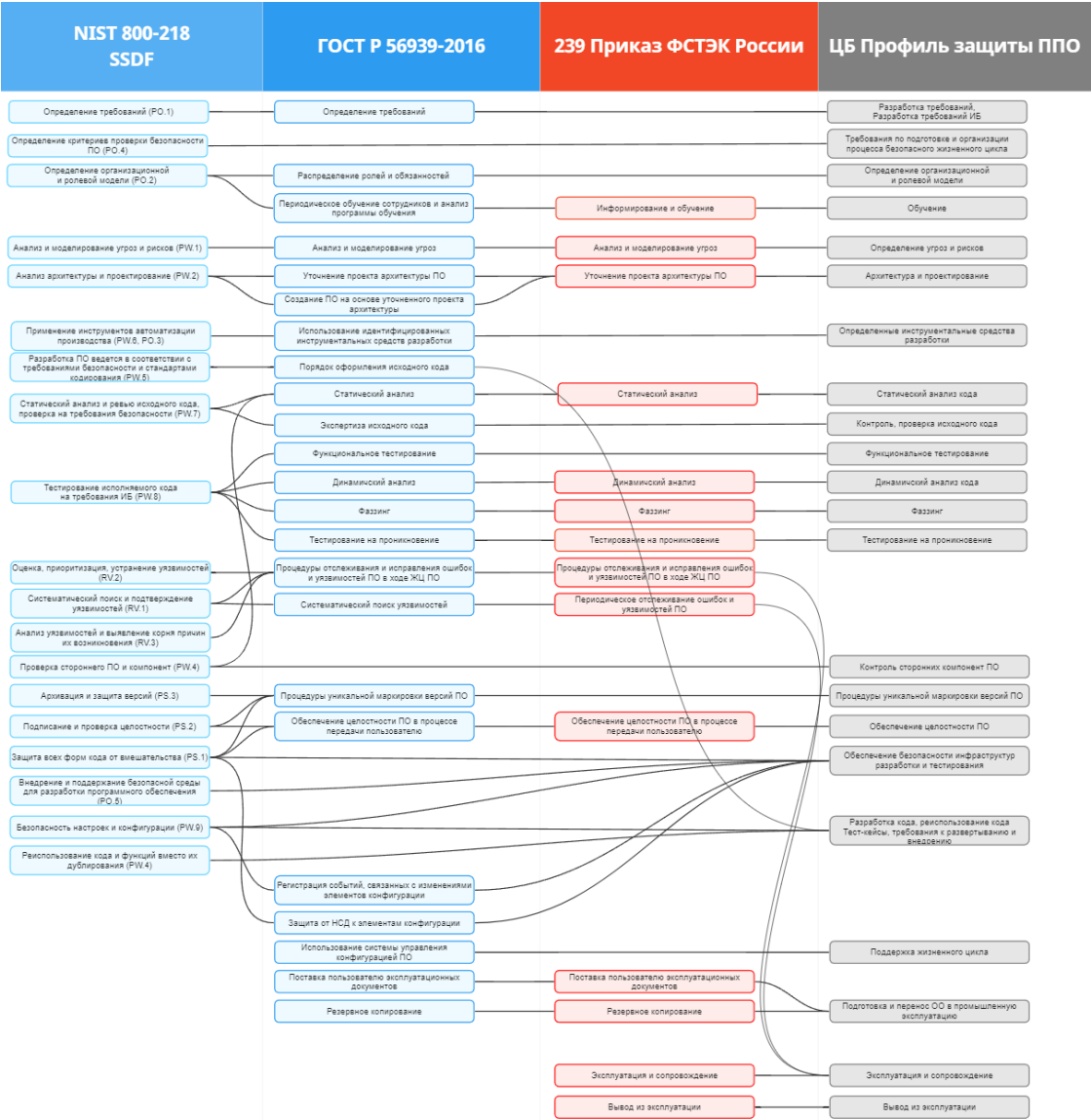


**Грабли
Story**





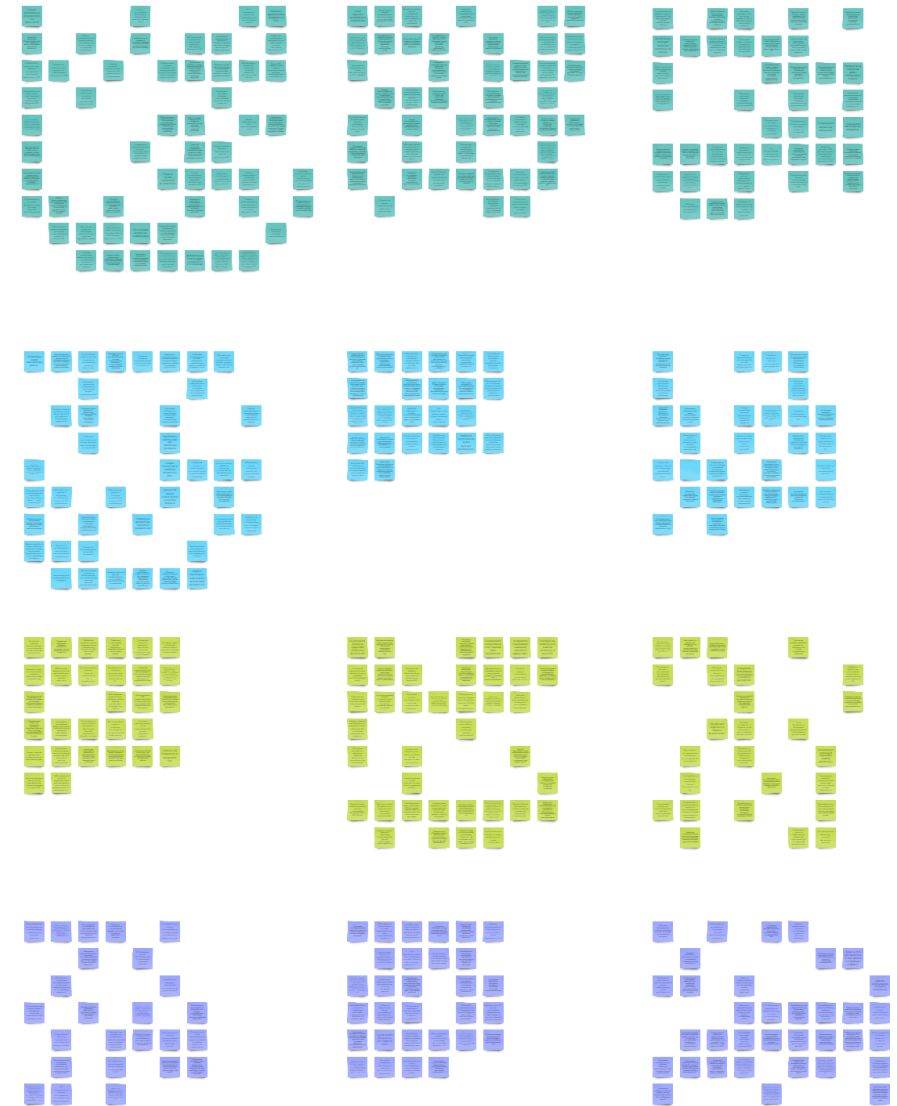
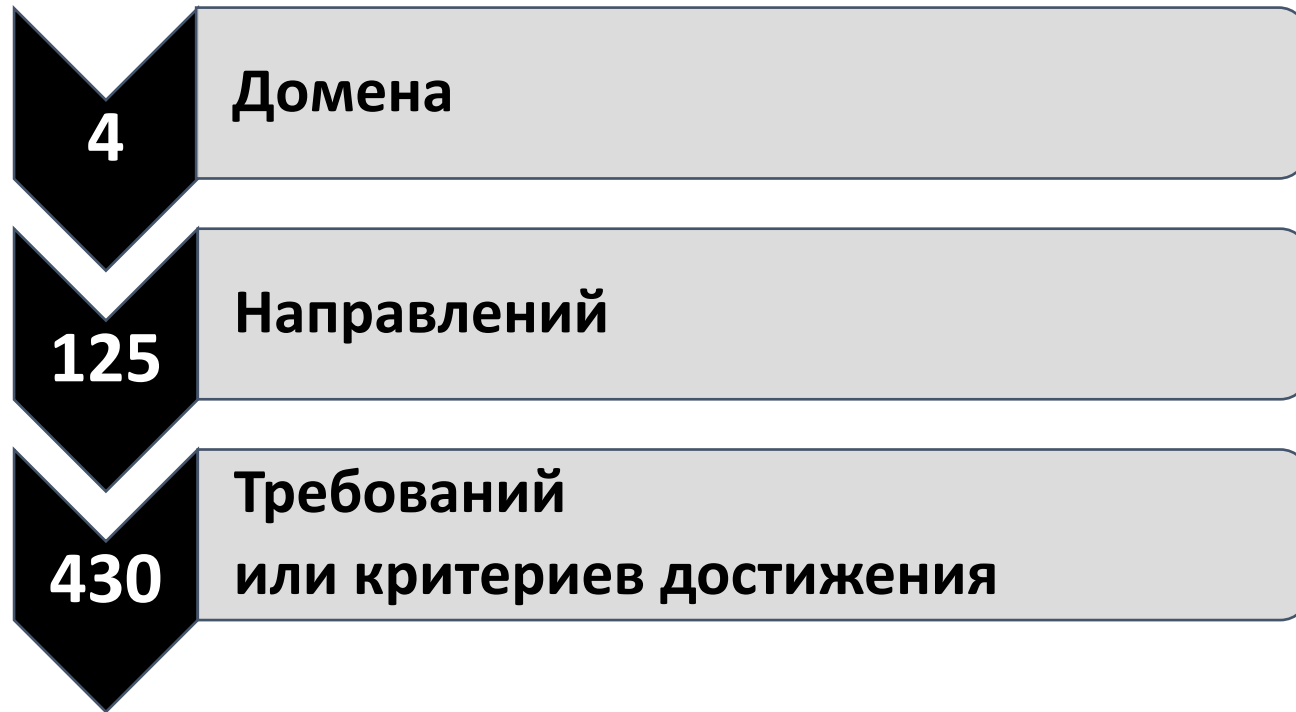
Обзорный матч по безопасной разработке



Обзорный матч по безопасной разработке



Скальпирование BSIMM



Лучшие практики DevSecOps vs РБПО

так в чем отличие

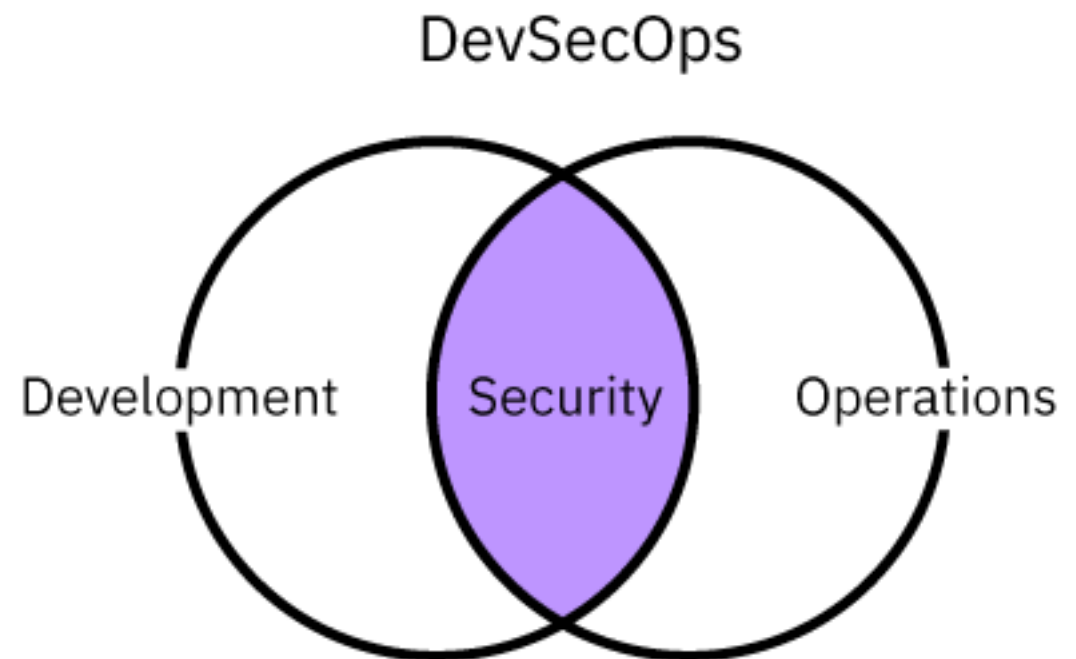
Лучшие практики

1. Системное или ежегодное обновление
2. Использование реальных данных, практик и опыта
3. Возможность сравнительного анализа с необходимой отраслью экономики
4. Имеют распределение по уровням зрелости
5. Позволяют покрыть требования регулятора

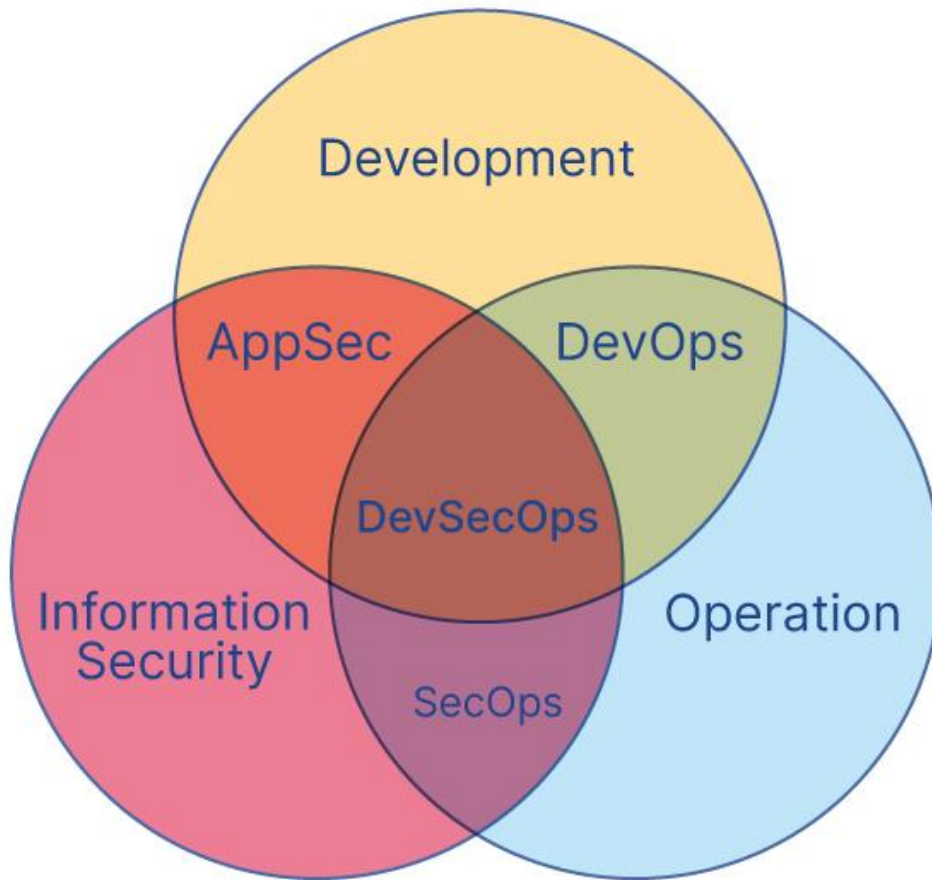
РБПО

1. **Некоторое отставание**
2. Конкретный конечный набор
 - Требований регулятора
 - Наименований документов их разделов
 - Типов проверок и процессов
3. **Не имеет уровней зрелости**

DevSecurityOps ...



DevSecOps это больше чем безопасность разработки приложений



Включает, но не ограничивается
обеспечением безопасности:

- Производственного процесса
- Разработки приложений
- Продуктовых окружений
- Процесса эксплуатации

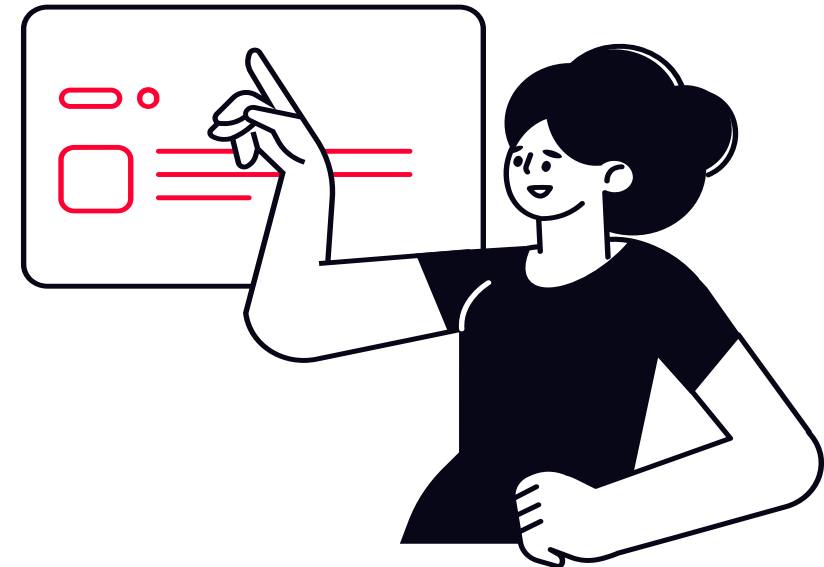
Пирамида практики применения DevSecOps



Цель
Задачи
Основание
Аргументация

Какую цель вы преследуете?
Какие задачи требуется решить?

...



Раздел 7.4 Профиль защиты ЦБ ППО

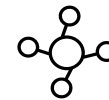
В связи с этим требования настоящего раздела могут использоваться в целях реализации требования доверия к безопасности (ТДБ) ОО (п. 7.2. настоящего документа) в случаях, когда финансовая организация либо разработчик ОО (далее при совместном упоминании – Разработчик) реализует документированный безопасный жизненный цикл ОО, основанный на современных гибких практиках разработки, тестирования и внедрения ОО, в основе которых лежат различные методологии безопасного жизненного цикла программных продуктов (например, такие международные и общепринятые в рамках соответствующих сообществ методологии, как SDLC1 , DevSecOps2 , BSIMM3 , OWASP4 и др.).



**Призма
требований**



**Стратегии
внедрения**



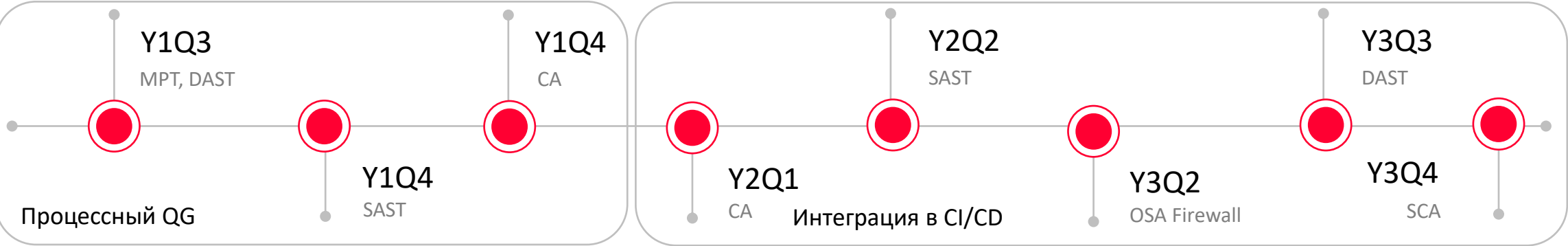
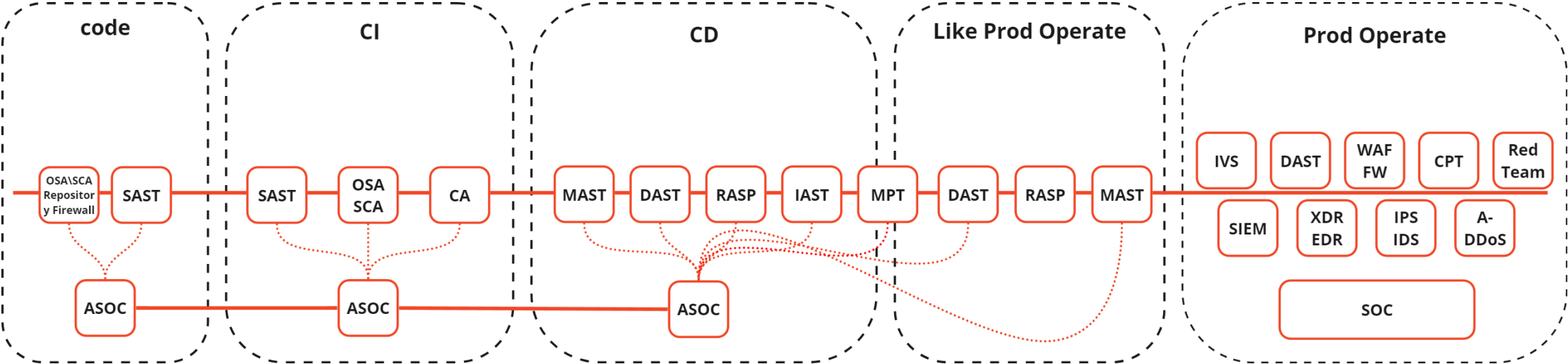
**Габли
Story**

Без чего не обойтись для успешной реализации

- ✓ **Орг.структура производства и обеспечения безопасности**
- ✓ **Сегментирование**
- ✓ **Инфраструктурная безопасность
Защита данных**
- ✓ **Соответствие требованиям
Непрерывность бизнеса**
- ✓ **Инструментальный аудит ИБ**
- ✓ **Защищенный доступ
Политики безопасности**
- ✓ **Конвейер DevOps
Производственный процесс**
- ✓ **ИБ на этапах архитектуры,
сопровождения разработки, ПСИ,
эксплуатации**

Подходы к стратегии внедрения

- Start чем левее тем лучше
- Постепенный сдвиг влево
- Смешанный



Open Source Tools set

Image Scan

Бесплатное решение:
GitLab Container Scanning

Open Source решения:
Trivy – (all-in-1 - IaC, k8s)
Clair

IaC Scan

Open Source решения:
Checkov
Tfscan
Trivy

SAST

Бесплатное решение:
GitLab SAST

Open Source решения:
SonarQube
Bandit
gitleaks
gosec
horussec
infer
njsscan
semgrep
spotbugs
trufflehog

SCA

Open Source решения:
Dependency track
Dependency check

ASOC & VM

Open Source решения:
Archery
DefecDojo

DAST

Open Source решения:
Zed Attack Proxy (ZAP)

MAST

Open Source решения:
MobSF

RASP

Open Source решения:
Falco
OpenRasp

Commercial Tools set

PVS Studio

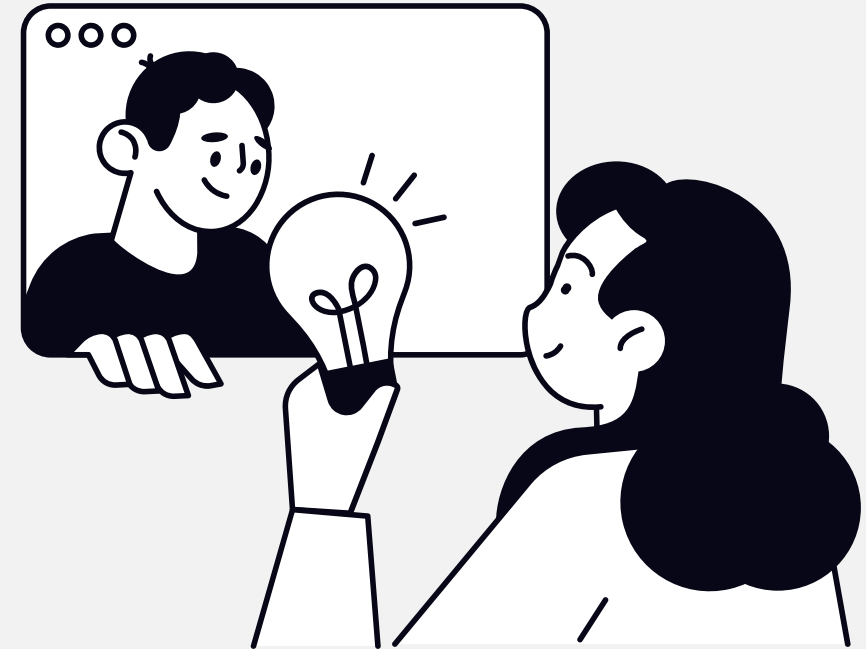
ИСП-РАН

Ростелеком-Солар

Positive Technology

Profiscope

AppSec Solutions



Стоп-слово

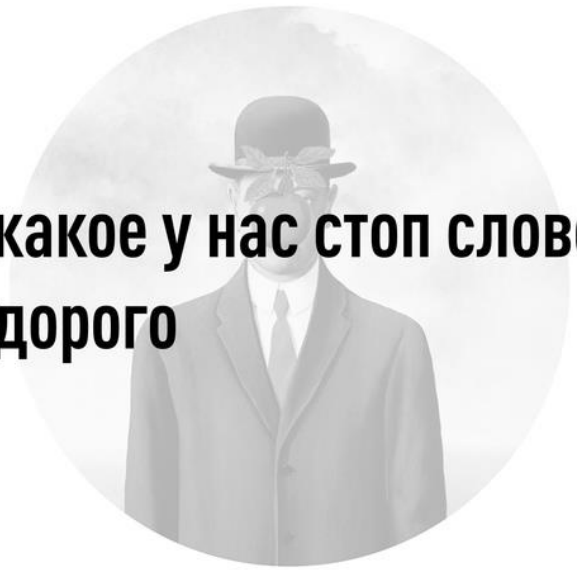
Предотвращение потерь – **сохраняет** деньги

Оптимизация процессов – **экономит** деньги

Инциденты ИТ/ИБ – **стоят** денег

Тестирование на поздних этапах – **стоит** денег

Собственные трудозатраты, а не заказ работ – **экономит*** деньги



- какое у нас стоп слово?
- дорого

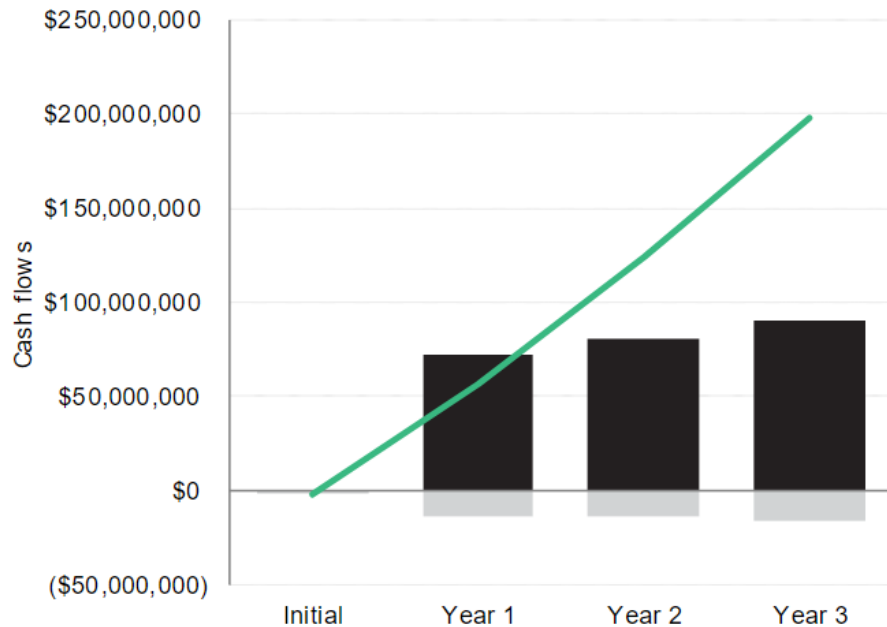
*Это не значит, что отсутствует потребность в внешних поставщиках услуг. Есть обратные примеры, делайте расчеты ☺

Каковы ваши аргументы

ROI 427%

Окупаемость
~ 6 месяцев

Financial Analysis (risk-adjusted)



Cash Flow Analysis (Risk-Adjusted Estimates)

	Initial	Year 1	Year 2	Year 3	Total	Present Value
Total costs	(\$1,942,600)	(\$13,745,512)	(\$13,438,612)	(\$16,645,222)	(\$45,771,946)	(\$38,050,613)
Total benefits	\$0	\$72,263,410	\$80,610,027	\$90,803,042	\$243,676,479	\$200,535,536
Net benefits	(\$1,942,600)	\$58,517,898	\$67,171,415	\$74,157,820	\$197,904,533	\$162,484,923

Значения рентабельности инвестиций, чистой приведенной стоимости и срока окупаемости приведены с поправкой на риск

\$48.3M

Повышение эффективности управления уязвимостями

\$44.0M

Сокращение времени, затрачиваемого на создание собственных инструментов безопасности и управление решениями с открытым исходным кодом

\$39.9M

Повышение эффективности разработки

\$29.1M

Улучшение качества кода

\$17.0M

Увеличение дохода за счет увеличения количества релизов

\$9.4M

Сокращение времени, затрачиваемого на интеграцию и настройку инструментов безопасности с инструментами разработки

\$4.8M

Возврат упущенного дохода от эффективности устранения инцидентов безопасности

\$3.2M

Экономия затрат на лицензирование и обслуживание за счет консолидации технических средств

\$3.1M

Экономия затрат на рабочую силу за счет сокращения количества инцидентов, требующих устранения

\$1.8M

Экономия затрат за счет эффективности подготовки к аудиту соответствия

Каковы ваши аргументы

В 8 раз сокращен
time-to-market

В программу «цифровой трансформации» банк ВТБ инвестировал **291,3 млрд. руб.**, стратегический цикл изменений охватил период **2020-2022** гг.

В 3 раза снижена аварийность

Экономический эффект цифровой трансформации ВТБ к концу 2022 г. достиг **более 300 млрд. руб**

91% систем с полным
комплектom документации

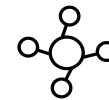
Прогнозируется, что к 2025 г. экономический эффект цифровой трансформации достигнет **600 млрд. руб**



**Призма
требований**



**Стратегии
внедрения**



**Грабли
Story**

Грабли #1 Как не нужно внедрять OSA Firewall



Дано

Штат специалистов «DevSecOps»

Действия команды

Внедрение OSA Firewall

lesson #1



Дано

Штат специалистов «DevSecOps»

Действия команды

Внедрение OSA Firewall

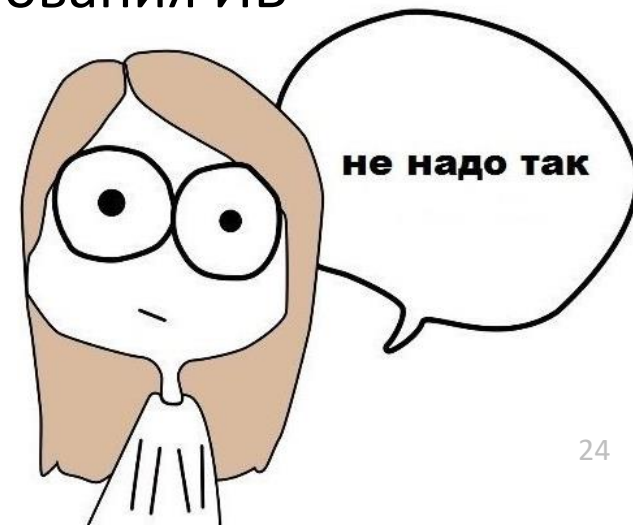
Но есть **нюанс**

- Штат DevOps, а не DevSecOps
- Без методологической подготовки
- Без привлечения экспертов по ИБ
- Без готовности подразделения ИБ
- Без функционального тестирования ИБ

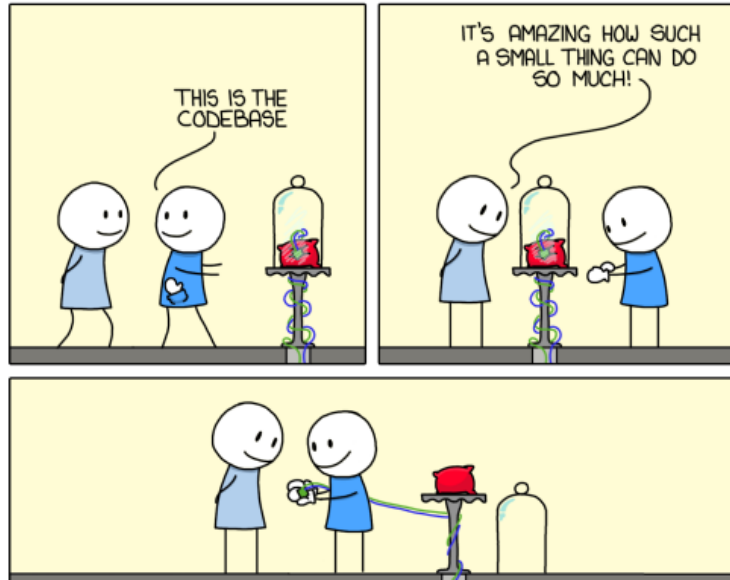
Последствия...

Ресурсы в трубу

Негативное восприятие ИБ



Грабли #2 Бизнес принимает риски



Дано

Промышленная эксплуатация, команда при разработке продукта привлекала специалистов безопасности

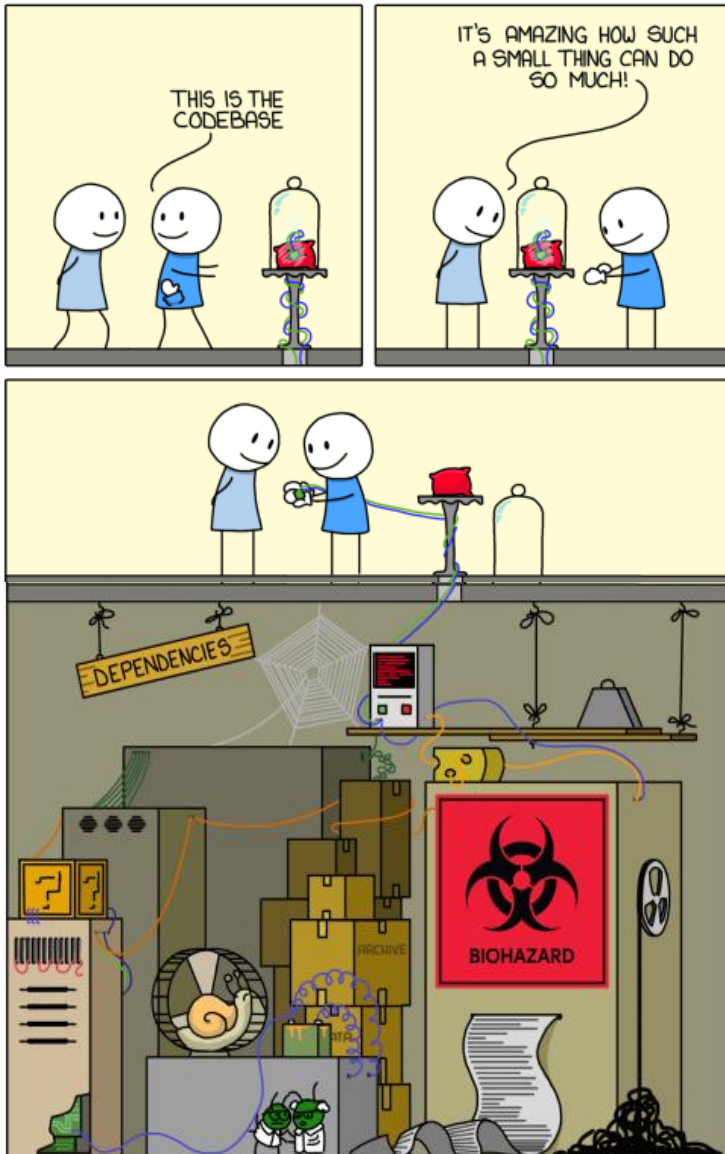
К продукту предъявлены требования безопасности, обязательства по которым не исполнялись должным образом

Действия команды

Применение административного ресурса

Накопление технического долга в части безопасности

lesson #2



Дано

Промышленная эксплуатация, команда при разработке продукта привлекала специалистов безопасности. К продукту предъявлены требования безопасности, обязательства по которым не исполнялись должным образом

Действия команды

Применение административного ресурса

Накопление технического долга в части безопасности

Последствия...

Реализация недопустимых событий

«Смена вертикали власти»

Откат разработки



Безопасность это процесс

А у процесса должен быть результат

Илья Шаров

