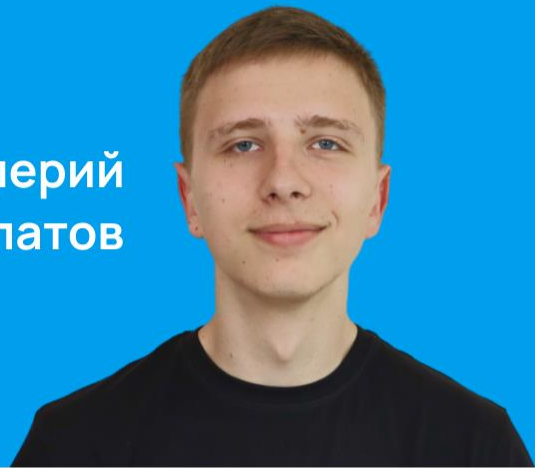


# Регулярный статический анализ по ГОСТу



Валерий  
Филатов



Семён  
Кашин





Цифровизация затрагивает все больше областей жизни человека



С 2023 года наблюдается мощный тренд атак на цепочки поставок ПО и «железа»



Большинство успешных атак задействует фишинг - «взлом» человека



Большая часть выявленных уязвимостей в заимствованных компонентах



У многих компаний не хватает компетенций и ресурсов для полноценного анализа



Внедрение мер безопасной разработки ПО



Поиск уязвимостей во всех компонентах ПО, для критически важных – независимая оценка



Делегировать задачи ИБ возможно, но в контролируемой среде



ГОСТ Р 56939-2024 Разработка безопасного программного обеспечения. Общие требования



Методика выявления уязвимостей и недеklarированных возможностей ФСТЭК России



ГОСТ Р 71207-2024 Статический анализ программного обеспечения. Общие требования



Не бюрократические документы, разработкой активно занимались практики



Нацелены на выявление и устранение недостатков, уязвимостей, в программном обеспечении



Упрощают и ускоряют формальную сертификацию программного обеспечения



Полноценное документирование всех процессов это сотни страниц документации



Затраты не только на этапе внедрения но и для поддержания работы



Одна из ключевых мер безопасной разработки



Получил отдельный стандарт ГОСТ Р 71207-2024



Позволяет быстро и с наименьшими затратами находить известные и типовые недостатки/уязвимости



Эффективность анализа очень сильно зависит от применяемых инструментов



Наиболее затратная часть – разметка срабатываний. Если много false-positive – затраты на разметку колоссальны



Высокий порог входа – квалифицированных специалистов на рынке труда немного



Информации по AppSec много, но она не структурирована и зачастую быстро устаревает



Дорого – чтобы постоянно анализировать весь свой код нужно не только купить инструменты анализа, но и держать штат AppSec безопасников



Долго – практические положительные результаты от внедрения мер безопасной разработки видны не сразу



Ford model T  
1910

VS



Ford model T  
1925





Ford model T  
1910

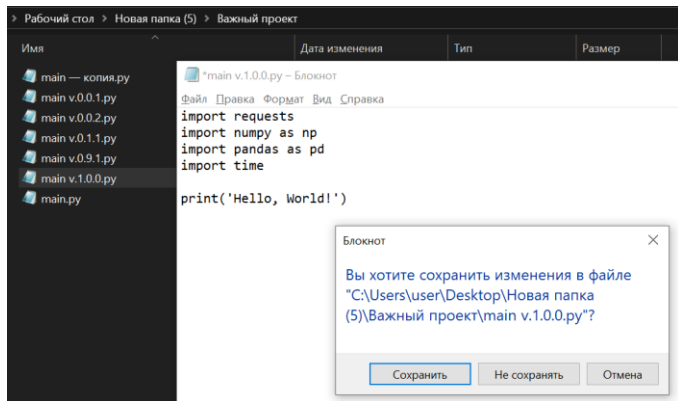
Цена 900\$  
Произведено 19 050 штук

VS

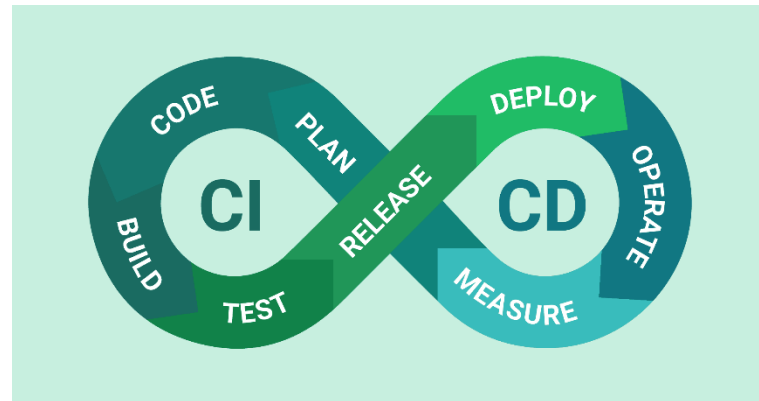


Ford model T  
1925

Цена 265\$  
Произведено 1 911 705 штук



VS





отсутствие автоматизации тестирования и развертывания



иллюзия безопасности



противостояние DevOps и Security команд



отсутствие единообразия кода



отсутствие политики выпуска релизов



несоответствие нормативным требованиям



сложность в подборе мер для соответствия нормативным требованиям



отсутствие контроля над процессами разработки



несоответствие переданных исходников фактически применяемым версиям программ



риск внедрения уязвимостей в код



риск потери возможности внесения изменений в продукт в случае проблем у поставщиков



завышенная стоимость разработки



фактическая невозможность сменить поставщика



Подход «shift-left» - думаем о безопасности при проектировании



Автоматизация процессов анализа кода и тестирования на уязвимости



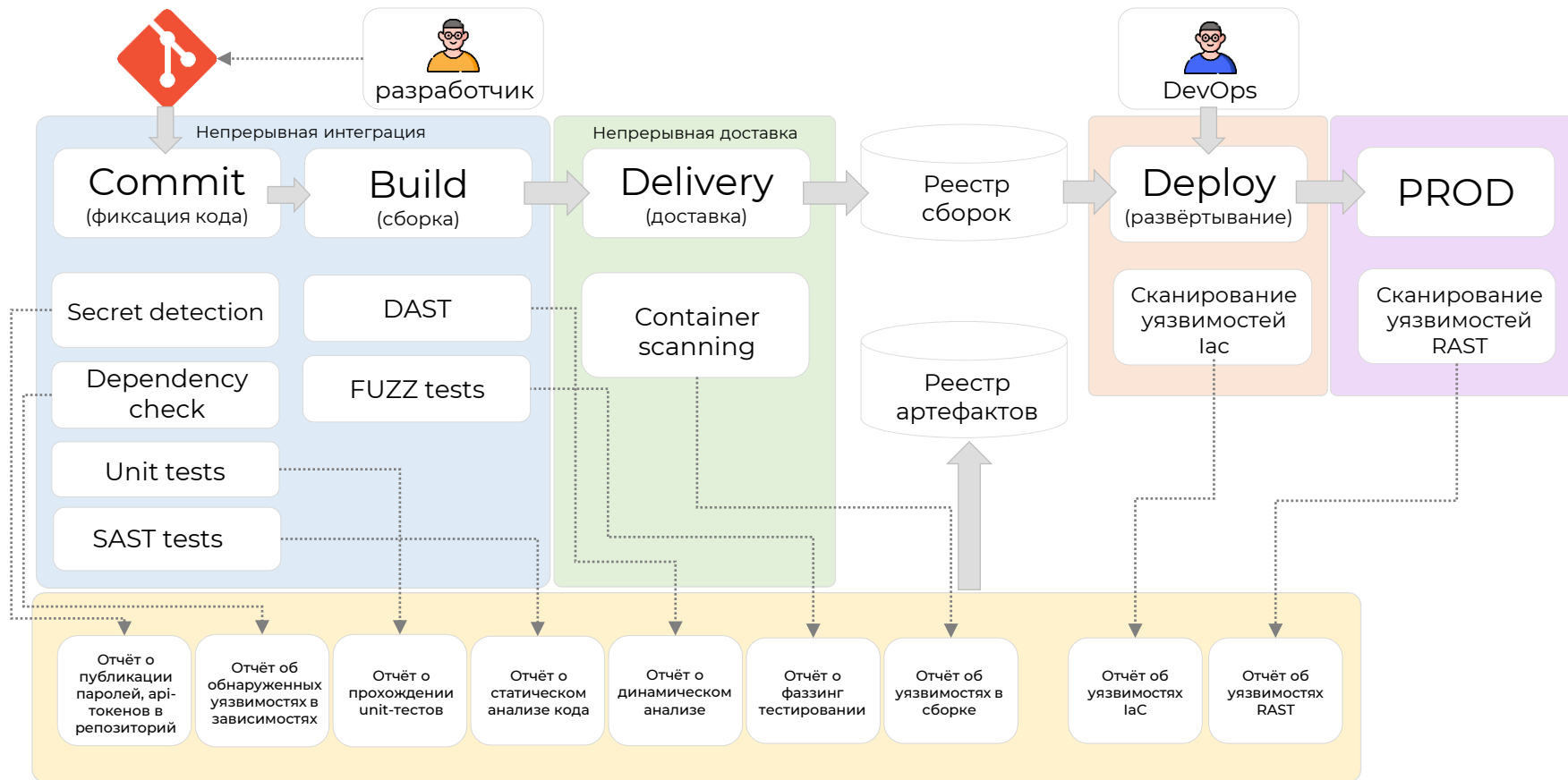
Переиспользование компонентов при разработке

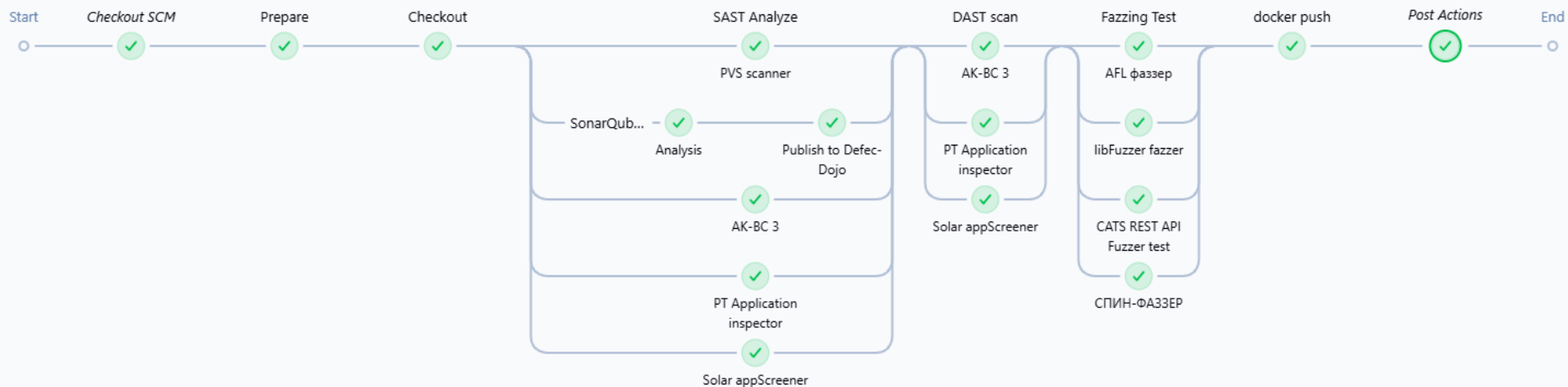


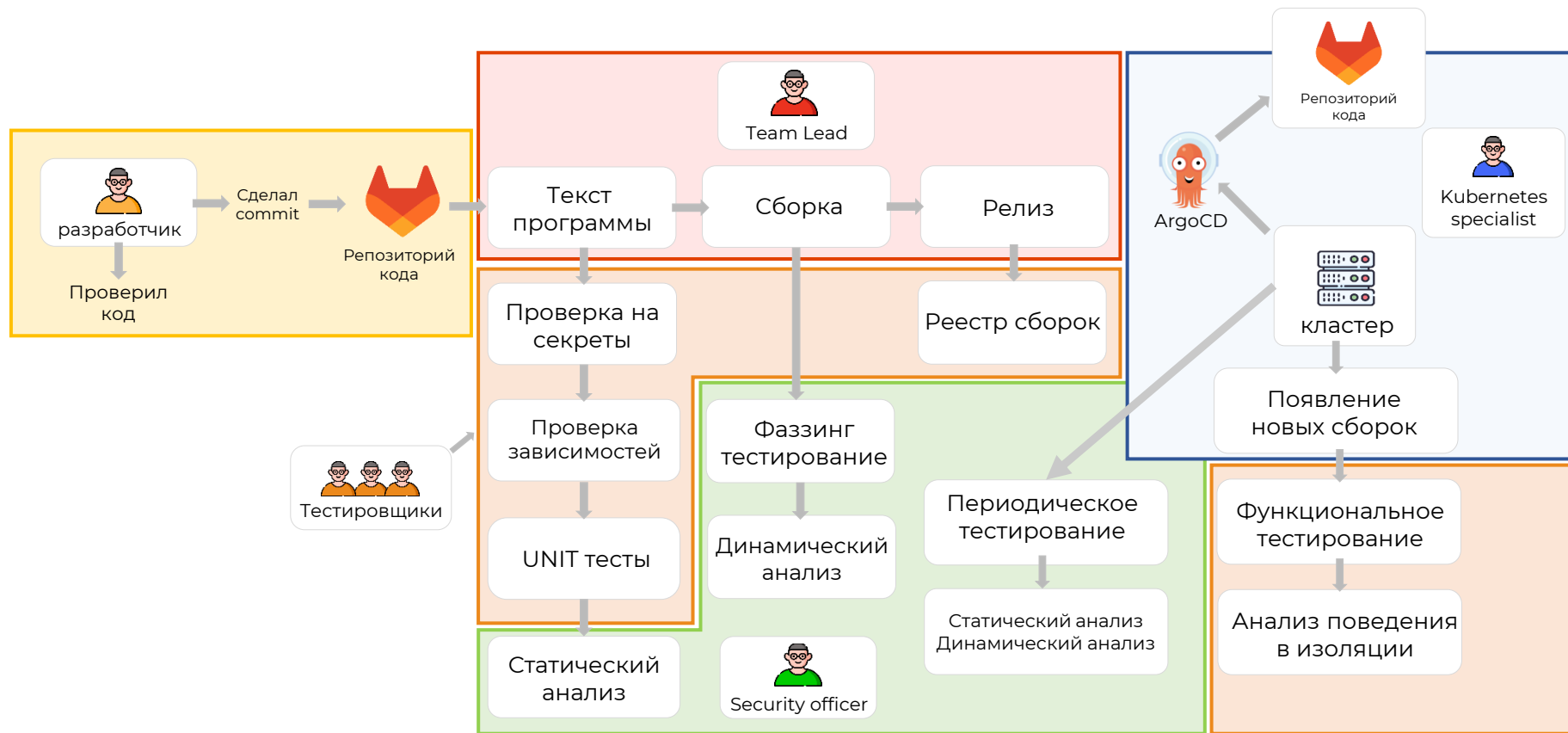
Формирование культуры информационной безопасности в команде



Применение принципа «безопасность по умолчанию»









## Легкий путь внедрения практик безопасной разработки

Комплексная система безопасной разработки **на основе популярных решений** с открытым исходным кодом

**Упрощённое внедрение** автоматического тестирования безопасности приложения (DAST, SAST, IAST, UNIT)

Возможность **гибкой подстройки** под ваши процессы

Материалы для формирования **культуры** безопасной разработки в комплекте

В комплекте документация по разработке безопасного ПО **в полном соответствии с ГОСТ Р 56939-2024**

По промокоду **rbpo\_2025** в течение месяца скидка 5% и бесплатная демонстрация продукта





## Затраты на устранение архитектурной уязвимости

## «Традиционная» разработка

**до ~30%**

от общей стоимости разработки

**~1-5%**

от общей стоимости разработки

Относительная стоимость  
исправления ошибки на  
разных этапах

\*NIST





Время реагирования на публикацию zero-day уязвимости

«Традиционная» разработка



На этапе сдачи проекта  
**по результатам утечки**

Разработка на безопасном конвейере



**от дня до месяца**



Время реагирования на проблемы  
в процессе разработки

«Традиционная» разработка



~~На сдаче-приёмке этапа работ~~  
**на этапе сдачи проекта**

Разработка на безопасном конвейере



**от дня до месяца**



Время, необходимое на сертификацию

«Традиционная» разработка



**7-8 месяцев,**

из которых непосредственно на  
испытания уходит 2-3 месяца

Разработка на безопасном конвейере



**3-4 месяца,**

из которых непосредственно на  
испытания уходит 1-2 недели





Система уже содержит необходимый набор инструментов и правильно сконфигурирована для реализации требований ГОСТ Р 56939 и лучших практик. Документация по РБПО в комплекте



Решение может поставляться как «железо», а может быть установлено в ваше корпоративное облако



Система гибкая. При необходимости можем подстроить под ваши существующие процессы разработки и орг.штат. структуру. Документацию тоже скорректируем



Осуществляем поддержку на всех этапах.



При необходимости можно делегировать часть задач нашим экспертам (написание документации, проведение тестов, SAST, DAST и пр.)



Сертификация



Подготовка к  
сертификации



Безопасная  
разработка ПО



Помощь в  
получении  
лицензий



Разработка и  
внедрение  
СМИБ, СМК



Аудит  
информационной  
безопасности



Аттестация



Проектирование  
комплексных  
СЗИ



Построение  
защищённых  
систем



Разработка ПО  
ИТ интеграция



Защита  
объектов КИИ



Защита ГИС



Защита  
персональных  
данных



Защита данных  
финансового  
сектора



Индивидуальные решения

# БЛАГОДАРИМ ЗА ВНИМАНИЕ!



InSeq.RBPO Легкий путь внедрения  
практик безопасной разработки



PVS-Studio 30 дней бесплатно по  
промокоду RBPO\_2025