KUPIBILET

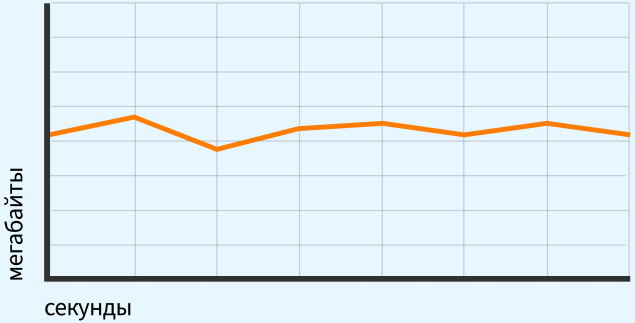
Избирательный подход к безопасности разработки в соответствии с бизнес-задачами

30

провайдеров опрашивает агентство, чтобы найти нужный билет

60

раз в секунду агентство опрашивает провайдеров



до 5мб

может занимать ответ провайдера

Смарт маршруты – это

- более 700 авиакомпаний
- 100 млрд. билетов
- на 30% дешевле
- выдача за 2 сек.

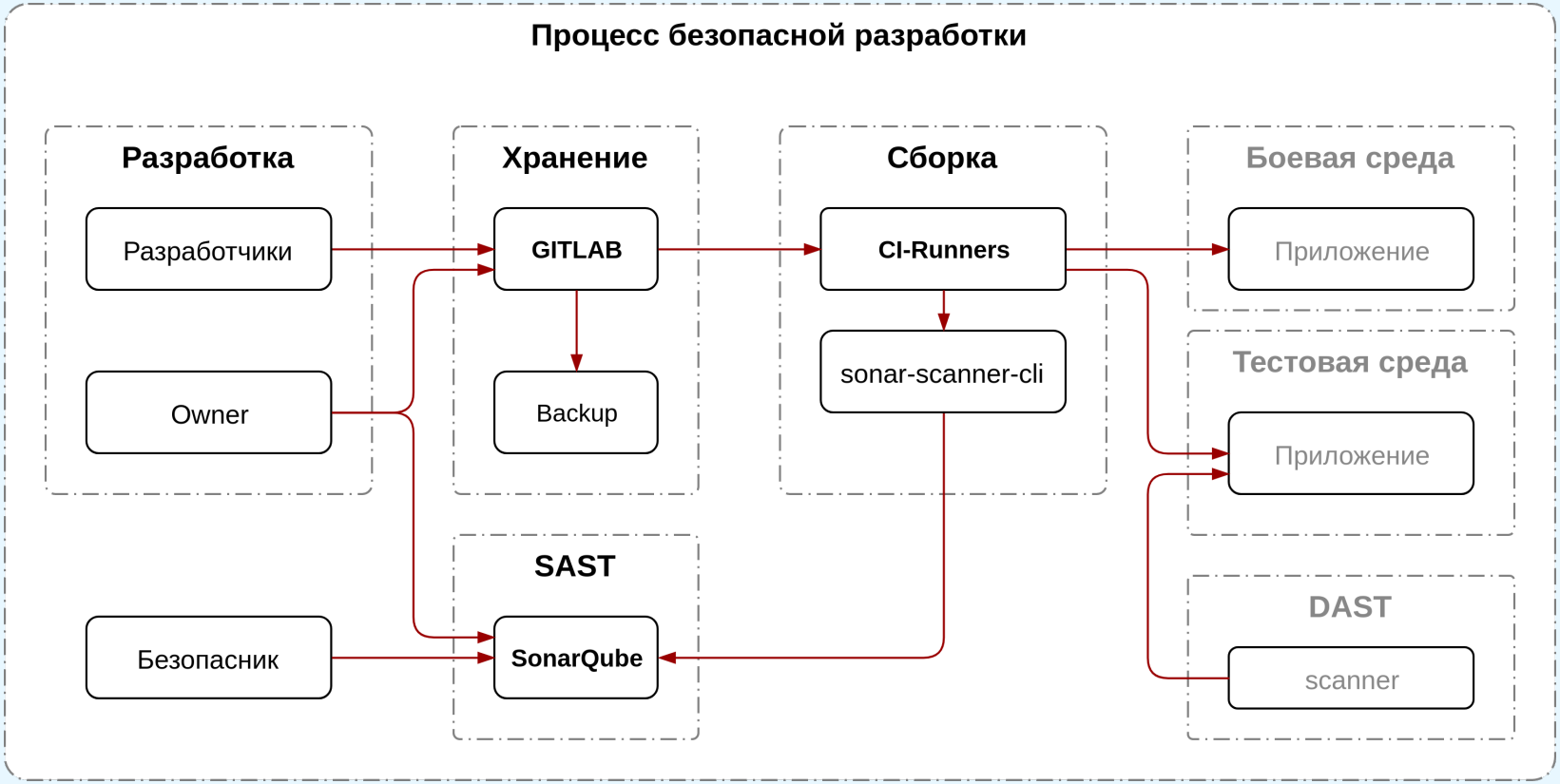
Процесс безопасной разработки

KUPIBILET

- **Разработка.** На данном этапе разработчики создают новый функционал, проверяют корректность его работы в среде разработки и сохраняют его в основной проект (commit) в GIT. Хорошим тоном является регулярное создание резервных копий репозитория, это позволяет снизить риск утраты важного актива.
- **Сборка.** После накопления необходимого количества изменений, по времени или по решению руководителя проекта в CI осуществляется сборка нового релиза проекта.
- **Контроль.** На данном этапе собранный релиз проекта отправляется на функциональное тестирование и проверку безопасности. Все тестовые испытания, обязательно, должны выполняться в тестовой среде и с использованием тестовых данных. По результатам тестирования формируется заключение о возможности промышленной эксплуатации новой версии программы.
- **Промышленная эксплуатация.** Если проект успешно прошел все проверки, тогда он передается в промышленную эксплуатацию. Т.е. выпускается новая версия программы.

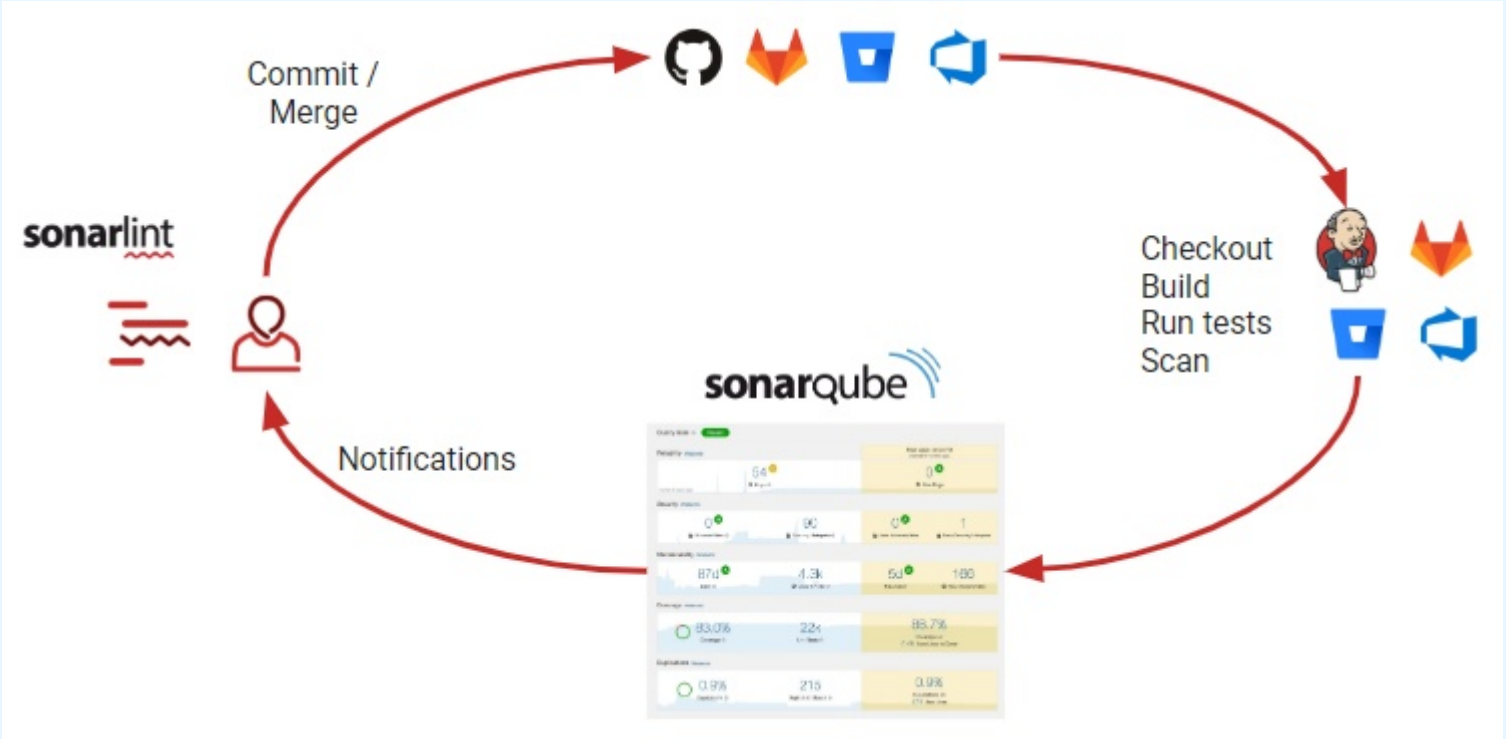
Общая схема

KUPIBILET



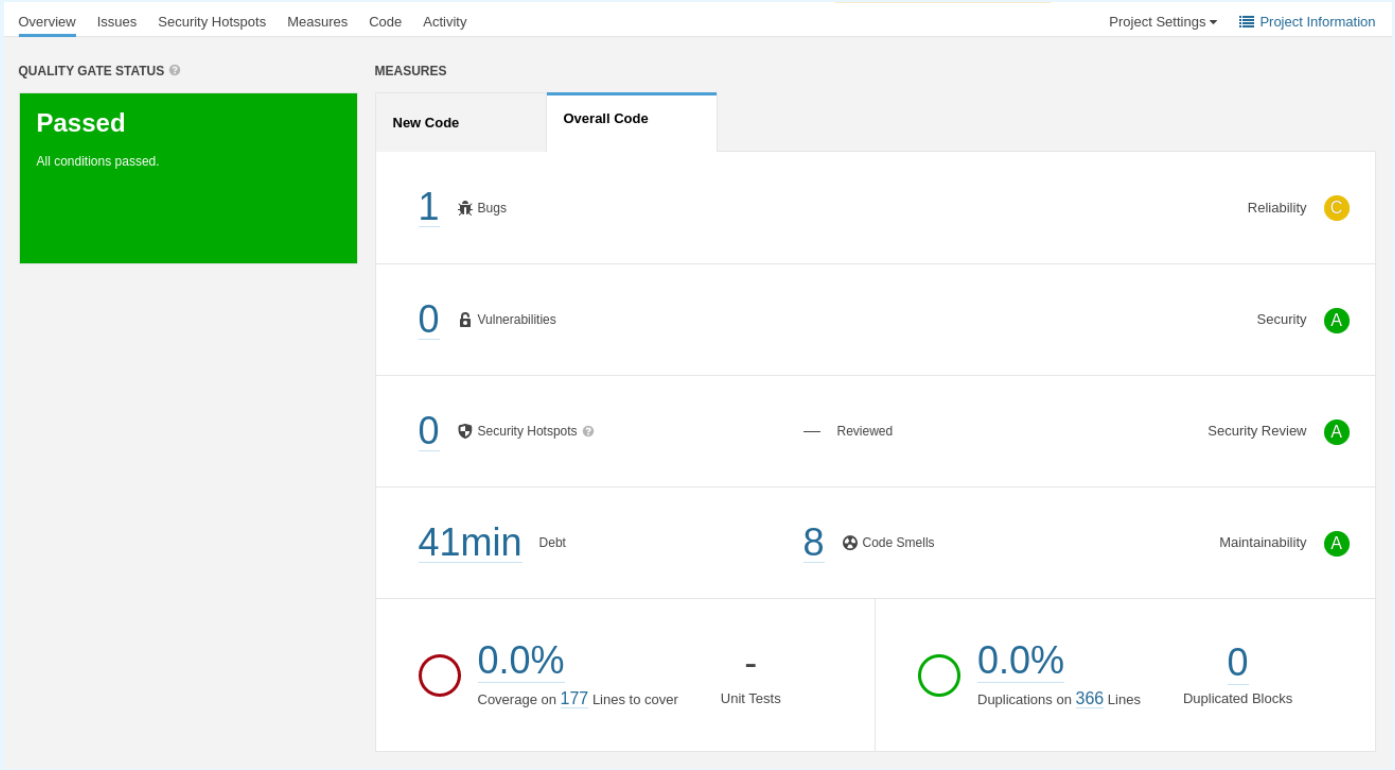
Пример реализации процесса безопасной разработки

KUPIBILET



Внедрение: Результат проверки

KUPIBILET



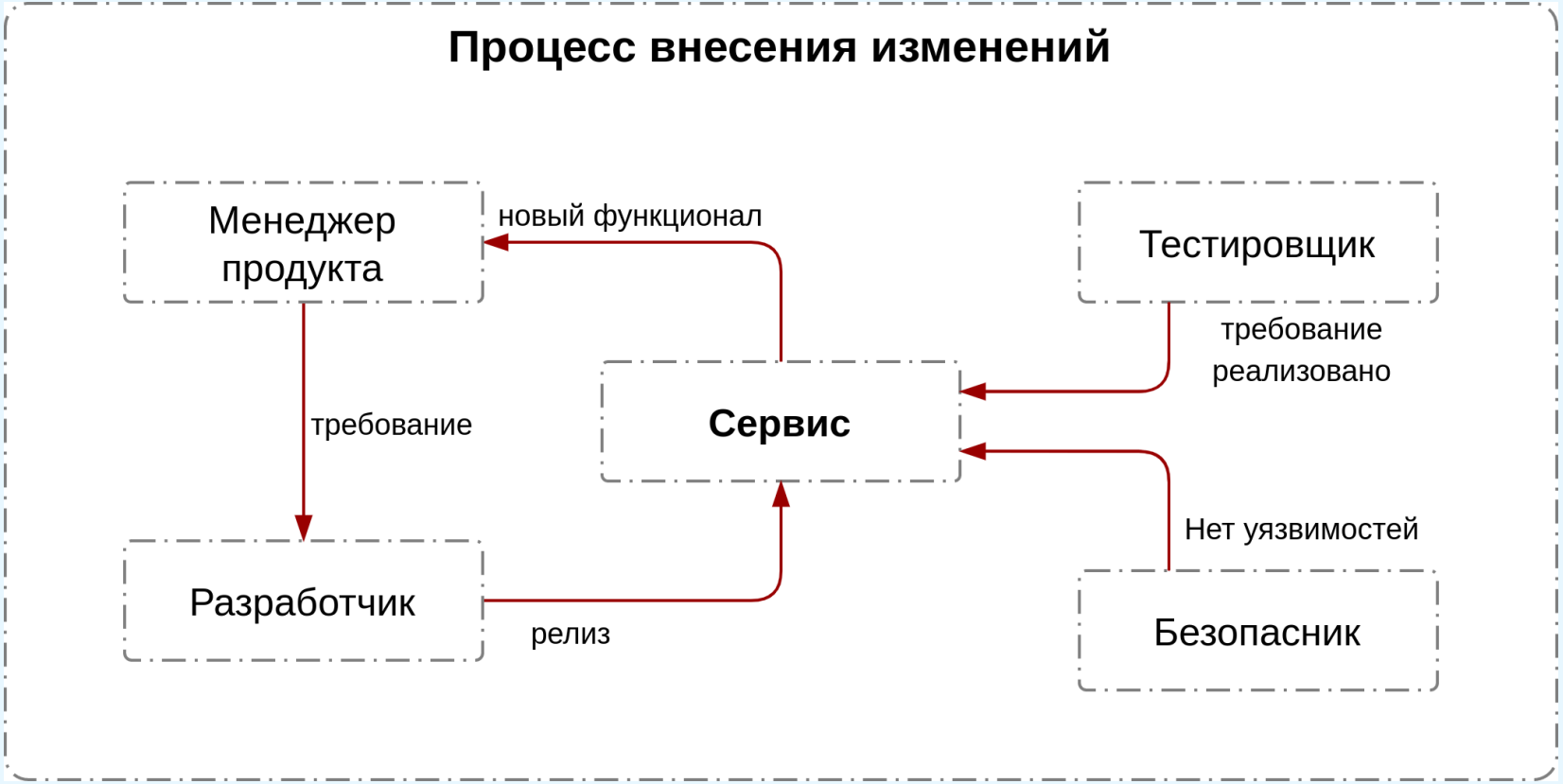
Участники процесса

KUPIBILET

Участник	Что делает	Цель
Менеджер продукта	Комплексный анализ рынка, продукта, конкурентов	Продукт должен быть конкурентным и приносить прибыль
Разработчик	Внедрение нового функционала и продукт	Реализовать требуемый функционал с минимальными затратами
Тестировщик	Проверка работоспособности продукта	Убедиться, что реализованный функционал соответствует требованиям
Безопасник	Проверка безопасности продукта	Убедиться в отсутствии уязвимостей в продукте

Конфликт интересов

KUPIBILET



Стандартный флоу изменения в продукте

KUPIBILET

1 Менеджер по продукту формулирует новое требование

2 Разработчик реализует новое требование и готовит релиз продукта

3 Новый релиз поступает на проверку безопасности, которая может быть реализована

3.1 В разрез

3.2 Постфактум

4 Новый релиз поступает на проверку качества, которая показывает корректность реализации требования.

5 Если все проверки прошли успешно, то релиз продукта, соответствующий новым требованиям поступает, в промышленную эксплуатацию.

Возможные сценарии: АСАП

KUPIBILET

Условия:

1. Утрата конкурентных преимуществ

2. Нарушение работы функционала, приносящего прибыль

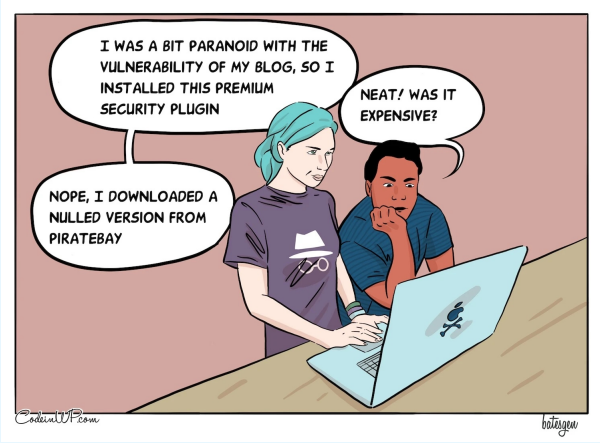
Возможные сценарии: Уязвимость

KUPIBILET

Условия:

1. Обнаружен риск утечки данных клиентов

2. Обнаружена уязвимость, реализация которой может привести к финансовым потерям



Изменения в процессе

KUPIBILET

Такие доработки реализуются с наивысшим приоритетом. Разработчики приступают незамедлительно.

Из проверок остаются:

Codereview — другие разработчики просматривают новый код.

Проверка качества — для подтверждения того, что было сделано именно то, что планировалось.

Проверка безопасности выполняется постфактум.

Thank you

Беляков Игорь
Belyakov.Igor@kupibilet.ru
+7 921 3089713

KUPIBILET