Microsoft

DevCon School

Технологии будущего

DevCon School
Технологии будущего

Построение процессов безопасной разработки

Алексей Жуков, Рами Мулейс
Positive Technologies

Цели

Безопасность?

Что такое (не)безопасный код?

Как найти уязвимость?

Вы узнаете это

А как ее не допустить?

Не допустить — ~~легче~~ дешевле, чем устранить

Уязвимости кода

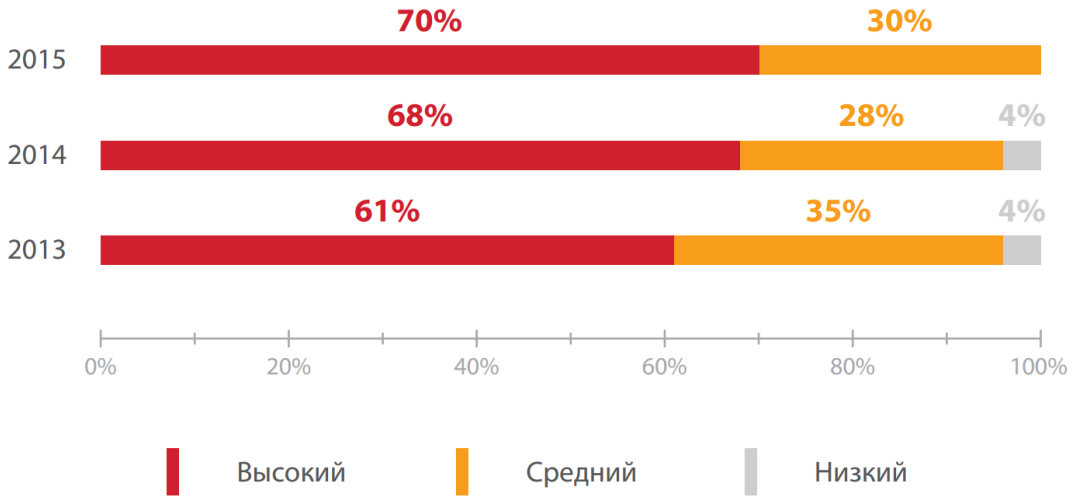
Что это? Они опасны? Чем?

#msdevcon

DevCon School
Технологии будущего

Уязвимость — это серьёзно

- Негативные тенденции роста числа уязвимостей:
  - Треть уязвимостей — критические, их доля растет
  - Две трети уязвимостей вызваны ошибками разработчика
- Никто не застрахован (утечки в DLH.net и поддоменах Mail.RU)
  - Уязвимость в фреймворках → уязвимость множества приложений



Отчет «Уязвимости веб-приложений» (Positive Technologies, 2016)

SQLi и с чем его едят

```
SQL = "SELECT cname FROM emp WHERE id = '" + ID + "'";
```

ID:	SQL:
Вася	`SELECT cname FROM emp WHERE id = 'Вася'`
Вася' OR 1 = 1 --	`SELECT cname FROM emp WHERE id = 'Вася' OR 1 = 1 -- '`

PT AI —реальная возможность создания **собственной** команды «белых шляп»

POSITIVE TECHNOLOGIES

(Совсем) немного теории

- Принципы:
  - уязвимости, точки входа/выхода, эксплойты
  - false positive
- Пример:

```
if (3 == 2 + 2) { // Код в {…} не вызывается, уязвимость ли это?
    String ID = request.getParameter("id");
    String SQL = "SELECT cname FROM emp WHERE id = '" + ID + "'";
    ResultSet RES = DB.createStatement().executeQuery(SQL);
}
```

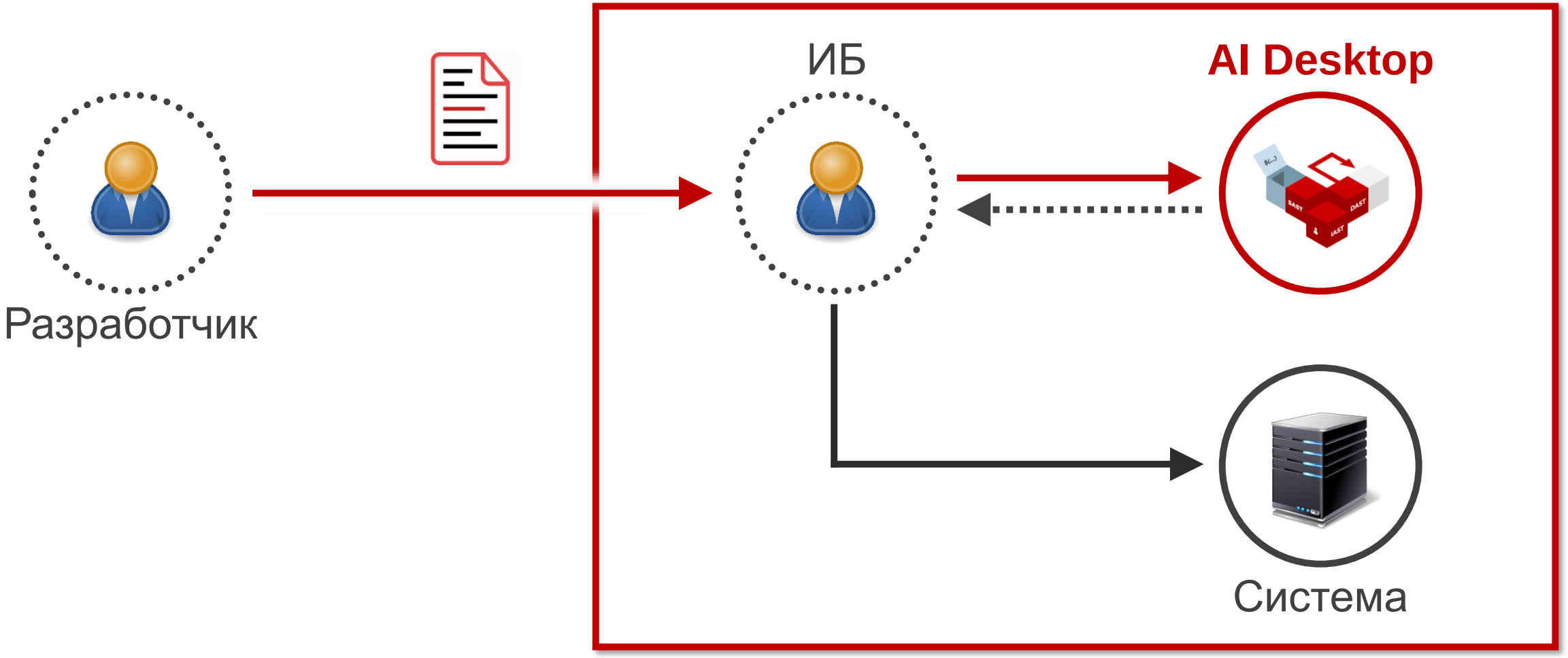
~~http://host/App?id=1' OR 1=1 --~~

⚠ ~~**SQL Injection**~~

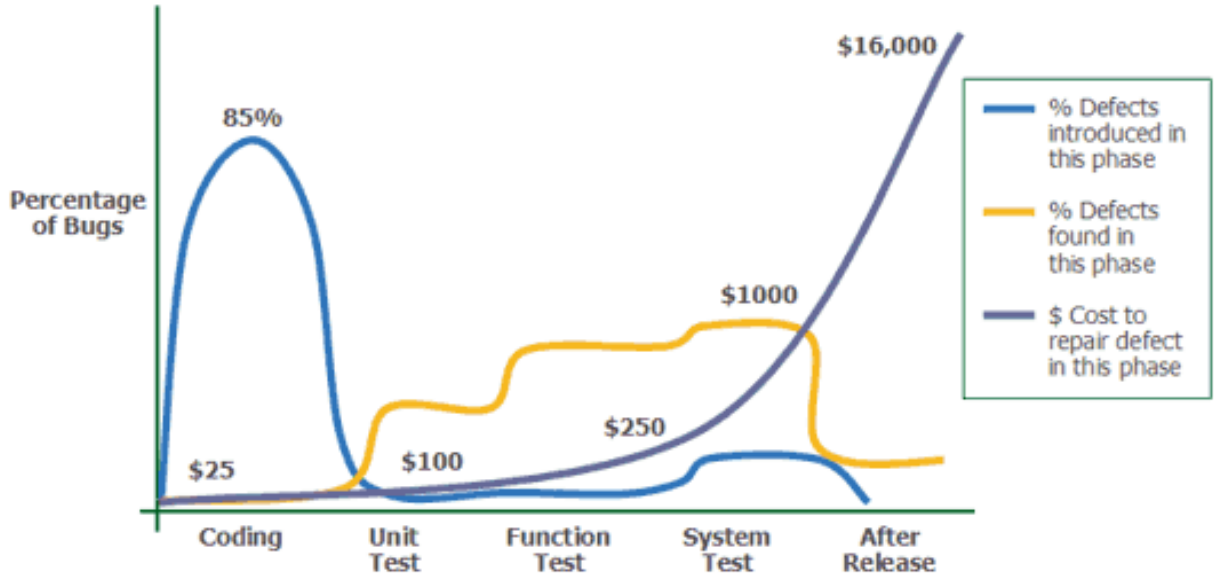
PT Application Inspector — варианты использования

POSITIVE TECHNOLOGIES

Вариант 1: «Приемка кода»



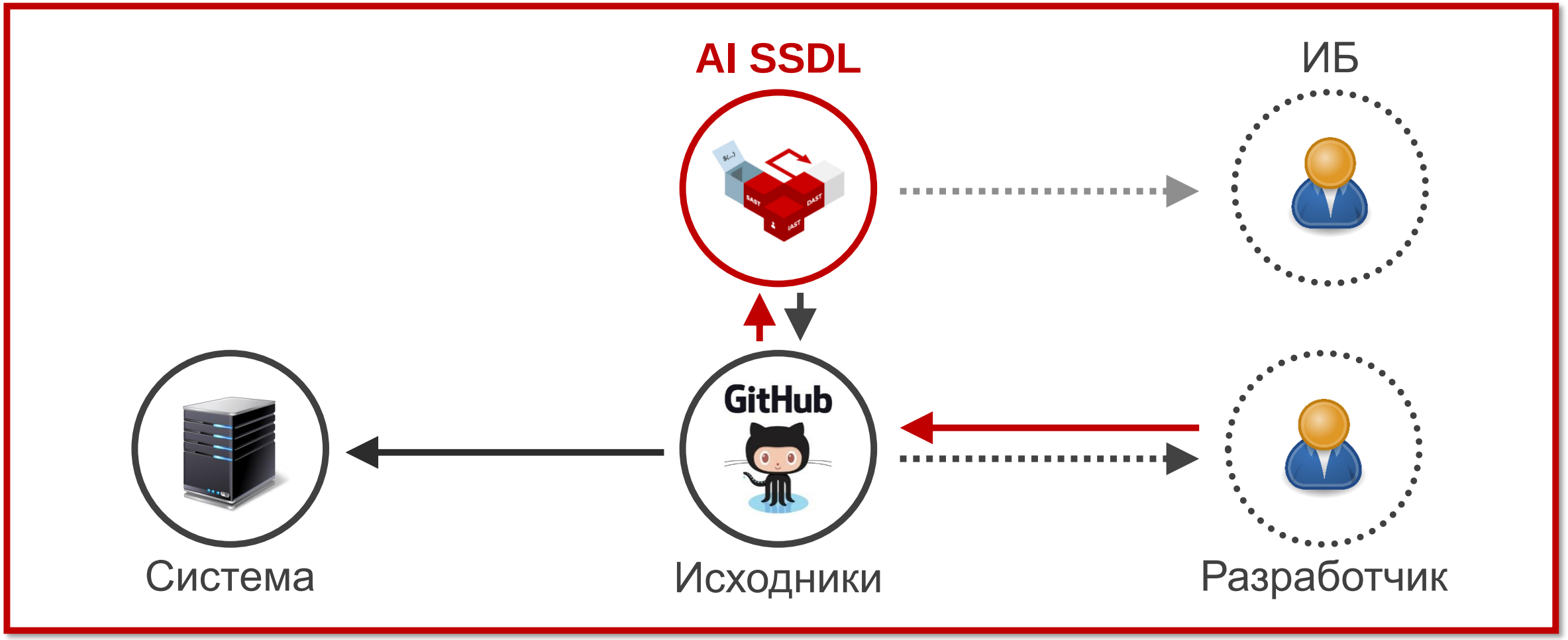
Разработка — экономика



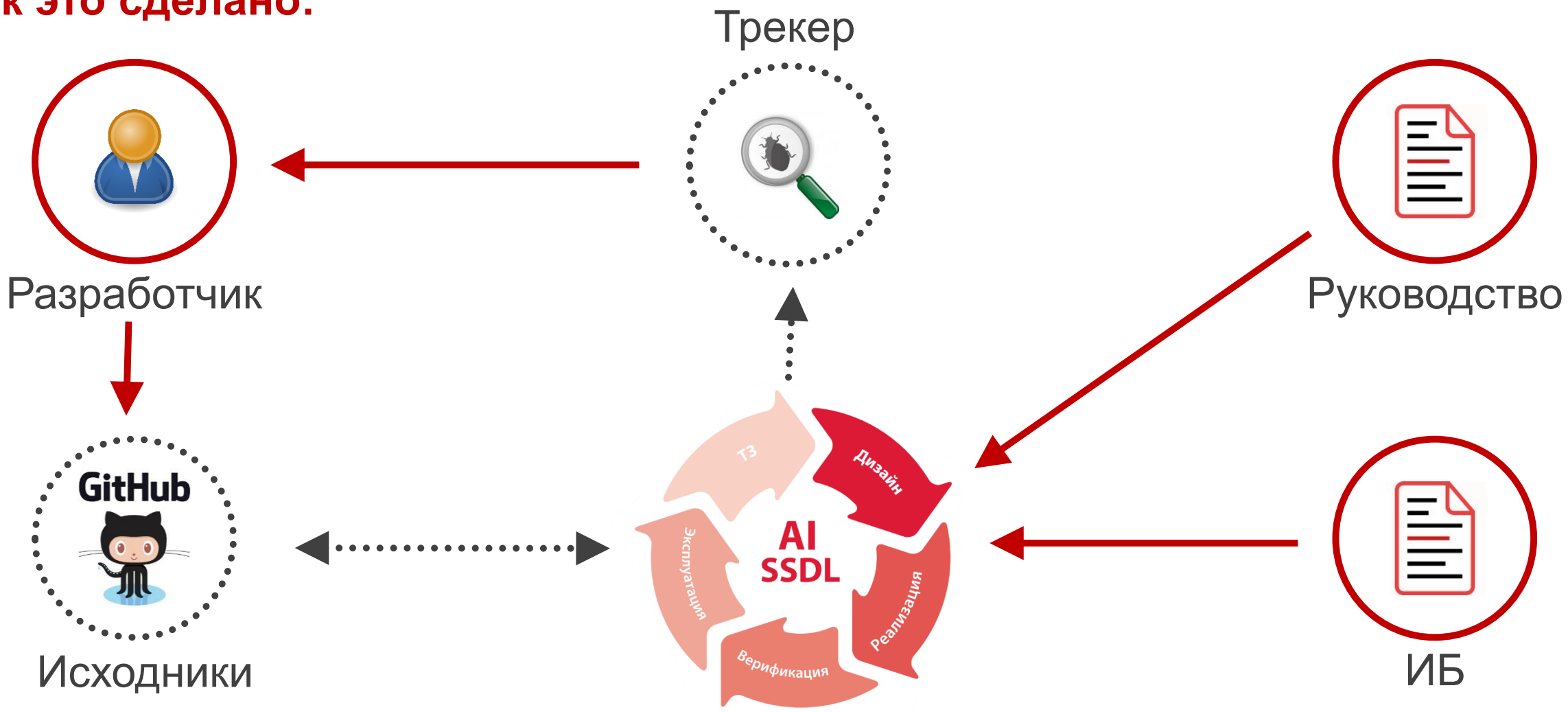
- Applied Software Measurement (Capers Jones, 1996)
- Software Engineering Economics (Barry W. Boehm, 1983)
- Кратность роста стоимости изменений — от ×4 до ×100(!)

Выход — выявление дефектов ПО на ранних стадиях разработки и методологии непрерывной интеграции Agile/DevOps

Вариант 2: «Встраивание в разработку»



Как это сделано:



Демонстрация

Сканирование кода

Desktop и SSDL

#msdevcon

DevCon School
Технологии будущего

Практика

Устранение уязвимостей

https://github.com/ptssdl/DevCon.2017.XX

https://goo.gl/VzEtiv

#msdevcon

DevCon School
Технологии будущего

Отзывы

Помогите нам стать лучше!

На вашу почту отправлена индивидуальная ссылка на электронную анкету. 3 июня в 23:30 незаполненная анкета превратится в тыкву.

Заполните анкету и подходите к стойке регистрации за приятным сюрпризом!

#msdevcon

Оставляйте отзывы в социальных сетях. Мы все читаем. Спасибо вам! ☺

DevCon School
Технологии будущего

Q&A

Построение процессов безопасной разработки

Алексей Жуков, Рами Мулейс
Positive Technologies

#msdevcon

DevCon School
Технологии будущего