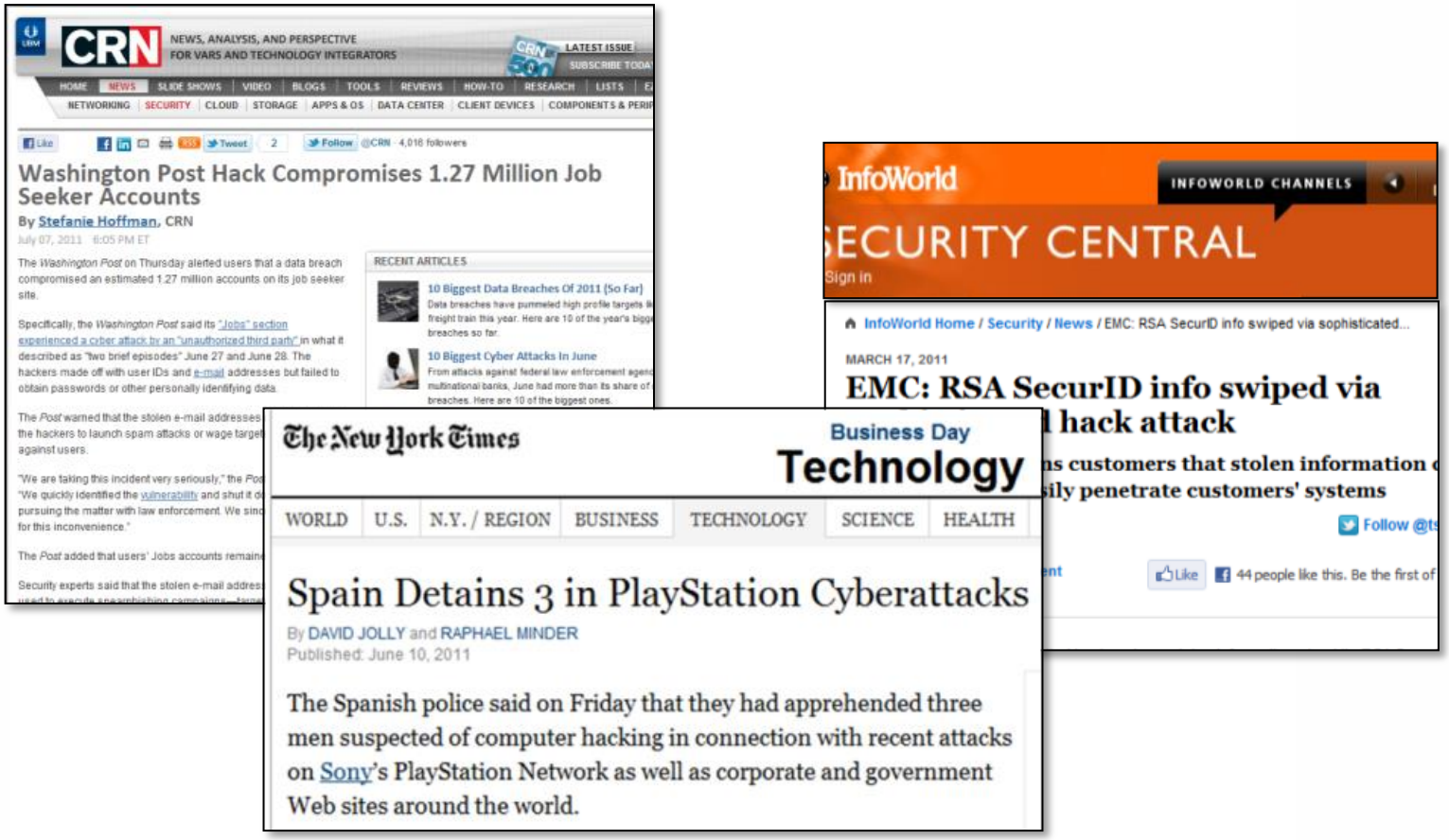
Анализ прикладного ПО для снижения рисков ИБ, связанных с его использованием

Жуков А.Н.

Рост киберпреступности



ЭЛВИС-ПЛЮС

Почему прикладное ПО?

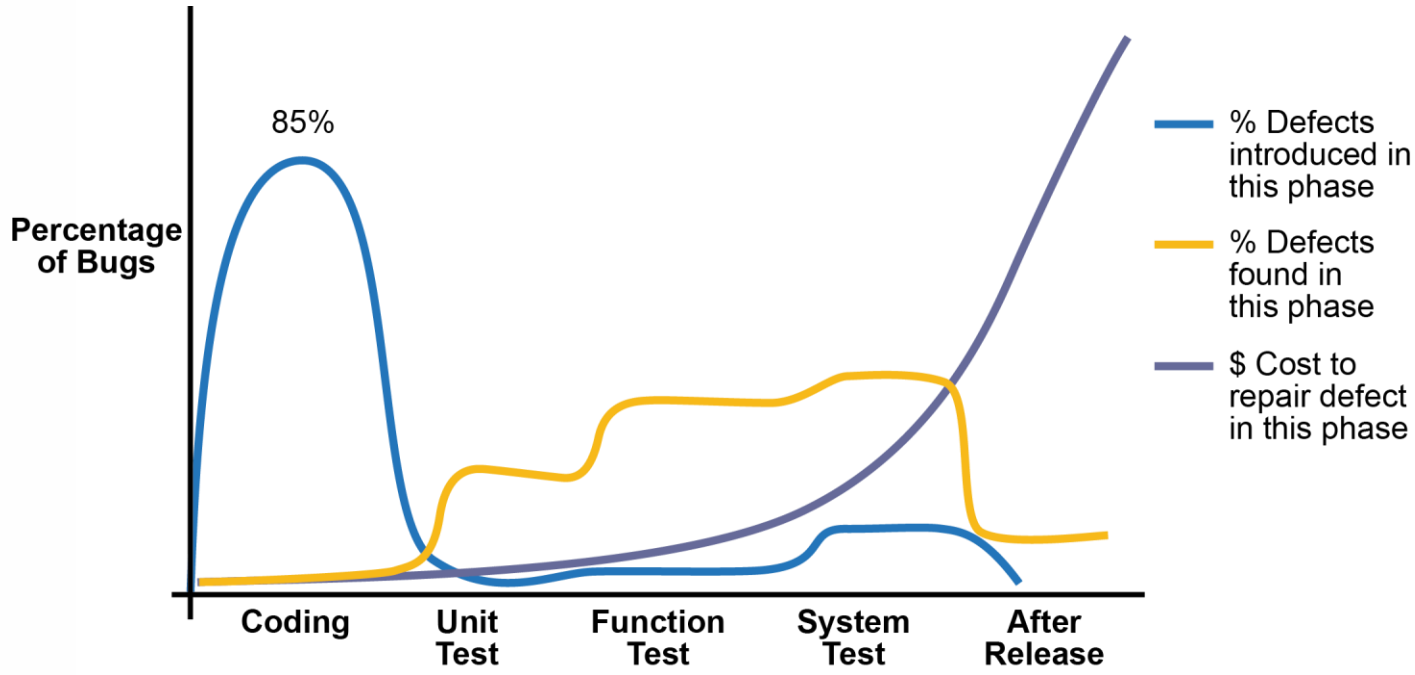
- **По оценкам аналитиков:**
  - Gartner – 75% проникновений вызваны дефектами ПО
  - NIST – 92% уязвимостей находятся в ПО
  - RSA 2013 – 86% успешных проникновений осуществляются на прикладном уровне
  - Cenzic – 99% веб-приложений являются уязвимыми
- **При этом, 90% затрат на безопасность относятся к защите периметра**

Ошибки и уязвимости в ПО - экономический аспект

- **IBM/Rational:**
  - 80% затрат на разработку приходится на выявление и исправление дефектов;
  - Этапы (данные 2008 года):
    - Определение требований – $80/дефект;
    - Проектирование - $240/дефект;
    - QA - $960/дефект;
    - Выпуск продукта - $7600/дефект;
- **Forrester:**
  - 1× - 5× - 10× - 15× - 30×

Когда?

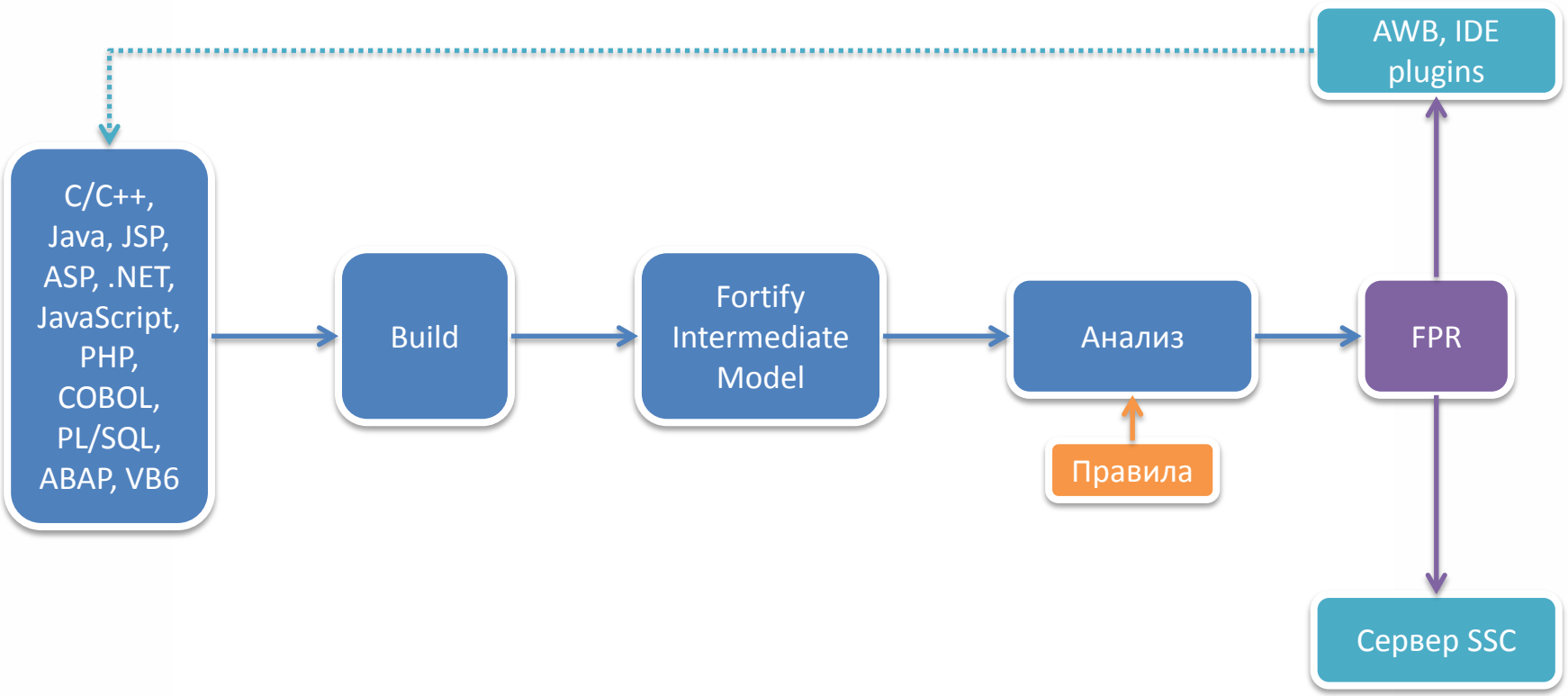
Чем раньше, тем лучше:



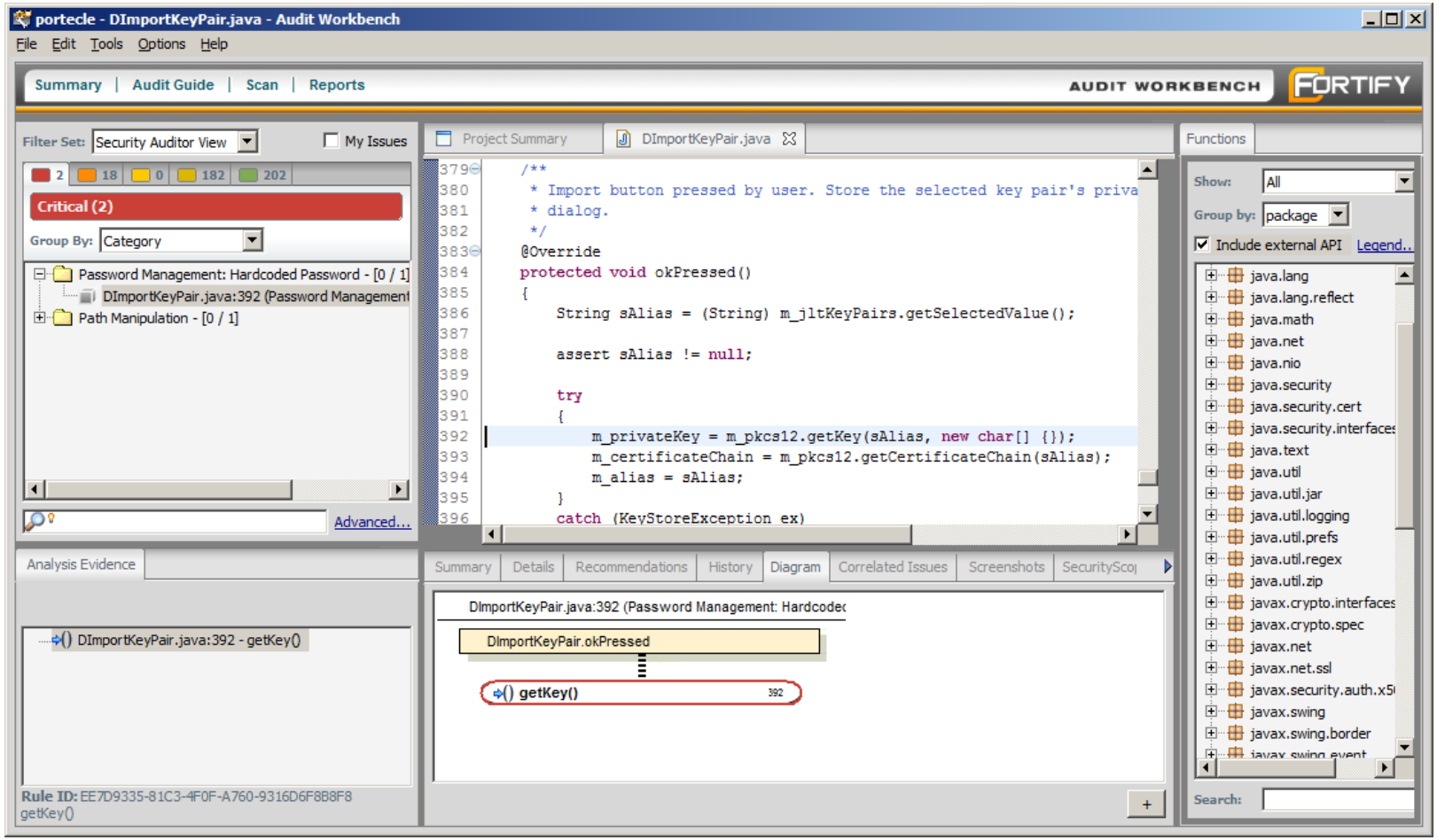
Анализ ПО – предлагаемые подходы

- **HP Fortify:**
  - Статический анализ кода;
  - Встраивание в SDLC
- **Defensics:**
  - Фаззинг (fuzzing) – тестирование на основе ввода неверных данных

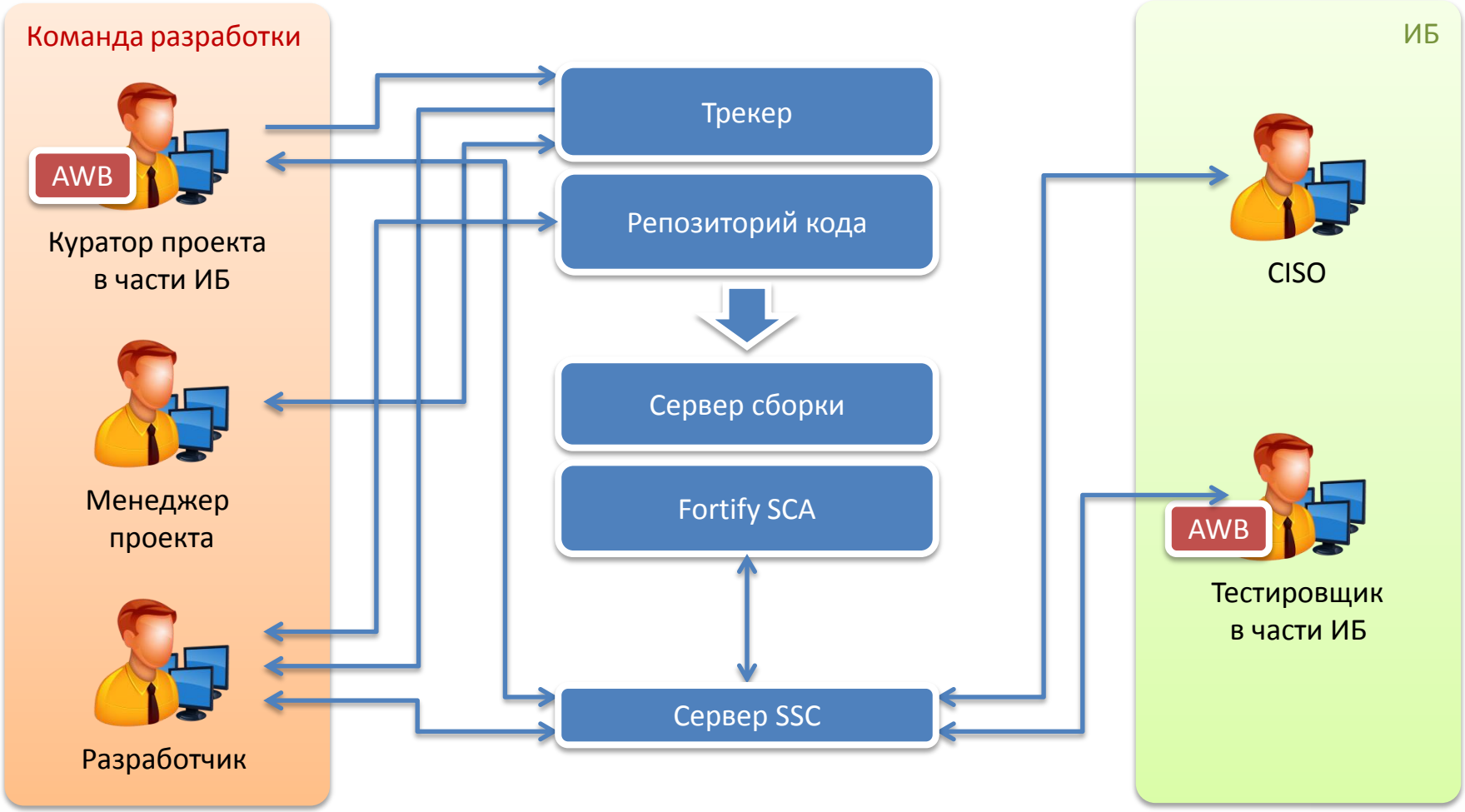
Статический анализ кода - архитектура



AWB - как это выглядит?



Статический анализ кода – встраивание в разработку



Fuzzing

- **Что это?**
  - Тестирование на основе ввода неверных данных;
- **Преимущества:**
  - Имитация реальных угроз;
  - Выявление 0-day уязвимостей;
  - Проверка надежности перед вводом в промышленную эксплуатацию;

ЭЛВИС-ПЛЮС

Defensics Codenomicon

- **Большое количество поддерживаемых сетевых протоколов**
  - Более 200;
  - Могут быть расширены;
- **Основа модулей - модели:**
  - Пакеты тестирования основаны на моделях протоколов;
  - Автоматическое создание сценариев;
- **Быстрота тестирования**
  - Тысячи сценариев в секунду;
- **Автоматическое формирование отчетов**

Ваши вопросы?

Жуков А.Н.