

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

Жуков А.Н.



# Рост киберпреступности

**CRN** NEWS, ANALYSIS, AND PERSPECTIVE FOR VAR'S AND TECHNOLOGY INTEGRATORS

HOME NEWS SLIDE SHOWS VIDEO BLOGS TOOLS REVIEWS HOW-TO RESEARCH LISTS E

NETWORKING SECURITY CLOUD STORAGE APPS & OS DATA CENTER CLIENT DEVICES COMPONENTS & PERIF

Like Follow @CRN - 4,016 followers

## Washington Post Hack Compromises 1.27 Million Job Seeker Accounts

By **Stefanie Hoffman**, CRN

July 07, 2011 8:05 PM ET

The Washington Post on Thursday alerted users that a data breach compromised an estimated 1.27 million accounts on its job seeker site.

Specifically, the Washington Post said its "Jobs" section experienced a cyber attack by an "unauthorized third party" in what it described as "two brief episodes" June 27 and June 28. The hackers made off with user IDs and e-mail addresses but failed to obtain passwords or other personally identifying data.

The Post warned that the stolen e-mail addresses could be used by hackers to launch spam attacks or wage targeted attacks against users.

"We are taking this incident very seriously," the Post said. "We quickly identified the vulnerability and shut it off, and we are pursuing the matter with law enforcement. We sincerely apologize for this inconvenience."

The Post added that users' Jobs accounts remain unaffected.

Security experts said that the stolen e-mail addresses could be used to launch targeted attacks against users.

**RECENT ARTICLES**

- 10 Biggest Data Breaches Of 2011 (So Far)  
Data breaches have pummeled high profile targets like the freight train this year. Here are 10 of the year's biggest breaches so far.
- 10 Biggest Cyber Attacks In June  
From attacks against federal law enforcement agencies to multinational banks, June had more than its share of breaches. Here are 10 of the biggest ones.

**InfoWorld** INFOWORLD CHANNELS

## SECURITY CENTRAL

Sign in

InfoWorld Home / Security / News / EMC: RSA SecurID info swiped via sophisticated...

MARCH 17, 2011

### EMC: RSA SecurID info swiped via sophisticated hack attack

EMC's customers that stolen information could be used to easily penetrate customers' systems

Like Follow @InfoWorld

44 people like this. Be the first of...

**The New York Times** Business Day Technology

WORLD U.S. N.Y. / REGION BUSINESS TECHNOLOGY SCIENCE HEALTH

## Spain Detains 3 in PlayStation Cyberattacks

By **DAVID JOLLY** and **RAPHAEL MINDER**

Published: June 10, 2011

The Spanish police said on Friday that they had apprehended three men suspected of computer hacking in connection with recent attacks on Sony's PlayStation Network as well as corporate and government Web sites around the world.



## 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**



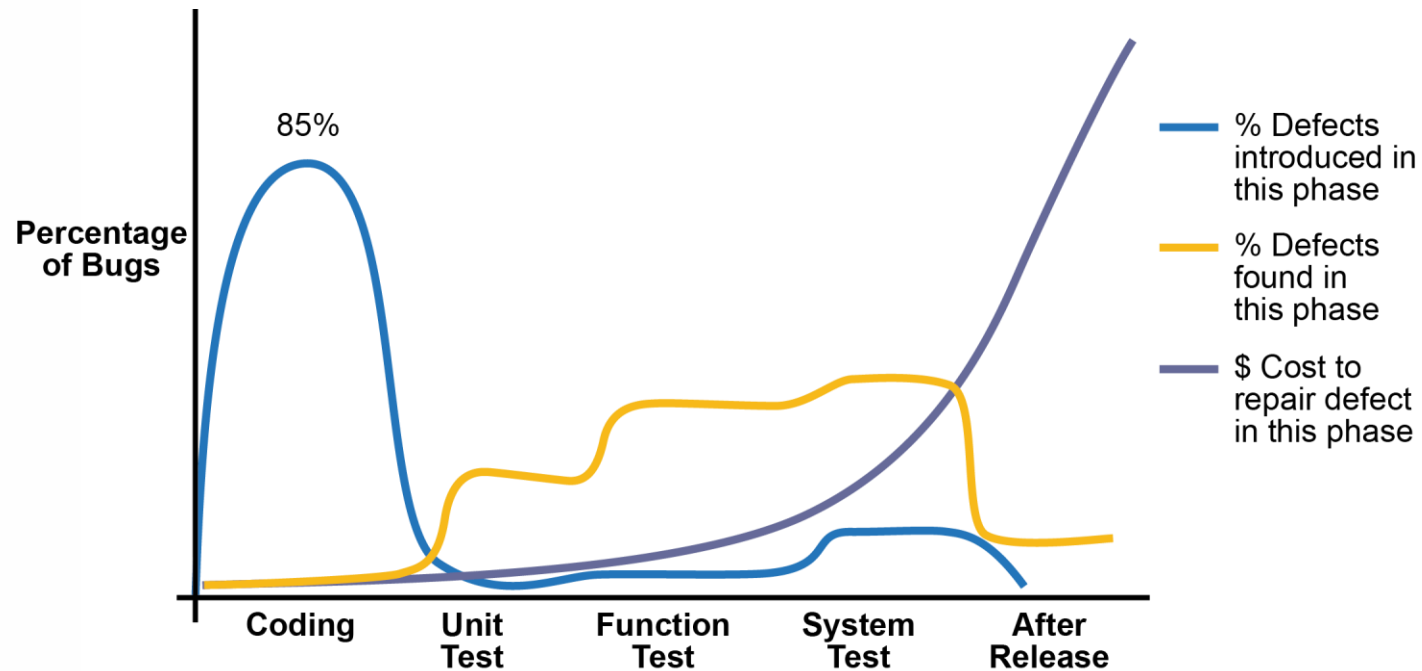
## Ошибки и уязвимости в ПО - экономический аспект

- **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:**
  - 1x - 5x - 10x - 15x - 30x



# Когда?

Чем раньше, тем лучше:





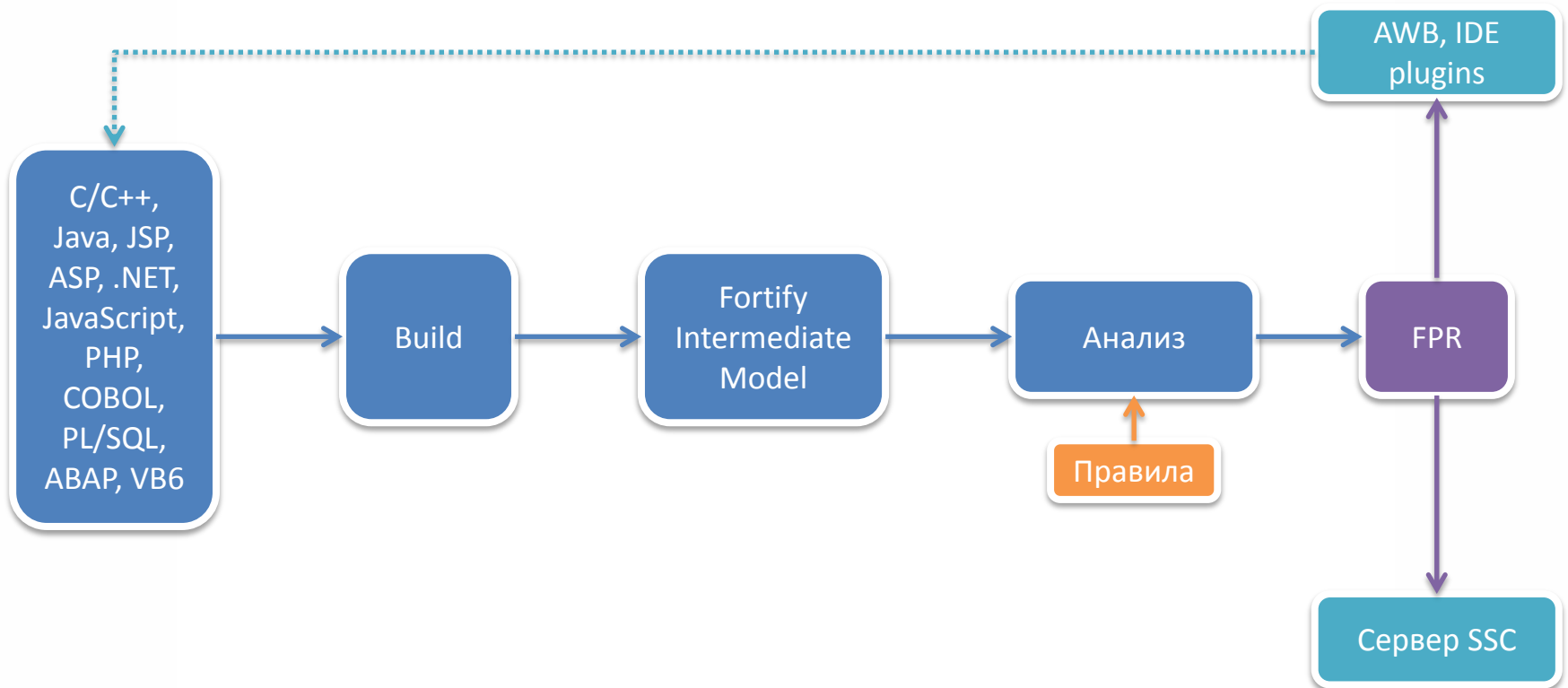
## Анализ ПО – предлагаемые подходы

- **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?

The screenshot displays the Fortify Audit Workbench (AWB) interface. The main window is titled "portecle - DImportKeyPair.java - Audit Workbench". The top menu bar includes "File", "Edit", "Tools", "Options", and "Help". The main toolbar shows "Summary", "Audit Guide", "Scan", and "Reports". The "AUDIT WORKBENCH" and "FORTIFY" logos are visible in the top right.

The left sidebar shows a "Filter Set" of "Security Auditor View" and a "My Issues" checkbox. Below this, there are issue counts: 2 Critical, 18 High, 0 Medium, 182 Low, and 202 Info. A "Group By" dropdown is set to "Category". The issue list shows "Password Management: Hardcoded Password - [0 / 1]" and "DImportKeyPair.java:392 (Password Management)".

The central code editor shows the following code snippet:

```
379  /**
380   * Import button pressed by user. Store the selected key pair's private key
381   * dialog.
382   */
383  @Override
384  protected void okPressed()
385  {
386      String sAlias = (String) m_jltKeyPairs.getSelectedValue();
387
388      assert sAlias != null;
389
390      try
391      {
392          m_privateKey = m_pkcs12.getKey(sAlias, new char[] {});
393          m_certificateChain = m_pkcs12.getCertificateChain(sAlias);
394          m_alias = sAlias;
395      }
396      catch (KeyStoreException ex)
```

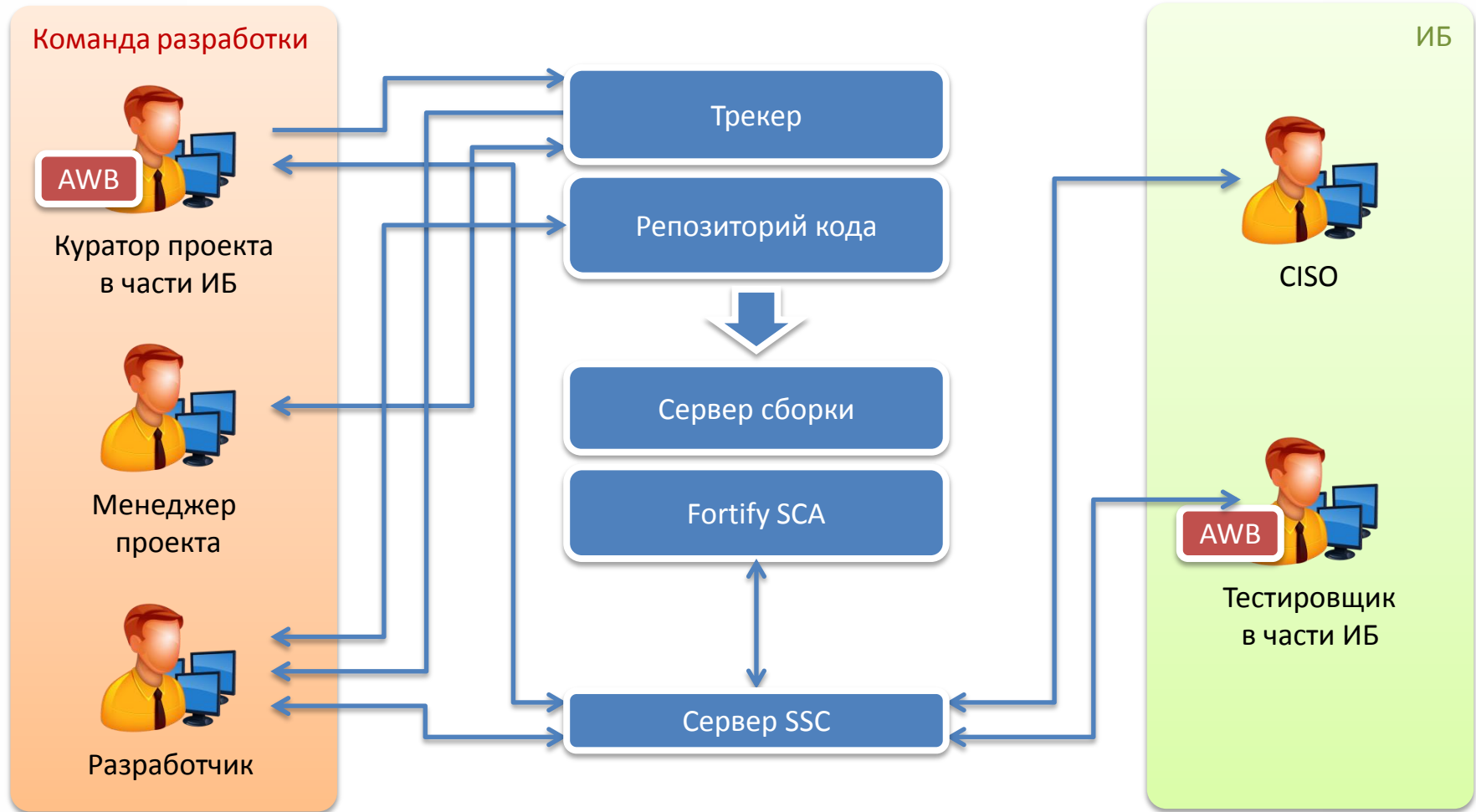
The line 392 is highlighted in blue, indicating a vulnerability. The right sidebar shows a "Functions" panel with a "Show:" dropdown set to "All" and a "Group by:" dropdown set to "package". A list of Java packages is shown, including java.lang, java.lang.reflect, java.math, java.net, java.nio, java.security, java.security.cert, java.security.interfaces, java.text, java.util, java.util.jar, java.util.logging, java.util.prefs, java.util.regex, java.util.zip, javax.crypto.interfaces, javax.crypto.spec, javax.net, javax.net.ssl, javax.security.auth.x500, javax.swing, javax.swing.border, and javax.swing.event.

The bottom section shows "Analysis Evidence" with a search bar and a list of issues. The "Summary" tab is active, showing a call stack diagram for "DImportKeyPair.java:392 (Password Management: Hardcoded)". The call stack shows "DImportKeyPair.okPressed" calling "getKey()", which is highlighted in red.

The bottom left corner displays the "Rule ID: EE7D9335-81C3-4F0F-A760-9316D6F8B8F8" and the rule name "getKey()".



# 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;





## 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.