ITGuard

Дистрибуция средств защиты информации

Контроль уязвимостей в банковских приложениях

к.ф.-м.н. Катерина Трошина

Москва, 2013 г.

IT Guard

План

- Особенности банковских приложений с точки зрения ИБ (информационной безопасности)
- Особенности разработки банковских приложений
- Современные методы и технологии повышения качества разработки и анализа приложений по требования информационной безопасности

Особенности банковских приложений с точки зрения ИБ (информационной безопасности)

- Интернет везде!
  - Интернет-банк
  - Мобильный банк
- Конкурентные преиму
  - Объем функционала, ко ся через Интернет
  - Надежность и защищенность

НЕ К

Cyber Crime

Финансовые потери от Cyber Crime по данным Ponemon Institution выросли на 30% за 2010-2012 гг.

Злоумышленники используют более «хитрые уязвимости»: их навыки и умения постоянно растут и совершенствуются!

IT Guard

План

- Особенности банковских приложений с точки зрения ИБ (информационной безопасности)
- **Особенности разработки банковских приложений**
- Современные методы и технологии повышения качества разработки и анализа приложений по требования информационной безопасности

Особенности разработки банковских приложений

Разработчики – это ЛЮДИ!!!

КОМАНДА

Особенности разработки банковских приложений

Разработчики - это наемные работники!

- Они уходят!
- Их МАЛО!
- Разработчику нужны **комфортные условия** и возможность РАЗВИВАТЬСЯ!

Разработчик – НЕ эксперт по информационной безопасности

Особенности разработки банковских приложений

Типичный г команды

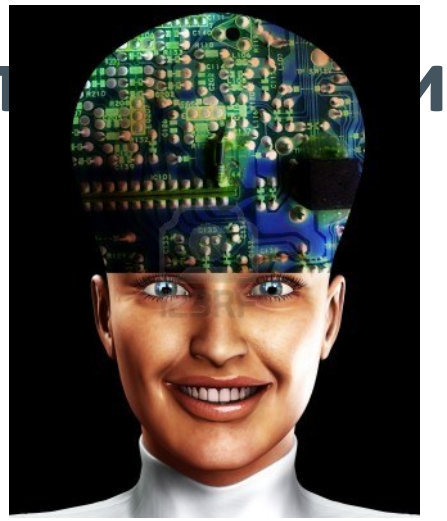
Особенности разработки банковских приложений

Современное программное обеспечение сегодня:

- Многоязычное
- Мультиплатформенное
- Связи между компонентами – очень сложные!

Банковские п ия

- **УЯЗВИМЫЕ!!!**



IT Guard

Откуда берутся уязвимости

- Культура разработки – разработчик не уделяет внимания:
  - Языковым конструкциям, которые использует
  - Коду, который используется как сторонний
  - Безопасности связей между компонентами, которые разрабатывает
- Недостаток времени:
  - Техническое задание разрабатывается быстро
  - Программное обеспечение разработается быстро: **задержка в разработке – потеря денег**

- Можно удовлетворить только **два** из трех желаний: быстро, качественно и недорого.

Обычно – это **быстро и недорого**.

Где взять безопасное ПО?

- Если ПО разрабатывается самостоятельно:
  - Дружите с р овать «Правильно
  - Проверяйте апуском в эксплуатаци
- Если ПО стор
  - проверяйте внедрением!

Не эксплуатируйте кота в мешке!!!

IT Guard

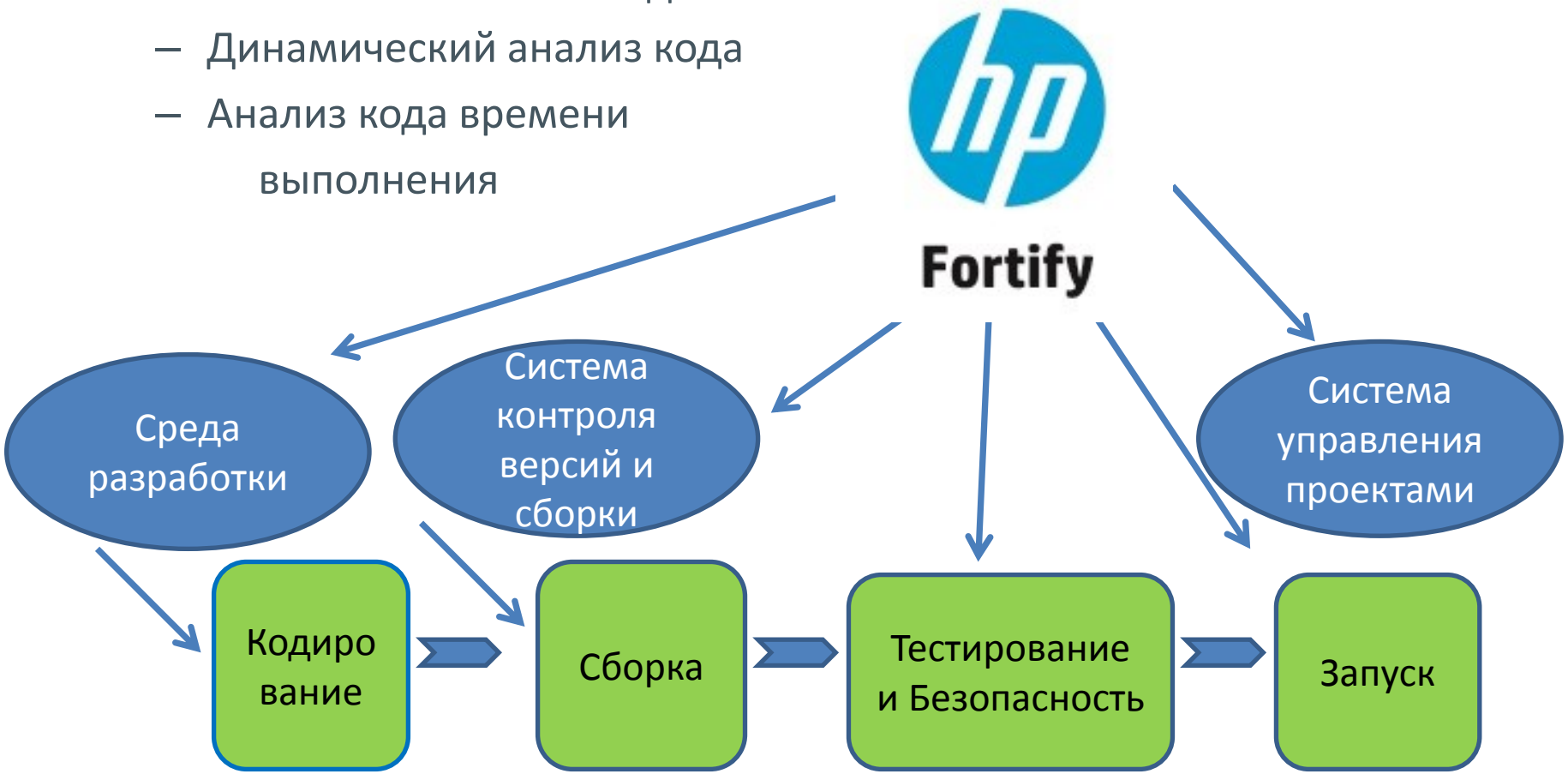
План

- Особенности банковских приложений с точки зрения ИБ (информационной безопасности)
- Особенности разработки банковских приложений
- **Современные методы и технологии повышения качества разработки и анализа приложений по требования информационной безопасности**

Повышение качества разработки

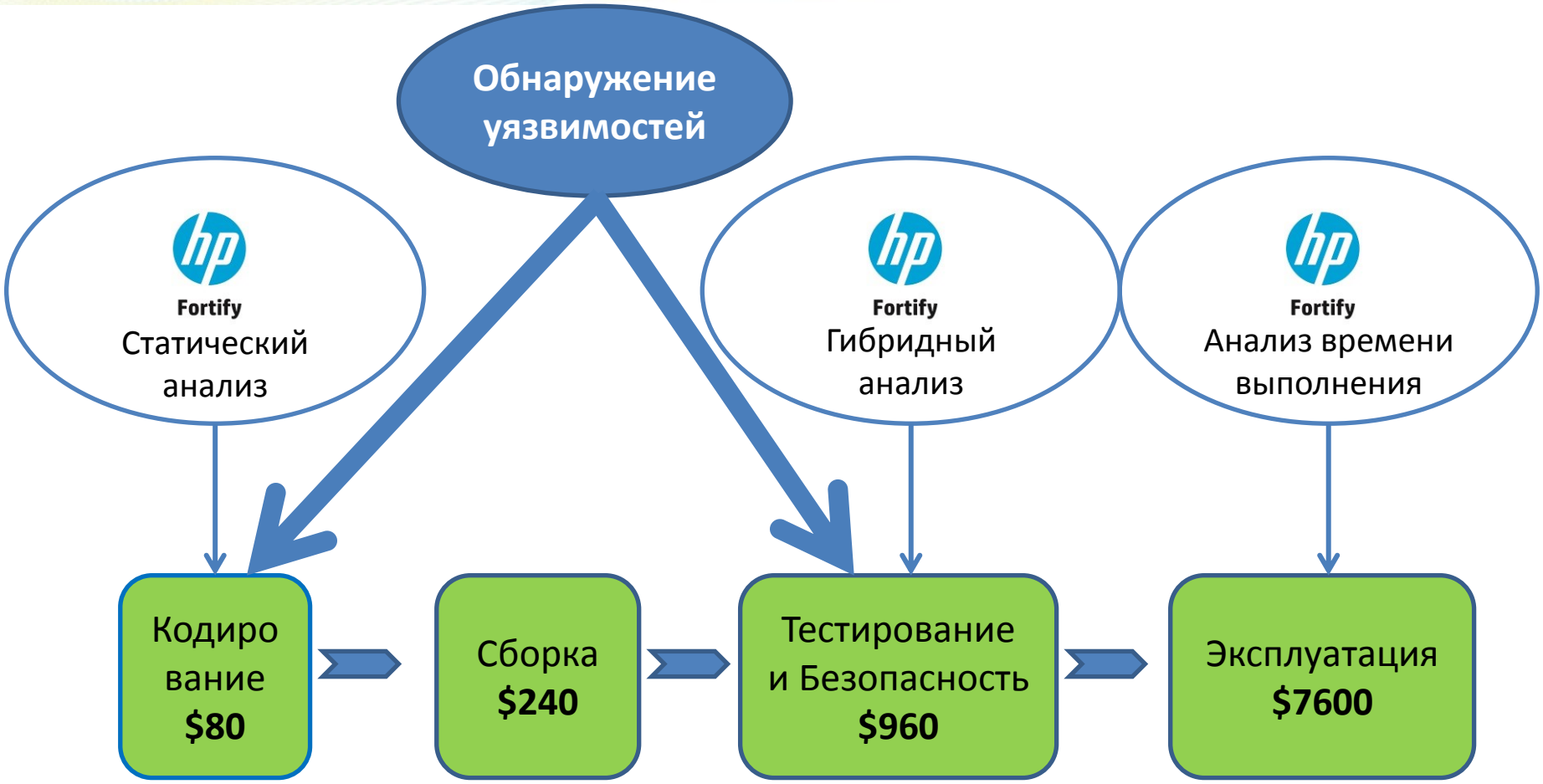
Встраивание в цикл разработки инструментальных средств, выполняющих:

- Статический анализ кода
- Динамический анализ кода
- Анализ кода времени выполнения



IT Guard

Повышение качества разработки



Повышение качества разработки

- Р
  - и получение р о
    либок и уязви я
    да
  - алификации р
  - Уменьшение стоимости разработки и повышение ск ки

IT Guard

Почему?

Fortify

IT Guard

Типы статического анализа кода

- Глубокий анализ с построением модели программы и вычислением ее свойств
- Поверхностный анализ на основе применения шаблонов к исходному тексту программы

Невозможно обнаружить СЛОЖНЫЕ уязвимости, которые УМЕЮТ эксплуатировать злоумышленники

IT Guard

Критерии

- Технология анализа приложения
- База уязвимостей
- Полнота обнаружения уязвимостей
- Поддержка многих языков программирования
- Дружественность интерфейса
- Полнота обоснования наличия уязвимости

Fortify

IT Guard

HP Fortify

- Технология анализа приложения: глубокий анализ приложения как единого целого
- База уязвимостей: работает институт Ponemon, ежедневное добавление новых правил
- Полнота обнаружения уязвимостей: минимальное количество пропущенных уязвимостей
- Поддержка множества языков программирования 21 язык
- Дружественность интерфейса:

HP Fortify – друг разработчиков!!!

- Полнота обоснования наличия уязвимости:

полный путь – от зарождения до проявления

IT Guard

Статический анализа кода

Анализ **исходного кода приложения**

Приложение анализируется по принципу **«белый ящик»**

- Обнаружение уязвимостей
- Ранжирование уязвимостей по приоритету устранения
- Рекомендации по устранению
- Описание возможностей эксплуатации

Fortify

IT Guard

Динамический анализ

Анализ **без** исходного кода приложения

Приложение анализируется по принципу

«черный ящик»

- Обнаружение уязвимостей
- Ранжирование уязвимостей по приоритету устранения
- Рекомендации по устранению
- Описание возможности эксплуатации
- Демонстрация результата эксплуатации уязвимостей

hp Fortify

IT Guard

Гибридный анализ

Динамический и статический анализ исходного кода приложения

Приложение анализируется по принципу **«прозрачный ящик»**

- Точное обнаружение уязвимостей:
  нет ложных срабатываний
- Связка с исходным кодом приложения

ГЛУБОКИЙ И ПОЛНЫЙ АНАЛИЗ ПРИЛОЖЕНИЯ!!!

hp Fortify

IT Guard

Анализ времени выполнения

Две технологии в одном модуле!

- Гибридный анализ или динамический анализ
- Защита приложения во время выполнения

Результат:

- Эффективное обнаружение уязвимостей в наиболее эксплуатируемом коде
- Защита приложения по периметру во время эксплуатации

IT Guard

Анализ стороннего кода

- HP Fortify по запросу:

Загрузка приложения в облако

- Полный отчет с описанием всех обнаруженных уязвимостей, возможностей их эксплуатации и рекомендациями к устранению

- HP Fortify WebInspect

Динамический анализ

- HP Fortify WebInspect Real-time

Анализ времени выполнения

Fortify

IT Guard

Заключение

- Если вы хотите эксплуатировать **качественные, защищенные** программные решения:
  - **помогайте** вашей команде разработчиков
  - подходите ответственно к выбору системного программного обеспечения
  - **проверяйте и контролируйте** ваше программное обеспечение

Fortify

IT Guard

Заключение

- Мы придем к вам и покажем на ВАШЕМ коде, как работает

Fortify

- Сколько уязвимостей содержит ваш код и как их можно эксплуатировать!

IT Guard

Хотите быть **лидером** –
работайте с
профессионалами!

Fortify

Контактная информация

- HP Россия:

  +7 (495) 287-89-01

  http://www.hp.com/

- Компания IT Guard:

  +7 (495) 767-16-19

  info@itgrd.ru

  http://itgrd.ru/

Fortify

1 — BIS Journal
2 — ISM Systems
3 — SafeTech
4 — Digital Security
5 — IT Guard
6 — BIFIT
7 — ЦИБИТ
8 — Oberon
9 — HP
10 — InfoWatch
11 — Setec
12 — Softline