ИНФОСИСТЕМЫ ДЖЕТ

Контроль уязвимостей в программных приложениях

к.ф.-м.н. Катерина Трошина
Ведущий специалист по анализу кода, ЦИБ
ЗАО «Инфосистемы Джет»

Особенности разработки приложений с точки зрения ИБ

Дефекты в программном обеспечении:

- Ошибки

- Уязвимости

- Недекларированные возможности

© 2014 Инфосистемы Джет

Особенности разработки приложений с точки зрения ИБ

Уязвимости – это ошибки разработчиков, которые потенциально могут эксплуатироваться злоумышленниками с целью получения несанкционированного доступа к управлению ПО

© 2014 Инфосистемы Джет

Особенности разработки приложений с точки зрения ИБ

Недекларируемые возможности – сюрпризы от разработчиков:

- секретный вход

- закладки

© 2014 Инфосистемы Джет

Откуда берутся уязвимости в коде?

Разработчики – это ЛЮДИ!!!

КОМАНДА

© 2014 Инфосистемы Джет

Особенности разработки программных приложений

Разработчики – это особенные работники высокой квалификации!

- Они уходят! – Важно собрать и сохранить знания разработчиков в компании
- Их МАЛО! – Важно эксплуатировать их умения максимально эффективно
- Разработчику нужны **комфортные условия** и возможность РАЗВИВАТЬСЯ! – Важно их беречь и о них заботиться

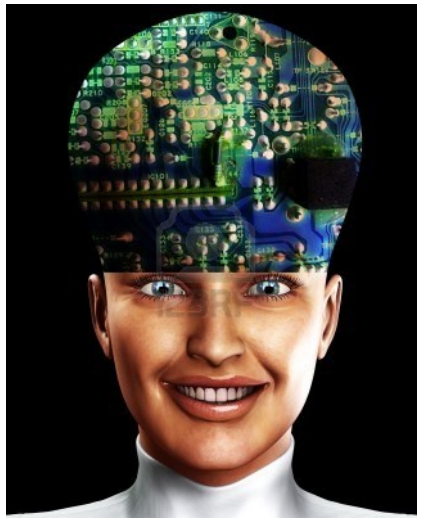
Разработчик – НЕ эксперт по информационной безопасности

© 2014 Инфосистемы Джет

Особенности разработки ПО

Современное приложение сегодня:

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



Программные приложения

- **УЯЗВИМЫЕ!!!**

© 2014 Инфосистемы Джет

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**.

© 2014 Инфосистемы Джет

Разновидности ПО

- Самостоятельная разработка
  - In house - силами своей IT-команды
  - На заказ по разработанному техническому заданию

- Стандартное ПО, разработанное российским разработчиком, возможно, настроенное и адаптированное под ваши особенности бизнеса

- ПО, разработанное иностранным небольшим производителем

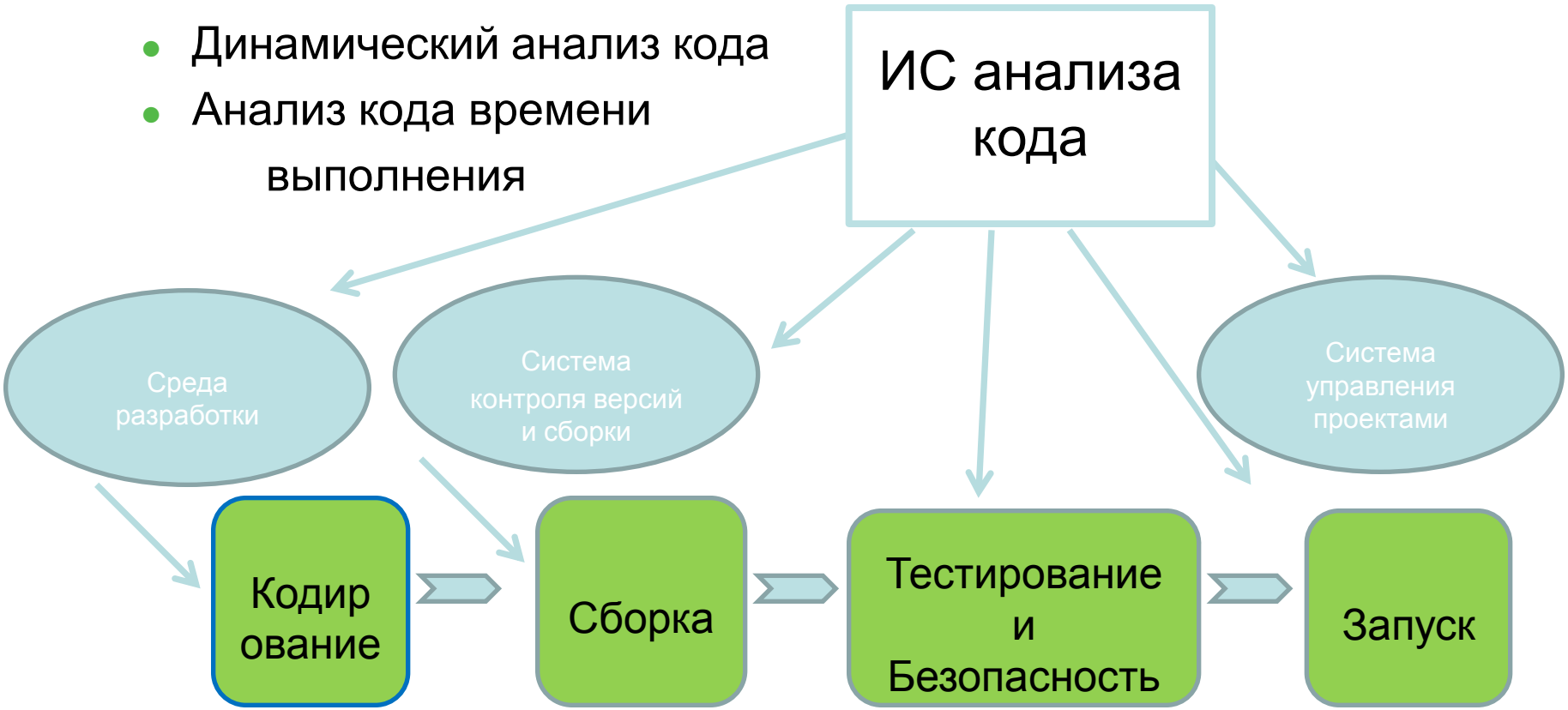
- ПО, разработанное иностранным большим производителем

© 2014 Инфосистемы Джет

Повышение качества разработки

Встраивание в цикл разработки инструментальных средств, выполняющих:

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



© 2014 Инфосистемы Джет

Повышение качества разработки

© 2014 Инфосистемы Джет

ПО, разработанное под заказ

Скрытое управление разработкой через ТЗ и процедуру приемки:

- ТЗ должны содержать требования ИБ
- Разработка ТЗ должна учитывать особенности разработки ПО
- Приемка должна содержать работы по проверке сначала защищенности ПО, а уже после - функциональности

© 2014 Инфосистемы Джет

ПО, разработанное сторонним разработчиком (не гигантом на рынке IT)

Информация о том, какие уязвимости имеются в ПО, позволяет:

- более точно настроить «умные» IT- системы защиты периметра

- модифицировать бизнес процессы так, чтобы обходить эксплуатацию выявленных уязвимостей

- разрабатывать проактивные меры предупреждения успешной эксплуатации известных уязвимостей

© 2014 Инфосистемы Джет

ПО, разработанное гигантом на рынке IT

Такому программному обеспечению можно только доверять и выстраивать защиту периметра:

- Большое количество пользователей – лучшие тестировщики в том числе и по требования ИБ

- Исправление выявленных уязвимостей стоит в очереди, и можно вообще не дождаться, когда уязвимость исправят

© 2014 Инфосистемы Джет

Анализ ПО по требованиям ИБ

Интересуйтесь, что внутри:

- Оболочка может не соответствовать
- содержимому
- Кто предупрежден, тот вооружен!

Не эксплуатируйте кота в мешке!!!

© 2014 Инфосистемы Джет

Где взять безопасное ПО?

Если ПО разрабатывается самостоятельно:

- Дружите с разработчиками и помогите им следовать «Правильному стилю разработки»
- Проверяйте программное обеспечение перед запуском в эксплуатацию по требованиям ИБ!

Если ПО стороннее:

- проверяйте программное обеспечение перед внедрением!
- проверяйте программное обеспечение по требованиям ИБ!
- выстраивайте «умную» защиту периметра, которая чувствительна именно к реальным угрозам вашего ПО…

© 2014 Инфосистемы Джет

Результаты проведения анализа кода

Результат:

- Информированность о том, какое ПО вы эксплуатируете -> Выстраивание «умной» защиты периметра
- Проактивное реагирование на инциденты -> снижение затрат на расследование устранение ущерба от интендантов

© 2014 Инфосистемы Джет

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

© 2014 Инфосистемы Джет

Спасибо за внимание
Ваши вопросы

к.ф.-м.н. Катерина Трошина
Ведущий специалист по анализу кода, ЦИБ
ЗАО «Инфосистемы Джет»

сентябрь 2014 года

Заключение

Насколько вы уверены в своем ПО?

- Мы предоставляем возможность провести пилотный проект
- Пилотный проект покажет вам сколько уязвимостей содержит ваш код и как их можно эксплуатировать!

© 2014 Инфосистемы Джет

Заключение

Мы предоставляем полный спектр услуг по ИБ:

- обнаружение НДВ
- обнаружение уязвимостей
- разработка рекомендаций по устранению выявленных уязвимостей
- разработка рекомендаций по защите, пока разработчики устраняют выявленные уязвимости
- построение полного цикла разработки защищенного кода (SDL)

© 2014 Инфосистемы Джет

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

© 2014 Инфосистемы Джет

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

© 2014 Инфосистемы Джет

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!!!

© 2014 Инфосистемы Джет

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

© 2014 Инфосистемы Джет