Вводная лекция

Данилов И. Г.
к.т.н, ассистент каф. МОП ЭВМ

Институт компьютерных технологий и информационной безопасности ЮФУ

4 сентября 2015 г.

Материалы для лекции

Используемые материалы:

- Методы верификации программного обеспечения, В.В. Кулямин

Сложность ПО

Возрастающая сложность ПО приводит к увеличению количества ошибок в нем, а одновременный рост количества и критичности выполняемых им функций влечет рост ущерба от этих ошибок.

Оценки потерь одной экономики США от некачественного программного обеспечения дают около 60 миллиардов долларов в год (на начало 2000х).

Ошибки в критических системах

Одна из первых хорошо описанных ошибок такого рода — ошибка в системе управления космическим аппаратом Mariner 1, которая привела к потере этого аппарата 22 июля 1962 года.

Ошибка заключалась в том, что в одном месте была пропущена операция усреднения скорости корабля по нескольким последовательно измеренным значениям.

В результате колебания значения скорости, вызванные ошибками измерений, стали рассматриваться системой как реальные, и она попыталась предпринять корректирующие действия, которые привели к полной неуправляемости аппарата.

Небольшая тайна

Людям свойственно ошибаться :-)

Верификация

Верификация (verification)

подтверждение на основе представления объективных свидетельств того, что **заданные требования полностью выполнены**.

Верификация в контексте жизненного цикла системы является совокупностью действий по сравнению полученного результата жизненного цикла системы с требуемыми характеристиками для этого результата. Результатами жизненного цикла могут являться (но не ограничиваются только ими): заданные требования, описание проекта и непосредственно система.

©ISO/IEC/IEEE 12207:2008 Systems and software engineering – Software life cycle processes

Валидация

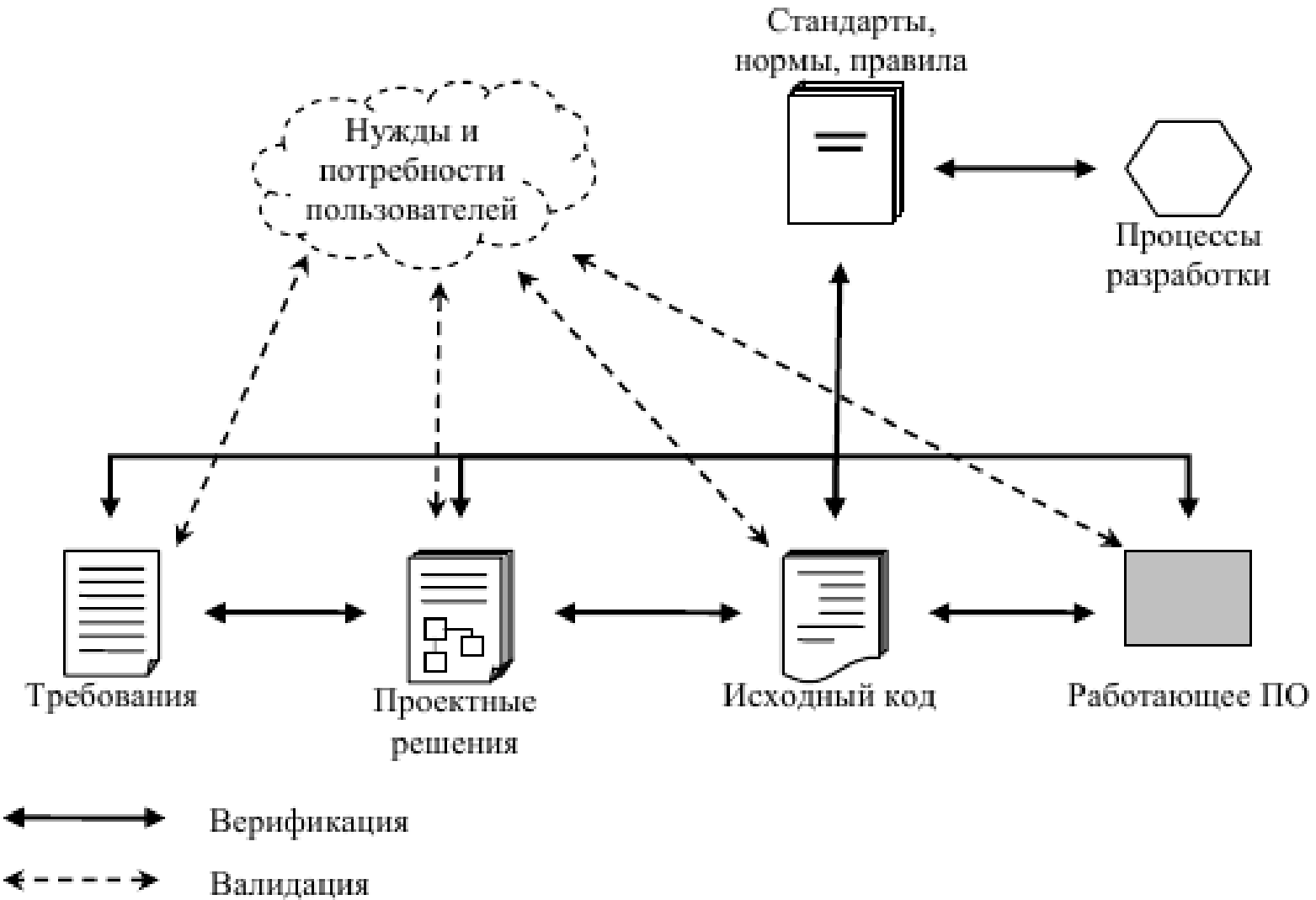
Валидация (validation)

подтверждение на основе представления объективных свидетельств того, что **требования, предназначенные для конкретного использования или применения, выполнены**.

Валидация в контексте жизненного цикла системы является совокупностью действий, гарантирующих и обеспечивающих уверенность в том, что система способна реализовать свое предназначение, текущие и перспективные цели.

©ISO/IEC/IEEE 12207

Различие между верификацией и валидацией

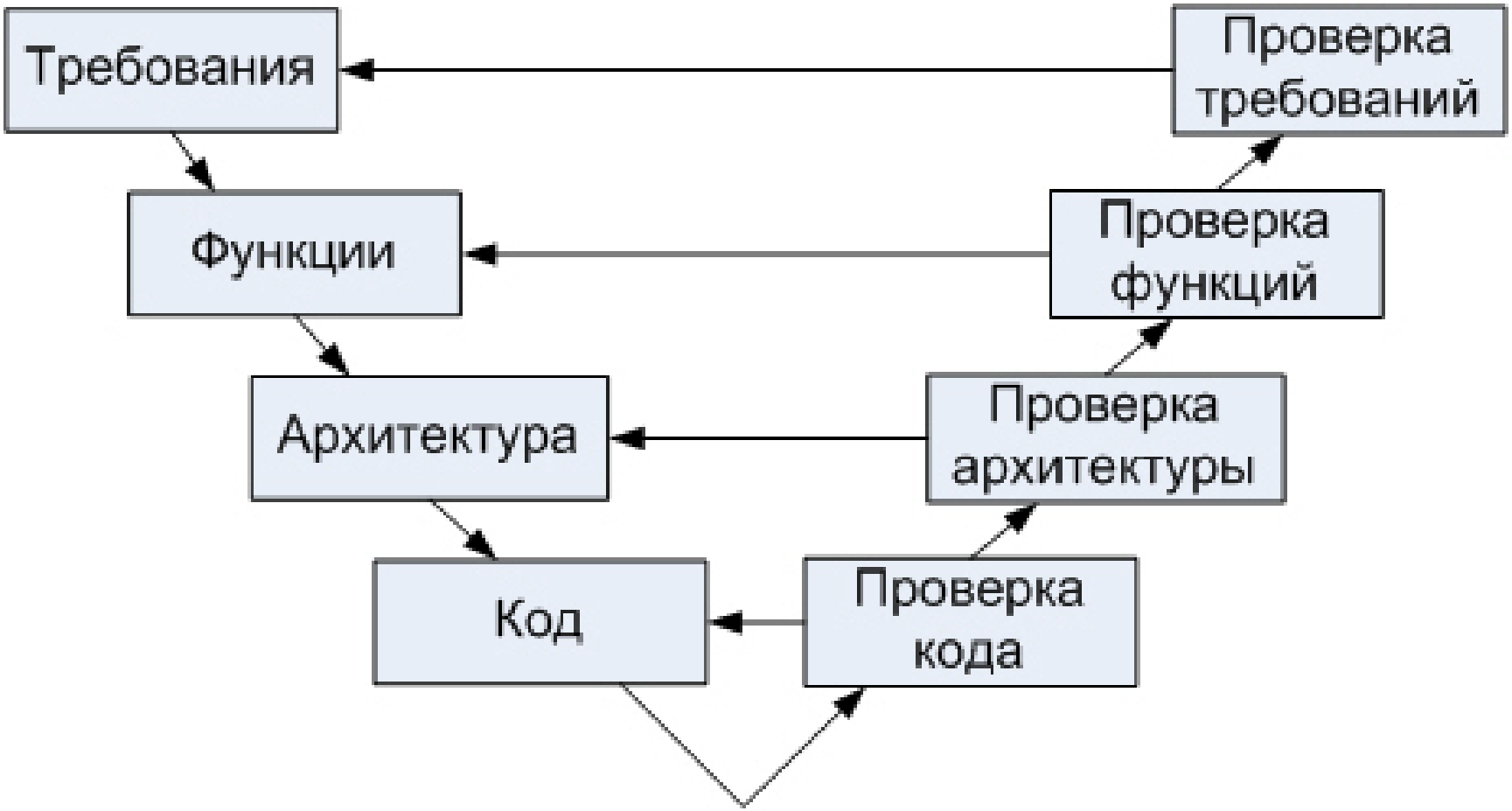


Основная задача верификации и валидации

Основной задачей верификации, как и валидации, является **контроль качества программного обеспечения**.

Факторы внешнего и внутренного качества ПО

Место верификации в ЖЦ ПО (V-модель)



Задачи верификации в рамках ЖЦ ПО

- Выявление дефектов (ошибок, недоработок, неполноты и пр.) различных артефактов разработки ПО (требований, проектных решений, документации или кода), что позволяет устранять их и поставлять пользователям и заказчикам более правильное и надежное ПО.
- Выявление наиболее критичных и наиболее подверженных ошибкам частей создаваемой или сопровождаемой системы.
- Контроль и оценка качества ПО во всех его аспектах.
- Предоставление всем заинтересованным лицам (руководителям, заказчикам, пользователям и пр.) информации о текущем состоянии проекта и характеристиках его результатов.
- Предоставление руководству проекта и разработчикам информации для планирования дальнейших работ, а также для принятия решений о продолжении проекта, его прекращении или передаче результатов заказчику.

Верификация и другие процессы разработки и сопровождения ПО

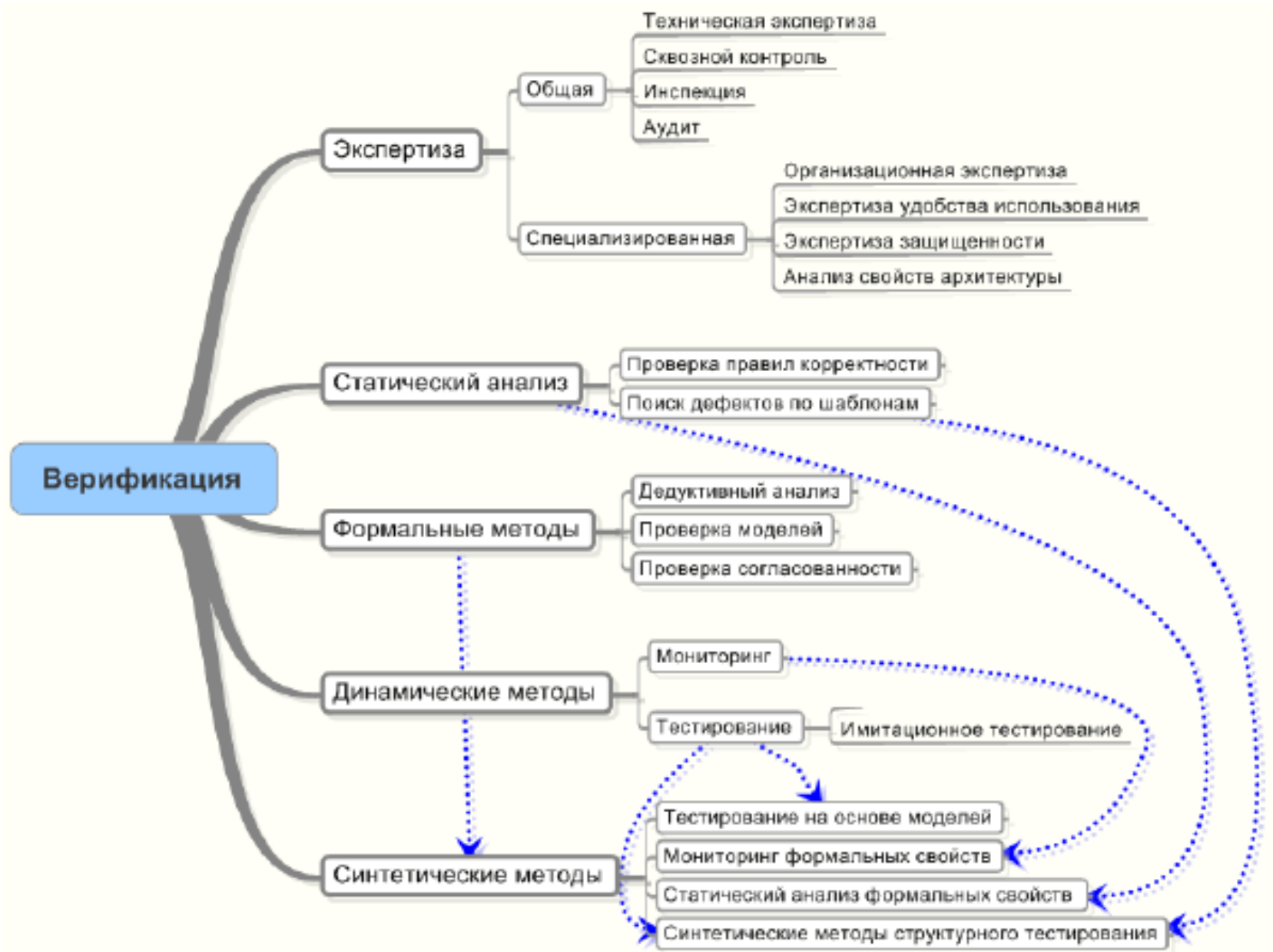
По ISO 12207 к верификации имеют отношение 5 процессов: обеспечение качества (quality assurance), собственно верификация, валидация, совместные экспертизы (joint review) и аудит (audit). Тестирование целиком отнесено к валидации. Кроме того, выделен процесс разрешения проблем (problem resolution), для которого верификация и валидация поставляют входные данные (те самые проблемы).

Верификация и другие процессы разработки и сопровождения ПО

С технической точки зрения экспертизы и аудит, в свою очередь, являются методами проведения верификации и валидации, такими же, как тестирование, оценка архитектуры на основе сценариев или проверка моделей.

В стандартах они рассматриваются как отдельные процессы, скорее всего, потому что применимы к произвольным артефактам жизненного цикла в рамках любого вида деятельности, а также часто используются для оценки процессов и организационных видов деятельности в проекте, в отличие от большинства других методов верификации.

Схема классфикации методов верификации



Экспертиза

Она позволяет выявлять практически любые виды ошибок, причем делать это на этапе подготовки соответствующего артефакта, тем самым минимизируя время существования дефекта и его последствия для качества производных артефактов.

В то же время экспертиза не может быть автоматизирована и требует активного участия людей.

Эффективность экспертизы существенно зависит от опыта и мотивации ее участников, организации процесса, а также от обеспечения корректного взаимодействия между различными участниками.

Статический анализ

Статический анализ свойств артефактов жизненного цикла ПО используется для проверки формализованных правил корректного построения этих артефактов и поиска часто встречающихся дефектов по некоторым шаблонам.

Такой анализ хорошо автоматизируется и может быть практически полностью возложен на инструменты, хотя иногда необходимо вручную определить, например, принятые в проекте стандарты кодирования.

Однако применим он лишь к коду или к определенным форматам представления проектных артефактов, и способен обнаруживать только ограниченный набор типов ошибок.

Формальные методы верификации

Формальные методы верификации используют для анализа свойств ПО формальные модели требований, поведения ПО и его окружения.

Анализ формальных моделей выполняется с помощью специфических техник, таких как дедуктивный анализ (theorem proving), проверка моделей (model checking) или абстрактная интерпретация (abstract interpretation).

Динамические методы верификации

Динамические методы верификации, в рамках которых анализ и оценка свойств программной системы делаются по результатам ее реальной работы или работы некоторых ее моделей и прототипов.

Примерами такого рода методов являются обычное тестирование или имитационное тестирование, мониторинг, профилирование.

Ситнетические методы

Общая идея таких методов вполне понятна — попытаться сочетать преимущества основных подходов к верификации, купировав их недостатки

Q&A

Вопросы?