

Российская Академия наук  
Санкт-Петербургский академический университет —  
Научно-образовательный центр нанотехнологий  
Санкт-Петербургская кафедра философии РАН

## История и методология формальной верификации программ

Реферат аспиранта СПбАУ  
Жаворонкова Эдгара Андреевича

Научный руководитель  
к.ф.-м.н., доцент  
Москвин Денис Николаевич

Санкт-Петербург  
2018

# Содержание

1	Введение	3
2	Понятие качества программного обеспечения	4
3	Виды методов обеспечения качества программного обеспечения	7
4	Формальная верификация программ	8
5	Список литературы	9

# 1. Введение

Вычислительная техника и программное обеспечение<sup>1</sup> уже настолько прочно вошли в обиход человечества, что невозможно представить нашу жизнь без них. Программное обеспечение решает задачи автоматизации процессов в самых разных областях, начиная от простейших вычислений и заканчивая медициной или атомной энергетикой. В зависимости от задачи, возложенной на программное обеспечение, отличаются и предъявляемые к нему требования. В том числе, требования к надежности и, как следствие – качеству.

В этом эссе я попробую привести исторические моменты, так или иначе связанные с вопросом обеспечения качества программного обеспечения и показать их методологический аппарат. Мы увидим различные трактовки понятия качества программного обеспечения, увидим, какие существуют методы для обеспечения качества ПО и поближе познакомимся в один из них – формальной верификацией.

---

<sup>1</sup>Я буду в равной степени употреблять термин "программное обеспечение" и соответствующую аббревиатуру – ПО

## 2. Понятие качества программного обеспечения

Существуют различные подходы к трактовке понятия качества программного обеспечения. Международный стандарт ISO 8402:94, например вводит качество программного обеспечения как "весь объем признаков и характеристик программ, который относится к их способности удовлетворять установленным или предполагаемым потребностям" – [3]. Стандарт IEEE Std 610.12-1990 определяет качество ПО как "степень, в которой система, компонент или процесс удовлетворяют потребностям или ожиданиям заказчика или пользователя" – [1]

Однако исторически, первой записью о качестве продукта можно считать определение Уолтера Шухарта (англ. Walter Andrew Shewhart) в книге [5] качества как сущности, состоящей из двух аспектов. Один из них имеет дело с рассмотрением качества как объективного факта, не зависящего от существования человека. Другой же, напротив, имеет дело с чувственными ощущениями реальности. Тем самым, Шухарт подводит нас к мысли, что у качества есть субъективная сторона.

Далее мысль Шухарта развил Джеральд Вайнберг (англ. Gerald Marvin Weinberg) в своей работе 1992 года [6], говоря о качестве, как о "значимом для какого-либо человека". Отсюда полезно задаться вопросом, какие люди будут оценивать качество отдельно взятого программного продукта и что будет ценным для них?

Отголосок этой мысли есть и в международном стандарте ISO/IEC 9126 – [4], который вводит так называемую модель качества, которая описывает различные подходы к нему в течение всего жизненного цикла ПО.

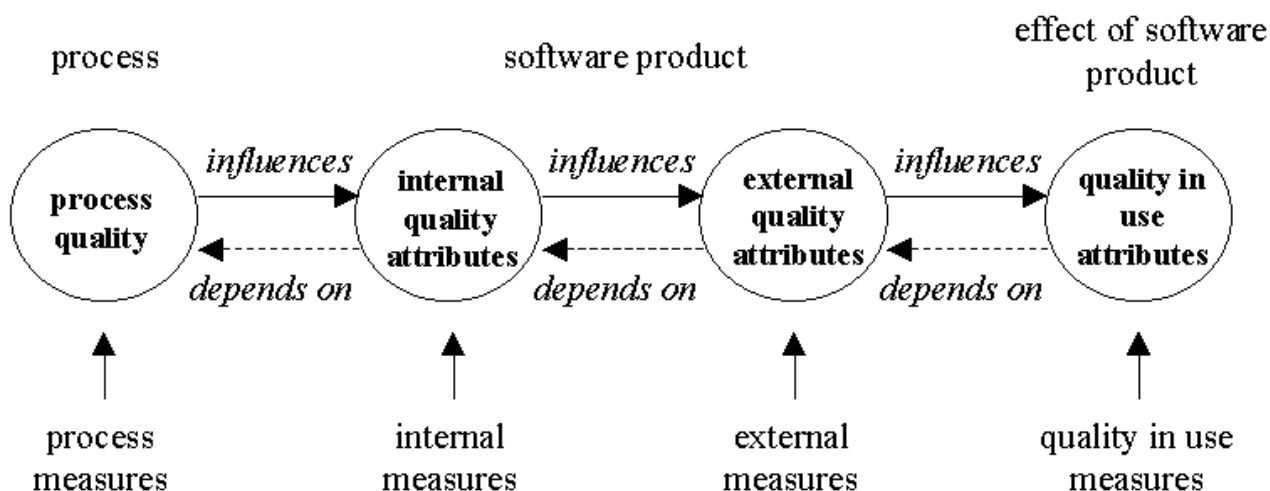


Рис. 1: Модель качества, согласно ISO/IEC FDIS 9126-1

Уже при первом взгляде на эту модель становится понятно, что на различных этапах жизненного цикла ПО используются различные, понятия

качества. Так, в ходе непосредственно разработки мы говорим о качестве *процесса* разработки, которое напрямую влияет на внутреннее качество программного продукта.<sup>2</sup> Внутреннее качество продукта, в свою очередь, влияет на внешнее качество продукта, которое, затем, определяет качество продукта с точки зрения пользователя.

Может возникнуть вопрос, чем отличаются внутреннее качество продукта, от внешнего? Можно считать, что внутреннее качество программного обеспечения связано с некоторыми внутренними метриками(метриками, которые можно получить не запуская программу). Внешнее качество, соответственно, связано с внешними метриками(например, как ведет себя запущенная в некотором внешнем окружении программа).

В рамках внутреннего и внешнего качества стандарт предлагает следующие характеристики, приведенные на рисунке ниже:

## Software Quality Characteristics



Рис. 2: Характеристики качества ПО, согласно ISO/IEC FDIS 9126-1

<sup>2</sup>Кроме того, я буду использовать термин "программный продукт", считая его синонимом для программы или программного обеспечения. Формально, это конечно же, неверно, но в нашем контексте это не играет большой роли.

1. Функциональность(*Functionality*) определяется способностью ПО решать возложенные на него задачи, соответствующие потребностям пользователя при заданных условиях использования. То есть эта характеристика говорит о том, что программа работает исправно точно и безопасно.
2. Надежность(*Reliability*) определяется способностью программы штатно завершаться, восстанавливаться в случае сбоев в работе. Другими словами – это способность программы выполнять требуемые задачи в обозначенных условиях, в течение обозначенных сроков.
3. Удобство использования(*Usability*) означает легкость в понимании и изучении ПО для пользователя. Эта характеристика больше относится к качеству ПО с точки зрения пользователя.
4. Эффективность(*Efficiency*) определяется способностью программы обеспечивать требуемый уровень производительности в условиях обозначенного времени или используемых ресурсов.
5. Удобство сопровождения(*Maintainability*) – это легкость, с которой программу можно анализировать, тестировать изменять с целью исправления каких-либо дефектов или для адаптации к новому окружению.
6. Переносимость(*Portability*) – это способность программного обеспечения запускаться и работать вне зависимости от программного или аппаратного окружения.

Нас будет интересовать в большей степени внутреннее качество ПО и способы его обеспечения, однако мы чуть-чуть коснемся и внешнего качества. Качество процесса разработки, равно как и качество ПО с точки зрения пользователя мы постараемся оставить за кадром.

### **3. Виды методов обеспечения качества программного обеспечения**

Бла - [2]

## 4. Формальная верификация программ

Бла



## 5. Список литературы

- [1] *IEEE Std 610.12-1990: IEEE Standard Glossary of Software Engineering Terminology*. IEEE, 1990.
- [2] Richard S Bird and Ross Paterson. De bruijn notation as a nested datatype. *Journal of functional programming*, 9(01):77–91, 1999.
- [3] ISO. *ISO 8402:1994 Quality management and quality assurance – Vocabulary*. ISO, 1994.
- [4] ISO/IEC. *ISO/IEC 9126. Software engineering – Product quality*. ISO/IEC, 2001.
- [5] Walter Andrew Shewhart. *Economic control of quality of manufactured product*. ASQ Quality Press, 1931.
- [6] Gerald M Weinberg. *Quality software management*. New York, 1993.