АНАЛИЗ МЕТОДОВ ОЦЕНКИ НАДЕЖНОСТИ ОБОРУДОВАНИЯ И СИСТЕМ

Пакулин Н.В., Лаврищева Е.М.

В докладе приводится анализ моделей и методв оценки надежности технических и программных средств. Отмечается, что теории надежности технических средств возникшая в рамках теории массового обслуживания систем и повлияла на развитие надежности компьютерных систем и программного обеспечения.

Теоретики изучая природу ошибок функционирования таких систем разработали более 100 математических моделей надежности, учитывающих ошибки, сбои, отказы и дефекты возникающие в системах на первых и последующих поколениях ЭВМ.

В результате надежность систем сформировалась как самостоятельная теоретическая и прикладная наука.

Надежность систем существенным образом отличается от надежности аппаратуры и оборудования.

Проблема надёжности оборудования существенно отличается от проблемы надёжности ПО. Основные отличия состоят в следующем.

1. Размерность. Программные системы создают огромное число кодов, которое обычно намного превышает число физических элементов системы. Кроме того, сложность взаимодействия компонент ПО намного превышает сложность взаимодействия элементов. Таким образом ПО как объект исследования является более сложным.
2. Элементы ПО не стареют, не деградируют во времени.
3. Методы введения избыточности в ПО существенно отличаются от методов используемых для оборудования. Это не касается и методов обеспечения эксплуатационной надёжности, таких как профилактика и замена. Так как в принципе весьма трудно получить программный продукт, не содержащий причин возникновения отказа, дефектов и т. п.
4. Хотя, с одной стороны, компоненты ПО не стареют, однако, в процессе эксплуатации могут вноситься искажения в компоненты ПО, что может приводить к возрастанию его интенсивности отказов.
5. В отличие от отказов аппаратуры отказы ПО являются не физическими, т.е. вызываемыми необратимыми изменениями в элементах, а конструктивных зон отказа труднее поддаются визуализации, классификации, обнаружению и коррекции. Как результат, надёжность ПО трудней измерить и анализировать, чем надёжность аппаратуры.
6. Структура и состав ПО динамически изменяются, что бывает трудно учесть в соответствующих моделях надёжности ПО.
7. Надёжность ПО в большей степени зависит от среды (например, вируса). Вирус может изменить ПО, в то время как изменить структуру аппаратной части случайным образом нельзя. Т.е. характер взаимодействия с внешней средой существенно различен.

Однако между проблемами надёжности аппаратуры и ПО имеется и сходство. В основе этих проблем лежат случайные явления и способы их анализа основываются на соответствующих методах теории вероятностей и случайных процессов.

Для многих систем надежность является главной целевой функцией реализации. К некоторым типам систем (реального времени, радарные системы, системы безопасности, медицинское оборудование со встроенными программами и др.) предъявляются высокие требования к надежности (недопустимость ошибок, достоверность, защищенность и др.).

Надежность систем зависит от числа оставшихся и не устраненных ошибок в отдельных программах.

Чем интенсивнее проводится эксплуатация, тем интенсивнее выявляются ошибки и быстрее растет надежность системы и соответственно ее качество. Надежность является функцией от ошибок, оставшихся в ПС после ввода его в эксплуатацию. Системы без ошибок можно считать абсолютно надежными.

Для оценки надежности систем используются такие собранные статистические данные как вероятность и время безотказной работы, отказы и частота (интенсивность) отказов.

Под *надежностью систем* понимается способность системы сохранять свои свойства (безотказность, восстанавливаемость) на заданном уровне в течение фиксированного промежутка времени при определенных условиях эксплуатации. Исследование надежности проводится с помощью методов теории вероятностей, математической статистики, теории массового обслуживания и теоретических методов надежности.

Главным источником информации, используемой в моделях надежности, является процесс тестирования, эксплуатации систем и разного вида ситуации, возникающие в них.

К базовым понятиям, которые используются в моделях надежности систем, относятся следующие.

Отказ ПС (failure) – это переход системы из рабочего состояния в нерабочее.

Дефект (fault) – это последствие выполнения элемента программы, приводящее к некоторому событию, например, в результате неверной интерпретации его компьютером или человеком. Дефекты в программе, не выявленные в результате проверок, является источником потенциальных ошибок и отказов системы.

Ошибка (error) может быть следствием недостатка в описании одной из программ или при принятии им неверных решений.

Интенсивность отказов – это частота появления отказов или дефектов в системе при ее тестировании или эксплуатации.

Процесс возникновения ошибок и отказов в ПС является случайным и в основном определяется временем их возникновения или частотой, числом и интенсивностью их.

В связи с этим все модели надежности основываются именно на нахождении случайной величины появления в ПС. числом и интенсивностью их появления в ПС.

Поиск случайных величин осуществляется стохастическими методами, процесс соответственно является стохастическим, вероятностным.

Если случайные величины (время между требованиями и время обслуживания и др.) распределены по показательному, эрланговскому или гиперэрланговскому законам, то поведение системы описывается Марковским процессом без непрерывных компонент Другим подходом к исследованию надежности на основе отказов в ПС является классическая теория вероятностей, согласно которой отказы в системе (в отличие от отказов технических средств) считаются случайными и зависят от дефектов, внесенных при разработке ПС.

Все модели оценки надежности основываются на статистике отказов и распределении интенсивности выявленных отказов в ПС.

Большинство моделей надежности исходят из предположения, что найденные дефекты устраняются немедленно (или временем их устранения можно пренебречь) и при этом новые дефекты не вносятся. В результате количество дефектов в ПС уменьшается, а надежность возрастает, такие модели получили название *моделей роста надежности*.
Хетч дает следующую классификацию моделей надежности.

Прогнозирующие модели надежности основаны на измерении технических характеристик создаваемой программы: длина, сложность, число циклов и степень их вложенности, количество ошибок на страницу операторов программы и др.

Модель Мотли–Брукса основывается на длине и сложности структуры программы (количество ветвей и циклов, вложенность циклов), количестве и типах переменных, а также интерфейсов.

Модель Холстеда дает прогнозирование количества ошибок в программе в зависимости от ее объема и таких данных, как число операций (n_1) и операндов (n_2), а также их общее число (N_1, N_2).

Измерительные модели предназначены для измерения надежности ПО, работающего с заданной внешней средой и следующими ограничениями:

– ПО не модифицируется во время периода измерений свойств надежности;

– обнаруженные ошибки не исправляются;

– измерение надежности проводится для зафиксированной конфигурации ПО.

Примером таких моделей является модель Нельсона и Рамамурти–Бастани и др.

Оценочные модели основываются на серии тестовых прогонов и проводятся на этапах тестирования ПС. В тестовой среде определяется вероятность отказа программы при ее выполнении или тестировании. Эти типы моделей могут применяться на этапах ЖЦ.

Модели без подсчета ошибок основаны на измерении интервала времени между отказами и позволяют спрогнозировать количество ошибок, оставшихся в программе. К моделям относятся модели Джелински и Моранды, Шика Вулвертона и Литвуда–Вералла

Модели с подсчетом отказов базируются на количестве ошибок, обнаруженных на заданных интервалах времени. К этому классу моделей относятся модели Шика–Вулвертона, Шумана, Пуассоновская модель и др.

Модели с подсевом ошибок основаны на количестве устраненных ошибок и подсеве, внесенном в программу искусственных ошибок, тип и количество которых заранее известны. При внесении изменений в программу проводится повторное тестирование и оценка надежности. Этот подход к базируется на тестировании и редко используется из-за дополнительного объема работ.

Модели с выбором области входных значений основываются на генерации множества тестовых выборок из входного распределения. К этому типу моделей относится модель Нельсона и др.

На процессах выявления отказов, их интенсивностью основаны еще такие группы:

1) модели, рассматривающие интенсивность отказов как марковский процесс;

2) модели, рассматривающие интенсивность отказов как пуассоновский процесс;

3) модели роста надежности.

Четкой границы между этими моделями провести нельзя, однако по фактору распределения интенсивности отказов и их поведению эти модели можно еще разделить на экспоненциальные, логарифмические, геометрические, байесовские и др.

В проблеме надежности ПО рассматривается такое понятие как способность ПО обладать свойствами, желательными для пользователя (английский термин dependability).

Dependability (D) характеризуется различными атрибутами (свойствами):

- availability – готовность к использованию,
- reliability – готовность к непрерывному функционированию,

- safety – безопасность для окружающей среды (для внешнего окружения). Способность не вызывать катострафических последствий в случае отказа.
- confidentability – секретность, сохранение секретности информации,
- integrity – способность к сохранению информации, устойчивость к её самопроизвольному изменению,
- aintainability – характеризует эксплуатационные способности ПО, простоту выполнения операций обслуживания, например, устранение ошибок, восстановление после ошибки и т.п.
- security – комбинация готовности и сохранности по отношению к административному лицу + скрытность confidentability,
- failure – отказ, отклонение поведения системы от предписанного, т.е. когда система перестаёт выполнять предписанные ей функции,
- error – ошибка, состояние системы, которое вызывает отказ, в случае человека используется термин mistake
- fault - отказ, в случае человека используют термин , это причина ошибки, что вызывает её.

Достижение Dependability обеспечивается многими методами, которые включают:

- fault preventation – предотвращение отказа,
- remival fault – устранение отказа,
- fault tolerance – возможность выполнения ПО при наличии
- fault forecasting – как оценить возможность появления отказа и его последствия.

Fault -------→ error -------→ failure

Различие между fault и failure не критическое и поэтому используется термин Defect. Он может означать либо fault (причина), либо failure (действие).

Оценка надежности ПС осуществляется по моделям надежности, соответствующим типу системы. Если обнаружены ошибки и внесены необходимые изменения в нее, проводят такие мероприятия:

– протоколирование отказов в ходе функционирования ПС и измерение надежности функционирования, а также использование результатов измерений при определении потерь надежности в период времени эксплуатации;

– анализ частоты и серьезности отказов для определения порядка устранения соответствующих ошибок;

– оценка влияния функционирования ПС на надежность в условиях усовершенствования технологии или использования новых инструментов разработки ПС.

Таким образом, показано, что надежность является одной и главных характеристик современных программных систем, для которой разработано большое количество моделей для разных ее видов и типов. Рассмотрены основные базовые понятия надежности, обеспечивающие оценку надежности по соответствующим моделям надежности ПС, основанным на времени функционирования и/или количестве отказов (ошибок), полученных в программах в процессе их тестирования или эксплуатации.

Литература.

1. *Липаев В.В.* Надежность программного обеспечения. –М.: СИНТЕГ, 1998.–231с.

2. *Липаев В.В*. Методы обеспечения качества крупномасштабных программных систем. – М.: СИНТЕГ, 2003.–510 с.

3. *Майерс Г.* Надежность программного обеспечения,– М.: Мир, 1980.–360с.

4. Мороз Г.Б., Лаврищева Е.М. Модели роста надежности программного обеспечения.– Киев: Препринт 92–38, 1992.– 23с.

5. *Shick G.J., Wolverton R.W.* An analysis of computing software reliability models /IEEE Tras. Software Eng. – V. SE–4. – № 2. – 1978. – P. 104–120.

6. *Shanthikumar J.G.* Software reliability models: A Review //Microelectron. Reliab. – 1983. –V. 23. –№ 5 – P. 903–943.

7.Goel Amrit L., "Software reliability models: Assumptions, limitations, and applicability. //IEEE Transactions on Software Engineering, Vol. SE–11, № 12. – 1985. –P. 1411–1423.

8. *Musa J.D. Okumoto K. A.* Logarithmic Poisson Time Model for Software Reliability Measurement //Proc. Sevent International Conference on Software Engineering. – Orlando, Florida. – 1984. –P. 230–238.

9. *Yamada S., Ohba M., Osaki S.* S–shaped software reliability grows modeling for software error detection // IEEE Trans. Reliability. – 1983. – R–32. – № 5. – P. 475–478.

10 *Chulani S.* Constructive quality modeling for defect density prediction: COQUALMO // Internat. Symposium on Software Reliability Engineering (ISSRE'99), Boca Raton, N. 1–4. – 1999.

11. Лаврищева Е.М. Методы программирования . Теория, Инженерия, практика. К.: 2006. Наук. Думка. 471с.

12. Лаврищева Е.М. Software Engineering компьютерных систем. Парадигмы, технологии, CASE-средства. –К.: 2014.-284 с.