Модели надежности ПС

С точки зрения прикладной науки *надежность* - это способность ПС сохранять свои свойства (безотказность, устойчивость и др.), преобразовывать исходные данные в результаты в течение определенного промежутка времени при определенных условиях эксплуатации. Снижение надежности ПС происходит из-за ошибок в требованиях, проектировании и выполнении. Отказы и ошибки зависят от способа производства продукта и появляются в программах при их исполнении на некотором промежутке времени.

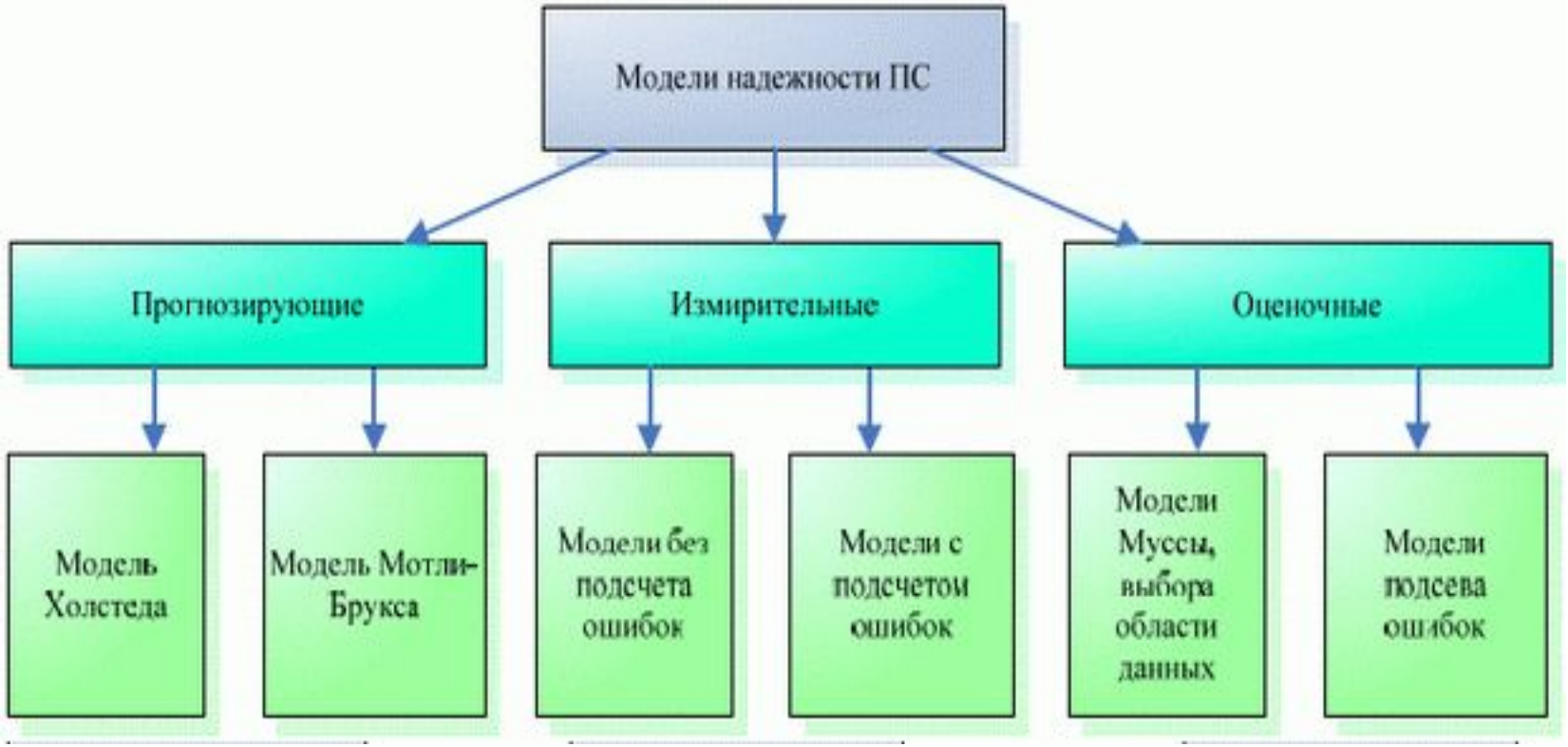
Для многих систем (программ и данных) надежность - главная целевая функция реализации. К некоторым типам систем (реального времени, радарные системы, системы безопасности, медицинское оборудование со встроенными программами и др.) предъявляются высокие требования к надежности, такие, как отсутствие ошибок, достоверность, безопасность и др.

Надежность является функцией от ошибок, оставшихся в ПС после ввода его в эксплуатацию. ПС без ошибок является абсолютно надежным. Но для больших программ абсолютная надежность практически недостижима. Оставшиеся необнаруженные ошибки проявляют себя время от времени при определенных условиях (например, при некоторой совокупности исходных данных) сопровождения и эксплуатации системы.

Для оценки надежности ПС используются такие статистические показатели, как вероятность и время безотказной работы, возможность отказа и частота (интенсивность) отказов. Поскольку в качестве причин отказов рассматриваются только ошибки в программе, которые не могут самоустраниться, то ПС следует относить к классу невосстанавливаемых систем.

на данный момент времени разработано большое количество моделей надежности ПС и их модификаций. Каждая из этих моделей определяет функцию надежности, которую можно вычислить при задании ей соответствующих данных, собранных во время функционирования ПС.

Ввиду большого разнообразия моделей надежности разработано несколько подходов к классификации этих моделей. Такие подходы в целом основываются на истории ошибок в проверяемой и тестируемой ПС на этапах ЖЦ. Одной из классификаций моделей надежности ПО является классификация Хетча. В ней предлагается разделение моделей на прогнозирующие, измерительные и оценочные.



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.

Например, модель *Мотли-Брукса* основывается на длине и сложности структуры программы (количество ветвей, циклов, вложенность циклов), количестве и типах переменных, а также интерфейсов. В этих моделях длина программы служит для прогнозирования количества ошибок, например, для 100 операторов программы можно смоделировать интенсивность отказов.

Измерительные модели предназначены для измерения надежности программного обеспечения, работающего с заданной внешней средой. Они имеют следующие ограничения:

- программное обеспечение не модифицируется во время периода измерений свойств надежности;
- обнаруженные ошибки не исправляются;
- измерение надежности проводится для зафиксированной конфигурации программного обеспечения.

Типичным примером таких моделей являются модели 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. Кроме того, результаты прогнозирующих моделей могут использоваться как входные данные для оценочной модели. Имеются модели (например, модель Муссы), которые можно рассматривать как оценочную и в то же время как измерительную модель.

Другой вид классификации моделей предложил Гоэл, согласно которой модели надежности базируются на отказах и разбиваются на четыре класса моделей:

- без подсчета ошибок;
- с подсчетом отказов;
- с подсевом ошибок;
- модели с выбором областей входных значений.

Модели без подсчета ошибок основаны на измерении интервала времени между отказами и позволяют спрогнозировать количество ошибок, оставшихся в программе. После каждого отказа оценивается надежность и определяется среднее время до следующего отказа. К таким моделям относятся модели Джелински и Моранды, Шика Волвертона и Литвуда-Вералла.

Модели с подсчетом отказов базируются на количестве ошибок, обнаруженных на заданных интервалах времени. Возникновение отказов в зависимости от времени является стохастическим процессом с непрерывной интенсивностью, а количество отказов является случайной величиной. Обнаруженные ошибки, как правило, устраняются и поэтому количество ошибок в единицу времени уменьшается. К этому классу моделей относятся модели Шумана, Шика- Волвертона, Пуассоновская модель и др.

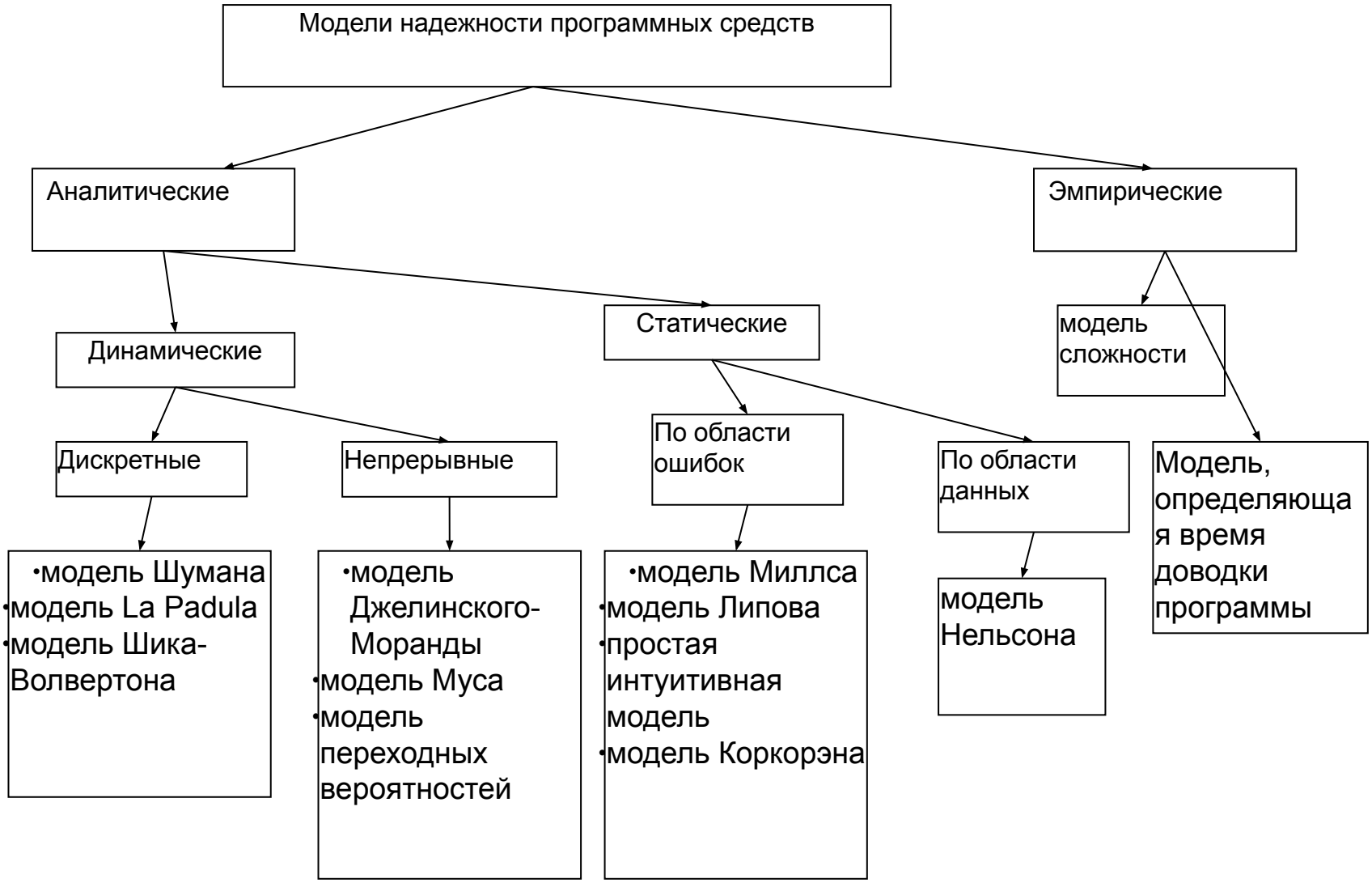
Модели с подсевом ошибок основаны на количестве устраненных ошибок и подсеве, внесенном в программу искусственных ошибок, тип и количество которых заранее известны. Затем определяется соотношение числа оставшихся прогнозируемых ошибок к числу искусственных ошибок, которое сравнивается с соотношением числа обнаруженных действительных ошибок к числу обнаруженных искусственных ошибок. Результат сравнения используется для оценки надежности и качества программы. При внесении изменений в программу проводится повторное тестирование и оценка надежности. Этот подход к организации тестирования отличается громоздкостью и редко используется из-за дополнительного объема работ, связанных с подбором, выполнением и устранением искусственных ошибок.

Модели с выбором области входных значений основываются на генерации множества тестовых выборок из входного распределения, и оценка надежности проводится по полученным отказам на основе тестовых выборок из входной области. К этому типу моделей относится модель Нельсона и др.

Классификация моделей роста надежности относительно процесса выявления отказов, фактически разделена на две группы:

- модели, которые рассматривают количество отказов как марковский процесс;
- модели, которые рассматривают интенсивность отказов как пуассоновский процесс.

Фактор распределения интенсивности отказов разделяет модели на экспоненциальные, логарифмические, геометрические, байесовские и др.


Модели надежности программных средств
Аналитические
Эмпирические
Динамические
Статические
модель сложности
Дискретные
Непрерывные
По области ошибок
По области данных
Модель, определяющая время доводки программы
•модель Шумана
•модель La Padula
•модель Шика-Волвертона
•модель Джелинского-Моранды
•модель Муса
•модель переходных вероятностей
•модель Миллса
•модель Липова
•простая интуитивная модель
•модель Коркорэна
модель Нельсона

Аналитические модели дают возможность рассчитать количественные показатели надежности, основываясь на данных о поведении программы в процессе тестирования. Эмпирические модели базируются на анализе структурных особенностей программ. В динамических моделях поведение ПС рассматривается во времени. В статических моделях появление отказов не связывают со временем, а учитывают только зависимость количества ошибок от числа тестовых прогонов или зависимость количества ошибок от характеристики входных данных.

Динамические модели

Модель La Padula. По этой модели выполнение последовательности тестов производится в m этапов. Каждый этап заканчивается внесением изменений в ПС. Возрастающая функция надежности базируется на числе ошибок, обнаруженных в ходе каждого тестового прогона. Надежность ПС в течении i-го этапа:

R(t)=R(∞)-A/i, где i=1,2,…; A-параметр роста; R(∞)=limR(i) – предельная надежность ПС.

Эти неизвестные величины вычисляют, решив следующие уравнения:

$$\sum_{i=1}^{m}\left\{\frac{S_i - m_i}{S_i} - R(\infty) + \frac{A}{i}\right\} = 0$$

$$\sum_{i=1}^{m}\left[\left(\frac{S_i - m_i}{S_i} - R(\infty) + \frac{A}{i}\right)\cdot\left(\frac{1}{i}\right)\right] = 0$$

где S_i – число тестов; m_i – число отказов во время i-го этапа; m – число этапов; i=1,2,...m.

Модель Джелинского-Моранды. При тестировании фиксируется время до очередного отказа. Основное положение, на котором строится модель, заключается в том, что значение интервалов времени тестирования между обнаружением двух ошибок имеет экспоненциальное распределение с частотой ошибок (интенсивностью отказов), пропорциональной числу еще не выявленных ошибок. Каждая обнаруженная ошибка устраняется, число оставшихся ошибок уменьшается на 1. Функция плотности распределения времени обнаружения i-ой ошибки, отсчитываемого от момента выявления (i-1) ошибки, имеет вид

$$P(t_i) = \lambda_i e^{-\lambda_i t_i}$$

$$\lambda_i = C(N - i + 1)$$

где λ_i – частота отказов, N – число ошибок, первоначально присутствующих в программе; C – коэффициент пропорциональности.

Наиболее вероятные значения величин N и C можно определить на основе данных тестирования. Для этого фиксируют время выполнения до очередного отказа t1, t2, t3, …tk.

$$\sum_{i=1}^{K}\left(\hat{N}-i+1\right)^{-1}=\frac{K}{\hat{N}+1-QK}$$

$$\hat{C}=\frac{K/A}{N+1-QK}$$

$$Q=B/AK$$

$$B=\sum_{i=1}^{K}i\cdot t_i$$

$$A=\sum_{i=1}^{K}t_i$$

Модель Шика-Волвертона. Модифицированная модель Джелинского-Моранды для случая возникновения на рассматриваемом интервале более одной ошибки. При этом считается, что исправление ошибок производится лишь после истечения интервала времени, на котором они возникли. В основе модели лежит предположение, согласно которому частота ошибок пропорциональна не только количеству ошибок в ПС, но и времени тестирования, т.е. вероятность обнаружения ошибок с течением времени возрастает. Частота ошибок λi предполагается постоянной в течении интервала времени ti и пропорциональна числу ошибок, оставшихся в ПС по истечении $(i-1)$ интервала; но она пропорциональна также и суммарному времени уже затраченному на тестирование:

$$\lambda i = C(N - ni - 1)(Ti - 1 + ti/2)$$

В данной модели наблюдаемым событием является число ошибок, обнаруживаемых в заданном временном интервале, а не время ожидания каждой ошибки, как в модели Джелинкого-Моранды.

Модель Муса. Считается, что не всякая ошибка ПС может вызвать отказ, поэтому допускается обнаружение более одной ошибки при выполнении программы до возникновения очередного отказа.

Считается, что на протяжении всего ЖЦ ПС может произойти M_0 отказов и при этом будут выявлены все N_0 ошибки, которые присутствовали в ПС до начала тестирования. Общее число отказов M_0 связано с первоначальным числом ошибок N_0 соотношением

$N_0 = BM_0$

где B – коэффициент обнаружения ошибок.

В момент, когда производится оценка надежности, после проведения тестирования, на которое потрачено определенное время τ, зафиксировано m отказов и выявлено n ошибок. Тогда из соотношения $n = Bm$ можно определить коэффициент уменьшения числа ошибок B как число, характеризующее количество устраненных ошибок, приходящихся на один отказ.

В модели Муса различают два вида времени:

- суммарное время функционирования т, которое учитывает чистое время тестирования до контрольного момента, когда производится оценка надежности;
- оперативное время т’ – время выполнения ПС, планируемое от контрольного момента и далее, при условии, что дальнейшего устранения ошибок не будет (время безотказной работы в процессе эксплуатации).

Для суммарного времени функционирования т предполагается:

- интенсивность отказов пропорциональна числу неустраненных ошибок;
- скорость изменения числа устраненных ошибок, измеряемая относительно суммарного времени функционирования, пропорциональна интенсивности отказов.

Один из основных показателей надежности, который рассчитывается по модели Муса, - средняя наработка на отказ. Средняя наработка на отказ

$$T = T_0 \exp(\frac{C \cdot \tau}{M_0 T_0})$$

где T_0 – средняя наработка на отказ в начале испытаний;
C – коэффициент сжатия тестов.
Параметр T_0 можно предсказать из соотношения:

$$T_0 = \frac{1}{fKN_0}$$

где f – средняя скорость исполнения ПС, отнесенная к числу команд;
К – коэффициент проявления ошибок;
N0 – начальное число ошибок (можно рассчитать с помощью другой модели).
Надежность для оперативного периода т’ выражается равенством

$$R = \exp(-\frac{\tau'}{T})$$

Модель переходных вероятностей. Эта модель основана на марковском процессе. В начальный момент тестирования (t=0) в ПС было n ошибок. Предполагается, что в процессе тестирования выявляется по одной ошибке. Тогда последовательность состояний системы {n, n-1, n-2, n-3, …} соответствует периодам времени, когда предыдущая ошибка уже исправлена, а новая еще не обнаружена. Например, в состоянии n-5 пятая ошибка уже исправлена, а шестая еще не обнаружена.

Последовательность состояний {m, m-1, m-2, m-3, …} соответствует периодам времени, когда ошибки исправляются. Например, в состоянии m-1 вторая ошибка уже обнаружена, но еще не исправлена. Ошибки обнаруживаются с интенсивностью λ, исправляются с интенсивностью μ.

Предположим, что в какой-то момент времени процесс тестирования остановился. Совокупность возможных состояний системы будет: S={n, m, n-1, m-1, n-2, m-2, …}. Система может переходить из одного состояния в другое с определенной вероятностью Pij.

Статические модели надежности программных средств

Модель Миллса

Использование этой модели предполагает необходимость **перед началом тестирования искусственно вносить в программу некоторое количество известных ошибок**. Ошибки вносятся искусственным образом и фиксируются в протоколе искусственных ошибок. Специалист, проводящий тестирование, не знает ошибки. Предполагается, что **все ошибки имеют равную вероятность быть найденными в процессе тестирования**.

Тестируя ПС, собирается статистика об ошибках. В момент оценки надежности по протоколу все ошибки делятся на искусственные и собственные.

$$N = \frac{S \cdot n}{V}$$

где N – первоначальное число ошибок;

S – количество искусственных ошибок;

n – число найденных собственных ошибок;

V – число обнаруженных к моменту оценки искусственных ошибок.

Вероятность когда n=N

$$C = \begin{cases} 1, \text{если} \quad n > K \\ \dfrac{S}{S + K + 1}, \quad \text{если} \quad n \le K \end{cases}$$

где К – собственные ошибки

Для случая, когда оценка надежности производится до момента обнаружения всех S рассеяных ошибок

$$C = \begin{cases} 1, \quad \text{если} \quad n > K \\ (\dfrac{S}{V - 1}) / \left(\dfrac{S + K + 1}{K + V} \right), \text{если} \quad n \le K \end{cases}$$

Модель Липова

Липов модифицировал модель Миллса, рассмотрев вероятность обнаружения ошибки при использовании различного числа тестов.

Вероятность обнаружения n собственных и V внесенных:

$$Q(n,V) = \left(\frac{m}{n+V}\right) \cdot q^{n+V} (1-q)^{m-n-V} \cdot \frac{\frac{N}{n} \cdot \frac{S}{V}}{\frac{N+S}{n+V}}$$

где m – количество тетсов; q – вероятность обнаружения ошибки в каждом из m тестов.

Для использования модели должны выполнятся условия

$$N \geq n \geq 0$$

$$S \geq V \geq 0$$

$$m \geq n + V \geq 0$$

Значения N задаются соотношением

$$N = \begin{cases} \frac{S \cdot n}{V} & при\ n \geq 1, \quad V \geq 1 \\ n \cdot S & при \quad V = 0 \\ 0 & при\ n = 0 \end{cases}$$

Простая интуитивная модель

$$P(N_{12}) = \frac{\frac{N_1}{N_{12}} \cdot \frac{N - N_1}{N_2 - N_{12}}}{\frac{N}{N_{12}}}$$

Модель Коркорэна использует изменяющиеся вероятности отказов для различных типов ошибок

$$R = \frac{N_0}{N} + \sum_{i=1}^{K} \frac{Y_i (N_i - 1)}{N}$$

Модель Нельсона учитывает вероятность выбора определенного тестового набора для очередного выполнения программы

$$R = 1 - \sum_{i=1}^{K} \frac{n_i}{N_i} \cdot P_i$$