УДК 621.3.019.3

А.В. ФЕДУХИН[*], Н.В. СЕСПЕДЕС ГАРСИЯ[**]

АТРИБУТЫ И МЕТРИКИ ГАРАНТОСПОСОБНЫХ КОМПЬЮТЕРНЫХ СИСТЕМ

[*]Институт проблем математических машин и систем НАН Украины, Киев, Украина
[**]Институт проблем математических машин и систем НАН Украины, Киев, Украина

Анотація. *Розглянута атрибутивна модель гарантоздатності систем, проведено комплексний аналіз основних атрибутів і метрик гарантоздатності систем.*
Ключові слова: *гарантоздатність, безвідмовність, готовність, живучість, цілісність, конфіденційність, обслуговуваність, функціональна безпека.*

Аннотация. *Рассмотрена атрибутивная модель гарантоспособности систем, проведен комплексный анализ основных атрибутов и метрик гарантоспособности систем.*
Ключевые слова: *гарантоспособность, безотказность, готовность, живучесть, целостность, конфиденциальность, обслуживаемость, функциональная безопасность.*

Abstract. *The attribute model of systems dependability was considered; a complex analysis of the key attributes and metrics of systems dependability were performed.*
Keywords: *dependability, reliability, availability, survivability, integrity, confidentiality, serviceability, functional safety.*

1. Введение

Впервые понятие «гарантоспособные системы» было введено литовским, а впоследствии американским ученым А. Авиженисом (A. Avizienis). Гарантоспособность определялась им как свойство системы избегать отказов и обслуживания, более частых и более серьезных, чем установлено в спецификации, т.е. гарантоспособность всецело сводилась к свойствам безотказности и отказоустойчивости системы. Позже понятие гарантоспособности было расширено атрибутами безопасность и живучесть и понятием гарантоспособные вычисления. В результате чего модель гарантоспособности систем А. Авижениса [1], названная нами атрибутивной моделью, на сегодняшний день включает следующие составляющие:

– безотказность – свойство системы непрерывно сохранять работоспособное состояние в течение некоторого времени или наработки;

– готовность – способность системы выполнять необходимые функции при определенных условиях эксплуатации и технического обслуживания в заданный момент или фиксированный интервал времени при условиях обеспечения необходимыми внешними ресурсами;

– живучесть – свойство системы сохранять или восстанавливать способность выполнять основные функции в определенном объеме и на протяжении заданной наработки при изменении условий эксплуатации, структуры системы и (или) алгоритмов;

– целостность (внешняя безопасность) – свойство системы быть неизменной при функционировании в условиях случайных или преднамеренных искажений или разрушающих воздействий извне системы (внешним агентом);

– конфиденциальность (внутренняя безопасность) – свойство системы обеспечивать защиту от несанкционированного использования информации или технического средства,

ISSN 1028-9763. Математичні машини і системи, 2013, № 2

подмены информации или технического средства, повреждения информации или технического средства изнутри системы (внутренним агентом);

– обслуживаемость – способность системы подлежать техническому обслуживанию, модификации и ремонту;

– функциональная безопасность – способность системы при наличии отказа не причинять опасных (катастрофических) воздействий на человека (пользователя) или окружающую среду его обитания.

Иными словами, гарантоспособные системы – это высоконадежные, отказоустойчивые, безопасные и живучие системы с гарантированно достоверными вычислениями.

Вводимое нами понятие как уровень гарантоспособности системы интересует нас прежде всего на этапе ее проектирования, когда сравниваются между собой различные варианты исполнения системы. Однако достигнутый уровень гарантоспособности можно оценивать и экспериментальным путем на этапе подконтрольной эксплуатации системы.

Целью настоящих исследований является идентификация основных атрибутов гарантоспособности систем и создание предпосылок для решения задачи формализации обобщенного показателя гарантоспособности в аналитическом виде.

2. Метрики атрибутов гарантоспособности

Наиболее важным свойством гарантоспособных систем является свойство отказоустойчивости. Без этого свойства невозможно создать систему с высоким уровнем гарантоспособности. Отказоустойчивость напрямую или косвенно влияет на такие атрибуты, как безотказность, готовность, живучесть и функциональная безопасность. Кроме того, отказоустойчивость, основанная, как известно, на структурной избыточности и методах многоверсийного проектирования, определяет уровень гарантоспособности вычислений, выполняемых программными средствами системы. Рассмотрим каждый атрибут гарантоспособности в отдельности, выделим и прокомментируем его метрики.

Безотказность [2, 3]

Классические метрики безотказности систем, такие как вероятность безотказной работы $R(t)$ – вероятность того, что в пределах заданной наработки отказ объекта не возникает, средняя наработка до отказа (на отказ) $T_{ср}$ – математическое ожидание наработки объекта до первого отказа (на отказ), параметр потока отказов $\omega(t)$ – отношение математического ожидания числа отказов восстанавливаемого объекта за достаточно малую его наработку к значению этой наработки не в полном объеме характеризует безотказность системы, так как не учитывает основное свойство гарантоспособных систем – их отказоустойчивость. Нами предлагается набор специальных метрик безотказности, учитывающих свойство отказоустойчивости системы, заложенное при проектировании.

Вероятность безотказной работы отказоустойчивой системы ${}^{f}_{c}R^{q}_{s}$:

$$ {}^{f}_{c}R^{q}_{s} = c^{s}(1-{}^{f}F^{q}_{s}), \qquad (1) $$

где ${}^{f}F^{q}_{s}$ – функция вероятности отказа;

s – количество резервов, изначально доступных для подключения;

q – количество модулей одного типа, работающих параллельно (характеристика актуальна для систем, производительность которых зависит от количества одновременно работающих ресурсов);

c – степень компенсации последствий отказа [1] (условная вероятность того, что при возникновении отказа в работающей системе последняя способна восстановить информацию и продолжить ее обработку без долговременной потери данных);

f – способность модуля допускать f одиночных отказов до того, как он станет неработоспособным.

Принимая гипотезу о DN-распределении наработки до отказа элементов, модулей и системы в целом, вероятность отказа будем вычислять следующим образом:

$$ {}^{f}F_{s}^{q} = DN(x; v, f, q, s), \tag{2}$$

где v – коэффициент вариации наработки до отказа;

x – относительная наработка ($x = \dfrac{t}{T_{ср}}$, t – время работы, $T_{ср}$ – средняя наработка до отказа (на отказ).

Функция вероятности отказа для DN-распределения имеет следующий вид:

$$ DN(x; v) = \Phi\left(\frac{x-1}{v\sqrt{x}}\right) + \exp\left(2v^{-2}\right)\Phi\left(-\frac{x+1}{v\sqrt{x}}\right), \tag{3}$$

где $\Phi(*)$ – функция нормированного нормального распределения.

Если любой из параметров метрики ${}_{c}^{f}R_{s}^{q}$ опускается, то по умолчанию предполагается $q=1$, $c=1$, $f=0$, $s=0$. Параметры s, c и f являются параметрами, увеличение которых приводит к увеличению общей безотказности системы.

Порог сравнения информации в системе M_c:

$$ M_c = \prod_{i=1}^{n} M_{ci}, \tag{4}$$

где M_{ci} - порог сравнения i-го последовательно включенного сравнивающего устройства.

Число работоспособных конфигураций системы U_c:

$$ U_c = \prod_{i=1}^{n} U_{ci}, \tag{5}$$

где U_{ci} - число работоспособных конфигураций i-ой подсистемы.

Число неизбыточных каналов системы N_c - характеристика объема аппаратных затрат, необходимого для достижения данного уровня безотказности системы.

Вероятность безотказной работы неизбыточного канала системы $R_к(t)$ - характеристика уровня надежности элементов и составных частей неизбыточного канала системы.

При сравнении вариантов исполнения системы по уровню безотказности рекомендуется использовать относительный критерий безотказности - отношение отрезков времени, по истечении которых вероятности безотказной работы конкурирующих конфигураций систем равны вероятности безотказной работы, установленной в спецификации $R_{спец}(t)$:

$$ I_{12} = \frac{t_{C2}}{t_{C1}}, \tag{6}$$

где t_{C1} – время достижения системой №1 характеристики безотказности $R_{C1}(t_{C1}) = R_{спец}$;

t_{C2} – время достижения системой №2 характеристики безотказности $R_{C2}(t_{C2}) = R_{спец}$.

Готовность [2, 4]

Готовность является очень важным атрибутом гарантоспособности, особенно для систем с непрерывным циклом функционирования и систем критического использования. Метриками данного атрибута являются:

1) Коэффициент готовности $K_г$ – вероятность того, что объект окажется в работоспособном состоянии в произвольный момент времени, кроме планируемых периодов, в течение которых применение объекта по назначению не предусматривается.

$$K_г = T_{ср} / (T_{ср} + T_в), \tag{7}$$

где $T_{ср}$ – средняя наработка на отказ (время работы без сбоев) системы;

$T_в$ – среднее время восстановления системы.

2) Коэффициент оперативной готовности $K_{ог}$ – вероятность того, что объект окажется в работоспособном состоянии в произвольный момент времени.

$$K_{ог} = K_г \cdot R(t_{рб}), \tag{8}$$

где $R(t_{рб})$ – вероятность безотказной работы системы на момент времени $t_{рб}$.

Живучесть [3, 5]

Живучесть является специфическим атрибутом гарантоспособности систем и раньше применялся исключительно для систем военного назначения. Живучесть – это свойство, закладываемое в систему во время проектирования, которое позволяет сохранять полную или ограниченную работоспособность системы вследствие изменения условий эксплуатации, структуры и алгоритмов при наличии отказавших составных частей и не допускать перехода их отказов в критические. В настоящее время это свойство распространяют и на распределенные системы общего назначения. Метрики данного атрибута вытекают из соответствующих метрик безотказности отказоустойчивых систем:

1) Коэффициент живучести $G(q^i)$ – отношение числа состояний, соответствующих работоспособной системе, ко всей совокупности состояний.

$$G(q^i) = M / C_l^i, \tag{9}$$

где M – количество работоспособных состояний системы для обобщенного отказа i-той кратности;

C_l^i – общее количество состояний системы;

i – кратность обобщенного отказа;

l – количество функциональных единиц живучести системы.

2) Коэффициент деградации $D(q^i)$ – отношение числа состояний, соответствующих неработающей системе, к общему количеству состояний системы.

$$D(q^i) = N / C_l^i, \tag{10}$$

где N – число состояний, соответствующих неработающей системе;

C_l^i – общее количество состояний системы;

i – кратность обобщенного отказа;

l – количество функциональных единиц живучести системы.

3) Выживаемость системы $R(n)$ – вероятность сохранения работоспособности при n-кратном неблагоприятном воздействии (НВ).

$$R(n)=1-Q(n)=P(F=1/A_n), \tag{11}$$

где F – функция работоспособности системы, принимающая значение 1, если система работоспособна, и 0, если система неработоспособна;

A_n – событие, происходящее при n-кратном появлении НВ.

Обслуживаемость [6]

Ослуживаемость является важным атрибутом для систем с непрерывным циклом функционирования и систем критического использования. Метриками данного атрибута являются:

1) Продолжительность технического обслуживания $T_{об}$ – среднее время выполнения работ по обслуживанию системы, предусмотренное технической документацией.

2) Трудоемкость технического обслуживания $T_{трi}$ – средние трудозатраты на проведение одного технического обслуживания (ремонта) системы i-го вида.

3) Стоимость технического обслуживания C_{i} – средняя стоимость одного технического обслуживания (ремонта) системы i-го вида.

4) Среднее время восстановления $T_в$ – промежуток времени, затраченный на восстановление работоспособного состояния системы или его составной части после отказа.

5) Коэффициент технического использования $K_{ти}$ – отношение математического ожидания интервалов времени пребывания системы в работоспособном состоянии за некоторый период эксплуатации к сумме математических ожиданий интервалов времени простоев, техобслуживания и ремонтов.

$$K_{ти}(t)=K_г(t)\frac{t_д}{t_н}, \tag{12}$$

где $K_г(t)$ – коэффициент готовности системы;

$t_н$ – годовой номинальный фонд времени, в течение которого объект может использоваться по назначению;

$t_д$ – годовой действительный фонд времени работы объекта, равный номинальному фонду, за вычетом простоев, связанных с проведением планового технического обслуживания (периодических профилактик) и ремонта.

Функциональная безопасность [7, 8]

Функциональная безопасность является очень важным атрибутом для систем критического использования, связанных с безопасностью людей и окружающей среды обитания человека (системы энергетики, химической промышленности, транспорта и т.д.). Для таких систем принято нормировать допустимые уровни всех или некоторых метрик. Метриками данного атрибута являются:

1) Вероятность безопасной работы $R_{ОП}(t)$ – вероятность того, что в пределах заданной наработки опасный отказ системы не наступает.

$$R_{ОП}(t)=1-F_{ОП}(t), \tag{13}$$

где $F_{ОП}(t)$ – функция распределения наработки до опасного отказа.

2) Вероятность опасного отказа $Q_{ОП}(t)$ – вероятность того, что в пределах заданной наработки опасный отказ наступает хотя бы один раз.

$$Q_{ОП}(t) = F_{ОП}(t) = 1 - R_{ОП}(t). \quad (14)$$

3) Средняя наработка до опасного отказа $T_{ОП}$ – математическое ожидание наработки системы до первого опасного отказа.

4) Параметр потока опасных отказов $\omega_{ОП}(t)$ – отношение математического ожидания числа опасных отказов восстанавливаемой системы за произвольно малую ее наработку к значению этой наработки.

5) Средняя наработка на опасный отказ $T_{ОПср}$ – отношение суммарной наработки восстанавливаемой системы к математическому ожиданию числа опасных отказов в течение этой наработки

6) Коэффициент безопасности $K_{Б}$ – вероятность того, что система окажется в работоспособном или защитном состоянии в произвольный момент времени, кроме планируемых периодов, в течение которых применение объекта по назначению не предусматривается.

$$K_{Б} = T_{ОПср} / (T_{ОПср} + T_{ОПв}), \quad (15)$$

где $T_{ОПв}$ — среднее время восстановления после опасного отказа.

Целостность [9]

Целостность является важным атрибутом для открытых и распределенных систем, в основе которых лежит сетевая идеология. Нами декларируется этот атрибут как свойство системы быть неизменной при функционировании в условиях случайных или преднамеренных искажений или разрушающих воздействий со стороны внешнего агента, то есть атрибут внешней безопасности системы. Метриками данного атрибута являются:

1) Уровень целостности вычислительных ресурсов L_{PC} – характеристика способности системы исключать непредусмотренные структурные изменения и предоставляемые услуги.

2) Уровень целостности программных ресурсов L_{P} – характеристика способности системы исключать непредусмотренные изменения программных ресурсов.

3) Уровень целостности информации L_{I} – характеристика способности системы обеспечивать неизменность информации в условиях случайного и(или) преднамеренного искажения (разрушения).

Конфиденциальность [10]

Конфиденциальность также является важным атрибутом для открытых и распределенных систем, в основе которых лежит сетевая идеология, а также для систем критического применения. Нами этот атрибут декларируется как свойство системы обеспечивать защиту от несанкционированного использования информации или технического средства, подмены информации или технического средства, повреждения информации или технического средства со стороны внутреннего агента, то есть атрибут внутренней безопасности системы. Метриками данного атрибута являются:

1) Вероятность угроз P_{D} – вероятность нарушений конфиденциальности технических средств и(или) информации.

2) Уровень доступности L_{A} – характеристика способности системы обеспечивать физическую защиту от возможности изменения заданных параметров технических и (или) информационных ресурсов в заданных точках за конечное время.

3) Уровень секретности L_S – характеристика способности системы сохранять секретность технических и (или) информационных ресурсов.

3. Выводы

Определение комплекса метрик атрибутов гарантоспособности позволяет подойти к решению задачи формализации обобщенного критерия уровня достигнутой гарантоспособности разрабатываемой системы.

С этой целью предлагается каждый атрибут модели разбивать на комплекс метрик, которые могут быть измеряемы расчетными, экспериментальными или экспертными методами.

На основе количественных оценок метрик предлагается вычислять количественные оценки атрибутов и далее через них вычислять количественные оценки достигнутого уровня гарантоспособности анализируемой системы для различных вариантов ее исполнения.

В качестве математической модели, необходимой для вычисления уровня гарантоспособности системы, предлагается использовать линейный функционал, составляющими которого являются нормированные значения атрибутов и метрик с соответствующими весовыми коэффициентами. Выбор величин весовых коэффициентов зависит от особенностей применения каждой конкретной системы.

В тех случаях, когда метрики не имеют аналитических оценок (например, метрики атрибутов целостность и конфиденциальность), их измерение предлагается осуществлять экспертными методами.

СПИСОК ЛИТЕРАТУРЫ

1. Avizienis A. Basic Concepts and Taxonomy of Dependable and Secure Computing / A. Avizienis, J.-C. Laprie, B. Randell [et al.] // IEEE Trans. on Dependable and Secure Computing. – 2004. – Vol. 1, N 1. – P. 11 – 33.
2. ДСТУ 2860-94. Надійність техніки. Терміни та визначення. – Киев: Изд-во Госстандарта, 1994. – 89 с.
3. Сербін В.Г. Визначення і формалізація основних показників гарантоздатності живучих комп'ютерних систем керування на основі ймовірнісно-фізичного підходу для їх проектної оцінки і прогнозування / В.Г. Сербін, А.І. Сухомлин // Математичні машини і системи. – 2012. – № 4. – С. 182 – 189.
4. Кривуля Г.Ф. Готовность компьютеризованных систем управления и компетентность пользователя / Г.Ф. Кривуля, А.С. Шкиль, Е.В. Гаркуша // Інфомаційно-керуючі системи на залізничному транспорті. – 2011. – № 5. – С. 12 – 17.
5. Черкесов Г.Н. Методы и модели оценки живучести сложных систем / Черкесов Г.Н. – М.: Знание, 1987. – 32 с.
6. ГОСТ 18322-78. Система технического обслуживания и ремонта техники. Термины и определения. – М.: Издательство стандартов, 1978. – 16 с.
7. ГОСТ 32.17–92. Безопасность железнодорожной автоматики и телемеханики. Термины и определения. – СПб.: ПИИТ, 1992. – 33 с.
8. Сертификация и доказательство безопасности систем железнодорожной автоматики / [В.В. Сапожников, Вл.В. Сапожников, В.И. Талалаев и др.]; под ред. Вл.В. Сапожникова. – М.: Транспорт, 1997. – 288 с.
9. Рекомендации по стандартизации «Информационные технологии. Основные термины и определения в области технической защиты информации» (Р 50.1.053-2005).
10. ITSEC (June 1991). Information Technology Security Evaluation Criteria (ITSEC): Preliminary Harmonised Criteria. Document COM (90) 314, Version 1.2. Commission of the European Communities [Електронний ресурс]. – Режим доступу: http://www.ssi.gouv.fr/site_documents/ITSEC/ITSEC-uk.pdf. Retrieved 2006-06-02.

Стаття надійшла до редакції 24.04.2013