УДК 621.3.019.3

А.В. ФЕДУХИН*

ЭКСПЕРТНАЯ ОЦЕНКА УРОВНЯ ГАРАНТОСПОСОБНОСТИ КОМПЬЮТЕРНЫХ СИСТЕМ

*Институт проблем математических машин и систем НАН Украины, г. Киев, Украина

Анотація. *У статті розглянуті питання використання атрибутивної моделі гарантоздатності (АМГ) для кількісної оцінки досягнутого рівня гарантоздатності розроблюваних комп'ютерних систем. Ідея назви «атрибутивна модель» запозичена з філософії, де аналогічну назву має атрибутивна модель поняття «матерія». У нашому випадку цю назву ми поширюємо на поняття «гарантоздатні комп'ютерні системи» (ГКС) і формулюємо атрибутивну модель як комплексну властивість, що включає такі атрибути: безвідмовність, готовність, обслуговуваність, достовірність, живучість, функціональну безпеку, конфіденційність і цілісність. З усіх вимірюваних атрибутів АМГ в останні роки найбільш пильна увага приділяється атрибутам готовність, функціональна безпека, живучість і конфіденційність. Це пов'язано з усе зростаючим впливом інформаційних технологій на всі сфери діяльності і існування людства. Як альтернатива розглядаються дві моделі: векторна і скалярна. Векторна модель являє собою набір векторів (характеристик), які оцінюють окремі властивості гарантоздатності (безвідмовність, готовність, живучість, обслуговуваність, достовірність, конфіденційність, цілісність, функціональну безпеку). Скалярна модель являє собою узагальнену (інтегральну) оцінку рівня гарантоздатності. Скалярна модель базується на метричному підході, при якому будується максимально деталізована модель гарантоздатності як ієрархія первинних і вторинних властивостей і їх характеристик, які оцінюються експертним шляхом або шляхом обчислень чи вимірювань. Далі проводиться згортка метрик за допомогою аналітичної моделі (функціоналу) обґрунтованого виду. Прагнення досягти максимально можливого рівня гарантоздатності має бути обґрунтованим, так як воно пов'язане з великими витратами коштів та часу на розробку і виробництво системи, що неминуче відіб'ється на збільшенні її вартості.*

Ключові слова: *атрибутивна модель, гарантоздатність, атрибути, метрики, критерії оцінки, рівень гарантоздатності.*

Аннотация. *В статье рассмотрены вопросы использования атрибутивной модели гарантоспособности (АМГ) для количественной оценки достигнутого уровня гарантоспособности разрабатываемых компьютерных систем. Идея названия «атрибутивная модель» заимствована из философии, где аналогичное название имеет атрибутивная модель понятия «материя». В нашем случае это название мы распространяем на понятие «гарантоспособность компьютерных систем» (ГКС) и формулируем атрибутивную модель как комплексное свойство, включающее следующие атрибуты: безотказность, готовность, обслуживаемость, достоверность, живучесть, функциональную безопасность, конфиденциальность и целостность. Из всех измеряемых атрибутов АМГ в последние годы наиболее пристальное внимание уделяется атрибутам готовность, функциональная безопасность, живучесть и конфиденциальность, что сопряжено с все возрастающим влиянием информационных технологий на все сферы деятельности и существования человечества. В качестве альтернативы рассматриваются две модели: векторная и скалярная. Векторная модель представляет собой набор векторов (характеристик), оценивающих отдельные свойства гарантоспособности (безотказность, готовность, живучесть, обслуживаемость, достоверность, конфиденциальность, целостность, функциональную безопасность). Скалярная модель представляет собой обобщенную (интегральную) оценку уровня гарантоспособности. Скалярная модель базируется на метрическом подходе, при котором строится максимально детализированная модель гарантоспособности как иерархия первичных и вторичных свойств и их характери-*

ISSN 1028-9763. Математичні машини і системи, 2019, № 2

стик, оцениваемых экспертным путем или путем вычислений или измерений. Далее производится свертка метрик с помощью аналитической модели (функционала) обоснованного вида. Стремление достичь максимально возможного уровня гарантоспособности должно быть обоснованным, так как оно сопряжено с большими затратами средств и времени на разработку и производство системы, что неминуемо отразится на увеличении ее стоимости.
Ключевые слова: *атрибутивная модель, гарантоспособность, атрибуты, метрики, критерии оценки, уровень гарантоспособности.*

Abstract. *The article deals with the use of the attribute model of dependability (AMD) for a quantitative assessment of the achieved level of dependability of the developed computer systems. The idea of the name "attribute model" is borrowed from philosophy, where the attribute name has the attribute model of the concept "matter". In our case, this name we extend to the concept of "dependable computer systems" (DCS) and formulate an attribute model as a complex property that includes the following attributes: reliability, availability, maintainability, reliability, survivability, functional security, confidentiality and integrity. Of all the measured attributes of AMD in recent years, the most attention is paid to the attributes readiness, functional safety, vitality and confidentiality, which is associated with the ever-increasing influence of information technologies on all spheres of activity and existence of mankind. As an alternative, two models are considered – vector and scalar. A vector model is a set of vectors (characteristics) that evaluate individual properties of warranty (non-failure operation, availability, survivability, maintainability, reliability, confidentiality, integrity, functional safety). The scalar model is a generalized (integral) assessment of the level of dependability. The scalar model is based on the metric approach, which builds the most detailed model of dependability, as a hierarchy of primary and secondary properties and their characteristics, estimated by expert means or by calculations or measurements. Next, the convolution of metrics using an analytical model (functional) of a reasonable form is performed. The desire to achieve the highest possible level of dependability should be justified, since it is associated with large expenditures of funds and times for the development and production of the system, which will inevitably affect the cost increase.*
Keywords: *attribute model, dependability, attributes, metrics, evaluation criteria, level of dependability.*

1. Введение

Целостное и систематизированное представление об изучаемой действительности целесообразно выражать в форме идеализированной модели, которая отражает ее фундаментальные объективные законы и делает их сущность наглядной.

Например, философское определение понятия «материя» строится на основе системы атрибутов (неотъемлемых, существенных свойствах объекта), раскрывающих ее сущность [1]. Такими атрибутами материи являются, прежде всего, движение, взаимодействие и отражение. Даже краткий анализ содержания атрибутов материи позволяет констатировать, что они диалектически связаны и взаимообусловлены между собой.

Идею построения атрибутивной модели понятия «материя» спроецируем на наш объект – понятие «гарантоспособность компьютерных систем» (ГКС) и сформулируем атрибутивную модель этого понятия (АМГ), включающую следующие атрибуты: безотказность, готовность, обслуживаемость, достоверность, живучесть, функциональную безопасность, конфиденциальность и целостность.

В тех случаях, когда атрибуты имеют абстрактный смысл, то есть недоступны прямому наблюдению (например, конфиденциальность и целостность), их значения определяются расчетным путем с использованием результатов замера других сопутствующих наблюдаемых величин или экспертным методом. Тем не менее, в общем виде они выступают как измеряемые характеристики, поэтому они также включаются в атрибутивную модель понятия ГКС. Из всех измеряемых атрибутов АМГ в последние годы наиболее пристальное внимание уделяют атрибутам готовность, функциональная безопасность, живучесть и конфиденциальность.

Предложенную атрибутивную модель ГКС можно рассматривать как средство реализации интеграционных тенденций современной науки и техники в сфере информационных технологий. Данная модель может определять направление и способ изучения не только частных, но и обобщенных характеристик гарантоспособности, положительно влиять на осмысление фундаментальных понятий, принципов и парадигм и служить методологической основой построения и развития современной теории гарантоспособных компьютерных систем.

Учитывая комплексный характер гарантоспособности как сложного свойства системы, для ее оценки могут использоваться два типа моделей [2]:

• векторная, которая представляет собой набор векторов (характеристик), оценивающих отдельные свойства гарантоспособности (безотказность, готовность, живучесть, обслуживаемость, достоверность, конфиденциальность, целостность, функциональную безопасность) [3];

• скалярная, которая представляет собой обобщенную (интегральную) оценку уровня гарантоспособности.

Скалярная модель может быть получена на основе метрического подхода, при котором строится максимально детализированная модель гарантоспособности как иерархия первичных и вторичных свойств и их характеристик, определяемых набором метрик, оцениваемых экспертным путем или путем вычислений или измерений. Далее производится свертка метрик с помощью аналитической модели (функционала) обоснованного вида.

Целью исследования является разработка методологического подхода к количественной оценке уровня гарантоспособности компьютерных систем на основе атрибутивной модели гарантоспособности в вектроной и скалярной формах представления.

2. Векторная модель гарантоспособности системы

2.1. Безотказность [4, 5]

Безотказность является очень важным атрибутом гарантоспособности, особенно для систем с высокими требования по надежности.

Метрики данного атрибута.

Вероятность безотказной работы $R(t)$ – вероятность того, что в пределах заданной наработки отказ объекта не возникает. Вероятность безотказной работы отказоустойчивой системы ${}^{f}_{c}R^{q}_{s}$ вычисляется по формуле

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

где ${}^{f}F^{q}_{s}$ – функция вероятности отказа с учетом параметров f, q и s, s – количество резервов, изначально доступных для подключения, q – количество модулей, обеспечивающих заданную производительность системы (характеристика актуальна для систем, производительность которых зависит от количества одновременно работающих ресурсов), c – степень компенсации последствий отказа (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.

Вероятность безотказной работы неизбыточного канала системы $R_{к}(t)$ – характеристика уровня надежности элементов и составных частей неизбыточного канала системы.

Коэффициент отказоустойчивости $K_{ОУ}$ – отношение средних наработок на отказ отказоустойчивой и нерезервированной системы:

$$K_{OУ} = \frac{T_{OУ}}{T_{HP}}, \tag{2}$$

где T_{HP} – средняя наработка на отказ нерезервированной системы, $T_{OУ}$ – средняя наработка на отказ отказоустойчивой системы.

Примечание 1. Ниже для каждого атрибута приводятся примеры вычисления параметров векторной модели гарантоспособности.

Экспертная оценка уровня исполнения метрики M_i (критерия U_i или K_i) осуществляется следующим образом:

- при полном отсутствии выполнения M_i =0;
- при выполнении на 10% – 90% M_i =0,1–0,9;
- при 100% выполнении M_i =1.

Таблица 1 – Атрибут *Безотказность*

№ п/п	Метрика	Уровень исполнения метрики, M_{ij}	Экспертная оценка уровня исполнения	Вес, β_{ij}	$\beta_{ij}M_{ij}$
1	${}_{c}^{f}R_{s}^{q}$	0-1	0,99	0,5	0,495
2	$R_к(t)$	0-1	0,9	0,1	0,09
3	$K_{OУ}$	0-1	0,99	0,4	0,396

$$A_Б = \sum_{j=1}^{m_i} \beta_{ij} M_{ij} = 0{,}981.$$

2.2. Готовность [6]

Готовность является очень важным атрибутом гарантоспособности, особенно для систем с непрерывным циклом функционирования и систем критического использования.

Метрики данного атрибута.

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.

$$K_Г = \frac{T}{(T + T_B)}, \tag{3}$$

где T – средняя наработка на отказ (время работы без сбоев) системы, T_B – среднее время восстановления системы.

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

$$K_{OГ} = K_Г \cdot R(t_н), \tag{4}$$

где $R(t_н)$ – вероятность безотказной работы системы на момент времени $t_н$.

Таблица 2 – Атрибут *Готовность*

№ п/п	Метрика	Уровень исполнения метрики, M_{ij}	Экспертная оценка уровня исполнения	Вес, β_{ij}	$\beta_{ij}M_{ij}$
1	$K_Г$	0-1	0,99	0,5	0,495
2	$K_{ОГ}$	0-1	0,9	0,5	0,45

$$A_Г = \sum_{j=1}^{m_i} \beta_{ij} M_{ij} = 0{,}945.$$

2.3. Обслуживаемость [7]

Обслуживаемость является важным атрибутом для систем с непрерывным циклом функционирования и систем критического использования.

Метрики данного атрибута.

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

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

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.

$$K_{ТИ}(t) = K_Г(t)\frac{t_{ДФ}}{t_{НФ}}, \qquad (5)$$

где $K_г(t)$ – коэффициент готовности системы, $t_{НФ}$ – годовой номинальный фонд времени, в течение которого объект может использоваться по назначению, $t_{ДФ}$ – годовой действительный фонд времени работы объекта, равный номинальному фонду, за вычетом простоев, связанных с проведением планового технического обслуживания (периодических профилактик) и ремонта.

Таблица 3 – Атрибут *Обслуживаемость*

№ п/п	Метрика	Уровень исполнения метрики, M_{ij}	Экспертная оценка уровня исполнения	Вес, β_{ij}	$\beta_{ij}M_{ij}$
1	$T_{ТО}$	0-1	0,9	0,2	0,18
2	$T_В$	0-1	0,999	0,4	0,3996
3	$K_{ТИ}$	0-1	0,95	0,4	0,38

$$A_О = \sum_{j=1}^{m_i} \beta_{ij} M_{ij} = 0{,}9596.$$

2.4. Достоверность [8–10]

При рассмотрении функционирования КС различных структур в качестве показателя достоверности будем использовать вероятность получения достоверного результата в ходе проведения вычислений (обработки данных).

Достоверность функционирования КС за время t предлагается вычислять с помощью феноменологической модели:

$$D = [d_M \cdot {}^{f}_{c} R_s^q] \cdot k, \tag{6}$$

где d_M – достоверность вычислений модуля – условная вероятность того, что значение вычисляемого модулем определяющего параметра π отличается от истинного значения этого параметра в пределах требуемой точности, π определяющий параметр – критерий правильного функционирования модуля, ${}^{f}_{c} R_s^q$ – вероятность безотказной работы системы за время t, k – коэффициент, учитывающий кратность сравнения информации между каналами в процессе функционирования системы или порог сравнения последовательно включенного сравнивающего устройства.

Таблица 4 – Атрибут *Достоверность*

№ п/п	Метрика	Уровень исполнения метрики, M_{ij}	Экспертная оценка уровня исполнения	Вес, β_{ij}	$\beta_{ij} M_{ij}$
1	*D*	0-1	0,99	1,0	0,99

$$A_Д = \sum_{j=1}^{m_i} \beta_{ij} M_{ij} = 0{,}99.$$

2.5. Живучесть [11–17]

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.

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

$$G(q^i) = \frac{M}{C_l^i}, \tag{7}$$

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.

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

$$D(q^i) = \frac{N}{C_l^i}, \tag{8}$$

где N – число состояний, соответствующих неработающей системе, C_l^i – общее количество состояний системы, i – кратность обобщенного отказа, l – количество функциональных единиц живучести системы.

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

$$R(n) = 1 - Q(n) = P(F = 1/ A_n), \tag{9}$$

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.

Таблица 5 – Атрибут *Живучесть*

№ п/п	Метрика	Уровень исполнения метрики, M_{ij}	Экспертная оценка уровня исполнения	Вес, β_{ij}	$\beta_{ij} M_{ij}$
1	$G(q^i)$	0-1	0,99	0,5	0,495
2	$D(q^i)$	0-1	0,9	0,1	0,09
3	$R(n)$	0-1	0,99	0,4	0,396

$$A_Ж = \sum_{j=1}^{m_i} \beta_{ij} M_{ij} = 0{,}981.$$

2.6. Функциональная безопасность [18–26]

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.

Метрики данного атрибута.

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

$$R_{ОП}(t) = 1 - F_{ОП}(t), \tag{10}$$

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

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

$$Q_{ОП}(t) = F_{ОП}(t) = 1 - R_{ОП}(t). \tag{11}$$

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

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.

$$K_Б = \frac{T_{ОП}}{(T_{ОП} + T_{ОПВ})}, \tag{12}$$

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

Таблица 6 – Атрибут *Функциональная безопасность*

№ п/п	Метрика	Уровень исполнения метрики, M_{ij}	Экспертная оценка уровня исполнения	Вес, β_{ij}	$\beta_{ij} M_{ij}$
1	$R_{ОП}(t)$	0-1	0,99	0,1	0,099
2	$Q_{ОП}(t)$	0-1	0,99	0,5	0,495
3	$T_{ОП}$	0-1	0,9	0,1	0,09
4	$K_Б$	0-1	0,99	0,3	0,297

$$A_{ФБ} = \sum_{j=1}^{m_i} \beta_{ij} M_{ij} = 0{,}981.$$

2.7. Конфиденциальность [27–30]

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, от подмены информации или технического средства, от повреждения информации или технического средства.

Метрики данного атрибута.

Вероятность угроз $P_У$ – вероятность нарушений конфиденциальности технических средств и/или информации.

Уровень доступности $L_Д$ – характеристика способности системы обеспечивать физическую защиту от возможности изменения заданных параметров технических и (или) информационных ресурсов в заданных точках за конечное время.

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

Общим для моделей обеспечения конфиденциальности является то, что все они направлены на введение определенных обязательных процедур анализа конфиденциальности программ, средств, ресурсов и пользователей, которые взаимодействуют с ГКС.

Предлагается наиболее общий подход к оценке конфиденциальности системы. Каждой метрике конфиденциальности соответствует набор критериев, по которым происходит ее оценка (табл. 8), которую и принимает во внимание эксперт. Набор критериев можно менять в зависимости от назначения и специфики функционирования конкретной ГКС.

Таблица 7 – Атрибут *Конфиденциальность*

№ п/п	Метрика	Уровень исполнения метрики, M_{ij}	Экспертная оценка уровня исполнения	Вес, β_{ij}	$\beta_{ij}M_{ij}$
1	$P_У$	0-1	0,95	0,2	0,19
2	$L_Д$	0-1	0,99	0,4	0,396
3	L_C	0-1	0,95	0,4	0,38

$$A_K = \sum_{j=1}^{m_i} \beta_{ij} M_{ij} = 0{,}966.$$

Таблица 8 – Метрики и критерии конфиденциальности

Метрики конфиденциальности	Наименование критерия	Уровень исполнения критерия, U_i
Вероятность угроз $P_У$ – вероятность нарушений конфиденциальности технических средств и (или) информации	Правильность эксплуатации ВР	0-1
	Безопасность эксплуатации ВР	0-1
	Способность проверять и сохранять данные	0-1
	Способность защиты от серьёзных последствий для конфиденциальности в случае ошибок	0-1
	Способность восстанавливать конфиденциальность после сбоев и ошибок	0-1
	Наличие защиты от нарушений авторского права	0-1
	Наличие функций восстановления конфиденциальности	0-1
	Наличие функций контроля конфиденциальности	0-1
	Наличие защиты конфиденциальности при работе в локальной сети	0-1
	Наличие защиты конфиденциальности при работе в среде Интернет	0-1
	Наличие функций идентификации и аутентификации	0-1
	Наличие средств мониторинга и оповещения	0-1
	Наличие средств обработки ошибок	0-1
Уровень доступности $L_Д$ – характеристика способности системы обеспечивать физическую защиту от возможности изменения заданных параметров технических и информационных ресурсов в заданных точках за конечное время	Наличие документа, регламентирующего доступ к секретной информации	0-1
	Наличие документа, регламентирующего доступ к техническим средствам	0-1
	Наличие паролей доступа к информационным ресурсам	0-1
	Наличие физической защиты технических ресурсов	0-1
	Наличие защиты технических ресурсов программными средствами	0-1
	Наличие у персонала разрешения на работу с секретными техническими и (или) информационными ресурсами	0-1

Продолж. табл. 8

	Наличие средств восстановления процесса в случае сбоев ОС, процессора, внешних устройств	0-1
	Наличие требований по устойчивости функционирования при наличии ошибок во входных данных, ошибок пользователя, отсутствия необходимых данных (на диске, в файле, в БД и т.д.)	0-1
	Совместимость с техническими средствами	0-1
	Совместимость с системными программными средствами	0-1
	Совместимость с другим программным обеспечением, включая обмен данными (с текстовыми, графическими редакторами, БД и др.)	0-1
	Наличие устойчивости функционирования при наличии ошибок во входных данных, ошибок пользователя, отсутствия необходимых данных (на диске, в файле, в БД и т.д.)	0-1
	Возможность обработки ошибочных ситуаций	0-1
	Наличие возможности повторного старта с точки останова	0-1
Уровень секретности L_C – характеристика способности системы сохранять секретность технических и(или) информационных ресурсов	Наличие документа, регламентирующего доступ к секретной информации по уровням секретности	0-1
	Наличие документа, регламентирующего доступ к техническим средствам по уровням секретности	0-1
	Наличие паролей доступа к информационным ресурсам	0-1
	Наличие физической защиты технических ресурсов	0-1
	Наличие защиты технических ресурсов программными средствами	
	Наличие у персонала разрешения на работу с секретными техническими и(или) информационными ресурсами	0-1
	Наличие информации о способности проверять правильность вводимой/выводимой информации	0-1
	Наличие информации о процедурах хранения данных	0-1
	Наличие тестов для проверки допустимых значений входных/выходных данных	0-1
	Наличие системы контроля полноты входных/выходных данных	0-1
	Наличие средств контроля корректности входных/выходных данных	0-1
	Наличие средств контроля непротиворечивости входных/выходных данных	0-1
	Наличие проверки параметров и адресов по диапазону значений	0-1
	Наличие обработки предельных значений	0-1
	Наличие информации о способности восстанавливаться после ошибок	0-1

Каждой метрике атрибута конфиденциальность соответствует набор критериев оценки, количество которых равно n. Уровень исполнения критерия оценки определяется величиной U_i $(i = 1, \ldots n)$, которая находится в диапазоне значений 0÷1. Далее, по формулам, приведенным ниже, рассчитываются показатели реализации метрик.

$$P_У = \frac{\sum_{i=1}^{n} U_i}{n},\ L_Д = \frac{\sum_{i=1}^{n} U_i}{n}.\ L_C = \frac{\sum_{i=1}^{n} U_i}{n}, \qquad (13)$$

где n – количество критериев метрики.

Примечание 2. Если значения метрик $P_У$, $L_Д$, L_C более 0,9, то система соответствует удовлетворительному уровню конфиденциальности.

2.8. Целостность [31–33]

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.

Метрики данного атрибута.

Уровень целостности вычислительных ресурсов $L_{ВР}$ – характеристика способности системы исключать непредусмотренные структурные изменения и предоставляемые услуги.

Уровень целостности программных ресурсов $L_{ПР}$ – характеристика способности системы исключать непредусмотренные изменения программных ресурсов.

Уровень целостности информации $L_И$ – характеристика способности системы обеспечивать неизменность информации в условиях случайного и(или) преднамеренного искажения (разрушения).

Общим для моделей обеспечения целостности является то, что все они направлены на введение определенных обязательных процедур анализа целостности программ, средств, ресурсов и пользователей, которые взаимодействуют с ГКС.

Подход к оценке метрик целостности аналогичен подходу, используемому при оценке метрик конфиденциальности, то есть с использованием табл. 10.

Таблица 9 – Атрибут *Целостность*

№ п/п	Метрика	Уровень исполнения метрики, M_{ij}	Экспертная оценка уровня исполнения	Вес, β_{ij}	$\beta_{ij} M_{ij}$
1	$L_{ВР}$	0-1	0,9	0,5	0,45
2	$L_{ПР}$	0-1	0,99	0,2	0,198
3	$L_И$	0-1	0,9	0,3	0,27

$$A_Ц = \sum_{j=1}^{m_i} \beta_{ij} M_{ij} = 0{,}918.$$

Таблица 10 – Метрики и критерии целостности

Показатели целостности	Наименование критерия	Уровень исполнения, K_i
Целостность вычислительных ресурсов $L_{ВР}$ – свойство исключать непредусмотренные структурные изменения системы и предоставляемых услуг	Правильность эксплуатации ВР	0-1
	Безопасность эксплуатации ВР	0-1
	Успешность эксплуатации ВР	0-1
	Способность проверять и сохранять данные	0-1
	Способность защиты от серьёзных последствий для целостности в случае ошибок	0-1
	Способность восстанавливать целостность после сбоев и ошибок	0-1
	Наличие защиты от нарушений авторского права	0-1
	Наличие функций восстановления целостности	0-1
	Наличие функций контроля целостности	0-1
	Наличие функций идентификации и аутентификации	0-1
	Наличие средств мониторинга и оповещения	0-1
	Наличие средств обработки ошибок	0-1
Целостность программных ресурсов $L_{ПР}$ – свойство исключать непредусмотренные изменения программных ресурсов системы	Наличие функций в ПР по восстановлению процесса выполнения в случае сбоя операционной системы, процессора, внешних устройств	0-1
	Наличие средств восстановления процесса в случае сбоев оборудования	0-1
	Наличие возможности повторного старта с точки останова	0-1
	Наличие автоматического резервирования для сохранения текущего состояния процесса	0-1
	Наличие требований по устойчивости функционирования при наличии ошибок во входных данных, ошибок пользователя, отсутствия необходимых данных (на диске, в файле, в БД и т.д.)	0-1
	Совместимость с техническими средствами	0-1
	Совместимость с системными программными средствами	0-1
	Совместимость с другим программным обеспечением, включая обмен данными (с текстовыми, графическими редакторами, БД и др.)	0-1
	Наличие устойчивости функционирования при наличии ошибок во входных данных, ошибок пользователя, отсутствия необходимых данных (на диске, в файле, в БД и т.д.)	0-1
	Возможность обработки ошибочных ситуаций	0-1
	Наличие возможности повторного старта с точки останова	0-1
Целостность информации $L_{И}$ – способность ГКС обеспечивать неизменность информации в условиях	Достоверность	0-1
	Точность	0-1
	Качество	0-1
	Своевременность	0-1
	Правильность	0-1

Продолж. табл. 10

случайного и (или) преднамеренного искажения (разрушения)	Наличие информации о способности проверять правильность вводимой/выводимой информации	0-1
	Наличие информации о процедурах хранения данных	0-1
	Наличие тестов для проверки допустимых значений входных/выходных данных	0-1
	Наличие системы контроля полноты входных/выходных данных	0-1
	Наличие средств контроля корректности входных/выходных данных	0-1
	Наличие средств контроля непротиворечивости входных/выходных данных	0-1
	Наличие проверки параметров и адресов по диапазону значений	0-1
	Наличие обработки предельных значений	0-1
	Наличие информации о способности восстанавливаться после ошибок	0-1

Степень влияния критериев на тот или иной показатель целостности (метрику) определяется уровнями исполнения, которые находятся в диапазоне значений 0÷1.

Далее, по формулам, приведенным ниже, рассчитываются уровни исполнения метрик.

$$L_{BP} = \frac{\sum_{i=1}^{n} K_i}{n},\ L_{ПР} = \frac{\sum_{i=1}^{n} K_i}{n},\ L_{И} = \frac{\sum_{i=1}^{n} K_i}{n}. \qquad (14)$$

Примечание 3. Если значения характеристик L_{BP}, $L_{ПР}$, $L_{И}$ больше 0,9, то система соответствует удовлетворительному уровню целостности.

Для большинства КС, используемых на объектах критических инфраструктур, целесообразно рассматривать полный комплекс атрибутов АМГ, однако для КС объектов специального назначения, принимая во внимание их специфику функционирования, комплекс атрибутов можно обоснованно минимизировать. Например, можно выделить следующие типы объектов специального назначения, для которых ряд атрибутов, входящих в состав АМГ, целесообразно изъять из рассмотрения без потери общности:

1. Необслуживаемые объекты короткого периода функционирования (ракеты, управляемые снаряды и авиабомбы).

2. Обслуживаемые объекты короткого периода функционирования (самолеты, многоразовые космические аппараты).

3. Автономные необслуживаемые объекты длительного периода функционирования (пункты управления подводными кабельными линиями связи, спутники, зонды).

4. Автономные обслуживаемые объекты длительного периода функционирования (корабли, поезда, шахтные пусковые установки ракет).

Например, для объектов 1-го типа неактуальными являются следующие атрибуты: Готовность, Обслуживаемость, Живучесть, Конфиденциальность и Целостность, для которых эксперты фактически должны проставит очень низкие коэффициенты влияния B_i.

3. Скалярная модель гарантоспособности системы

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.

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 АМГ, предназначенной для вычисления уровня гарантоспособности системы, предлагается использовать функционал $G_{AMГ}$, составляющими которого являются нормированные значения количественных оценок уровней реализации атрибутов и метрик с соответствующими весовыми коэффициентами. Величины весовых коэффициентов зависят от особенностей применения каждой конкретной системы и могут быть вычислены аналитически или оценены экспертным методом.

$$G_{AMГ} = \sum_{i=1}^{n} B_i A_i \,, \tag{15}$$

где n – количество атрибутов АМГ, B_i – коэффициент влияния i-го атрибута, A_i – количественная оценка уровня исполнения i-го атрибута в относительных величинах.

$$A_i = \sum_{j=1}^{m_i} \beta_{ij} M_{ij}, \tag{16}$$

где m_i – количество метрик i-го атрибута, β_{ij} – вес j-ой метрики i-го атрибута, M_{ij} – количественная оценка уровня исполнения j-ой метрики i-го атрибута в относительных величинах.

Подставив (16) в (15), получим выражение для уровня гарантоспособности КС:

$$G_{AMГ} = \sum_{i=1}^{n} B_i \sum_{j=1}^{m_i} \beta_{ij} M_{ij} \,. \tag{17}$$

Примечание 4. Количественные оценки уровня исполнения метрик M_{ij} представляют собой экспертные значения в диапазоне от 0 до 1. Для своего анализа эксперт принимает во внимание аналитические расчеты, результаты испытаний элементов оцениваемой КС и их аналогов, а также свой опыт по оценке качества функционирования КС на основе стандартов менеджмента качества ISO серии 9000.

В связи с тем, что количество метрик i-го атрибута невелико, то для реализации метода экспертных оценок рекомендуется принимать условие $\sum_{j=1}^{m} \beta_{ij} = 1$. Что касается оценки влияния атрибутов на уровень гарантоспособности, диапазон от 0 до 1 не позволя-

ет эксперту существенно выделить важность того или иного атрибута. Поэтому для реализации метода экспертных оценок рекомендуется принимать условие $\sum_{i=1}^{n} B_i = 10$.

4. Параметризация скалярной модели гарантоспособности системы

Для каждой метрики экспертным методом устанавливается значение критерия реализации от 0 до 1 и экспертным или расчетным методом устанавливается значение веса β_{ij}. Далее для каждого атрибута вычисляется комплексная оценка (16).

С целью комплексной оценки уровня гарантоспособности системы для каждого атрибута АМГ экспертным методом устанавливается значение коэффициента влияния B_i, а общая комплексная оценка гарантоспособности системы вычисляется по формуле (17).

Пример 1. Предположим, что коэффициенты влияния i-го атрибута B_i, установленные экспертами, равны:

- безотказность – B_1=1,5;
- готовность – B_2=2;
- обслуживаемость – B_3=1;
- достоверность – B_4=1,5;
- живучесть – B_5=0,5;
- функциональная безопасность – B_6=2,5;
- конфиденциальность – B_7=0,5;
- целостность – B_8=0,5.

Вычислим обобщенную характеристику гарантоспособности КС по формуле (17):

$$G_{AMГ} = \sum_{i=1}^{n} B_i \sum_{j=1}^{m_i} \beta_{ij} M_{ij} = B_1 A_Б + B_2 A_Г + B_3 A_О + B_4 A_Д + B_5 A_Ж + B_6 A_{ФБ} + B_7 A_К + B_8 A_Ц =$$

$$=1{,}5\cdot 0{,}981+2\cdot 0{,}945+1\cdot 0{,}9596+1{,}5\cdot 0{,}99+0{,}5\cdot 0{,}981+2{,}5\cdot 0{,}981+0{,}5\cdot 0{,}966+0{,}5\cdot 0{,}918=9{,}691.$$

Максимальное значение $G_{AMГ}^{\max}$ при 100% исполнении метрик и критериев по всем атрибутам равно $G_{AMГ}^{\max} = \sum_{i=1}^{n} B_i A_i = \sum_{i=1}^{n} B_i \cdot 1 = 10$.

Относительный уровень реализации проекта КС по обеспечению гарантоспособности вычисляется по формуле

$$\delta_{G_{AMГ}} = \frac{G_{AMГ}}{G_{AMГ}^{\max}} \cdot 100\%. \qquad (18)$$

Для нашего примера $\delta_{G_{AMГ}}$=[9,691/10]·100=96,9 %, то есть исследуемый проект КС удовлетворяет требованиям по гарантоспособности ($\delta_{G_{AMГ}}$>90%) и лишь на 3,1% меньше максимально возможного уровня.

Необходимо иметь в виду, что желание заказчика проекта получить КС с максимально возможным уровнем гарантоспособности должно быть обосновано, так как оно сопряжено с излишними затратами средств и времени на разработку и производство системы, что неминуемо отразится на увеличении ее стоимости.

5. Выводы

В работе предложено математическое представление АМГ, предназначенное для вычисления уровня гарантоспособности системы. В качестве аналитического выражения скалярной модели предложено использовать функционал $G_{АМГ}$, составляющими которого являются нормированные значения количественных оценок уровней реализации атрибутов и метрик с соответствующими весовыми коэффициентами. Величины весовых коэффициентов зависят от особенностей применения каждой конкретной системы и могут быть оценены аналитическими или экспертными методами.

Данная модель может определять направление и способ изучения не только частных, но и интегральных характеристик гарантоспособности, положительно влиять на осмысление фундаментальных понятий, принципов и парадигм и служить методологической основой построения и развития современной теории гарантоспособных компьютерных систем.

Автор не претендует на последнюю инстанцию в решении задачи количественной оценки уровня гарантоспособности КС, возможны и другие альтернативные подходы, основанные, например, на вычислении вероятностей реализации функций системы, но если наши выкладки верны, а рассуждения убедительны, то данный подход также имеет право на существование и является достаточно эффективным.

СПИСОК ИСТОЧНИКОВ

1. Похлебаев С.М., Третьякова И.А. Атрибутивная модель понятия «материя» как логическая основа построения и развития современной общенаучной картины мира. *Наука и школа*. 2011. № 3. С. 65–68.
2. Харченко В.С., Скляр В.В., Тарасюк О.М. Методы моделирования и оценки качества и надежности программного обеспечения. Х.: НАКУ «ХАИ», 2004. 159 с.
3. Федухин А.В., Сеспедес Гарсия Н.В. Атрибуты и метрики гарантоспособных компьютерных систем. *Математичні машини і системи*. 2013. № 2. С. 195–201.
4. Стрельников В.П., Федухин А.В. Оценка и прогнозирование надёжности электронных элементов и систем. К.: Логос, 2002. 486 с.
5. Федухин А.В., Пасько В.П. К вопросу о количественных характеристиках безотказности избыточных компьютерных систем. *Математичні машини і системи*. 2012. № 1. С. 145–156.
6. Кривуля Г.Ф., Шкиль А.С., Гаркуша Е.В. Готовность компьютеризованных систем управления и компетентность пользователя. *Інфомаційно-керуючі системи на залізничному транспорті*. 2011. № 5. С. 12–17.
7. ГОСТ 18322-78. Система технического обслуживания и ремонта техники. Термины и определения. М.: Издательство стандартов, 1978. 16 с.
8. Шербаков Н.С. Достоверность работы цифровых устройств. М.: Машиностроение, 1989. 288 с.
9. Федухин А.В., Сеспедес Гарсия Н.В., Муха Ар.А. К вопросу о связи надежности и достоверности функционирования компьютерных систем. *Математичні машини і системи*. 2017. № 2. С. 145–155.
10. Сеспедес Гарсия Н.В. Достоверность работы компьютерных систем. *Математичні машини і системи*. 2016. № 4. С. 146–151.
11. Черкесов Г.Н. Методы и модели оценки живучести сложных систем. М.: Знание, 1987. 32 с.
12. Додонов А.Г., Кузнецова М.Г., Горбачик Е.С. Введение в теорию живучести вычислительных систем. К.: Наукова думка, 1990. 184 с.
13. Зыбин С.В., Лихицкая И.В. Принципы и способы обеспечения живучести компьютерных систем. *Наукові записки Українського науково-дослідного інституту зв'язку*. 2016. № 2 (42). С. 67–71.
14. Сербін В.Г., Сухомлин А.І. Визначення і формалізація основних показників гарантоздатності живучих комп'ютерних систем керування на основі ймовірнісно-фізичного підходу для їх проектної оцінки і прогнозування. *Математичні машини і системи*. 2012. № 4. С. 182–189.

15. Федухин А.В., Муха Ар.А. Обеспечение живучести систем противоаварийной автоматики на гидроэлектростанциях. *Математичні машини і системи*. 2018. № 2. С. 169–194.
16. Муха Ар.А. Обеспечение живучести систем противоаварийной автоматики ГЭС. *Математичні машини і системи*. 2018. № 2. С. 169–194.
17. Муха Ар.А. К вопросу о живучести систем противоаварийной автоматики на гидроэлектрических станциях. *Молодий вчений*. 2018. № 3 (55). С. 399–405.
18. EN 61508: Функциональная безопасность систем управления. URL: https://www.pilz.com/ru-RU/knowhow/law-standards-norms/functional-safety/en-iec-61508.
19. ОСТ 32.17-92. Безопасность железнодорожной автоматики и телемеханики. Термины и определения. СПб.: ПИИТ,1992. 33 с.
20. Сапожников В.В., Сапожников Вл.В., Талалаев В.И. [и др.]. Сертификация и доказательство безопасности систем железнодорожной автоматики / ред. Вл.В. Сапожникова. М.: Транспорт, 1997. 288 с.
21. Функциональная безопасность – неотъемлемая часть общей безопасности. URL: http://pubweb2.iec.ch/about/brochures/pdf/technology/functional_safety_ru.pdf.
22. Функциональная безопасность – старшая сестра информационной безопасности. Ч. 1. URL: https://habr.com/ru/post/308634/.
23. Функциональная безопасность. Ч. 2: МЭК 61508. URL: https://habr.com/ru/post/309636/
24. Функциональная безопасность. Ч. 5: Процессы управления и оценивания функциональной безопасности. URL: https://www.securitylab.ru/analytics/486866.php?R=1.
25. Функциональная безопасность. Ч. 7: Оценивание показателей функциональной безопасности и надежности. URL: https://www.securitylab.ru/analytics/487137.php.
26. Функциональная безопасность компьютерных систем управления. Ч. 8: Методы обеспечения информационной и функциональной безопасности. URL: https://www.securitylab.ru/analytics/487450.php?R=1.
27. Галицкий А.В., Рябко С.Д., Шаньгин В.Ф. Защита информации в сети. Анализ технологий и синтез решений. М.: ДМК Пресс, 2004. 616 с.
28. Норткатт С. Защита сетевого периметра / пер. с англ. К.: ООО «ТИД «ДС», 2004. 672 с.
29. Сеспедес Гарсия Н.В. Оценка уровня конфиденциальности гарантоспособных компьютерных систем. *Математичні машини і системи*. 2014. № 3. С. 158–164.
30. Сеспедес Гарсия Н.В. О контроле соблюдения конфиденциальности компьютерных систем. *Математичні машини і системи*. 2015. № 3. С. 57–66.
31. Р 50.1.053-2005. Рекомендации по стандартизации «Информационные технологии. Основные термины и определения в области технической защиты информации». URL: http://docs.cntd.ru/document/1200039555.
32. Власова Л.А. Защита информации. Хабаровск: РИЦ ХГАЭП, 2007. 84 с.
33. Сеспедес Гарсия Н.В. Оценка уровня целостности гарантоспособных компьютерных систем. *Математичні машини і системи*. 2013. № 4. С. 204–210.

Стаття надійшла до редакції 15.05.2019