УДК 004.052:681.3

В.С. ХАРЧЕНКО

Національний аерокосмічний університет ім. Жуковського М.Є. «ХАІ», Україна

ГАРАНТОЗДАТНІСТЬ КОМП'ЮТЕРНИХ СИСТЕМ: МЕЖА УНІВЕРСАЛЬНОСТІ У КОНТЕКСТІ ІНФОРМАЦІЙНО-ТЕХНІЧНИХ СТАНІВ

Проаналізовано структуру та таксономічні особливості гарантоздатності як комплексної властивості комп'ютерних систем (КС) для різних застосувань. Уточнено модель станів гарантоздатних КС як сукупності технічних та інформаційних станів. Визначено множину можливих помилок при ідентифікації інформаційно-технічних станів систем при контролі та управлінні. Сформульовано елементи стратегії управління гарантоздатністю за фактичним інформаційно-технічним станом.

гарантоздатність, таксономія, комп'ютерна система, інформаційно-технічний стан, помилки контролю та управління

Вступ. Ризики впровадження інформаційних технологій та проблема гарантоздатності КС

Розвиток інформаційних технологій (ІТ) та їх незворотна інтеграція у світ систем і світ людей має два аспекти. Перший - це безумовні позитиви та можливості революційного характеру, що надають такі технології. Внаслідок цього технічні системи та людство в цілому стають все більш залежним від інформаційних технологій, їх якості, надійності та безпеки. Поглиблення такої залежності зініціювало наявність іншої, на жаль, негативної сторони – набуття комп'ютерними засобами і системами ознак одного з впливових факторів відмов, аварій та катастроф складних технічних та організаційно-технічних комплексів (СТК). Кожна п'ята аварія або передумова до неї у ракетно-космічній техніці та атомній енергетиці пов'язана з відмовами КС [1, 2]. Складові цього протиріччя «ІТ як чинник удосконалення та підвищення надійності СТК – ІТ як фактор додаткових ризиків», відповідні виклики та шляхи зменшення ризиків досліджуються у [3 – 6] щодо атомної енергетики та ракетно-космічних систем.

Аналізуючи негативну складову впровадження інформаційних технологій у критичних і бізнес-критичних сферах, слід зазначити, що однією з домінантних рис у цьому процесі є інтегральне оцінювання якісного (або неякісного) виконання (або невиконання) функцій, надання (або ненадання послуг) при використанні комп'ютерних засобів і систем. Тобто для замовника або користувача КС важливим є кінцевий результат - отримання послуги (виконання відповідної функції) незалежно від сутності можливих причин або ризиків її ненадання. У визначальній роботі [7] надано деталізовану таксономію таких причин, що в кінцевому варіанті зводяться до трьох - фізичних дефектів (несправностей) технічних засобів (ДФ), дефектів проектування, перш за все, програмних засобів (ДП) і так званих дефектів взаємодії (ДВ), які мають місце внаслідок дії екстремальних факторів зовнішнього середовища фізичного та інформаційного, випадкового або цілеспрямованого характеру.

Внаслідок цього класичне вихідне поняття надійності КС набуло нових ознак, що потребує або розширення та відповідної формалізації його змісту, або використання іншого інтегративного поняття, складовою якого може бути «традиційна» надійність. Поява та вживання терміну «гарантоздатність» (але не «гарантоспроможність») є наслідком реалізації другого шляху, що спонукає не тільки проаналізувати термінологічний аспект, але що, на нашу думку, не менш важливо, визначитися зі змістом і наслідками процесів, які викликають власне постановку задачі.

Аналіз літератури, публікацій матеріалів наукових конференцій, зокрема, МНТК «Гарантоздатні (надійні та безпечні) системи, сервіси та технології» (DESSERT2006, 2007), обговорення цієї проблематики на наукових семінарах показує на необхідність не тільки уточнення таксономічного (змістовного) наповнення поняття «гарантоздатність», але й додаткової аргументації щодо використання самого терміну.

Слід відзначити, що така ситуація обумовлена суттєвою розбіжністю структури поняття гарантоздатності не тільки у наукових статтях, але й у стандартах, як національних, так і міжнародних, зокрема, у галузі якості, надійності та безпеки інофрмаційно-управляючих систем ISO/IEC [8], атомної енергетики IAEA [9], космічних систем ECSS [10] і телекомунікацій ITU [11]. Вони визначають різний ступінь універсальності гарантоздатності щодо її складових властивостей. Ураховуючи «конфедеративне» входження інформаційної безпеки, а саме цілісності та конфіденційності, до гарантоздатності відповідно до [7], слід більш ретельно проаналізувати інформаційну складову станів гарантоздатних комп'ютерних систем.

Саме ці обставини обумовили власне назву статті та її **мету** – проведення аналізу таксономічних аспектів гарантоздатності та визначення межі універсальності цієї властивості у контексті технічної та інформаційної складової станів гарантоздатних КС. Дана робота є природним розвитком методологічних положень щодо гарантоздатності та гарантоздатних КС, сформульованих у [12] як результату аналізу та гармонізації з таксономічною системою гарантоздатності, описаною в [7].

1. Таксономічний аспект

1.1. Ще раз про термін «гарантоздатність»

Варто нагадати, що «гарантоздатність» як модерновий термін з'явився у російськомовній літературі у другій половині 80-х років при перекладі та обговоренні [13] роботи [14] як своєрідна відповідь на розширення меж надійності на програмні засоби, ураховуючи суттєвий вплив їх дефектів на працездатність КС. Це обумовило появу симетричних термінів «dependable computing» – «надійні (гарантоздатні) обчислення». Подальшу еволюцію змісту понять проаналізовано в [12]. Слід зазначити декілька обставин щодо власне терміну «гарантоздатність» та його сучасного застосування.

1. Будь-який термін є семантичною ознакою відповідного поняття і формулюється або як нове унікальне слово, або як поєднання відомих терміноутворюючих елементів. Такими елементами у даному випадку є «здатність» і «гарантія» (тобто «здатність гарантувати»). Це викликає певні природні асоціації з відомим термінами і поняттями, зокрема, «гарантійний ресурс (напрацювання)». У даному випадку така асоціація не є визначальною, оскільки, як вже неодноразово підкреслювалося, термін «гарантоздатність» доцільно вживати як розширене поняття надійності КС, що включає додаткові складові. У цьому сенсі гарантоздатність (як і надійність) може характеризуватися як властивість виконувати певні функції або послуги за певних, але більш розширених чинників і «гарантувати» це з певною імовірністю.

2. З іншого боку, слід зазначити, що введення і вживання любого терміну є результатом певного компромісу, узгодженої домовленості щодо його відповідності деякому поняттю та його таксономічному змісту. Саме у такий спосіб, здається, йде розвиток змісту поняття, якому відповідає термін «гарантоздатність». Тобто гарантоздатність не є у буквальному розумінні здатність тільки «гарантувати щось», а є «здатність надавати задані послуги, яким можна виправдано довіряти» [7,12] за умов виникнення або прояву ДФ, ДП, і ДВ.

3. Якщо межі та зміст поняття і відповідного терміну окреслені та зафіксована певна домовленість науково-технічної спільноти, навіть за умов відсутності національного стандарту, його вживання повинно бути доречним та коректним. Вживання «всує», особливо ураховуючи складну еволюцію та зміст поняття гарантоздатності, тільки зашкоджує його становленню та утверджуванню.

4. Існує певна асиметрія термінів і відповідних понять у україно-, російськомовній та англомовній

літературі щодо «надійності» та «гарантоздатності». В англомовній літературі термін «dependability» з'явився і затвердився досить давно, майже паралельно з терміном «reliability» (безвідмовність) і відповідав поступовому розширенню поняття «надійності». На даному етапі, після публікації [7], процес його формування, на нашу думку, завершився. В україно- та російськомовній літературі маємо дещо іншу ситуацію, коли термін «надійність» фіксує класичну, так би мовити, консервативну складову, а «гарантоздатність» включає додаткові ознаки, обумовлені інтегруванням з поняттями інформаційної та функціональної безпеки.

1.2. Структура поняття гарантоздатності

Аналіз сучасної наукової літератури та нормативної бази показує, що поняття гарантоздатності (dependability) характеризується не співпадаючими таксономічними схемами у різних галузях. Це стосується різних елементів таксономічних схем, перш за все, властивостей, що входять до складу гарантоздатності. Результати відповідного стандартів і публікацій наведені в табл. 1, де використано такі позначки: Н – складова надійності, НВ – вторинна властивість, що входить до складу надійності, НС – суміжна до надійності властивість, Д – dependability (для аналогових джерел), ДС – суміжна до неї властивість, Г– складова гарантоздатності, ГП – складова, що може входити до гарантоздатності залежно від призначення КС.

За стандартами ГОСТ 2700 [15], ДСТУ 2860 [16] маємо класичні складові надійності, для якої готовність є вторинною властивістю, а живучість – суміжною. За стандартом ITU E800 [11] та стандартами IEC серії 60300, ECSS–Q–30A поняття dependability вужче за складом ніж надійність. Для стандартів IAEA NS-G-1.3. [9] і ECSS–Q–80–3 [10] властивості цілісності та конфіденційності є суміжними для dependability. За стандартом IAEA NS-G-1.3 [9] поняття dependability розширюється за рахунок функціональної безпеки (safety) і, так би мовити, «поглинається» цією властивістю з огляду на її важливість для АЕС. Крім того, ця властивість є суміжною до dependability за стандартами ISO/IEC 9126 [8] і ECSS–Q–80–3 [10].

Таблиця 1

Аналіз складу властивостей гарантоздатності

Складові властивості	Стандарти						Публікації		
	ГОСТ [15]	ДСТУ [16]	ITU [11]	ISO/ IEC [8]	IAEA [9]	ECSS [10]	[7]	[12]	[17]
Безвідмовність (безотказность, reliability)	Н	Н	Д	Д	Д	Д	Д	Г	Д
Ремонтопридатність (ремонтопригодность, pairability)	Н	Н							
Обслуговуваність (обслуживаемость, maintainability)			Д	Д	Д	Д	Д	Г	
Готовність (готовность, availability)	НВ	НВ	Д	Д	Д	Д	Д	Г	Д
Довговічність (долговечность, durability)	Н	Н							
Збереженість (сохраняемость, preservability)	Н	Н							
Живучість (живучесть, survivability)	НС	НС					ДС	ГП	
Функціональна безпека (безопасность, safety)				ДС	Д	ДС	Д	Г	Д
Цілісність (целостность, integrity)					ДС	ДС	Д	Г	Д
Конфіденційність (конфиденциальность, confidentiability)							Д	ГП	
Достовірність (достоверность, high confidence)								ГП	

Виходячи з цих результатів, слід підкреслити, що наукові публікації [7, 12, 17] в цілому надають розширеного тлумачення поняттю гарантоздатність (dependability) відносно існуючої нормативної бази, що є досить природним, оскільки в стандартах повинна фіксуватися більш-менш узгоджена, стала ситуація.

Іншим важливим елементом таксономії гарантоздатності є відмовостійкість (fault-tolerance), що за [7] тлумачиться не як властивість, а як принцип, механізм підтримки властивостей гарантоздатності, що проаналізовано і відображено у деталізованих таксономічних схемах [12]. Табл. 2 – це матриця відповідності між властивостями гарантоздатності

та узагальненими операціями (функціями) відмовостійкості: прогнозування відмов (forecasting, prediction) F1, запобігання (preventation) F2, виявлення (detection) F3, пошуку дефектів або локалізації відмови (diagnosis) F4, парирування (маскування) прояву відмов (tolerating) F5, ізоляції компонента, що відмовив (isolation), F6 та його заміни – реконфігурації структури (reconfiguration) F7, відновлення інформації (recovery) F8, відновлення функціонування (restarting) F9. Ці операції утворюють у часі цикл забезпечення відмовостійкості FT та виконуються за послідовно-паралельною схемою (рис. 1), деякі елементи якої можуть бути або відсутні, або реалізовуватися сумісно у часі.

Таблиця 2

Матриця відповідності властивостей гарантоздатності та операцій відмовостійкості

Складові властивості	Операції (функції) відмовостійкості								
	F1, прогнозування	F2, попередження	F3, виявлення	F4, локалізація	F5, парирування	F6, ізоляція	F7, реконфігурація	F8, відновлення	F9, рестарт
Безвідмовність			+		+				
Ремонтопридатність		+	+	+		+	+	+	
Обслуговуваність	+	+	+	+			+		
Готовність			+	+		+			+
Живучість	+	+	+	+	+	+	+	+	+
Функціональна безпека	+	+	+		+	+	+		
Цілісність			+		+				
Конфіденційність			+		+				
Достовірність			+						

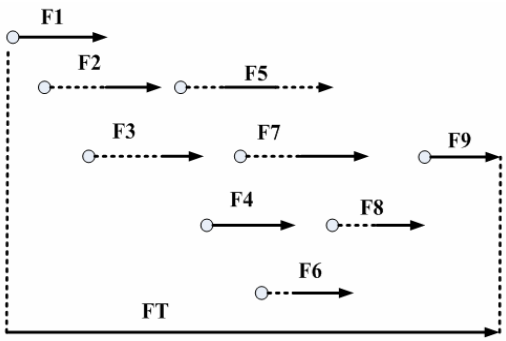


Рис. 1. Діаграма операцій відмовостійкості

Ключовим питанням щодо структури гарантоздатності, яке визначає його інтегративну сутність, є включення властивостей інформаційної безпеки (цілісності, а за відповідних умов і конфіденційності) до її складу. Відмовостійкість та її засоби може бути підтвердженням такої інтеграції через спільні процедури, засоби запобігання та нейтралізації наслідків відмов, обумовлених ДФ, ДП і ДВ, при використанні багатоверсійних технологій [12], спеціальних механізмів реалізації функцій F1-F9. Цікавим є питання формування архітектурних рішень у просторі «диверсність – відмовостійкість – інформаційна безпека», тобто розробка відмовостійких засобів забезпечення цілісності та конфіденційності з використанням багатоверсійності засобів інформаційного захисту багатоверсійних систем [18].

2. Інформаційно-технічний стан

2.1. Поняття інформаційно-технічного стану

Поняття інформаційно-технічного стану при аналізі гарантоздатності є, на нашу думку, визначальним, оскільки акумулює всі її складові властивості, дозволяє з більш загальних позицій розглядати інші поняття, а саме відмови та відмовостійкості.

Питання про інформаційно-технічний стан (ІТС) було сформульовано у [12], де множина станів (справних – несправних, працездатних – частково працездатних непрацездатних, безпечних – потенційно небезпечних – небезпечних або критичних) розглядалася з урахуванням того, що переходи між ними можуть здійснюватися внаслідок не тільки виникнення або прояву ДФ, ДП, але й внаслідок дефектів взаємодії, у тому числі зовнішніх інформаційних втручань. Тобто, якщо такі дефекти спричинять або

перекручення інформації, або несанкціонований доступ до неї (що не допускається за умовами її використання відповідно до технічного завдання), це можна тлумачити як перехід системи у несправний, непрацездатний, частково працездатний або небезпечний стан залежно від обсягу та наслідків такого переходу. Таким чином, під ІТС слід розуміти сукупність властивостей і ознак як технічного, так і інформаційного характеру, притаманних системі у певний момент часу. Ця сукупність може бути специфікована у більш розширеному контексті ніж технічний стан і визначати критерії щодо класифікації станів комп'ютерної системи. При такому розгляді ІТС, фактично, реалізується у повному обсязі принцип доповнення – один з важливих принципів теорії систем, за яким КС та її стани повинні розглядатися з урахуванням взаємодії із зовнішнім середовищем. Тобто, якщо скажімо, внаслідок порушення конфіденційності зовнішня система отримала несанкціонований доступ до частки «внутрішньої» інформації КС, це повинно кваліфікуватися як перехід цієї системи у несправний (непрацездатний, небезпечний) інформаційно-технічний стан, а відповідна подія – як пошкодження, збій або відмова.

Слід відзначити, що необхідність такого комплексного розгляду станів КС підтверджується тим, що наявність одних дефектів створюють умови для виникнення інших. Найбільш характерною є така залежність між дефектами проектування програмних засобів і дефектами взаємодії інформаційного типу, оскільки ДП є причиною так званих уразливостей (уязвимость, vulnerability) комп'ютерних систем, через які здійснюються несанкціоновані впливи, хакерські атаки та інш. Зараз існують спеціальні бази даних про таку інформацію щодо найбільш поширених програмних продуктів [19], яка є підставою для оперативної розробки та впровадження відповідних засобів захисту, зокрема, патчів (patch), а також розробки спеціальних гарантоздатних систем з використанням принципу диверсності та урахуванням, при виборі альтернативних версій для їх компонент, наявності та ступеня перетину можливих наслідків використання уразливостей [20].

Крім того, поняття ІТС узгоджує певним чином давнє протистояння понять «надійність апаратних (технічних) засобів» і «надійність програмних засобів», оскільки дефекти проектування, якщо їх відносити тільки до програмної компоненти, при прояві призводять фактично до порушення саме інформаційної складової стану КС.

2.2. Складові стану ІТС і переходів між ними

Отже у загальному випадку система може знаходитися у одному з восьми ІТС, кількість яких визначається комбінацією трьох типів дефектів - ДФ, ДП, ДВ. У середині кожної вершини (рис. 2) трьохрозрядний код $<\sigma_{ДФ}, \sigma_{ДП}, \sigma_{ДВ}>$ описує наявність відповідних дефектів (1 – присутній, 0 – відсутній). Переходи, на яких виникають два або три дефекти, показані пунктиром як менш ймовірні.

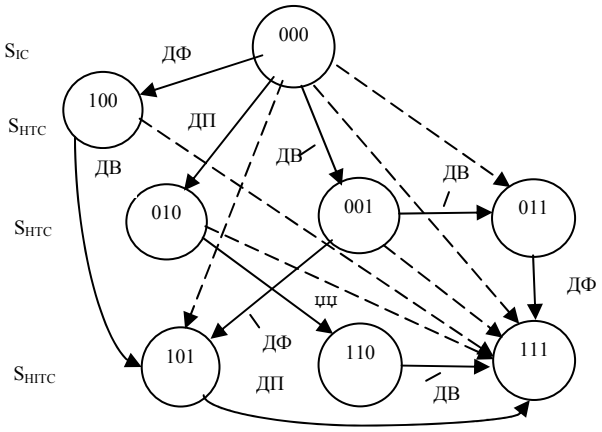


Рис. 2. Граф ІТС системи

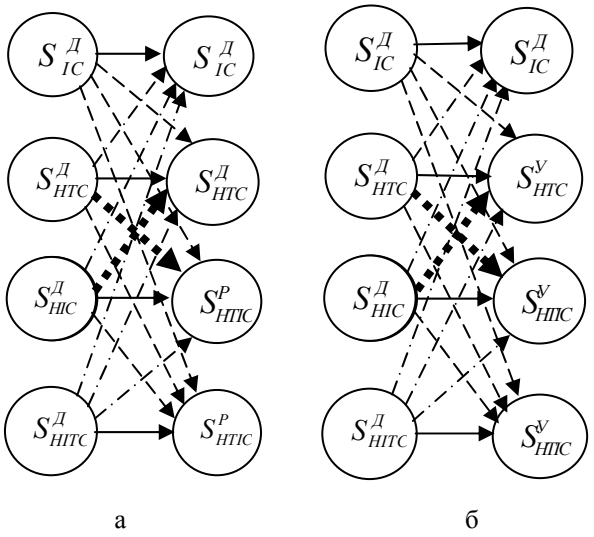
Наявність (виникнення) ДФ призводить до непрацездатного технічного стану $S_{НТС}$ (100), а прояв ДП або виникнення ДВ - до непрацездатного інформаційного стану $S_{НІС}$ (010, 001, 011).

Якщо стан системи характеризується порушенням справності як за технічною, так і за інформаційною складовими, можна казати про несправний (непрацездатний, небезпечний) стан $S_{НІТС}$. До множини $S_{НІТС}$ входять підмножини $S_{НІТС1}$(101), $S_{НІТС2}$(110), $S_{НІТС3}$(111) залежно від комбінації дефектів ДП і ДВ при наявності ДФ.

3. Помилки контролю та управління ІТС

З урахуванням розглянутого поняття ІТС може бути узагальнена множина помилок контролю станів КС (або комп'ютерної системи та об'єкту управління). Для цього слід співвіднести множину дійсних $MS^{Д}$ та розпізнаних $MS^{Р}$ інформаційно-технічних станів і визначити відповідно до [21] помилки першого, другого, третього, (а при необхідності, четвертого) роду. Перші пов'язані з помилковою ідентифікацією «руху вниз» («ризик постачальника»), другі – з помилковою ідентифікацією «руху вгору» («ризик замовника»), треті - з помилковою ідентифікацією стану у межах правильного визначеної підмножини станів («ризик діагноста»).

Узагальнена логічна модель помилок контролю ілюструється рис. 3, а, де безперервними лініями показані варіанти, штриховою – помилки першого роду, а штрих-пунктирною – другого роду. Помилки третього роду, до яких доречно віднести неправильне визначення несправних (непрацездатних) інформаційного або технічного станів за умов знаходження системі у несправному (непрацездатному) технічному або інформаційному станах відповідно, позначені стовщеними переривчастими лініями.



а б

Рис. 3. Модель помилок контролю(а) та управління (б) ІТС

Слід підкреслити, що означена модель потребує більш детального аналізу за рівнем працездатності (небезпечності) станів шляхом їх співставлення з інформаційною та технічною складовими.

Крім того, вона може бути поширена на фазу управління системою (об'єктом) при її побудові за схемою [21]: об'єкт контролю та управління (ОКУ), що характеризується множиною дійсних ІТС $MS^{Д}$, підсистема контролю (ПК), що визначає його ІТС і формує множину розпізнаних станів $MS^{Р}$, підсистема управління (ПУ), яка відповідно до $MS^{Р}$ формує управляючі сигнали, що подаються на ОКУ, і характеризується множиною станів $MS^{У}$.

Тоді внаслідок різних дефектів ПУ фазі управління можуть бути притаманні помилки, аналогічні помилкам фази контролю (рис. 3, б), тобто, наприклад, помилка управління другого роду $S^{Р}_{НТС} \to S^{У}_{ІС}$ визначає ситуацію, коли ПУ формує на ОКУ сигнали як на об'єкт, що знаходиться у стані $S^{У}_{ІС}$, не зважаючи на те, що він знаходиться у розпізнаному стані $S^{Р}_{НТС}$.

Зрозуміло, що різні типи помилок контролю та управління можуть накладатися і визначати сумісно з об'єктом, ПК, ПУ стан системи в цілому. Це вимагає уточнення відповідних процедур відновлення системи.

4. Управління гарантоздатністю. Елементи стратегії

Узагальнення поняття інформаційно-технічного стану КС і комп'ютеризованих СТК надає можливості формування розширеної множини стратегій технічного (інформаційно-технічного) обслуговування та управління станом за планово-попереджувальними та гнучкими схемами. Відповідно до [12] та проведеного аналізу доцільним є перехід від ***концепції управління надійністю (готовністю) за фактичним технічним станом*** до ***концепції управління гарантоздатністю за фактичним ІТС.***

Сутність такої стратегії полягає в тому, що:

– обслуговування технічних і програмно-технічних засобів з метою профілактичних цілей та виявлення прихованих відмов внаслідок ДФ і прогнозованих або виявлених ДП, а також заходи щодо

обслуговування (перевірки та модернізації) засобів інформаційної безпеки (та забезпеченню живучості) з урахуванням ДВ проводяться не у фіксовані – планові моменти часу, а відповідно до фактичного інформаційно-технічного стану;

– моменти часу, тривалість та обсяг заходів щодо обслуговування залежать від контрольованого рівня гарантоздатності.

При цьому множина можливих стратегій управління класифікується за двома основними, на наш погляд, ознаками: ступенем та порядком суміщення профілактичних або ремонтних заходів щодо ризиків, обумовлених ДФ, ДП і ДВ; складовими гарантоздатності та відповідними показниками цих складових, їх комбінаціями або гарантоздатністю в цілому. Для реалізації стратегій управління гарантоздатністю КС необхідно мати спеціальні засоби, які забезпечують:

– оперативний контроль ІТС, його технічної та інформаційної складових;

– прогнозування зміни ІТС та оцінки показників гарантоздатності з урахуванням результатів моніторингу та використанням відповідних математичних моделей;

– визначення моменту, номенклатури та обсягу профілактичних заходів відповідно до вимог до гарантоздатності, її поточного та прогнозованого значень;

– реалізацію прийнятих рішень та оцінки їх впливу на фактичний рівень гарантоздатності.

З урахуванням сутності ІТС слід розглядати ***політику управління гарантоздатністю як узагальнення політики інформаційної безпеки КС***.

Висновки

Необхідність спільного розгляду різних чинників порушення стану КС внаслідок фізичних дефектів, дефектів проектування та дефектів взаємодії є об'єктивною вимогою часу. Це потребує інтегрованого підходу як у термінологічному, так і сутнісному аспектах.

Здається більш доцільним для комп'ютерних систем (мереж, комплексів) використання терміну «гарантоздатність», який визначає (узагальнює) поняття щодо, перш за все, надійності, функціональної та інформаційної безпеки, ніж модернізація (розширення) існуючого поняття надійності. «Конфедеративний» характер поняття гарантоздатності на даному етапі повинен здійснюватися у напрямку поглиблення інтеграції відповідних методів, засобів і технологій оцінки, забезпечення та управління гарантоздатністю, її складовими залежно від типів систем у різних галузях, вимог до них та її складових.

Одними із визначальних у цьому сенсі є, на наш погляд, поняття інформаційно-технічного стану, а також поняття контролю та управління ІТС. Важливими похідними поняттями є дійсний, розпізнаний та управляючий стани, що пов'язані з процесами контролю та управління ІТС. Запропонована узагальнена модель помилок щодо визначення дійсного ІТС потребує деталізації множини станів, засобів їх виявлення та відновлювальних процедур, розробки архітектури відмовобезпечних комп'ютерних систем.

Важливим, з методологічної точки зору, є співставлення існуючих та перспективних гарантоздатних комп'ютерних систем з урахуванням всієї сукупності операцій, що утворюють цикл відмовостійкості.

Вельми складними, перспективними і цікавими є задачі управління гарантоздатністю КС за фактичним інформаційно-технічним станом – розробки відповідних стратегій, математичних моделей та технологій, їх поширення на більш масштабні утворення – інфраструктури різного рівня та призначення.

Література

1. Информационно-управляющие системы АЭС: проблемы безопасности / Под ред. М.А. Ястребенецкого. – К.: Техніка, 2004. – 472 с.

2. Харченко В.С., Скляр В.В., Тарасюк О.М. Анализ рисков аварий для ракетно-космической техники: эволюция причин и тенденций // Радіоелектронні і комп'ютерні системи. – 2003. – № 3. – С. 135-149.

3. Липаев В.В. Функциональная безопасность ПО. – М.: Синтег, 2004. – 281 с.

4. Харченко В.С., Ястребенецкий М.А., Скляр В.В. Новые информационные технологии и безопасность информационно-управляющих систем АЭС // Ядерная и радиационная безопасность. – 2003. – Т. 6, № 2. – С. 19-28.

5. Айзенберг Я.Е., Ястребенецкий М.А. Сопоставление принципов обеспечения безопасности систем управления ракето-носителями и атомными электростанциями // Космічна наука та технологія. – 2002. – № 1. – С.55-60.

6. Микрин Е.А. Бортовые комплексы управления космическими аппаратами и проектирование их программного обеспечения. – М.: МГТУ им. Н.Э. Баумана, 2003. – 336 с.

7. Avizienis A., Laprie J.-C., Randell B., Landwehr C. Basic Concepts and Taxonomy of Dependable and Secure Computing // IEEE Trans. On Dependable and Secure Computing. – 2004. – Vol. 1, № 1. – P. 11-33.

8. ISO/IEC 9126-1:1999. Information technology. Software product quality. Part 1: Quality model.

9. IAEA NS-G-1.3. Instrumentation and control systems important to safety nuclear power plants // Safety guide. – Vienna. – 2002.

10. ECSS–Q–80–3. Guidelines for software dependability and safety techniques. ECSS Secretariat ESA–ESTEC.Requirements & Standards Division. – Noordwijk : The Netherlands. – 1996.

11. ITU-T. Terms and Definitions Related to QoS and Network Performance Including Dependability. Recommendations E800. – Geneva. – 1994. – 65 p.

12. Харченко В.С. Гаратноспособность и гарантоспособные системы: элементы методологии // Радіоелектронні і комп'ютерні системи. – 2006. – № 5. – С.7-19.

13. Харченко В.С., Паршин В.В. Многоверсионные системы и обеспечение гарантоспособности. – Препринт № 321. – Х.: ИПМаш, 1989. – 33 с.

14. Avizienis A., Laprie J.-C. Dependable Computing: From Concepts to Application // IEEE Trans. on Computers. – 1986. – № 74 (5). – P. 629-638.

15. ГОСТ 2700-89. Надежность в технике. Термины и определения. – М.: Изд-во стандартов, 1989. – 12 с.

16. ДСТУ 2860-94. Надійність техніки. Основні терміни та визначення. – К.: Держстандарт України, 1994. – 19 с.

17. Соммервил И. Инженерия программного обеспечения. – СПб.: Вильямс, 2002. – 624 с.

18. Харченко В.С. Гарантоздатність комп'ютерних систем: проблеми та результати // Авіаційно-космічна техніка і технологія. – 2005. – № 7 (23). – С.352-357.

19. National Vulnerability Database [Електрон. ресурс]. – Режим доступу: http://nvd.nist.gov (February 2007).

20. Gorbenko A., Kharchenko V., Tarasyuk O, Furmanov A. F(I)MEA-Technique of Web-services Analysis and Dependability Ensuring. LNCS 4157. Rigorous Development of Complex Fault-Tolorant Systems / Butler M., Jones C., Romanovsky A., Trubitsyna E. (eds.). – Springer. – 2006. – P.153-168.

21. Харченко В.С., Аль Тарази А.Х. Логические модели ошибок контроля и управления опасными объектами в информационно-управляющих системах // Вісник Технологічного університету Поділля. – 2004. – № 2, Т. 2. – С. 127-131.

Надійшла до редакції 23.02.2007

Рецензент: д-р техн. наук, проф. І.А. Жуков, Національний авіаційний університет, Київ.