УДК 681.518.09 **doi: 10.32620/reks.2020.3.05**

Ю. Л. ПОНОЧОВНИЙ[1,2], В. С. ХАРЧЕНКО[1]

[1] ***Національний аерокосмічний університет імені М. Є. Жуковського «Харківський авіаційний інститут»***
[2] ***Полтавська державна аграрна академія***

МЕТОДОЛОГІЯ ЗАБЕЗПЕЧЕННЯ ГАРАНТОЗДАТНОСТІ ІНФОРМАЦІЙНО-КЕРУЮЧИХ СИСТЕМ З ВИКОРИСТАННЯМ БАГАТОЦІЛЬОВИХ СТРАТЕГІЙ ОБСЛУГОВУВАННЯ

У статті розглянуто методологію забезпечення гарантоздатності інформаційно-керуючих систем з використанням багатоцільових стратегій обслуговування. Актуальність досліджень зумовлена необхідністю забезпечення функціонування гарантоздатних інформаційно-керуючих систем в умовах змін вимог, параметрів середовища та прояву неспецифікованих відмов їх компонент. Методологія представлена на системному рівні як поєднання концепції багатоцільового обслуговування, а також принципів: врахування змін в інформаційно-керуючій системі та середовищі протягом життєвого циклу; комплексного врахування різних видів відмов та впливів змін; багатоцільового обслуговування та об'єднує комплекс нових моделей та методів визначення параметрів гарантоздатних інформаційно-керуючих систем та вибору параметрів процедур їх обслуговування. Пропонована концепція багатоцільового обслуговування отримана шляхом розвитку парадигми Фон-Неймана і формулюється як концепція побудови надійних і безпечних систем з недостатньо гарантоздатних компонентів та багатоцільового обслуговування за комбінованими стратегіями в умовах зміни вимог та середовища їх функціонування. Сфера дії пропонованої концепції має застосування у випадках, коли принципи Фон-Неймана не дозволяють будувати гарантоздатну систему через обмеження економічного, часового характеру, чи з інших причин. У такому випадку використання принципів, методів та моделей, що є концептуальними, розповсюджується на інформаційно-керуючі системи, побудовані з використанням обслуговуваних компонент і системних багатоцільових стратегій обслуговування. Запропонований принцип врахування змін передбачає розширення класичного контуру управління відмовостійкої системи, що забезпечує реакцію на прояв дефектів у вигляді помилок та відмов. Принцип комплексного врахування різних видів відмов та впливів змін є продовженням принципів єдності та зв'язків під час процедур системного аналізу. Він також є логічним продовженням фасетного упорядкування видів несправностей та ланцюгів причинно-наслідкових зв'язків від несправностей та дефектів до відмов, збоїв та помилок. У рамках запропонованої методології розроблено стратегії багатоцільового обслуговування, множину варіантів цілей, типів, процесів, властивостей та параметрів інформаційно-керуючих систем, що дозволяє знизити модельну невизначеність та обґрунтувати практичні заходи щодо забезпечення гарантоздатності на різних етапах життєвого циклу.

Ключові слова: *методологія забезпечення гарантоздатності; багатоцільове обслуговування; інформаційно-керуюча система.*

Вступ

Безперервне гарантоване функціонування інформаційно-керуючих систем (ІКС) є на сьогодні беззаперечним пріоритетом для різних галузей промисловості, забезпечення життєдіяльності людей та суспільства. В останні роки актуалізуються питання комплексного забезпечення показників гарантування нормального функціонування ІКС, які раніше виокремлювалися в різні дисципліни. Кіберінциденти у галузі енергопостачання України, розбір яких наведено в проектах американських стандартів NIST [1, 2], чи злам інфраструктури SoftServe [3], який негативно вплинув на рейтинг вітчизняної ІТ сфери, інші приклади підтверджують необхідність комплексного розгляду проблем гарантоздатності ІКС критичних та бізнес-критичних ІКС.

На сьогодні, окрім стандартизованих положень [4 - 6] існують різні наукові школи, які досліджують питання комплексування показників якості функціонування ІКС. У першу чергу, слід відмітити роботу А. Авіженіса, Ж. К. Лапрі, Б. Рендела [7], які на початку 90-х років минулого сторіччя визначили поняття гарантоздатності, основні її складові і методи їх забезпечення. З часом таксономія гарантоздатності оновилася [8 - 10], практичний досвід показав необхідність розвитку і адаптування положень концепції гарантоздатності до специфіки функціонування

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

ІКС різного призначення.

Слід зазначити, що сама концепція гарантоздатності є логічним розвитком запропонованої Дж. Фон-Нейманом парадигми побудови надійних обчислювальних систем із ненадійних компонент [11]. Важливо відмітити, що у Фон-Неймана пропонувалося використовувати принципи надмірності та резервування апаратних засобів (АЗ), оскільки тоді саме АЗ були ключовим джерелом відмов обчислювальних систем. В процесі розвитку обчислювальної техніки та інформаційних систем доля відмов АЗ поступово зменшувалася у порівнянні з відмовами, обумовленими дефектами програмних засобів (ПЗ). Це обумовило розвиток парадигми Фон-Неймана іншими дослідниками. У роботах В. С. Харченка [9, 12] розвинуто концепцію побудови гарантоздатних систем із негарантоздатних компонент, узагальнено таксономію гарантоздатності. Наступним етапом розвитку є специфікація концепції гарантоздатності під конкретний клас систем, а також під окремі якісні характеристики. А. В. Горбенко сформулював концепцію створення гарантоздатних компонентно-інтегрованих сервіс-орієнтованих систем із негарантоздатних Web-компонент з невизначеними характеристиками [8, 13]. У роботах В. В. Скляра [14] та Є. В. Брежнєва [15] розглянуто методологію побудови безпечних систем і інфраструктур з недостатньо безпечних компонент, тобто серед складових гарантоздатності акцентується увага на властивості функційної безпеки.

Варто зазначити, що відомі автори зосередилися на розгляді концепції Фон-Неймана для класа необслуговуваних систем або обслуговуваних з жорстким регламентом відновлення. Враховуючи мінливість фізичного та інформаційного середовищ функціонування ІКС використання необслуговуваних систем, тобто систем з відсутністю різних опцій відновлення, є не завжди рентабельним за ціновою політикою, а у деяких випадках і зовсім неможливе.

Метою даного дослідження є розвиток методології забезпечення гарантоздатності ІКС шляхом розроблення комплексу взаємоузгоджених концепції, принципів, моделей і методів, враховуючи особливості використання обслуговуваних програмно-апаратних компонентів та можливості реалізації стратегій багатоцільового обслуговування (БЦО).

Концепція гарантоздатних ІКС з БЦО

Відповідно до результатів аналізу пропонується концепція гарантоздатних ІКС з багатоцільовим обслуговуванням. Вона отримана шляхом розвитку парадигми Фон-Неймана і формулюється як концепція побудови надійних і безпечних систем з недостатньо гарантоздатних компонентів та БЦО за комбінованими стратегіями в умовах зміни вимог та середовища їх функціонування.

Пропонована концепція базується на таких положеннях.

1. Розвиток парадигми Фон-Неймана «побудови надійних систем із ненадійних компонентів» за напрямом забезпечення гарантоздатності, тобто побудови гарантоздатних ІКС з недостатньо надійних та безпечних (з точки зору функційної та кібербезпеки) компонентів.

2. Використання ІКС за призначенням в умовах зміни вимог, зміни параметрів середовища, виникнення неспецифікованих відмов, обумовлених фізичними і проектними дефектами та вразливостями, унеможливлює або суттєво ускладнює пряме застосування парадигми Фон-Неймана для необслуговуваних компонентів ІКС та потребує оновлення й відновлення системи, або / та надання їй властивостей резильєнтності.

3. Використання багатоцільового обслуговування з використанням стратегій, комбінованих за різними ознаками, зокрема, мети обслуговування (підтвердження вимог, зміни параметрів, зміни функцій…); процесів обслуговування (верифікації, оновлення, корекції), властивостей, які підтримуються завдяки обслуговуванню (надійності, функційної безпеки, кібербезпеки).

Сфера дії пропонованої концепції має застосування у випадках, коли принципи Фон-Неймана не дозволяють будувати гарантоздатну систему через обмеження економічного, часового характеру, чи з інших причин. У такому випадку використання принципів, методів та моделей, що є концептуальними, розповсюджується на ІКС, побудованих з використанням обслуговуваних компонент і системних багатоцільових стратегій обслуговування.

Оскільки після впровадження ІКС буде функціонувати в умовах змін параметрів середовища, то можливо два варіанти розвитку подій. У випадку використання парадигми Фон-Неймана, при змінах вимог, середовища, чи прояву неспецифікованих відмов, системі необхідний певний «запас міцності», який забезпечується підвищенням ступеня резервування (структурного, часового, версійного). При використанні БЦО на етапі проектування передбачена можливість гнучкого вибору його стратегії чи зміни параметрів за для забезпечення гарантоздатності ІКС.

Таким чином. пропонована концепція полягає у забезпеченні гарантоздатності ІКС шляхом БЦО в умовах змін параметрів середовища, вимог до системи та стійкості до відмов, обумовлених фізичними та проектними дефектами і атаками на вразливості.

На рис. 1 показано концептуальні зв'язки між розробленими елементами методології.

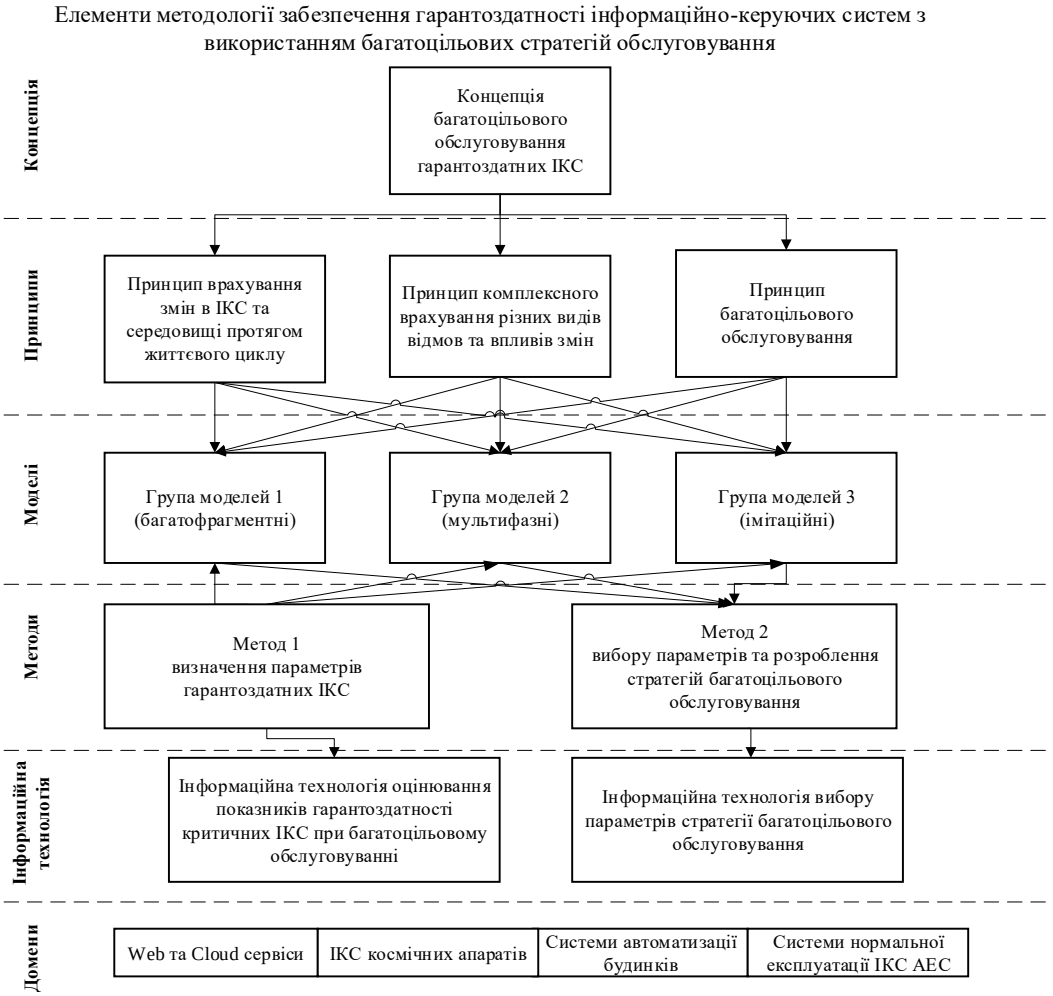


Рис. 1. Розроблені елементи методології забезпечення гарантоздатності ІКС

Запропонована концепція базується на використанні трьох основних принципів, які прямо пов'язані із розвитком відомих принципів системного аналізу [16, 17], а саме: а) розвитку, б) єдності та зв'язків, в) модульної побудови та функційності.

Принцип врахування змін в ІКС та середовищі протягом життєвого циклу

Принцип врахування змін є продовженням описаного в [18] принципу розвитку (історичності, або відкритості) систем під час процедур системного аналізу. Окрім необхідності врахування системних змін під час розвитку, еволюції, адаптації, заміни компонент чи розширення системи, потребує уваги зміна параметрів зовнішнього середовища/середовищ.

Протягом життєвого циклу ІКС можливі зміни як системи чи її компонент, так і середовищ, у яких система проектується, розробляється, тестується та експлуатується (функціонує).

Запропонований принцип врахування змін передбачає розширення класичного контуру управління відмовостійкої (fault-tolerant) системи, що забезпечує реакцію на прояв дефектів (fault, f) у вигляді помилок (error, e) та відмов (failure, F). На рис.2 показано основні елементи реакційного контуру та його розширення для реакції на зміни.

Класифікатор зовнішніх (по відношенню до системи) змін, наведений у [19] включає:

– зміни вимог до системи (функціональних $\{r_{fq}\}$, $q = 1,...,n_f$ та/або нефункціональних вимог, зокрема, вимог до складових гарантоздатності $\{r_{cw}\}$, $w = 1,..n_d$), які повинна реалізувати система;

– зміни параметрів середовища $\{r_{ej}\}$, $j = 1,..n_e$, які вона повинна ураховувати.

Запропонований класифікатор слід уточнити типом середовища, а саме:

$$\{r_e\}=\{r_{e\_pr}, r_{e\_dev}, r_{e\_test}, r_{e\_expl}\},$$

де $\{r_{e\_pr}\}$ – зміни у середовищі проектування,

$\{r_{e\_dev}\}$ – зміни у середовищі розробки,

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

$\{r_{e\_test}\}$ – зміни у середовищі тестування,

$\{r_{e\_expl}\}$ – зміни у середовищі експлуатації (функціонування).

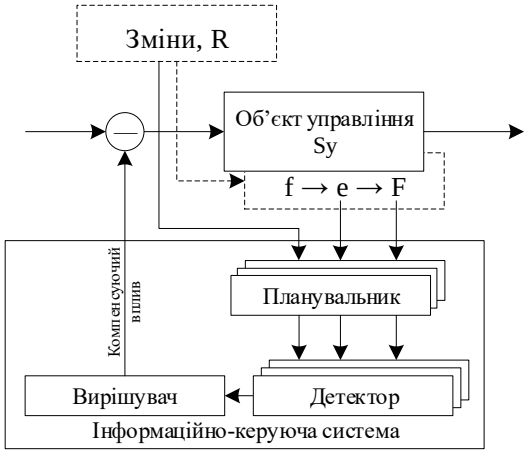


Рис. 2. Розширення елементів контуру управління fault-tolerant системи за принципом врахування змін

Множину R_{out}, що об'єднує множини $\{r_{fq}\}\{r_{cw}\}\{r_{ej}\}$, назвали факторами еволюції:

$$R_{out} = \{r_{fq}\} \cup \{r_{cw}\} \cup \{r_{ej}\}.$$

З математичної позиції зміни можливо описати за допомогою детермінованих або випадкових законів, при чому серед детермінованих законів окремо виділяють групу періодичних функцій. Таким чином, можна ввести додаткові уточнюючі класифікатори змін:

$$r_{math}=\{r_q\},\ q=(det, rand);$$
$$r_{det}=\{r_{det\_p}\},\ p=(period, aperiod),$$

де детерміновані зміни $\{r_{det}\}$:

– періодичні зміни $\{r_{det\_period}\}$,

– аперіодичні (неперіодичні) зміни $\{r_{det\_aperiod}\}$,

– випадкові зміни $\{r_{rand}\}$.

Уточнений класифікатор зовнішніх змін розширює їх множину наступним чином:

$$R_{out} = \{r_{fq}\} \cup \{r_{cw}\} \cup \{r_{ej}\} \cup \{r_{math}\}.$$

Класифікатор внутрішніх системних змін включає їх опис відносно двох груп компонент системи, що відносяться до апаратного $\{r_{HW}\}$ та програмного $\{r_{SW}\}$ забезпечення:

$$R_{in} = \{r_{HW}\} \cup \{r_{SW}\}.$$

Одним із прикладів, що ілюструє зміни у ІКС є використання впродовж життєвого циклу різних версій системи чи її компонент. Потрібно розрізняти висхідне (підвищення версії) на низхідне (пониження версії) версіонування. Оскільки для позначення версій розробники використовують двох- (i.j) та тризначну (i.j.k) порядкову нумерацію, її доцільно дотримуватися і при розробці множини внутрішніх змін.

Відношення між множинами R_{in} та R_{out} є причинно-наслідковими, і тому розглядаються у вигляді ланцюгів. Оскільки такі ланцюги можуть мати різну довжину та вкладеність, в межах принципу врахування змін вони будуються, починаючи з певної причини і обов'язково закінчуються подією зміни параметрів, що впливають на гарантоздатність системи.

Більш детально причинно-наслідкові ланцюги змін знаходять відображення при побудові моделей оцінювання складових гарантоздатності (безвідмовності, готовності, доступності, функційної безпеки). Окрім розглянутого як приклад версіонування, ІКС та їх компоненти можуть набути змін під час корекції за допомогою встановлення патчів для усунення виявлених дефектів та вразливостей. За певних обставин (космічний простір, віддалене керування) для підтримки працездатного стану в ІКС може бути ініційований процес керованої деградації для відключення дефектних ділянок. Ці процедури обслуговування будуть розглянуті далі. Зміни у середовищах проектування, розроблення та тестування можна описати за допомогою розглянутого вище механізму змін ІКС. Це справедливо за умови використання таких середовищ обмеженою кількістю користувачів з мінімізацією функцій доступу до глобальної мережі та ризиками зловмисних дій.

Принцип комплексного врахування різних видів відмов та впливів змін

Даний принцип є продовженням описаних в [16, 17] принципів єдності та зв'язків під час процедур системного аналізу. Він також є логічним продовженням запропонованого у роботі [7] фасетного упорядкування видів несправностей та ланцюгів причинно-наслідкових зв'язків від несправностей та дефектів до відмов, збоїв та помилок.

Згідно з запропонованим у [7] підходом, порушення працездатного стану ІКС обумовлено проявом видів несправностей (faults), що мають різну природу. Множину несправностей можна розбити на підмножини за рядом ознак, наприклад, за ознакою етапу прояву (конструктивні і експлуатаційні несправності). У дослідженнях [20,21] розглядається окрема група дефектів, пов'язаних зі старінням "aging" програмного забезпечення, яка була включена до розширеної фасетної класифікації несправностей.

Верхній рівень ознак запропонованої розширеної класифікації займає розподіл видів несправностей на чотири групи:

– фізичні дефекти (ДФ) (physical faults), які призводять до стійких відмов або короткочасних збоїв апаратних засобів ІКС;

– несправності, викликані дефектами проектування і виробництва (ДП) (design faults), які є наслідком помилкових дій, допущених при створенні системи; і призводять до появи конструкційних несправностей як апаратних, так і програмних засобів ІКС;

– несправності, викликані дефектами взаємодії (ДВ) (interaction faults), які є наслідком впливу зовнішніх факторів на апаратні та програмні засоби системи;

– несправності, викликані ефектом старіння програмного забезпечення (ДС), які призводять до стійких відмов або короткочасних збоїв програмних засобів ІКС. Цей тип несправностей додано відповідно до відомої класифікації дефектів програмних засобів, запропонованої у [22].

Відмови системи та її компонент, можуть бути викликані одиночною несправністю, групою несправностей чи послідовним проявом несправностей у вигляді «паталогічного» ланцюга.

Фізичні дефекти або несправності апаратних засобів (physical fault, fp) призводять до порушень або помилок обчислювального процесу (error, ep), які визначають відповідну подію для системи – збій або відмову (failure, Fp) і перехід у непрацездатний (частково непрацездатний) стан, тобто маємо патологічний ланцюжок fp → ep → Fp.

Аналогічні ланцюжки існують для проектних дефектів (design fault, fd) і дефектів взаємодії (interaction fault, fa = {fap, fai} внаслідок фізичних (fap) і інформаційних (fai) впливів, тобто: fd → ed → Fd, fa→ ea → Fa (fap → eap → Fap та/або fai → eai → Fai). Також, подібний ланцюг побудовано для дефектів старіння ПЗ: fsa → esa → Fsa.

На базі означених f-e-F ланцюжків побудована спеціальна нотація для аналізу подій та моделювання поведінки інформаційно-керуючої системи (рис.4). Вона є модифікацією нотації Occurence Nets (Causal Nets або Occurence Graphs), яка була запропонована B. Randell для фізичних і проектних несправностей та отримала назву Structured Occurence Nets [23].

За явних ознак виклику відмови (failure) окремою несправністю дослідники надають ознаки несправності цій відмові. Не для усіх класів систем характерні, або критичні для аналізу несправності з їх повної множини, оскільки вони (в силу об'єктивних обставин) не приведуть до відмови системи чи її компонент. Виключення деяких видів несправностей приводить до спрощення розробки моделей гарантоздатності. Також, наведене як приклад у роботі [24], групування несправностей у підмножини не є визначальним, але також призводить до спрощення моделей. Слід зазначити, що ознаками групування можуть виступати як додаткові ознаки, так і фасетні ознаки класифікації (рис. 3).

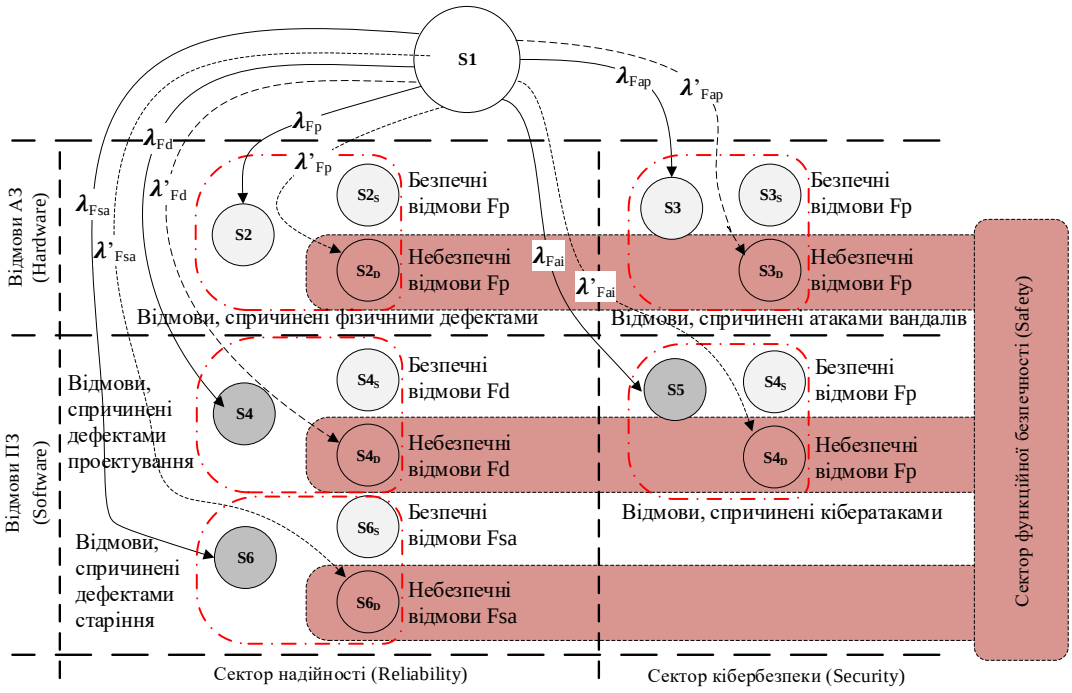


Рис. 3. Схема побудови загальної моделі функціонування ІКС з урахуванням різних груп причин відмов

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

Крім дефектів (faults) та обумовлених ними відмов (failures), можливі інші виклики. При деталізації причинно-наслідкових зв'язків, що приводять до прояву несправності, як відмови системи чи її компонентів необхідно враховувати не тільки внутрішньосистемні фактори, а й зовнішні по відношенню до системи події. Принцип комплексного врахування різних видів відмов та впливів середовища передбачає виконання наступних підготовчих етапів моделювання ІКС (рис. 4).

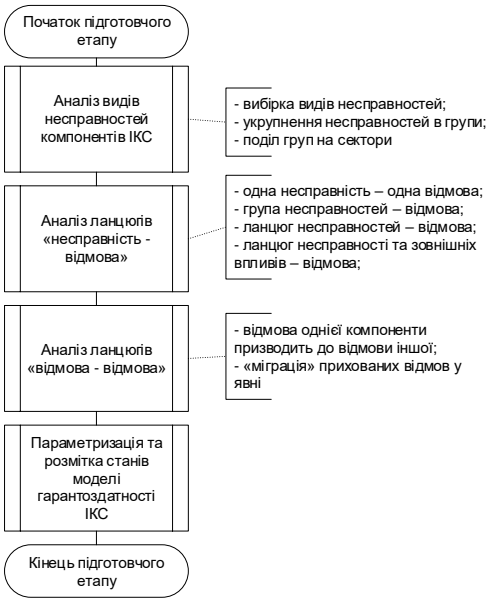


Рис. 4. Послідовність підготовчих етапів моделювання гарантоздатності ІКС

Принцип багатоцільового обслуговування

Він полягає у використанні в ІКС компонент, що передбачають комбіноване обслуговування протягом життєвого циклу для гарантування збереження чи змін у заданих межах результуючих показників надійності, інформаційної (кібер-) чи функційної безпеки.

Оскільки запропонована концепція спирається на поняття багатоцільової стратегії обслуговування ІКС, формування таких стратегій та їх вибір для забезпечення гарантоздатності, то першим завданням є їх класифікація. Для ідентифікації стратегії обслуговування та її складових використано скорочення, представлені у табл. 1.

У множинному аспекті стратегія обслуговування буде визначена як набір ідентифікованих складових у вигляді:

$$\mathrm{StrMaint} = \{\{\mathrm{GM_i}\},\{\mathrm{TM_i}\},\ \{\mathrm{ProcM_i}\},\{\mathrm{PropM_i}\},\{\mathrm{ParM_i}\}\}.$$

Таблиця 1

Позначення багатоцільових стратегій обслуговування та їх складових

Стратегія та її складові	Позначення	Скорочення
Стратегія обслуговування	StrMaint	
Ціль обслуговування	GoalMaint	GM
Тип обслуговування	TypeMaint	TM
Процес обслуговування	ProcMaint	ProcM
Властивості, задля яких виконується обслуговування	PropMaint	PropM
Параметри обслуговування	ParMaint	ParM

Ціль обслуговування формується на основі перетину підмножин мети та об'єкту (рис. 5).

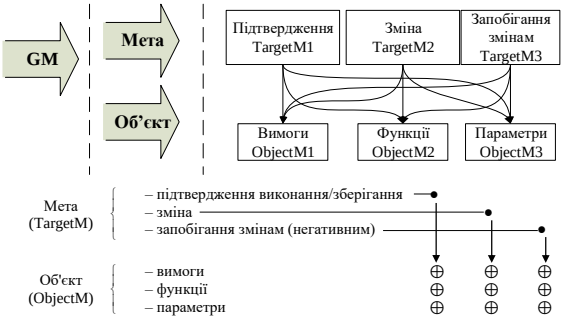


Рис. 5. Підмножини формування цілі обслуговування

Використання в ІКС апаратних та програмних засобів, які необхідно обслуговувати; часові параметри обслуговування (періодичність, за вимогою, за прогнозом, одночасність чи роздільність); обслуговування для забезпечення різних показників зумовлюють множину варіантів/сценаріїв. Для регламентування обслуговуючих процедур передбачено формування окремих політик і стратегій, проте їх реалізація не завжди забезпечує очікуваний ефект.

Таким чином, множина одиничних цілей формується як декартовий добуток множини мети на множину об'єкту обслуговування та має вигляд:

$$\mathrm{GM^I_i} = \{\mathrm{TargetM}\}\times\{\mathrm{ObjectM}\} = \\ = \left\{(\mathrm{T,O}) \mid \mathrm{T_i} \in \{\mathrm{TargetM}\}, \mathrm{O_j} \in \{\mathrm{ObjectM}\}\right\}.$$

Прикладами одиничних цілей є:
- (T1,O1) підтвердження вимог;
- (T2,O2) зміна функцій;
- (T3,O3) запобігання змін параметрів.

При багатоцільовому обслуговуванні множина цілей формується за рахунок комбінування елементів, що входять до множини одиничних цілей. Умовою комбінування одиничних цілей є неоднаковість об'єктів у них, адже неможливо одночасно забезпечити і підтвердження і зміну вимог, функцій чи параметрів (а тим паче зміну та запобігання змінам!).

$$GM^{II}{}_i = \left(T_i, O_j\right) \times \left(T_k, O_n\right) \mid O_i \neq O_n;$$
$$T_i, T_k \in \{TargetM\}; O_j, O_n \in \{ObjectM\}.$$

Потужність множини комбінованих цілей для двократного комбінування одиничних цілей становить 54 елементи.

Приклади подвоєного комбінування одиничних цілей є:

- (T1,O1;T2,O2) підтвердження вимог при зміні функцій;

- (T1,O2;T2,O1) підтвердження функцій при зміні вимог;

- (T3,O3;T2,O1) запобігання змін параметрів при зміні вимог.

Повна множина комбінованих цілей буде утворена шляхом потроєного комбінування одиничних цілей та має вигляд:

$$GM^{III}{}_i = \left(T_i, O_j\right) \times \left(T_k, O_n\right) \times \left(T_p, O_q\right) \mid O_i \neq O_n \neq O_q;$$
$$T_i, T_k, T_p \in \{TargetM\}; O_j, O_n, O_q \in \{ObjectM\}.$$

Потужність множини комбінованих цілей для трикратного комбінування одиничних цілей становить 162 елементи.

Приклади потроєного комбінування одиничних цілей:

- (T1,O1;T1,O2;T1,O3) підтвердження вимог, функцій та параметрів;

- (T1,O2;T2,O2;T2,O3) підтвердження функцій при зміні вимог та параметрів;

- (T1,O2;T3,O3;T2,O1) підтвердження функцій та запобігання змін параметрів при зміні вимог.

Запропоновані класифікатори типів обслуговування мають ієрархічну структуру, наведену у табл. 2.

Таблиця 2

Класифікатори типів обслуговування

Позн.	Ознака класифікатора	Значення класифікатора		
ТМ1	За повнотою охоплення компонент системи	ТМ11 – часткове	ТМ12 – повне	
ТМ2	За покриттям цілей	ТМ21 – одноцільове	ТМ22 – багатоцільове	
ТМ3	За часом проведення	ТМ31 – детерміноване (планове, періодичне)	ТМ32 – у випадкові моменти часу	
ТМ4	За місцем проведення	ТМ41 – локальне / місцеве	ТМ42 – віддалене	
ТМ5	За потребою підключення до глобальної мережі	ТМ51 – онлайн	ТМ52 – оффлайн	
ТМ6	За способом визначення моменту проведення	ТМ61 – за розкладом	ТМ62 – за напрацюванням	ТМ63 – за прогнозом

Часткове обслуговування (ТМ11) проводиться для підтримки працездатного стану окремих компонент ІКС, наприклад окремо проводиться обслуговування АЗ, а через деякий час – оновлення ПЗ. Також під частковим обслуговуванням слід розуміти і обслуговування окремих блоків / модулів АЗ у різні часові проміжки, або ж оновлення різних програмних компонент інфраструктури у різні періоди. Повне обслуговування (ТМ12), навпаки, передбачає проведення процедур із усіма компонентами ІКС. Зрозуміло, що в ІКС зі складною інфраструктурою проведення повного обслуговування може не відбуватися жодного разу за весь життєвий цикл через складність та різноманітність їх компонент. Але в окремих випадках, наприклад для ІКС АЕС, є чіткі регламентні вказівки щодо проведення proof test – «поглибленого тестування» усіх модулів і це є вважатимемо різновидом повного обслуговування.

Обслуговування у детерміновані моменти часу (ТМ31) передбачено спеціальною документацією – регламентами, планами, політикою, стандартами. Прикладами планового обслуговування є:

- планові поточний та капітальний ремонти;

- перехід на нову версію програмної компоненти за умови завчасного попередження компанії – розробника про припинення супроводу старої версії;

- обслуговування за наявності стійкого зв‘язку між наземним центром керування польотами та ІКС штучного супутника Землі на еліптичній орбіті;

- проведення proof test для виявлення прихованих відмов у системах, критичних для функціональної безпеки.

Обслуговування у випадкові моменти часу (ТМ32) виконується за настанням явної (неприхованої) непередбачуваної події – відмови АЗ та / або ПЗ, кібератаки, розробки патча, який необхідно встановити, помилки мажоритарного елементу за умови справності усіх каналів, тощо.

Локальне (ТМ41) проведення обслуговування ІКС передбачає безпосередній контакт обслуговуючого персоналу та систем з компонентами ІКС. Локальне обслуговування надає більше можливостей щодо доступу до усіх компонент, виміру їх параметрів, локалізації та усунення дефектів та прихованих відмов. Але у ряді випадків (космічні апарати, компоненти ІКС АЕС у небезпечній реакторній зоні) можливе проведення лише віддаленого обслуговування (ТМ42). Також віддалене обслуговування широко розповсюджене для компонент ІКС, що мають підключення до глобальної мережі. Слід зазначити, що у статті обслуговування ІКС космічних апаратів (КА) розглядається як онлайн-обслуговування, оскільки потребує активного (хоч і не Internet) каналу зв’язку між КА і наземним центром.

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

Визначення часових моментів проведення обслуговування може здійснюватися завчасно ще на етапі проектування ІКС і оформлюється у вигляді плану-розкладу з жорстким регламентом. Дослідження останніх десятиріч вказують на кращий з точки зору ефективності підхід гнучкого планування обслуговувань. При такому підході визначення моментів часу для обслуговування може здійснюватися на основі спостережень за станом компонент системи та зміною її параметрів. Також базою для корегування інтервалів між обслуговуваннями та типів, цілей, властивостей та параметрів можуть виступати незалежні до системи зовнішні фактори: річні прогнози експертів щодо тенденцій у сфері кібербезпеки, попередні плани з випуску нових версій ПЗ, тощо.

Повна множина типів обслуговування має вигляд:

$$\mathrm{TM} = (\{\mathrm{TM1}\} \times \{\mathrm{TM2}\} \times \{\mathrm{TM3}\} \times \{\mathrm{TM4}\} \times \{\mathrm{TM5}\} \times \{\mathrm{TM6}\} \mid \mathrm{TM4}_2 \neq \mathrm{TM5}_2; \mathrm{TM3}_2 \neq \mathrm{TM6}_1),$$

де $\mathrm{TM4}_2 \neq \mathrm{TM5}_2$ – умова суперечності віддаленого та оффлайн обслуговування; $\mathrm{TM3}_2 \neq \mathrm{TM6}_1$ – умова суперечності планового обслуговування у випадковий час.

Без врахування обмежень, пов'язаних зі зв'язками із зовнішніми множинами, та врахувавши два випадки взаємозалежності між елементами всередині множини типів обслуговування; потужність цієї множини складає 60 елементів.

Проведення обслуговування передбачає виконання великої кількості як типових, так і унікальних для конкретного класу ІКС процедур, розгляд яких виходить за рамки даної роботи. Для висвітлення запропонованих у роботі концептуальних засад прийнято рішення обмежитись чотирма процедурами (табл. 3).

Таблиця 3

Класифікатори виокремлених процедур багатоцільового обслуговування

Класифікатор	Англ. позначення	Укр. позначення
ProcM1	Update / upgrade	Оновлення
ProcM2	Correction / patching	Корекція
ProcM3	Verification	Верифікація
ProcM4	Testing / proof testing	Профілактичне тестування

Оновлення (ProcM1) є процедурою, що полягає в заміні компонент ІКС з метою розширення набору функцій, які реалізує система. Розрізняють оновлення ПЗ (update software) та оновлення АЗ (upgrade hardware). Оновлення ПЗ може реалізовуватися віддалено, для АЗ можлива організація віддаленого оновлення проектів ПЛІС. Оскільки оновлення часто виконується планово та вимагає тривалого простою компонент системи, до його процедур можуть додавати корекцію дефектних ділянок коду, що реалізує старий функціонал ІКС.

Корекція (ProcM2) передбачає заміну блоків / модулів чи ділянок програмного коду з виявленими дефектами чи вразливостями. В окремих випадках, за допомогою корегуючих дій виконується відключення дефектних блоків чи ділянок коду. При цьому система деградує, але зберігає частково працездатний стан. Ключовим моментом є виконання корегуючих дій після виявлення дефекту чи прояву його як відмови або збою.

Верифікація (ProcM3) є процесом підтвердження виконання формальних вимог. За більшості випадків вона проводиться перед початком експлуатації. Для ряду ІКС, зокрема, КА, відтворення умов експлуатації на етапі проектування неможливе чи занадто дороге. Тому підтвердження виконання усіх вимог здійснюється після запуску КА в умовах відкритого космічного простору. Такі процедури отримали назву онлайн-верифікації.

Профілактичне тестування ІКС критичного застосування (ProcM4) має на меті виявлення небезпечних прихованих відмов. Таке тестування характеризується параметром DC (diagnostic coverage), значення якого хоч і обмежене галузевими стандартами, та може коливатися і повинне бути обґрунтованим. За певних обставин виявлення прихованих відмов можливе без проведення діагностичних тестів під час опрацювання інших дефектів, що проявилися у вигляді явних відмов. Таке явище назвали «міграцією» прихованих відмов у явні відмови. Для резервованих архітектур ІКС врахування «міграції» відмов дозволяє скорегувати міжтестові інтервали.

Таким чином, множина елементів процедур обслуговування, що розглянуті у цій роботі, обмежується потужністю у 4 елементи:

$$\mathrm{ProcM} = \{\mathrm{ProcM_i}\} \mid \mathrm{i} \in [1..4].$$

Питання комплексування процедур обслуговування взаємопов'язані із доменом використання ІКС та моделями оцінювання підвластивостей гарантоздатності. Перелік властивостей та параметрів ІКС, які визначають їх якість та використовуються для кількісного оцінювання вимог досить обширний. Для демонстрації реалізації концептуальних засад, принципів та методів, прийнято рішення обмежитися трьома властивостями та їх окремими компонентами, представленими у таблиці 4.

Таблиця 4

Класифікатори виокремлених властивостей гарантоздатності

Класифікатор	Властивість	Підвластивість	Англ. термін	Позначення	Врахування
PropM1	Надійність	Безвідмовність	Reliability	R(t)	PropM11
		Ремонтопридатність	Maintainability		
		Довговічність	Durability		
		Збережуваність	Storabilily		
		Готовність	Availability	A(t)	PropM12
		Оперативна готовність	Operational availability		
PropM2	Інформаційна (кібер) безпека	Цілісність	Integrity		
		Конфіденційність	Confidentiality		
		Доступність	Availability	A(t)	PropM2
PropM3	Функційна безпека	Усереднена ймовірність небезпечних відмов за запитом	Average Probability of dangerous Failure on Demand	PFDavg	PropM3
		Усереднена частота небезпечних відмов	Average frequency of dangerous failure	PFH	
PropM4*	Готовність		Availability	A(t)	PropM4

Примітка *: Властивість готовності може виступати як складова надійності, інформаційної/кібербезпеки чи функційної безпеки (як протилежне PFDavg), то вона розглядається як окремий інтегрований показник гарантоздатності (PropM4)

У загальному випадку показники гарантоздатності сучасних ІКС оперують із множинами відмов апаратного та програмного забезпечення. Конкретизація причин відмов АЗ та ПЗ залежить від конкретного домену застосування ІКС, і буде розглянута нижче. Для оцінювання показників гарантоздатності були побудовані моделі станів та переходів систем (марковські, багатофрагментні та мультифазні), які базуються на представленні у вигляді множини станів MS та множини зміни станів ME. Тоді:

$$MS=\{S_{Pi}, S_{Hi}\}=\{S_{Pi\,HW}, S_{Pi\,SW}\} \cup \{S_{Hi\,HW}, S_{Hi\,SW}\},$$

$$ME=\{E_{Fi}, E_{Ri}\}=\{E_{Fi\,HW}, E_{Fi\,SW}\} \cup \{E_{Ri\,HW}, E_{Ri\,SW}\},$$

де $\{S_{Pi\,HW}, S_{Pi\,SW}\}$ – підмножина працездатних станів АЗ та ПЗ,

$\{S_{Hi\,HW}, S_{Hi\,SW}\}$ – підмножина непрацездатних станів АЗ та ПЗ,

$\{E_{Fi\,HW}, E_{Fi\,SW}\}$ – підмножина змін станів, спричинених відмовами АЗ та ПЗ,

$\{E_{Ri\,HW}, E_{Ri\,SW}\}$ – підмножина змін станів, спричинених відновленням АЗ та ПЗ.

Для невідновлювальних систем (домен ІКС космічних апаратів) використовується показник безвідмовності (PropM11), що визначається як:

$$R(t)=\sum P_i(t);\ i:S_i \in S_P;$$

$$S_P \in M\{S_P, S_H\}; M\{E_{Ri}\}=\varnothing.$$

Для відновлювальних систем $M\{E_{Ri}\} \neq \varnothing$ і використані показники PropM12, PropM2, PropM3, PropM4.

В доменах ІКС космічних апаратів досліджені відмови АЗ та ПЗ, спричинені фізичними дефектами та дефектами проектування. Як показник гарантоздатності використано функцію готовності (для багатофрагментних моделей) та усереднену функцію неготовності для мультифазної моделі:

$$A(t)=\sum P_i(t);\ i:S_i \in S_P;$$

$$S_P \in M\{S_{P\,HW}, S_{H\,HW\,pf}, S_{P\,SW}, S_{H\,SW\,df}\},$$

$$U_{avg}(\tau)=\int_0^{\tau} U(t)\,dt=\int_0^{\tau}(1-A(t))\,dt,$$

$$ME=\{E_{Fi}, E_{Ri}, E_{Ver\,i}, E_{Corr\,i}\},$$

де $\{S_{P\,HW}, S_{H\,HW\,pf}\}$ – підмножина працездатних станів АЗ та непрацездатних станів АЗ, спричинених фізичними дефектами,

$\{S_{P\,SW}, S_{H\,SW\,df}\}$ – підмножина працездатних станів ПЗ та непрацездатних станів ПЗ, спричинених дефектами проектування,

Uavg – усереднена функція неготовності ІКС (аналог PropM3),

$E_{Ver\,i}$ – множина змін станів, спричинених процедурами оперативної верифікації;

$E_{Corr\,i}$ – множина змін станів, спричинених процедурами корекції програмного коду.

У доменах Web-сервісів та систем автоматизації розумних будинків досліджені відмови АЗ та ПЗ, спричинені фізичними дефектами, дефектами проектування та кібератаками на ПЗ (дефектами взаємодії f_{ai}). Також у домені систем кіберфізичного захисту досліджені атаки вандалів на апаратні засоби зовнішнього периметру (дефекти взаємодії f_{ap}). Для

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

оцінювання гарантоздатності використано інтегровану функцію готовності (PropM4):

$$A(t) = \sum P_{S_{Pi}}(t);$$

$$S_P \in M\left\{S_{P\,HW}, S_{H\,HW\,pf}, S_{P\,SW}, S_{H\,SW\,df}, S_{H\,SW\,ai}\right\},$$

$$A(t) = \sum P_{S_{Pi}}(t);$$

$$S_P \in M\begin{Bmatrix} S_{P\,HW\,pf}, S_{H\,HW\,pf}, S_{P\,SW\,df}, S_{H\,SW\,df}, \\ S_{P\,HW\,ap}, S_{H\,HW\,ap}, S_{P\,SW\,ai}, S_{H\,SW\,ai} \end{Bmatrix},$$

$$ME = \left\{E_{Fi}, E_{Ri}, E_{Path\,i}, E_{Up\,i}\right\},$$

де $\{S_{P\,SW}, S_{H\,SW\,ai}\}$ – підмножина працездатних станів ПЗ та непрацездатних станів ПЗ, спричинених кібератаками,

$\{S_{P\,HW}, S_{H\,HW\,ai}\}$ – підмножина працездатних станів АЗ та непрацездатних станів АЗ, спричинених атаками вандалів;

$E_{Path\,i}$ – множина змін станів, спричинених встановленням патчів;

$E_{Up\,i}$ – множина змін станів, спричинених процедурами оновлення ПЗ;

У домені ІКС СНЕ АЕС множина відмов деталізується підмножинами безпечних (MS) і небезпечних (MD). Застосування засобів контролю, тестування в реальному часі і діагностування дозволяє детектувати відмови, що обумовлює виділення чотирьох підмножин відмов:

- SD: безпечні виявлені (safe detected),
- SU: безпечні невиявлені (safe undetected),
- DD: небезпечні виявлені (dangerous detected),
- DU: небезпечні невиявлені (dangerous undetected),

причому кожна підмножина відмов характеризується відповідним параметром - інтенсивністю.

Для оцінювання гарантоздатності використано усереднену ймовірність небезпечних відмов за запитом (PropM3) та функцію готовності до небезпечних відмов (PropM4):

$$U_{avg}(\tau) = \int_0^\tau U(t)\,dt = \int_0^\tau \left(\sum P_{S_{Di}}(t)\right) dt;$$

$$S_D \in M\left\{S_{DU\,HW}, S_{DD\,HW}, S_{DU\,SW}, S_{DD\,SW}\right\},$$

$$A(t) = \sum P_{S_{PSi}}(t);$$

$$S_{PS} \in M\left\{S_{P\,HW}, S_{P\,SW}, S_{SU\,HW}, S_{SD\,HW}, S_{SU\,SW}, S_{SD\,SW}\right\},$$

$$ME = \left\{E_{Fi}, E_{Ri}, E_{Path\,i}, E_{Migr\,i}\right\},$$

де $\{S_{DU\,HW}, S_{DD\,HW}\}$ – підмножина станів АЗ із проявленими небезпечними відмовами,

$\{S_{DU\,SW}, S_{DD\,SW}\}$ – підмножина станів ПЗ із проявленими небезпечними відмовами,

$\{S_{SU\,HW}, S_{SD\,HW}\}$ – підмножина станів АЗ із проявленими безпечними відмовами,

$\{S_{SU\,SW}, S_{SD\,SW}\}$ – підмножина станів ПЗ із проявленими безпечними відмовами,

$E_{Migr\,i}$ – множина змін станів, спричинених міграцією прихованих відмов у явні.

Множина підвластивостей гарантоздатності, що розглянуті у цій роботі, обмежується потужністю у 5 елементів:

$$PropM = \left\{PropM_i\right\} \mid i \in [11, 12, 2, 3, 4].$$

Слід зазначити, що у разі комбінування властивостей, що входять до множини {PropM}, наприклад, якщо розглядається комплексний вплив на надійність та кібербезпеку, то використовується елемент множини PropM4. Комбінування інших елементів множини {PropM} не використовується.

У даній роботі для оцінювання підвластивостей гарантоздатності використовується три групи вхідних параметрів обслуговування (табл. 5).

Множина параметрів, що розглянуті у цій роботі, обмежується потужністю у 3 елементи:

$$ParM = \left\{ParM_i\right\} \mid i \in [1, 2, 3].$$

Питання комплексування параметрів обслуговування взаємопов'язані із доменом використання ІКС та моделями оцінювання підвластивостей гарантоздатності.

Повна множина стратегій обслуговування визначається шляхом прямого множення підмножин цілі, типу, процесу, властивостей та параметрів обслуговування:

$$M_U\left\{StrMaint\right\} = GM \times TM \times ProcM \times PropM \times ParM.$$

Потужність повної множини стратегій обслуговування складає 583200 елементів

Реальна множина стратегій обслуговування враховує додаткові обмеження, що стосуються специфіки доменів використання ІКС, вимог нормативних документів для конкретних галузей, обмеження та допущення математичного апарату оцінювання підвластивостей гарантоздатності. Вказані обмеження звужують потужність реальної множини стратегій обслуговування так, що:

$$M_R\left\{StrMaint\right\} \subset M_U\left\{StrMaint\right\}.$$

Таблиця 5

Класифікатори виокремлених параметрів обслуговування

Класифікатор	Характеристика параметра	Підхарактеристика	Узагальнена назва	Конкретизація / можливе позначення
ParM1	Часові	Детерміновані	Період	T
			Регламентна тривалість	Δt
		Випадкові	Інтенсивність проведення	λ, μ
			Середня тривалість проведення	$T_c=1/\lambda$
ParM2	За охопленням	Кількість блоків/модулів, що обслуговуються		Блоків АЗ
				Блоків ПЗ
		Кількість виявлених дефектів / вразливостей		Явних дефектів
				Прихованих дефектів
				Відомих вразливостей
				Вразливостей нульового дня
		Кількість усунених дефектів / вразливостей		Явних дефектів
				Прихованих дефектів
				Відомих вразливостей
				Вразливостей нульового дня
		Кількість внесених нових дефектів / вразливостей		Явних дефектів
				Прихованих дефектів
				Відомих вразливостей
				Вразливостей нульового дня
ParM3	Ймовірнісні	Ймовірність успішного виявлення дефекту / вразливості (N дефектів / вразливостей)		α, β
		Ймовірність усунення дефекту / вразливості (N дефектів / вразливостей) за час, відведений на обслуговування		D
		Діагностичне охоплення (Diagnostic coverage)		DC

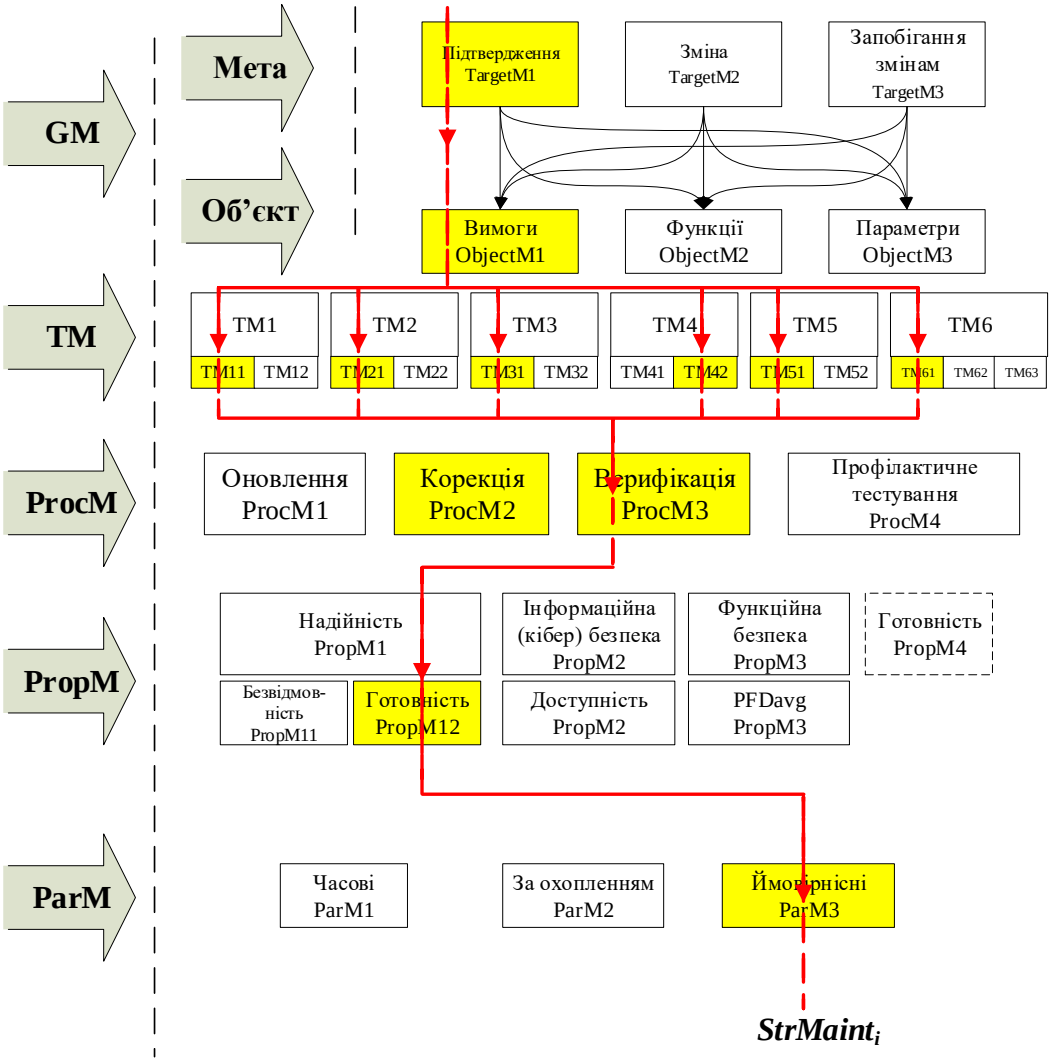
У домені ІКС космічних апаратів стратегії обслуговування направлені на забезпечення вимог до збереження функціонування (підтвердження функцій) за умови зміни даних про середовище космічного простору (зміна параметрів). Специфіка функціонування космічних апаратів передбачає проведення часткового одноцільового обслуговування у детерміновані чи випадкові моменти часу. Це також віддалене (аналог онлайн типу) обслуговування, яке проводиться з використанням процедур корекції та верифікації. Таке обслуговування направлене на забезпечення показників безвідмовності та готовності (з точки зору надійності) через керуючий вплив на часові параметри його проведення як за розкладом, так і за результатами напрацювання. На рис.7 проілюстровано варіант побудови стратегії обслуговування у домені ІКС космічних апаратів.

У доменах Web-сервісів та хмарних (Cloud) систем реалізовані стратегії обслуговування, які направлені на забезпечення показників якості (зокрема, надійності та кібербезпеки) для користувачів цих ресурсів. Функціонування сервісів в умовах жорсткої конкурентної боротьби за клієнтів обумовлює проведення оновлень для покращення чи розширення їх функціональної складової. Поширеними варіантами цілей обслуговування таких систем є зміна функцій, підтвердження вимог, зміна параметрів та їх комбінування.

Враховуючи специфіку функціонування Web-сервісів та хмарних (Cloud) систем, тип їх обслуговування має наступні ознаки: часткове, багатоцільове, детерміноване/у випадкові моменти часу, віддалене, онлайн, може проводитися як за розкладом, так і за напрацюванням (особливо, в залежності від навантаження), а також і за прогнозом. При обслуговуванні Web-сервісів та хмарних (Cloud) систем як правило використовують процеси оновлення та корекції. Обслуговування спрямовано на забезпечення показників готовності (як складової надійності), доступності (як складової кібербезпеки), або інтегрального показника. Параметри стратегій обслуговування, через які здійснюється керуючий вплив мають часовий та ймовірнісний склад.

У доменах систем автоматизації будинків та систем фізичного захисту цілями обслуговування часто є підтвердження вимог при зміні функцій. Типам обслуговування притаманні наступні значення класифікаторів: як часткове, так і повне, багатоцільове, проводиться і у детерміновані (за розкладом чи за прогнозом), і у випадкові моменти часу. Обслуговування може проводитися локально (офлайн) та віддалено (онлайн) через процедури оновлення і корекції. Розглядається вплив на інтегрований показник готовності через керуючий вплив на часові та ймовірнісні параметри. У домені систем автоматизації будинків пріоритет має забезпечення

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)



$$\mathrm{StrMaint}_{\mathrm{I\&CSSC}} = (\mathrm{T1}, \mathrm{O1}; \mathrm{TM11}, \mathrm{TM21}, \mathrm{TM31}, \mathrm{TM42}, \mathrm{TM51}, \mathrm{TM61}; \mathrm{ProcM3}; \mathrm{PropM12}; \mathrm{ParM3})$$

Рис. 7. Ілюстрація вибору значень класифікаторів
для стратегії обслуговування ІКС космічних апаратів

функційної безпеки, а у домені систем фізичного захисту – забезпечення інформаційної та/або кібербезпеки.

У домені ІКС АЕС проведення обслуговування направлене як на підтвердження вимог, так і на запобігання змін параметрів. Специфіка проведення обслуговування визначається такими типами: як часткове, так і повне, одноцільове, і детерміноване (всі три типи – за розкладом, за напрацюванням і за прогнозом) і у випадкові моменти часу, локальне, оффлайн. Розглянуто процедури обслуговування – корекція та профілактичне тестування. Обслуговування у першу чергу направлене на забезпечення показника функційної безпеки (PFDavg), іноді – на забезпечення інтегрального показника готовності через керуючий вплив на всі три групи параметрів (часові, за обсягом та ймовірнісні).

Висновки

Запропонована методологія забезпечення гарантоздатності інформаційно-керуючих систем, на відміну від відомих, базується на уніфікованому аналізі впливу змін вимог та середовища й комплексного врахування різних видів відмов, формалізованому поданні та виборі багатоцільових стратегій обслуговування. Вона складається з концепції багатоцільового обслуговування, а також принципів: врахування змін в ІКС та середовищі протягом життєвого циклу; комплексного врахування різних видів відмов та впливів змін; багатоцільового обслуговування та об'єднує комплекс нових моделей та методів визначення параметрів гарантоздатних ІКС та вибору параметрів процедур їх обслуговування , що надає змогу підвищити точність оцінювання та по-

казники складових властивостей та гарантоздатності систем в цілому.

У рамках запропонованої методології розроблено стратегії багатоцільового обслуговування, множину варіантів цілей, типів, процесів, властивостей та параметрів гарантоздатності ІКС, що дозволяє знизити модельну невизначеність та обґрунтувати практичні заходи щодо забезпечення гарантоздатності на різних етапах життєвого циклу.

Подальші дослідження слід спрямувати на розроблення і дослідження комплексів моделей (багатофрагментних, мультифазних, імітаційних) оцінювання гарантоздатності ІКС різних доменів; а також методів та інформаційних технологій, які є елементами запропонованої методології.

Література

1. Developing Cyber Resilient Systems: A Systems Security Engineering Approach [Text] / R. Ross, V. Pillitteri, R. Graubart, D. Bodeau, R. Mcquaid. – Gaithersburg : U.S. Department of Commerce, NIST Special Publication 800-160. – 2019. – Vol. 2. – 229 p.

2. Assante, M. TLP: White - ICS Defense Use Case. Modular ICS Malware [Text] / M. Assante, R. Lee, T. Conway. – Washington : Electricity Information Sharing and Analysis Center (E-ISAC), 2017. – 27 p.

3. Яровая, М. SoftServe подверглась атаке хакеров [Електронний ресурс] / М. Яровая. – Режим доступу: https://ain.ua/2020/09/01/softserve-haknuli/ – 21.08.2020.

4. IEC 60050-192:2015: International Electrotechnical Vocabulary (IEV) - Part 192: Dependability [Text] ; impl. 2015-02-26. – Brussels : European Committee for Electrotechnical Standardization, 2015. – 239 p.

5. ISO/IEC 60300-1:2014: Dependability management –Part 1: Guidance for management and application [Text] ; impl. 01.05.2014. – Brussels : European Committee for Electrotechnical Standardization, 2014. – 98 p.

6. ДСТУ 2861-94. Надійність техніки. Аналіз надійності. Основні положення [Текст] ; введений 01.01.1996. – К. : Держстандарт України, 1995. – 35 с.

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

8. Gorbenko, A. On Composing Dependable Web Services Using Undependable Web Components [Text] / A. Gorbenko, V. Kharchenko, A. Romanovsky // International Journal on Simulation and Process Modelling (IJSPM). – 2007. – Vol. 3, No. 1/2. – P. 45–54.

9. Kharchenko, V. Dependability of Safety–Critical Computer Systems through Component–Based Evolution [Text] / V. Kharchenko, V. Sklyar, A. Siora // Dependability of Computer systems "DepCoS – RELCOMEX 2009": proceedings of International Conference. – Poland, Brunow, 2009. – P. 42–49.

10. Critical Energy Infrastructure Safety Assurance Strategies Considering Emergent Interaction Risk [Text] / E. Brezhnev, V. Kharchenko, V. Manulik, K. Leontiev // Advances in Dependability Engineering of Complex Systems. – 2017. – Vol. 582. – P. 67-78.

11. Фон-Неман, Дж. Вероятностная логика и синтез надежных организмов из ненадежных компонент [Текст] / Дж. Фон-Неман // Автоматы. – 1956. – С. 68–139.

12. Харченко, В. С. Гарантоздатні системи та багатоверсійні обчислення: аспекти еволюції [Текст] / В. С. Харченко // Радіоелектронні і комп'ютерні системи. – 2009. – № 7. – С. 46–59.

13. Gorbenko, A. Dependable Composite Web Services with Components Upgraded Online [Text] / A. Gorbenko, V. Kharchenko, P. Popov, A. Romanovsky // Architecting Dependable Systems III, LNCS 3549 / Eds.: R. de Lemos, C. Gacek, A. Romanovsky. – Berlin, Heidelberg (Germany) : Springer-Verlag, 2005. – P. 92–121.

14. Hardware diversity and modified NUREG/CR-7007 based assessment of NPP I&C safety [Text] / O. Illiashenko, V. Kharchenko, A. Kor, A. Panarin and V. Sklyar // 2017 9th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS). – 2017. – P. 907-911

15. Brezhniev, Ye. Multilevel Fuzzy Logic-Based Approach for Critical Energy Infrastructure's Cyber Resilience Assessment [Text] / Ye. Brezhnev // 2019 10th International Conference on Dependable Systems, Services and Technologies (DESSERT). – 2019. – P. 213-217.

16. Системный анализ в управлении: учеб. пособие [Текст] / О. В. Булыгина, А. А. Емельянов, Н. З. Емельянова, А. А. Кукушкин ; под ред. д-ра экон. наук, проф. А. А. Емельянова. – 2-е изд., перераб. и доп. – М. : ФОРУМ : ИНФРА-М, 2017. – 450 с.

17. Прокопенко, Т. О. Теорія систем і системний аналіз [Текст] : навч. посіб. / Т.О. Прокопенко. – Черкаси : ЧДТУ, 2019. – 139 с.

18. Гейда, А. С. Задачи исследования операционных свойств совершенствуемых систем и процессов их функционирования: Концептуальные аспекты [Текст] / А. С. Гейда, И. В. Лысенко // Прикладная информатика. – 2017. – № 5(71). – С. 93-106.

19. Cybernetic Approach to Developing Resilient Systems: Concept, Models and Application [Text] / V. Kharchenko, S. Dotsenko, Yu. Ponochovnyi, O. Illiashenko // Information & Security : An International Journal. – 2020. – Vol. 47, No. 1. – P. 77-90.

20. Menasche, D. Rejuvenation and the Age of Information [Text] / D. Menasche, K. Trivedi, E. Altman // 2019 IEEE International Symposium on Software

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

Reliability Engineering Workshops (ISSREW). – 2019. – P. 225-231.

21. Analyzing Software Rejuvenation Techniques in a Virtualized System: Service Provider and User Views [Text] / J. Bai, X. Chang, F. Machida, K. S. Trivedi, Z. Han // IEEE Access. – 2020. – Vol. 8. – P. 6448-6459.

22. Grottke, M. An empirical investigation of fault types in space mission system software [Text] / M. Grottke, A. P. Nikora, K. S. Trivedi // 2010 IEEE/IFIP International Conference on Dependable Systems & Networks (DSN). – 2010. – P. 447-456.

23. Randell, B. Occurrence Nets Then and Now: The Path to Structured Occurrence Nets [Text] / B. Randell // Applications and Theory of Petri Nets. – 2011. – P. 1-16.

24. Abdulmunem, A. Availability and Security Assessment of Smart Building Automation Systems: Combining of Attack Tree Analysis and Markov Models [Text] / A. Abdulmunem, V. Kharchenko // 2016 Third International Conference on Mathematics and Computers in Sciences and in Industry (MCSI). – 2016. – P. 302-307.

References

1. Ross, R., Pillitteri, V., Graubart, R., Bodeau, D. and McQuaid, R. Developing Cyber Resilient Systems: A Systems Security Engineering Approach. *NIST Special Publication 800-160*, vol. 2, 2019. 229 p. doi: 10.6028/NIST.SP.800-160v2.

2. Assante, M., Lee, R. and Conway, T. TLP: White - ICS Defense Use Case. Modular ICS Malware. *Electricity Information Sharing and Analysis Center (E-ISAC)*, 2017. 27 p.

3. Yarovaya, M. *Softserve Has Been Attacked by Hackers*. Available at: https://ain.ua/2020/09/01/ softserve-haknuli/ (accessed 21.08. 2020).

4. *IEC 60050-192:2015: International Electrotechnical Vocabulary (IEV) - Part 192: Dependability*. European Committee for Electrotechnical Standardization Publ., 2015. 239 p.

5. *ISO/IEC 60300-1:2014: Dependability Management – Part 1: Guidance For Management And Application.* European Committee for Electrotechnical Standardization Publ., 2014. 98 p.

6. *DSTU 2861-94. Nadiynist' tekhniky. Analiz nadiynosti. Osnovni polozhennya* [Reliability of equipment. Reliability analysis. Substantive provisions]. Derzhstandart Ukrayiny Publ., 1995. 35 p.

7. Avizienis, A., Laprie, J., Randell, B. and Landwehr, C. Basic concepts and taxonomy of dependable and secure computing. *IEEE Transactions on Dependable and Secure Computing*, 2004, vol. 1(1), pp. 11-33. doi: 10.1109/TDSC.2004.2.

8. Gorbenko, A., Kharchenko, V. and Romanovsky, A. On composing Dependable Web Services using undependable web components. *International Journal of Simulation and Process Modelling*, 2007, vol. 3(1/2), pp. 45-54. doi: 10.1504/IJSPM.2007.014714

9. Kharchenko, V., Sklyar, V. and Siora, A. Dependability of Safety-Critical Computer Systems through Component-Based Evolution. *2009 Fourth International Conference on Dependability of Computer Systems*, 2009, pp. 42-49. doi: 10.1109/DepCoS-RELCOMEX.2009.22.

10. Brezhnev, E., Kharchenko, V., Manulik, V. and Leontiev, K. Critical Energy Infrastructure Safety Assurance Strategies Considering Emergent Interaction Risk. *Advances in Dependability Engineering of Complex Systems*, 2017, pp. 67-78. doi: 10.1007/978-3-319-59415-6_7.

11. Von Neumann, J. Probabilistic logics and the synthesis of reliable organisms from unreliable components. *Avtomaty*, 1956, pp. 68-139.

12. Kharchenko, V. S. Harantozdatni systemy ta bahatoversiyni obchyslennya: aspekty evolyutsiyi [Dependable systems and multiversion computing: aspects of evolution]. *Radioelectronic and computer systems*. 2009, vol. 7, pp. 46-59.

13. Gorbenko, A., Kharchenko, V., Popov, P., Romanovsky, A. Dependable Composite Web Services with Components Upgraded Online. In: de Lemos, R., Gacek, C., Romanovsky, A. (eds). *Architecting Dependable Systems III. Lecture Notes in Computer Science*, 2005, vol. 3549, pp. 92–121. doi: 10.1007/11556169_5.

14. Illiashenko, O., Kharchenko, V., Kor, A., Panarin, A. and Sklyar, V. Hardware diversity and modified NUREG/CR-7007 based assessment of NPP I&C safety. *2017 9th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)*, 2017, pp. 907-911. doi: 10.1109/IDAACS.2017.8095218.

15. Brezhniev, Ye. Multilevel Fuzzy Logic-Based Approach for Critical Energy Infrastructure's Cyber Resilience Assessment. *10th International Conference on Dependable Systems, Services and Technologies (DESSERT)*, 2019, pp. 213-217, doi: 10.1109/DESSERT.2019.8770034.

16. Bulygina, O., Emel'yanov, A., Emel'yanova, N. and Kukushkin, A. *Sistemnyi analiz v upravlenii* [System analysis in management]. Moscow, FORUM: INFRA-M Publ., 2017. 450 p. doi: 10.12737/ textbook_5923d5ac7ec116.40684446.

17. Prokopenko, T. O. *Teoriya system i systemnyy analiz* [Systems theory and systems analysis]. Ministry of Education and Science of Ukraine, Cherkas. derzh. tekhnol. un-t Publ., 2019. 139 p.

18. Geida, A. and Lysenko, I. Operational Properties Of Agile Systems And Their Functioning Investigation Problems: Conceptual Aspects. *Applied Informatics*, vol. 5 (71), 2017, pp. 93-106.

19. Kharchenko, V., Dotsenko, S., Ponochovnyi, Yu., and Illiashenko, O. Cybernetic Approach to Developing Resilient Systems: Concept, Models and Application. *Information & Security: An International Journal* 2020, vol. 47, no. 1, pp. 77-90.

20. Menasche, D., Trivedi, K., and Altman, E. Rejuvenation and the Age of Information. *2019 IEEE In-*

ternational Symposium on Software Reliability Engineering Workshops (ISSREW), 2019, pp. 225-231. doi: 10.1109/ISSREW.2019.00076.

21. Bai, J., Chang, X., Machida, F., Trivedi, K. and Han, Z. Analyzing Software Rejuvenation Techniques in a Virtualized System: Service Provider and User Views. *IEEE Access*, vol. 8, 2020, pp. 6448-6459. doi: 10.1109/ACCESS.2019.2963397.

22. Grottke, M., Nikora, A. and Trivedi, K. An empirical investigation of fault types in space mission system software. *2010 IEEE/IFIP International Conference on Dependable Systems & Networks (DSN)*, 2010, pp. 447-456, doi: 10.1109/DSN.2010.5544284.

23. Randell, B. Occurrence Nets Then and Now: The Path to Structured Occurrence Nets. *Applications and Theory of Petri Nets*, 2011, pp. 1-16. doi: 10.1007/978-3-642-21834-7_1.

24. Abdulmunem, A. and Kharchenko, V. Availability and Security Assessment of Smart Building Automation Systems: Combining of Attack Tree Analysis and Markov Models. *2016 Third International Conference on Mathematics and Computers in Sciences and in Industry (MCSI)*, 2016, pp. 302-307, doi: 10.1109/MCSI.2016.062.

Надійшла до редакції 12.08.2020, розглянута на редколегії 15.09.2020

МЕТОДОЛОГИЯ ОБЕСПЕЧЕНИЯ ГАРАНТОСПОСОБНОСТИ ИНФОРМАЦИОННО-УПРАВЛЯЮЩИХ СИСТЕМ С ИСПОЛЬЗОВАНИЕМ МНОГОЦЕЛЕВЫХ СТРАТЕГИЙ ОБСЛУЖИВАНИЯ

Ю. Л. Поночовный, В. С. Харченко

В статье рассмотрена методология обеспечения гарантоспособности информационно-управляющих систем с использованием многоцелевых стратегий обслуживания. Актуальность исследований обусловлена необходимостью обеспечения функционирования гарантоспособных информационно-управляющих систем в условиях изменений требований, параметров среды и проявления неспецифицированных отказов их компонент. Методология представлена на системном уровне как сочетание концепции многоцелевого обслуживания, а также принципов: учета изменений в информационно-управляющей системе и среде в течение жизненного цикла; комплексного учета различных видов отказов и воздействий изменений; многоцелевого обслуживания; и объединяет комплекс новых моделей и методов определения параметров гарантоспособных информационно-управляющих систем и выбора параметров процедур их обслуживания. Предлагаемая концепция многоцелевого обслуживания получена путем развития парадигмы Фон-Неймана и формулируется как концепция построения надежных и безопасных систем из недостаточно гарантоспособных компонент и многоцелевого обслуживания по комбинированным стратегиям в условиях изменения требований и среды их функционирования. Сфера действия предлагаемой концепции имеет применение в случаях, когда принципы Фон-Неймана не позволяют строить гарантоспособные системы из-за ограничений экономического, временного характера или по другим причинам. В таком случае использование принципов, методов и моделей, являющихся концептуальными, распространяется на информационно-управляющие системы, построенные с использованием обслуживаемых компонентов и системных многоцелевых стратегий обслуживания. Предложенный принцип учета изменений предусматривает расширение классического контура управления отказоустойчивой системы, обеспечивающей реакцию на проявление дефектов в виде ошибок и отказов. Принцип комплексного учета различных видов отказов и воздействий изменений является продолжением принципов единства и связей во время процедур системного анализа. Он также является логическим продолжением фасетного упорядочения видов неисправностей и цепей причинно-следственных связей от неисправностей и дефектов до отказов, сбоев и ошибок. В рамках предложенной методологии разработаны стратегии многоцелевого обслуживания, множество вариантов целей, типов, процессов, свойств и параметров информационно-управляющих систем, что позволяет снизить модельную неопределенность и обосновать практические меры по обеспечению гарантоспособности на разных этапах жизненного цикла.

Ключевые слова: методология обеспечения гарантоспособности; многоцелевое обслуживание; информационно-управляющая система.

DEPENDABILITY ASSURANCE METHODOLOGY OF INFORMATION AND CONTROL SYSTEMS USING MULTIPURPOSE SERVICE STRATEGIES

Yu. Ponochovnyi, V. Kharchenko

The article considers the methodology of ensuring the dependability of information and control systems using multi-purpose maintenance strategies. The relevance of research is due to the need to ensure the functioning of dependable information and control systems in the face of changes in requirements, environmental parameters, and the manifestation of unspecified failures of their components. The methodology is presented at the system level as a combination of the concept of multi-purpose maintenance, as well as the principles of taking into account changes in the information and control system and environment during the life cycle; comprehensive consideration of different

ISSN 1814-4225 (print)
ISSN 2663-2012 (online)

types of failures, and the effects of change; multi-purpose maintenance and combines a set of new models and methods for determining the parameters of dependability information and control systems and the choice of parameters for their maintenance procedures. The proposed concept of multi-purpose maintenance is obtained by developing the Fon-Neumann paradigm and is formulated as a concept of building reliable and secure systems from insufficiently dependable components and multi-purpose maintenance on combined strategies in changing conditions and environment. The scope of the proposed concept is applicable in cases where the principles of von-Neumann do not allow building a viable system due to economic, temporal, or other reasons. In this case, the use of principles, methods, and models that are conceptual, extends to information and control systems built using maintained components and system multi-purpose service strategies. The proposed principle of taking into account changes involves the expansion of the classical control circuit of the fault-tolerant system, which response to the fault occurrence as errors and failures. The principle of comprehensive consideration of different types of failures and the effects of change is a continuation of the principles of unity and connection during the procedures of system analysis. It is also a logical continuation of the facet arrangement of fault types and chains of causal relationships from faults and defects to faults, failures, and errors. Within the framework of the proposed methodology, multi-purpose maintenance strategies, a set of options for goals, types, processes, properties, and parameters of information and control systems have been developed, which reduces model uncertainty and justifies practical measures to ensure dependability at different stages of the life cycle.

Keywords: dependability assurance methodology; multi-purpose maintenance; information and control systems.

Поночовний Юрій Леонідович – канд. техн. наук, старш. наук. співроб., доцент кафедри інформаційних систем та технологій, Полтавської державної аграрної академії, Полтава, Україна; докторант кафедри комп'ютерних систем, мереж та кібербезпеки Національного аерокосмічного університету ім. М. Є. Жуковського «Харківський авіаційний інститут», Харків, Україна

Харченко Вячеслав Сергійович – Лауреат Державної премії України, заслужений винахідник України, д-р техн. наук, професор, завідувач кафедри комп'ютерних систем, мереж та кібербезпеки Національного аерокосмічного університету ім. М.Є. Жуковського «Харківський авіаційний інститут», Харків, Україна.

Yuriy Ponochovnyi - Ph.D., Senior researcher, Associate Professor of the Department of Information Systems and Technologies, Poltava State Agrarian Academy, Poltava, Ukraine; DrS student of the Department of Computer systems, networks and cybersecurity, National Aerospace University "Kharkiv aviation institute", Kharkiv, Ukraine, e-mail: yuriy.ponch@gmail.com,
ORCID Author ID: 0000-0002-6856-2013, Scopus Author ID: 56446990700, ResearcherID: J-5732-2017
https://scholar.google.com.ua/citations?user= A4nhkGoAAAAJ

Vyacheslav Kharchenko – Honored inventor of Ukraine, Doctor of Science on Engineering, Professor, Head of the Department of Computer systems, networks and cybersecurity, National Aerospace University "Kharkiv aviation institute", Kharkiv, Ukraine, e-mail: V.Kharchenko@csn.khai.edu.
ORCID Author ID: 0000-0001-5352-077X, Scopus Author ID: 22034616000, ResearcherID: A-7719-2017