УДК 004.052.3:004.94 DOI https://doi.org/10.35546/kntu2078-4481.2025.3.2.61

Д. Є. ФРОЛОВ
аспірант, асистент кафедри електронних обчислювальних машин
Харківський національний університет радіоелектроніки
ORCID: 0009-0009-3291-3561

МОДЕЛЬ ЗАБЕЗПЕЧЕННЯ ВІДМОВОСТІЙКОСТІ ІНФОРМАЦІЙНИХ СИСТЕМ НА ОСНОВІ БАГАТОРІВНЕВИХ СТРУКТУР

У статті сформульовано задачу забезпечення відмовостійкості сучасних динамічних інформаційних систем на основі багаторівневих структур, як важливу умову її стабільного функціонування. Обґрунтовано необхідність багаторівневого підходу, оскільки класичні методи резервування та дублювання не забезпечують комплексної стійкості, особливо у випадках міжрівневих взаємодій. В якості розв'язання поставленої задачі запропоновано використовувати інтегративний підхід в частині подання рівнів інформаційної системи (фізичний, мережний, прикладний, організаційний та рівень віртуалізації), її функціоналів разом із процесною інтерпретацією, що їх супроводжують у разі виникнення відмов та відновлень. У якості описового апарату використано логіку Хоара, яка оперує з кортежним представленням, власне, запропонованої моделі. Базовий кортеж включає залежності та умови, зокрема, дефіцит ресурсів інформаційної системи на підтримку задовільного рівня виконання процесів, впливів міжрівневих взаємозв'язків. Працездатність окремих елементів інформаційної системи, узгодженості процесів між елементами, у тому числі на міжрівневих площинах, на прикладі моделі, може бути оцінена на підставі критеріального аналізу, що використовує показники доступності, відмовостійкості, ізоляції та ресурсно-вартісні характеристики інформаційної системи. Проведено експериментальні дослідження запропонованої моделі. Зокрема, досліджено встановлення відповідності структурним припущенням і процесному опису властивостей реальних систем запропонованій моделі. Також досліджено коректність прогнозів щодо збереження працездатності критичних функціоналів системи за стохастичних відмов і керованих політик відновлення. Дослідження проведені на базі обчислювальних потужностей інформаційно-обчислювального центру Харківського національного університету радіоелектроніки. Результати досліджень наведені у статті та є задовільними – модель є адекватною.

Ключові слова: *інформаційна система, модель, відмовостійкість, багаторівневість, логіка Хоара, математичне моделювання.*

D. YE. FROLOV
Postgraduate Student, Assistant at the Department of Electronic Computers
Kharkiv National University of Radio Electronics
ORCID: 0009-0009-3291-3561

MODEL FOR ENSURING FAULT TOLERANCE OF INFORMATION SYSTEMS BASED ON MULTI-LEVEL STRUCTURES

The article formulates the problem of ensuring fault tolerance in modern dynamic information systems based on multilevel structures as an important condition for their stable functioning. The necessity of a multilevel approach is substantiated, since classical methods of reservation and duplication do not provide comprehensive resilience, especially in cases of interlevel interactions. To solve this problem, an integrative approach is proposed that encompasses the representation of the levels of an information system (physical, network, application, organizational, and virtualization), its functionalities, and the process interpretation that accompanies them in the event of failures and recoveries. Hoare logic, operating with a tuple-based representation of the proposed model, serves as the descriptive apparatus. The basic tuple incorporates dependencies and conditions, including resource shortages within the information system that hinder the maintenance of an acceptable level of process execution and the influence of interlevel interactions. The operability of individual components of the information system and the consistency of processes across elements, including across interlevel planes, can be evaluated within the model using a criteria analysis based on indicators of availability, fault tolerance, isolation, and the resource-cost characteristics of the system. The paper presents experimental studies of the proposed model. In particular, the research examined the correspondence between the structural assumptions and the process description of real system properties and the proposed model. This study examined the validity of the model's predictions concerning the preservation of critical system functionalities under stochastic failures and controlled recovery policies. The research used the computing resources of the Information and Computing Center of Kharkiv National University of Radio Electronics. The results, presented in the article, demonstrate satisfactory outcomes, confirming the adequacy of the model.

Key words: *information system, model, fault tolerance, multilevel structure, Hoare logic, mathematical modeling.*

Постановка проблеми

Відмовостійкість інформаційної системи є базовою характеристикою її надійності, що визначає здатність системи підтримувати працездатність за наявності відмов окремих компонентів [1–5]. В умовах сьогодення цільові завдання інформаційних систем виходять за межі традиційних ІТ-сервісів і дедалі частіше набувають синергетичного характеру, формуючи основу безперервності бізнес-процесів і забезпечуючи керування критично важливими технологічними процесами у сферах оборони та безпеки [6–8].

Останнім часом теорія побудови сучасних інформаційних системи все більше ґрунтується на розгляді інформаційної системи як певної багаторівневої сутності, яка органічно враховує процесність від рівня апаратно-мережного шару до прикладних сервісів [9]. Прикладні аспекти застосовності таких інформаційних систем на основі багаторівневих структур враховують умови їх функціонування як то: стохастичні відмови елементів системи, приховані дефекти, мережні аномалії тощо [10–12]. За зазначених умов поняття відмовостійкості та апарат, який за ним стоїть, відносно інформаційних систем на основі багаторівневих структур – є основною складовою комплексної надійності інформаційної системи [13].

Класичні прикладні рішення задачі забезпечення відмовостійкості інформаційних систем (резервування, протоколи узгодження, самовідновлювальні механізми) – ефективні у межах окремих інформаційних систем або її елементів, однак їх композиційне поєднання відносно багаторівневої інформаційної системи породжує непередбачувані ефекти, які складно прогнозувати, а час на їх усунення може вплинути на роботоздатність всієї системи. До таких ефектів можуть відноситися, наприклад, каскадні відмови, розрив зв'язків між рівнями тощо [14].

Таким чином, класичні підходи дозволяють здійснювати: агрегацію показників доступності в межах одного рівня багаторівневої інформаційної системи для прийняття системою рішень щодо подальшого сценарію функціонування або задавати множини рішень для керуючого впливу на окремі механізми узгодження й реплікації у міжрівневій архітектукрі інформаційної системи, залишаючи, власне міжрівневі залежності поза уваги. Це створює передумови до необхідності розробки моделі, яка б одночасно враховувала ієрархію рівнів та зв'язки між ними в інформаційній системі, дозволяла здійснювати композиційне оцінювання показника відмовостійкості та містила інтерфейс для застосування темпорального критерію оптимальності конфігурацій у певних проміжках її застосовності при стабільних показниках зовнішнього впливу.

Методологічна проблема полягає у наявних міжрівневих розривах інформаційної системи на основі багаторівневих структур: навіть за умови забезпечення відмовостійкості на окремих рівнях, зберігається вразливість на вузлах взаємодії між ними. Взаємозалежності різних рівнів нерідко залишаються поза єдиною узгодженою політикою, що призводить до несумісності прикладних підходів підвищення відмовостійкості інформаційних систем. Як наслідок, локально коректні рішення не узгоджуються композиційно в системну відмовостійкість інформаційної системи, а міжрівневі ефекти здатні зводити нанівець переваги захисних механізмів усередині окремих рівнів. Все це є однією із причин розробки моделі відмовостійкості інформаційної системи на основі багаторівневих структур.

Для формулювання задачі дослідження, розглянемо інформаційну систему на основі багаторівневих структур у вигляді наступного кортежу:

$$S = \left\langle L, \rho, \{\Sigma_i\}_{i\in L}, \{E_i\}_{i\in L}, \Upsilon \right\rangle, \tag{1}$$

де $L = \{0, \ldots, k\}$ – множина рівнів; ρ – відношення впорядкування рівнів в інформаційній системі ($\rho \subseteq L_k \times L_{k+1}$, $0 \le k \le n$, $n = 1, 2, 3, \ldots$); Σ_i – простір станів рівня i; E_i – множина елементарних подій; Υ – інтерфейси міжрівневого впливу.

Додатково необхідно ввести такі сутності, що уточнюють траєкторію функціонування багаторівневої структури:

– F – множина функціоналів, що реалізується на базі структури S. Кожна функція $f \in F$ реалізується на основі станів та подій одного чи кількох рівнів інформаційної системи на основі багаторівневих структур:

$$f : \left(\Sigma_{i1} \times \ldots \times \Sigma_{im}\right) \to \Sigma_j, \quad i_1, \ldots, i_m,\ j \in L, \tag{2}$$

тобто функціонал спирається на підмножину рівнів і чинить вплив на результат роботи інформаційної системи на іншому рівні;

– F_{crit} – множина критичних функціоналів ($F_{crit} \in F$), яка включає критичні функції, для яких необхідно гарантувати відмовостійкість навіть за умов часткових відмов елементів інформаційної системи на основі багаторівневих структур;

– $G = (F, \Xi)$ – граф залежностей функціоналів, в якому дуги $(f_p, f_q) \in \Xi$ встановлюють залежність функціоналу f_p від роботоздатності f_q. Такий граф може формалізувати залежності між функціоналами рівнів;

– $\varphi_f(t) \in \{0, 1\}$ – функція доступності функціоналу f, яка визначає стан доступності в момент часу t для функціоналів з множин F та F_{crit};

– $R_f(T)$ – функція надійності, яка відображає імовірність безвідмовної роботи інформаційної системи на основі багаторівневих структур на інтервалі часу $[0, T]$;

– ζ – конфігураційна сутність, яка визначається параметрами інформаційної системи в залежності від особливостей її функціонального призначення;

– $N(\zeta)$ – ресурсно-вартісна функція, яка характеризує витрати на підтримку конкретної конфігурації ζ інформаційної системи на основі багаторівневих структур;

– $X_h(\zeta)$ – показники якості виконання основної функції інформаційної системи, зокрема $h = \{D_F(\zeta), W_F(\zeta), V_F(\zeta)\}$, де ($D_F(\zeta)$ – затримка виконання функції, $W_F(\zeta)$ – пропускна здатність під час міжрівневої взаємодії функціоналів, $V_F(\zeta)$ – узгодженість у досяжності спільної функції);

Виходячи з вищенаведеного, задача забезпечення відмовостійкості інформаційної системи на основі багаторівневих структур може бути сформульована як синтез конфігурацій ζ, що враховує систему обмежень для конфігурацій інформаційної системи на основі багаторівневих структур може бути записана у вигляді:

$$\Omega = \begin{cases} \forall f \in F_{crit} \forall t \in [0,T]: \ \varphi_f(t) = 1; \\ \zeta \ \textit{узгоджена з} \ \left(L, \rho, \{\Sigma_i\}_{i\in L}, \{E_i\}_{i\in L}, \Upsilon\right); \\ \forall f \in F_{crit}: \mathrm{X}_h(\zeta) \geq X_h^{\min}(\zeta); \\ \min\limits_{\zeta} \mathrm{X}_h(\zeta) \ \textit{при фіксованих} \ R_f(T), \end{cases} \tag{3}$$

де: $X_h^{\min}(\zeta)$ – мінімально необхідні умови забезпечення якості виконання функціоналів *h*.

Аналіз останніх досліджень і публікацій

У праці [15] запропоновано модульний підхід до моделювання систем на основі багатоорендних сервісів із використанням багаторівневих мереж Петрі (*n*-NLS). Автори фокусуються на формалізації компонентів і рівнів системи, визначенні правил синхронізації та координації між ними, а також на забезпеченні диференціації продуктивності для орендарів відповідно до угод про рівень обслуговування та планів варіативності. Такий процесний формалізм зменшує неоднозначності в описі поведінки та підвищує керованість багатоорендного середовища. Водночас, робота не декларує синтезу конфігурацій з урахуванням обмежень надійності й якості.

У праці [16] представлено техніку PreLoFT, зокрема прогнозний розподіл навантаження між fog-вузлами з розщепленням ресурсоємних задач і оперативним перерозподілом у разі відмов. Підхід зосереджено на внутрішньому рівні fog без явної підтримки багаторівневості; не показано, як PreLoFT узгоджується з глобальними обмеженнями якості та ресурсно-вартісними вимогами системи. Тому робота [16] має науковий інтерес у контексті цієї роботи як приклад формулювання локальної евристики керування на рівні fog при розробці багаторівневої моделі відмовостійкості з формальними гарантіями.

У роботі [17] автори розглянули напрям багаторівневої відмовостійкості в IoT-системах на прикладі власної програмної розробки FaTEMa. Він базується на подієво-орієнтованій архітектурі та забезпечує обмін інформацією між шарами системи з метою прискорення виявлення і відновлення після збоїв, що дозволило покращити показники надійності й доступності. Втім, відсутність узагальненої моделі обмежує масштабованість їхнього підходу.

Розглянуті [15–17] праці репрезентують комплементарні підходи, але спільним є відсутність єдиної багаторівневої формальної структури з явно визначеними інтерфейсами та композиційними властивостями та формальної постановки синтезу конфігурацій під жорсткі обмеження доступності/надійності і показників якості. Отже, можна зазначити, що наразі відсутній композиційний апарат для інформаційних систем на основі багаторівневих структур, у якому локальні механізми відмовостійкості інтерпретуються як морфізми між рівнями з гарантованим забезпеченням відмовостійкості і можливістю верифікованого синтезу конфігурацій під задані обмеження. Саме це обґрунтовує актуальність роботи статті, яка присвячена побудові формальної багаторівневої моделі відмовостійкості з явними інтерфейсами та системою обмежень на рівні всієї інформаційної системи, а не лише окремих її рівнів чи методів їх взаємодії.

Формулювання мети дослідження

Метою дослідження є розробка моделі забезпечення відмовостійкості інформаційних систем на основі багаторівневих структур, яка враховує підпорядкованість (вкладеність) рівнів та функціонали на них, забезпечує композиційну верифікацію доступності, відмовостійкості та ізоляції за умов стохастичних відмов в інформаційній системі і керованих політик відновлення її функціональності, а також створює підґрунтя для оптимізації існуючих конфігурацій з урахуванням ресурсної вартості резервування елементів інформаційної системи.

Викладення основного матеріалу дослідження

Процесна формалізація моделі інформаційної системи на основі багаторівневих структур з використанням логіки Хоара. Застосування логіки Хоара обґрунтовано тим, що вона є одним із базових формалізмів опису та верифікації процесних систем, що дозволяє задавати коректність виконання дій у вигляді певного математичного апарату [18].

Для інформаційних систем на основі багаторівневих структур, у яких відмови та відновлення описуються як події, а взаємодія між рівнями має стохастичний і керований характер, логіка Хоара надає можливість задати

процесність моделі, зокрема відобразити, за яких умов виконання певної події чи переходу застосовується вибір режиму доступності або відмовостійкості. Таким чином, логіка Хоара виступає методологічним підґрунтям для композиційної перевірки властивостей у багаторівневій структурі, так як кожна локальна подія може бути формально описана через свої передумови та післяумови, а їхня композиція забезпечує цілісну верифікацію траєкторії функціонування інформаційної системи на основі багаторівневих структур при стохастичних відмовах і процесам по відновленню функціональної здатності.

Отже, беручи за основу кортеж (1), вихідний вигляд моделі інформаційної системи на основі багаторівневих структур можна записати як:

$$S = \left\langle L, \rho, \{\Sigma_i\}_{i\in L}, \{E_i\}_{i\in L}, \Upsilon, F, F_{crit}, G, \varphi_f(t), R_f(T), \zeta, C(\zeta), X_h(\zeta) \right\rangle, \tag{4}$$

при умовах, викладених у формулі (3).

Для процесного опису функціонування інформаційної системи введемо сутність події як $e \in E_i$, яка відображає процес відмови чи відновлення функціонування рівня чи всієї інформаційної системи (приналежно до індексу). В такому разі, маємо:

– у якості передумови P визначає поточний стан системи (наприклад, множину доступних функціоналів, дотримання обмежень Ω);

– команда Uвідповідає за такі події в системі як відмови чи відновлення;

– післяумова Q фіксує новий стан, у якому має виконуватися із забезпечення відмовостійкості (наприклад, доступність усіх $f \in F_{crit}$).

Звідси отримуємо:

$$\{P\}e\{Q\},\ e \in E_i, \tag{5}$$

де: $P : \Omega \wedge \bigwedge\limits_{f\in F_{crit}} \varphi_f(t) = 1;\ \ Q : \Omega \wedge \bigwedge\limits_{f\in F_{crit}} \varphi_f(t') = 1.$

Відповідно, у разі відмови, маємо:

$$\left\{\varphi_f(t) = 1, \forall f \in F_{crit}\right\}\ \ fail(i)\left\{\exists \zeta' \in Z : \varphi_f(t+\Delta) = 1,\ \forall f \in F_{crit}\right\}. \tag{6}$$

Це показує про досяжність і можливість використання такої конфігурації ζ', яка збереже роботу критичних функціоналів навіть при відмові рівня з точки зору розладу роботи його елементів.

А у разі відновлення роботи критичних елементів рівня i:

$$\left\{\neg\varphi_{f''}(t)\right\}\ \ rec(i)\left\{\exists\varphi_{f''}(t+\Delta) = 1\right\},\ \ f'' \in F_{crit}. \tag{7}$$

Це показує те, що після відновлення рівня, критичний функціонал знову стає доступним.

Нарешті, композиція подій матиме вигляд:

$$\{P\}U_1 : U_2\{Q\},\ \text{якщо}\ \{P\}U_1\{R\},\quad \{R\}U_2\{Q\}. \tag{8}$$

Отже, маємо апарат, який дозволяє описати траєкторію відмови та відновлення в межах кількох рівнів і довести, що система виконує Ω.

Апарат, який описує міжрівневі процеси, аналогічно (6)–(8), виходячи з того, що $(i, j) \in L$, де $i \prec j$ у межах відношення (4) ρ, а подія на рівні i може змінювати доступність функціоналів на рівні j, то:

$$\{P_i \wedge P_j\}U_{i\to j}\{Q_i \wedge Q_j\}, \tag{9}$$

де P_i – умови стану рівня i перед подією; P_j – умови стану рівня j, що залежать від i; $U_{i\to j}$ – подія міжрівневого впливу; Q_i, Q_j – післяумови для обох рівнів.

Якщо критичний функціонал рівня i недоступний, то після поширення відмови втрачається працездатність пов'язаного функціоналу на рівні j. Відповідно, міжрівнева відмова має вид:

$$\left\{\varphi_{f_i}(t) = 0 \wedge \varphi_{f_j}(t) = 1\right\}\ \ levelfail(i \to j)\left\{\varphi_{f_j}(t+\Delta) = 0\right\}, \tag{10}$$

де $f_i \in F_{crit}(i), f_j \in F_{crit}(j)$.

Якщо рівень i відновлено, то функціонал на рівні j, залежний від i, також відновлюється. Відповідно, міжрівневе відновлення має вид:

$$\left\{\varphi_{f_i}(t) = 1 \wedge \varphi_{f_j}(t) = 0\right\}\ \ levelrec(i \to j)\left\{\varphi_{f_j}(t+\Delta) = 1\right\}. \tag{11}$$

Якщо рівень i забезпечує мінімально необхідні умови якості, то після виконання переходу гарантовано, що рівень j також залишається у допустимій області QoS:

$$\left\{X_i(\zeta) \geq X_i^{\min}\right\}\ ensure(i \to j)\left\{X_j(\zeta) \geq X_j^{\min}\right\}. \tag{12}$$

У такий спосіб можна для кожної залежності $(i, j) \in \rho$ формально задати передумови й післяумови, які здійснюють контроль поширення подій відмов / відновлень та узгодженість рівнів у багаторівневій структурі.

Таким чином, введення передумов і післяумов для міжрівневих переходів дає змогу фіксувати та описувати локальні події на окремих рівнях, відслідковувати динаміку впливу у межах усієї інформаційної системи на основі багаторівневих структур. Тобто, події відмов і відновлень задаються як процеси з наслідками у часі – стан на рівні *i* стає передумовою, а стан на рівні *j*, пов'язаний через ρ та ϒ – післяумовою. Завдяки цьому можна композиційно описати траєкторії за напрямом «відмова – поширення – відновлення». Це означає, що за будь-якої послідовності подій зберігаються умови доступності критичних функціоналів за умови виконання обмежень (3). Застосування логіки Хоара дозволило формалізувати динамічність поведінки інформаційної системи на основі багаторівневих структур, зокрема, розвиток подій у часі, їхній вплив між рівнями та можливість верифікації відмовостійкості через послідовності процесів.

Модель забезпечення відмовостійкості інформаційних систем на основі багаторівневих структур. Наступним кроком є побудова саме моделі забезпечення відмовостійкості, яка інтегрує структурний і процесний рівні, формалізує умови збереження працездатності критичних функціоналів та вводить засоби оцінки й оптимізації конфігурацій.

Модель забезпечення відмовостійкості інформаційної системи на основі багаторівневих структур можна представити у вигляді кортежу:

$$\Psi = \langle S, \Pi, O, \Xi \rangle, \tag{13}$$

де: S – структурно-процесна модель інформаційної системи, визначена раніше у (4). Вона є базовим елеентом моделі забезпечення відмовостійкості інформаційної системи на основі багаторівневих структур та використовується для складання опису середовища, в якому реалізується забезпечення відмовостійкості; П – множина політик відновлення, які визначають допустимі дії у відповідь на відмови. До таких дій відносяться, але не вичерпуються визначеним пулом дій – дублювання / реплікація, резервування на рівнях, міграція функціоналів, перезапуск функціоналів, використання альтернативних функціоналів. Кожну політику можна інтерпретувати як перетворення над S, що забезпечує збереження функціональної здатності інформаційної системи; О – множина варіативних траєкторій функціонування інформаційної системи. Ця множина описує пул сценаріїв реагування на події відмов і відновлень, сформованих на підставі застосуванням політик П. Таким чином, О є простором можливих процесних сценаріїв, які гарантують відновлення критичних функціоналів; Ξ – множина критеріїв забезпечення, яка включає: доступність критичних функціоналів у часі, відмовостійкість як здатність зберігати працездатність за множини відмов, ізоляцію збоїв (обмеження поширення каскадних відмов у та між рівнями), ресурсно-вартісні характеристики та якісні показники визначені експертом (за наявності такого функціоналу).

Функціонально модель має можливість композиційної верифікації. Відповідно, замість перевірки всієї інформаційної системи як цілісного утворення, доцільно виконувати локальну верифікацію подій і політик на рівнях, а потім за формальними правилами композиції робити висновок про відмовостійкість інформаційної системи в цілому.

У більшості відомих підходів верифікація відмовостійкості зводиться до статичних обчислень показників надійності [19], або до імітаційного моделювання [20]. Відмінність підходу, який пропонується у даній роботі, полягає в інтеграції логіки Хоара у багаторівневу модель, коли для кожної події $e \in E_i$ задається локальна «трійка» $\{P\}e\{Q\}$, для кожної політики – також локальна «трійка», а для траєкторії подій і політик – композиційно виводиться глобальна трійка. Таким чином, властивості доступності, відмовостійкості та ізоляції перевіряються індуктивно по траєкторії, а не за принципом «усе або нічого».

Так як у інформаційних системах на основі багаторівневих структур відмовостійкість ґрунтується на множині альтернативних сценаріїв функціонування, які охоплюють усі можливі послідовності подій і політик відновлення, оскільки відмови носять стохастичний характер і можуть поєднуватися різними способами, то доцільно розглянути механізм введення варіативів для гарантування роботи критичних функціоналів. Тоді, нехай множина варіативів буде задана як

$$\Gamma = \{\xi_1, \xi_2, \ldots, \xi_k\}, \tag{14}$$

де кожна траєкторія ξ задається послідовністю подій відмов і застосованих політик:

$$\xi = e_1; \vartheta_1; e_1; \vartheta_1; \ldots, e_m; \vartheta_m, \tag{15}$$

де $e_m \in E_i$ – подія відмови чи відновлення на рівні i; $\vartheta_m \in \Pi$ – політика реагування.

Таким чином, вимога гарантування критичних функціоналів формулюється як:

$$\forall f \in F_{crit} : \exists \xi \in \Gamma : \{P\}\xi\{\varphi_f(t_{fin}) = 1\}. \tag{16}$$

На відміну від відомих підходів, у яких варіативність найчастіше розглядається на рівні архітектурних конфігурацій (резервування чи реплікація), у запропонованій моделі вперше: варіативи інтегруються з логікою Хоара, що

дозволяє доводити коректність кожного альтернативного сценарію як послідовності подій; кожна множина Γ не є довільною, а формується через правила композиції локальних «трійок», що гарантує верифікацію всіх сценаріїв.

Виходячи з загальноприйнятої теорії, що забезпечення відмовостійкості інформаційної системи супроводжується додатковими витратами (дублювання ресурсів, резервування каналів, підтримка надмірних компонентів) [2], поряд із формальною верифікацією роботоздатності критичних функціоналів необхідно мати апарат оптимізації конфігурацій, що дозволяє знаходити баланс між рівнем відмовостійкості та ресурсно-вартісними обмеженнями.

Задача оптимізації може бути представлена як:

$$\min_{\zeta,\vartheta,\xi} C(\zeta,\vartheta,\xi), \tag{17}$$

за умов:

$$\mathrm{I}=\begin{cases}\Omega(\zeta)=1;\\ \forall f\in F_{crit}:\exists\xi\in\Gamma:\{P\}\,\xi\{\varphi_f=1\};\\ X(\zeta)\geq X^{\min}.\end{cases} \tag{18}$$

Новизна зазначеного підходу полягає в тому, що оптимізація здійснюється за трикутником «структура – процес – політика», тому, відповідно, оптимізаційна задача для запропонованої моделі формулюється як спільний вибір конфігурації, політики і сценарію, що мінімізує витрати, одночасно гарантуючи збереження критичних функціоналів інформаційної системи на основі багаторівневої структури.

Інтеграція запропонованих моделей полягає у побудові єдиної конструкції, де структурна модель (4), процесна інтерпретація подій (5)–(12) та модель забезпечення (13)–(17) функціонують як взаємопов'язані складові однієї сутності. Структурний рівень визначає ієрархію L, зв'язки ρ, інтерфейси ϒ, множини функціоналів F і F_{crit} та обмеження (3), які задають допустимі конфігурації. Процесна складова, що базується на логіці Хоара, задає правила перетворення станів системи під дією подій E_i, формалізуючи послідовності «відмова – поширення – відновлення» у вигляді композицій «трійок». Модель забезпечення відмовостійкості (13) доповнює цю основу множиною політик П, варіативними сценаріями О та критеріями Ξ, що забезпечують збереження працездатності критичних функціоналів і враховують ресурсно-вартісні характеристики. У такій інтеграції структурний рівень фіксує межі простору рішень, процесний рівень описує динаміку переходів між станами, а П, О, Ξ реалізують механізм забезпечення з можливістю порівняння й відбору альтернативних конфігурацій. Схематично цей підхід може бути поданий як багатошаровий конвеєр «структура → події → сценарії → критерії», у якому й реалізується модель забезпечення відмовостійкості для інформаційних систем на основі багаторівневих структур.

Дослідження моделі забезпечення відмовостійкості інформаційних систем на основі багаторівневих структур за критерієм адекватності. Дослідження проводилося на відповідність моделі структурним припущенням і процесного опису фактичним властивостям інформаційних систем на основі багаторівневих структур та коректність прогнозів щодо збереження працездатності критичних функціоналів за стохастичних відмов і керованих політик відновлення у трьох взаємопов'язаних вимірах: структурному (відповідність ієрархії рівнів, зв'язків та інтерфейсів реальній архітектурі), процесному (відповідність опису подій відмов/відновлень спостережуваній динаміці) та прогностичному (узгодженість очікуваних показників доступності, якості та вартості з емпірично досяжними). У якості інформаційної системи було обрано відому інформаційну систему багатошарової віртуалізації [21], яка була розгорнута на базі інформаційно-обчислювального центру Харківського національного університету радіоелектроніки [22].

За результатами досліджень отримано наступні результати:

1. Для обраної інформаційної системи [21] зафіксовано відображення реальних рівнів, зв'язків та інтерфейсів на елементи S; виконано перевірку, що допустимі конфігурації ξ не виходять за межі обмежень Ω і відтворюють фактичні політики резервування та розміщення функціоналів.

2. Логи експлуатації відображаються на послідовності подій і політик; для кожної спостереженої траєкторії ξ ∈ О було перевірено «трійки» виду $(P)\xi(Q)$, де P, Q були сформовані за наявних умов Ω та вимог $\varphi_f(t) = 1$ для всіх $f \in F_{crit}$. Отримана узгодженість таких трійок із даними свідчить про правильність процесного опису.

3. Для репрезентативних конфігурацій ζ та політик П були порівняні отримані в моделі (4) значення $C(\zeta)$, $X_h(\zeta)$ з виміряними значеннями; додатково виконано звірку частки часу з $\varphi_f(t) = 1$ із фактичною доступністю критичних функціоналів. Прийнятні розбіжності були в межах допустимих значень, визначених інформаційною системою [21].

4. Досліджено варіювання параметрів у межах експлуатаційної невизначеності (навантаження, інтенсивності відмов, тривалості відновлень) та проаналізовано стабільність рішення задачі збереження виконання Ω і незначної зміни оптимальних ζ при малих варіаціях вхідних даних.

5. Для множини О було проведено ранжування сценаріїв за критеріями Ξ і перевірено, що сценарії, визнані кращими у моделі, що було підтверджено експериментально (табл. 1).

6. Вимикаючи окремі політики з П та повторюючи дослідження у п. 2 та п. 5, демонструється причинний внесок кожної політики у виконання вимог до відмовостійкості.

Таблиця 1

Результати перевірки адекватності моделі для системи вкладеної віртуалізації

№ перевірки	Рівні вкладеності	Схема резервування	Політика відновлення	Сценарій	Кількість відмов	Прогнозована доступність критичних функціоналів	Спостережна доступність критичних функціоналів	Відхилення прогнозу від експерименту	Прогнозований середній час відновлення, с	Виміряний середній час відновлення, с	Відхилення прогнозу від експерименту, с	Частка часу, коли інформаційна система виконує основну функцію, %	Чи задовольняє система обмеження Ω
1	2	Гарячий резерв @L2	Перезапуск + реплікація	ξ_1	50	99.90	99.86	–0.04	18.0	19.4	1.4	98.7	Так
2	2	Холодний резерв @L2	Міграція	ξ_2	50	99.40	99.31	–0.09	75.0	79.2	4.2	96.1	Так
3	3	Гарячий резерв @L2,L3	Перезапуск+міграція	ξ_3	80	99.95	99.93	–0.02	12.0	12.8	0.8	99.0	Так
4	3	Без резерву@L3	Локальний відкат	ξ_4	80	98.80	98.55	–0.25	140.0	152.5	12.5	90.4	Ні
5	4	Змішаний: гарячий@L3, холодний@L2	Реплікація + checkpoint	ξ_5	120	99.74	99.70	–0.04	28.0	29.6	1.6	97.8	Так
6	4	Гарячий резерв на всіх рівнях	Актив-актив	ξ_6	120	99.997	99.992	–0.005	6.0	6.7	0.7	99.4	Так
7	2	Без резерву	Лише перезапуск	ξ_7	50	97.90	97.43	–0.47	210.0	228.3	18.3	84.2	Ні
8	3	Гібридний: гарячий@L2, холодний@L3	Гібридна міграція	ξ_8	80	99.60	99.55	–0.05	36.0	37.9	1.9	96.9	Так

За результатами досліджень видно (рис. 1), що модель коректно відтворює архітектуру й динаміку інформаційної системи [21], забезпечує достовірні оцінки $N(\zeta)$, $X_h(\zeta)$ для всіх $f \in F_{crit}$ і може слугувати надійною основою для синтезу конфігурацій у інших реальних умовах експлуатації.

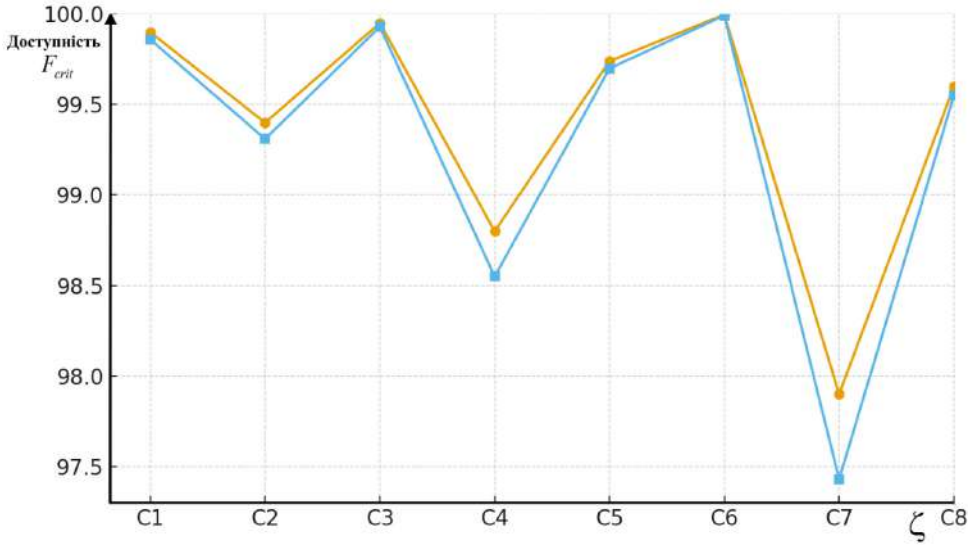

Рис. 1. Графік порівняння прогнозованої та спостереженої доступності $f \in F_{crit}$ для різних конфігурацій ζ

Висновки

У роботі запропоновано новий підхід до побудови моделі забезпечення відмовостійкості інформаційних систем на основі багаторівневих структур.

Вперше запропоновано математичну модель забезпечення відмовостійкості інформаційних систем на основі багаторівневих структур, яка інтегрує структурне подання рівнів і функціоналів із процесною інтерпретацією відмов та відновлень у логіці Хоара, що дозволяє композиційно верифікувати доступність, відмовостійкість та ізоляцію критичних функціоналів. Додатково введено множину політик відновлення, множину варіативів як формалізованих траєкторій функціонування, а також критерії оцінки, що охоплюють показники доступності, відмовостійкості, ізоляції та ресурсно-вартісні характеристики. Це дозволяє не лише перевіряти працездатність критичних функціоналів, а й здійснювати синтез оптимальних конфігурацій з урахуванням вартості резервування.

Подальші дослідження будуть спрямовані на удосконалення моделі шляхом розробки функціоналу автоматизованої генерації варіативів і побудови методів синтезу конфігурацій у реальному часі, на розширення моделі до багатокритеріальної оптимізації з урахуванням ризиків і часу відновлення.

Список використаної літератури

1. Додонов О. Г., Кузнєцова М. Г., Горбачик О. С. Моделювання і оцінювання функціональної стійкості інформаційних систем. Реєстрація, зберігання і обробка даних. 2025. Т. 27, № 1. С. 76–88.

2. Лейченко К. М., Скоробогатько С. В., Фесенко Г. В., Харченко В. С., Яковлев С. В. Оцінювання надійності бездротових сенсорних мереж систем моніторингу лісових пожеж з урахуванням фатальних комбінацій множинних відмов сенсорів. Кібернетика та системний аналіз. 2025. Т. 61, № 1. С. 161–173. URL: http://jnas.nbuv.gov.ua/article/UJRN-0001535211 (дата звернення: 19.09.2025).

3. Tkachov, V., Kovalenko, A., Kharchenko, V., Hvozdetska, K., Hunko, M. An Overlay Network Based on Cellular Technologies for the Secure Control of Intelligent Mobile Objects. ICTERI 2021 Workshops. Communications in Computer and Information Science. Cham 2022. P. 480–490. URL: https://doi.org/10.1007/978-3-031-14841-5_32 (дата звернення: 19.09.2025).

4. Додонов О. Г., Путятін В. Г., Додонов В. О., Куценко С. А., Германюк А. П., Ізварін І. В., Кравчук К. О. Технологія забезпечення живучості територіально-розподілених інформаційних комп'ютерних систем в єдиному інформаційному просторі. Реєстрація, зберігання і обробка даних. 2024. Т. 26, № 1. С. 121–143. URL: https://doi.org/10.35681/1560-9189.2024.26.1.308659 (дата звернення: 19.09.2025).

5. Моделювання та оптимізація процесів безпечної та відмовостійкої маршрутизації в телекомунікаційних мережах : монографія / О. В. Лемешко, О. С. Єременко, М. О. Євдокименко, А. С. Шаповалова, Б. Слейман. Харків : ХНУРЕ, 2022. 198 с. URL: https://doi.org/10.30837/978-966-659-378-1 (дата звернення: 19.09.2025).

6. Кірпічніков Ю., Рибидайло А., Литовченко Г., Бутенко М. Обґрунтування підходу до удосконалення інформаційної інфраструктури Міністерства оборони України для функціонування в умовах збройної агресії. Збірник наукових праць Центру воєнно-стратегічних досліджень НУОУ імені Івана Черняховського. 2023. С. 87–97.

7. Панченко С., Антонюк А., Новицький Д., Заморский С.. Загальні підходи до створення системи управління і контролю функціонування сервісів інформаційних систем у Збройних Силах України. Сучасні інформаційні технології у сфері безпеки та оборони. 2023. Т. 48, № 3. С. 98–106.

8. Андрощук О., Черевко Р., Петрушен М., Голобородько, М. Актуальні підходи до побудови інформаційної інфраструктури на основі хмарних технологій з використанням референсної архітектури. Сучасні інформаційні технології у сфері безпеки та оборони. 2023. Т. 46, № 1. С. 89–94.

9. Міхнов Є. Д. Огляд технології балансування навантаження у міксованих VPN-ланцюгах. Радіоелектроніка та молодь у XXI столітті : матеріали 28-го Міжнародного молодіжного форуму. 2024. Т. 5. С. 34–37. URL: https://doi.org/10.30837/IYF.PCEIP.2024.034 (дата звернення: 19.09.2025).

10. Замрій І. В., Собчук А. В., Лаптєв С. О., Лаптєва Т. О., Копитко, С. Б. Алгоритм контролю та прогнозування функціональної стійкості складних інформаційно-технічних систем. Телекомунікаційні та інформаційні технології. 2022. Т. 1. С. 4–14.

11. Шовкошитний І. Підхід до захисту інформаційно-телекомунікаційних систем на основі автокомпенсаційного принципу адресно-часової селекції аномалій мережевого трафіка. Сучасні інформаційні технології у сфері безпеки та оборони. 2023. Т. 48, № 3. С. 5–10.

12. Мартовицький В., Свиридов А., Авдєєв О., Гудзинський І., Коротецький О. Дослідження методів виявлення аномалій у арі журналах для забезпечення безпеки та надійності програмних систем. Вісник Херсонського національного технічного університету. 2025. Т. 2, № 1(92). С. 142–148.

13. Tkachov V., Chepurna I., Frolov D. The promising method of secure transmission of inelastic data in peer-to-peer networks. Computer and information systems and technologies: proceedings of seventh international scientific and technical conference. 2024. P. 15−16.

14. Кузьменко Д. Методи та моделі емуляції негативних впливів на ресурси інформаційних систем. Технічні науки та технології. 2024. Т. 4, № 38. С. 189–196.

15. Hattab N., Belalem G. Modular models for systems based on multi-tenant services: a multi-level Petri-net-based approach. Journal of King Saud University – computer and information sciences. 2023. P. 101671. URL: https://doi.org/10.1016/j.jksuci.2023.101671 (дата звернення: 19.09.2025).

16. Kashyap V., Ahuja R., Kumar A. Predictive analysis-based load balancing and fault tolerance in fog computing environment. Cluster Computing. 2025. Vol. 28, № 5. URL: https://doi.org/10.1007/s10586-024-04984-5 (дата звернення: 19.09.2025).

17. Melo M., Aquino G. FaTEMa: a framework for multi-layer fault tolerance in IoT systems. Sensors. 2021. Vol. 21, № 21. P. 7181. URL: https://doi.org/10.3390/s21217181 (дата звернення: 19.09.2025).

18. Hoare C. A. R. An axiomatic basis for computer programming. Communications of the ACM. 1969. Vol. 12, № 10. P. 576–580.

19. Yang S., Tan J., Lei T., Linares-Barranco B. Smart traffic navigation system for fault-tolerant edge computing of internet of vehicle in intelligent transportation gateway. IEEE Transactions on Intelligent Transportation Systems. 2023. Vol. 24, № 11. P. 13011–13022. URL: https://doi.org/10.1109/TITS.2022.3232231 (дата звернення: 19.09.2025).

20. Wang Y., Wang Z. Distributed model free adaptive fault-tolerant consensus tracking control for multiagent systems with actuator faults. Information sciences. 2024. P. 120313. URL: https://doi.org/10.1016/j.ins.2024.120313 (дата звернення: 19.09.2025).

21. Tkachov V., Hunko M., Volotka V. Scenarios for implementation of nested virtualization technology in task of improving cloud firewall fault tolerance. 2019 IEEE International Scientific-Practical conference Problems of Infocommunications, Science and Technology (PIC S&T). 2019. URL: https://doi.org/10.1109/picst47496.2019.9061473 (дата звернення: 19.09.2025).

22. Сектор інформаційного забезпечення інформаційно обчислювального центру. Харківський національний університет радіоелектроніки – ХНУРЕ, NURE. https://nure.ua/branch/informatsiyno-obchislyuvalniy-tsentr/struktura-iots/sektor-informatsijnoho-zabezpechennia (дата звернення: 19.09.2025)

References

1. Dodonov, O. H., Kuznietsova, M. H., & Horbachyk, O. S. (2025). Modeliuvannia i otsiniuvannia funktsionalnoi stiikosti informatsiinykh system. Reiestratsiia, zberihannia i obrobka danykh, 27(1), 76–88.

2. Leichenko, K. M., Skorobohatko, S. V., Fesenko, H. V., Kharchenko, V. S., & Yakovlev, S. V. (2025). Otsiniuvannia nadiinosti bezdrotovykh sensornykh merezh system monitorynhu lisovykh pozhezh z urakhuvanniam fatalnykh kombinatsii mnozhynnykh vidmov sensoriv. Kibernetyka ta systemnyi analiz, (61,1), 161-173. URL: http://jnas.nbuv.gov.ua/article/UJRN-0001535211

3. Tkachov, V., Kovalenko, A., Kharchenko, V., Hvozdetska, K., Hunko, M. (2022). An Overlay Network Based on Cellular Technologies for the Secure Control of Intelligent Mobile Objects. In: Ignatenko, O., et al. ICTERI 2021 Workshops. ICTERI 2021. Communications in Computer and Information Science, vol 1635. Springer, Cham. https://doi.org/10.1007/978-3-031-14841-5_32

4. Dodonov, O. H., Putiatin, V. H., Dodonov, V. O., Kutsenko, S. A., Hermaniuk, A. P., Izvaryn, I. V., & Kravchuk, K. O. (2024). Tekhnolohiia zabezpechennia zhyvuchosti terytorialno-rozpodilenykh informatsiinykh kompiuternykh system v yedynomu informatsiinomu prostori. Reiestratsiia, zberihannia i obrobka danykh, 26(1), 121–143. https://doi.org/10.35681/1560-9189.2024.26.1.308659

5. Lemeshko, O. V., Yeremenko, O. S., Yevdokymenko, M. O., Shapovalova, A. S., & Sleiman, B. (2022). Modeliuvannia ta optymizatsiia protsesiv bezpechnoi ta vidmovostiikoi marshrutyzatsii v telekomunikatsiinykh merezhakh. https://doi.org/10.30837/978-966-659-378-1

6. Kirpichnikov, Yu., Rybydailo, A., Lytovchenko, H., & Butenko, M. (2023). Obgruntuvannia pidkhodu do udoskonalennia informatsiinoi infrastruktury Ministerstva oborony Ukrainy dlia funktsionuvannia v umovakh zbroinoi ahresii. Zbirnyk naukovykh prats Tsentru voienno-stratehichnykh doslidzhen NUOU imeni Ivana Cherniakhovskoho, 87–97.

7. Panchenko, C., Antoniuk, A., Novytskyi, D., & Zamopckyi, C. (2023). Zahalni pidkhody do stvorennia systemy upravlinnia i kontroliu funktsionuvannia servisiv informatsiinykh system u Zbroinykh Sylakh Ukrainy. Suchasni informatsiini tekhnolohii u sferi bezpeky ta oborony, 48(3), 98–106.

8. Androshchuk, O., Cherevko, R., Petrushen, M., & Holoborodko, M. (2023). Aktualni pidkhody do pobudovy informatsiinoi infrastruktury na osnovi khmarnykh tekhnolohii z vykorystanniam referensnoi arkhitektury. Suchasni informatsiini tekhnolohii u sferi bezpeky ta oborony, 46(1), 89–94.

9. Mikhnov, Ye. D. (2024). Ohliad tekhnolohii balansuvannia navantazhennia u miksovanykh VPN-lantsiuhakh. Radioelektronika ta molod u XXI stolitti : materialy 28-ho mizhnarodnoho molodizhnoho forumu, 5, 34–37. https://doi.org/10.30837/IYF.PCEIP.2024.034

10. Zamrii, I. V., Sobchuk, A. V., Laptiev, S. O., Laptieva, T. O., & Kopytko, S. B. (2022). Alhorytm kontroliu ta prohnozuvannia funktsionalnoi stiikosti skladnykh informatsiino-tekhnichnykh system. Telekomunikatsiini ta informatsiini tekhnolohii, (1), 4–14.

11. Shovkoshytnyi, I. (2023). Pidkhid do zakhystu informatsiino-telekomunikatsiinykh system na osnovi avtokompensatsiinoho pryntsypu adresno-chasovoi selektsii anomalii merezhevoho trafika. Suchasni informatsiini tekhnolohii u sferi bezpeky ta oborony, 48(3), 5–10.

12. Martovytskyi, V., Svyrydov, A., Avdieiev, O., Hudzynskyi, I., & Korotetskyi, O. (2025). Doslidzhennia metodiv vyiavlennia anomalii u api zhurnalakh dlia zabezpechennia bezpeky ta nadiinosti prohramnykh system. Visnyk Khersonskoho natsionalnoho tekhnichnoho universytetu, 2(1 (92)), 142–148.

13. Tkachov, V., Chepurna, I., & Frolov, D. (2024). The promising method of secure transmission of inelastic data in peer-to-peer networks. Computer and information systems and technologies: proceedings of seventh international scientific and technical conference, 15–16.

14. Kuzmenko, D. (2024). Metody ta modeli emuliatsii nehatyvnykh vplyviv na resursy informatsiinykh system. Tekhnichni nauky ta tekhnolohii, (4 (38)), 189–196.

15. Hattab, N., & Belalem, G. (2023). Modular models for systems based on multi-tenant services: a multi-level Petri-net-based approach. Journal of King Saud University – computer and information sciences, 101671. https://doi.org/10.1016/j.jksuci.2023.101671

16. Kashyap, V., Ahuja, R., & Kumar, A. (2025). Predictive analysis-based load balancing and fault tolerance in fog computing environment. Cluster Computing, 28(5). https://doi.org/10.1007/s10586-024-04984-5

17. Melo, M., & Aquino, G. (2021). FaTEMa: a Framework for Multi-Layer Fault tolerance in IoT Systems. Sensors, 21(21), 7181. https://doi.org/10.3390/s21217181

18. Hoare, C. A. R. (1969). An axiomatic basis for computer programming. Communications of the ACM, 12(10), 576–580.

19. Yang, S., Tan, J., Lei, T., & Linares-Barranco, B. (2023). Smart Traffic Navigation System for Fault-Tolerant Edge Computing of Internet of Vehicle in Intelligent Transportation Gateway. IEEE Transactions on Intelligent Transportation Systems, 24(11), 13011-13022. https://doi.org/10.1109/tits.2022.3232231

20. Wang, Y., & Wang, Z. (2024). Distributed model free adaptive fault-tolerant consensus tracking control for multiagent systems with actuator faults. Information sciences, 120313. https://doi.org/10.1016/j.ins.2024.120313

21. Tkachov, V., Hunko, M., & Volotka, V. (2019). Scenarios for implementation of nested virtualization technology in task of improving cloud firewall fault tolerance. In 2019 IEEE International Scientific-Practical conference Problems of Infocommunications, Science and Technology (PIC S&T). IEEE. https://doi.org/10.1109/picst47496.2019.9061473

22. Sektor informatsiinoho zabezpechennia informatsiino obchysliuvalnoho tsentru. (2025, September 10). Kharkivskyi natsionalnyi universytet radioelektroniky – KhNURE, NURE. https://nure.ua/branch/informatsiyno-obchislyuvalniy-tsentr/struktura-iots/sektor-informatsijnoho-zabezpechennia

Дата першого надходження рукопису до видання: 29.09.2025
Дата прийнятого до друку рукопису після рецензування: 24.10.2025
Дата публікації: 28.11.2025