

ТАКСОНОМІЯ ТА МЕТРИКИ ОЦІНЮВАННЯ ПІДХОДІВ ДО ЗАБЕЗПЕЧЕННЯ ЖИВУЧОСТІ ІНФОРМАЦІЙНИХ СИСТЕМ

Рубан І.В., Ткачов В.М. (ihor.ruban@nure.ua, vitalii.tkachov@nure.ua)
Харківський національний університет радіоелектроніки (Україна)

У роботі подано систематизацію та порівняльний аналіз відомих підходів до забезпечення живучості інформаційних систем. Запропоновано узгоджену таксономію за рівнями організації (дані, процеси, ресурси), механізмами (маскування відмов, відновлення стану, адаптивна перебудова, ізоляція, різноманіття, виявлення відхилень), припущеннями щодо середовища (зв'язність, спостережуваність, синхронізація, ресурсні обмеження), часовим масштабом рішень та типами гарантій. Уніфіковано набір метрик (експлуатаційні, узгодженості даних, якості обслуговування, ризик-орієнтовані, просторово-часові, ресурсно-вартісні) й сформовано порівняльну матрицю. Результати виявляють сильні та слабкі сторони класів методів і окреслюють прогалини, пов'язані з переривчастою зв'язністю, частковою спостережуваністю та хвостовими ризиками, що слугує підґрунтям для подальшого інтегрування політик забезпечення живучості.

Сучасні інформаційні системи функціонують у середовищі високої невизначеності та збурень – від відмов компонентів і збоїв програмного забезпечення до навмисних впливів [1]. Це висуває підвищені вимоги до їх живучості – здатності зберігати цільову функціональність шляхом перебудови структури та зміни пріоритетів процесів у межах виконання основної функції [2-5]. Попри значний доробок у зазначеній предметній області, підходи до забезпечення живучості залишаються фрагментарними, оскільки спираються на несумісні припущення, різні рівні моделювання та неоднорідні критерії оцінювання.

Метою роботи є систематизація та порівняльний аналіз відомих моделей і методів забезпечення живучості інформаційних систем із побудовою уніфікованої схеми їх зіставлення. Методична основа охоплює класифікацію за рівнями організації (дані, процеси, ресурси), за типами загроз (відмови, збої, атаки, деградації) та режимами спостережуваності й зв'язності. Уніфікований набір показників для порівняння включає доступність, середній час відновлення, інваріанти причинно-часової узгодженості даних, а також ризик-чутливі метрики деградації сервісу.

Узагальнення відомих рішень доцільно виконувати за кількома ортогональними ознаками, що дозволяє зіставляти методи на спільній основі припущень, механізмів і гарантій. Пропонується наступна таксономія:

а) за рівнем організації системи:

– на рівні даних – надлишкове кодування, контроль цілісності, контрольні суми, інваріанти причинно-часової узгодженості, відкладене узгодження, буферизація;

– на процесному рівні – журналювання відновлення, реплікація виконання, керована деградація, дублювання маршрутів;

– на ресурсному рівні – резервування, перепланування та міграція навантаження, ізольовані середовища виконання, політики доступу до ресурсів;

б) за механізмом забезпечення:

– маскування відмов – надлишковість, кодова надлишковість;

– відновлення стану – контрольні точки, журналювання подій, селективне відновлення;

– адаптивна перебудова – перемикання режимів, самоналаштування параметрів, міграція компонентів, перепризначення ролей;

– ізоляція та обмеження поширення збурень – контейнеризація/віртуалізація, просторово-часова ізоляція, кордони поширення даних;

– захист від навмисних впливів – виявлення відхилень, динамічне укріплення конфігурацій, локалізація компрометованих компонентів;

в) за припущеннями щодо середовища:

– зв'язність – постійна, переривчаста, опортуністична;

– спостережуваність – повна; часткова; із затримками вимірювань;

– синхронізація – синхронні/квазі-асинхронні моделі часу;

- ресурсні обмеження – жорсткі та м'які;
- г) за часовим масштабом прийняття рішень:
 - реактивні локальні стратегії (швидкі правила реагування);
 - прогнозно-орієнтовані (горизонт передбачення, оцінювання стану й навантаження);
 - стратегічні (довгострокове планування ресурсів і конфігурацій);

г) за типом гарантій:

- жорсткі детерміновані (гарантовані межі часу/ресурсів, незмінні інваріанти);
- ймовірнісні (виконання з заданою довірою);
- середні (показники на середніх значеннях);

– хвостові ризик-чутливі (умовне сподівання перевищення для відмов і дефіцитів якості обслуговування);

д) за методами обґрунтування та перевірки:

- формальна верифікація властивостей і політик (інваріанти, досяжність, здійсненність);
- експериментальна валідація (полігон, цифровий двійник, відтворювані сценарії збурень);
- експлуатаційний моніторинг з аудитом подій і післядією.

Оцінювання живучості доцільно виконувати за узгодженим набором показників, згрупованих за змістом та масштабом вимірювання:

а) експлуатаційні показники – доступність (частка часу роботоздатності), середній час безвідмовної роботи, середній час відновлення, інтенсивність відмов, ймовірність відмови на інтервалі;

б) структурно-логічні показники узгодженості даних – кількість і тривалість порушень інваріантів причинно-часової узгодженості, час перебування за межами допустимої області, відстань до «ядра живучості» (ступінь відновлення до множини допустимих станів);

в) якісні показники надання послуг – частка виконаних вимог до якості обслуговування, інтегральний дефіцит якості (площа відхилення нижче встановлених рівнів у часі), максимальна глибина деградації під збуреннями;

г) ризик-орієнтовані показники – ймовірність перевищення критичного відхилення, умовне середнє перевищення, що відображає «хвостовий» ризик рідкісних, але значних збоїв, довірчі межі для базових метрик;

г) просторово-часові показники локалізації – частка уражених компонентів, радіус поширення збурення, час локалізації та ізоляції, швидкість переходу до безпечної конфігурації; показник плавності деградації/відновлення (відсутність різких стрибків);

д) ресурсно-вартісні показники – рівень надлишковості, додаткове споживання ресурсів під час відновлення, коефіцієнт «ефект/вартість» для порівняння альтернативних політик.

У табл. 1 наводиться порівняльна матриця класів підходів до забезпечення живучості інформаційних систем за рівнем застосування, ключовим механізмом, ефективністю ($E = [0;3]$), вартістю ресурсів ($C = [0;3]$).

Для коректного зіставлення методів усі метрики нормують (наприклад, до інтервалу $[0;1]$), супроводжують набором даних (визначення, одиниці, спосіб вимірювання, інтервал довіри) та агрегують за вагами з урахуванням пріоритетів системи (критичні сервіси, обмеження часу/ресурсів). Це забезпечує об'єктивну порівняльну оцінку підходів у різних умовах.

Узагальнення показало низку системних вад наявних підходів. Зокрема, до таких вад відносяться: відсутність єдиного термінологічного поля та зіставних описів метрик, розрив між рівнями моделювання (дані – процеси – ресурси), що ускладнює композиційність політик, слабке врахування переривчастої зв'язності та часткової спостережуваності, нестача методів з гарантованими межами для рідкісних, але руйнівних подій (хвостові ризики); обмежена здатність до локалізації спільних причин відмов і стримування каскадних ефектів, відсутність процедур оперативної перевірки здійсненності рішень у заданих ресурсно-часових межах, невизначеність співвідношення «ефект/вартість» у реальному часі; брак інструментів для адаптивного синтезу політик та їх формальної верифікації у динамічних умовах.

Проведена систематизація окреслює узгоджену таксономію підходів до забезпечення живучості інформаційних систем і уніфікований набір метрик оцінювання. Порівняльний аналіз свідчить, що універсальних рішень не існує. Ефективність визначається поєднанням механізмів (ізоляція, надлишковість, відновлення, адаптивна перебудова, керована деградація) під конкретні припущення щодо зв'язності, спостережуваності та ресурсних обмежень. Найперспективнішими

виглядають багаторівневі стратегії з явними інваріантами причинно-часової узгодженості, локалізацією збурень і ризик-чутливими критеріями, що враховують хвостові події. Практична придатність таких стратегій залежить від наявності описових метрик, засобів моніторингу та відтворених сценаріїв випробувань.

Таблиця 1 – Порівняльна матриця класів підходів до забезпечення живучості

Клас підходу	Рівень застосування	Ключовий механізм	E	C
Маскування відмов	дані / процеси	надлишковість	3	3
Журналювання	процеси / дані	знімки стану, відкат	2	2
Реплікація виконання/даних	дані / процеси / комунікації	активна/пасивна, синхрон./асинхрон.	3	3
Адаптивна перебудова конфігурації	ресурсний	перемикання режимів, переналаштування	2	1
Перепланування та міграція	ресурсний	перерозподіл ресурсів	2	2
Ізоляція/віртуалізація	архітектурний / ресурсний	ізолюючі контури, «пісочниці»	2	1
Багатоверсійність	програмний / процеси	незалежні реалізації	2	3
Виявлення відхилень і локалізація	моніторинг / керування	порогові та статистичні правила	2	1
Керована деградація якості	процеси / сервіси	зміна пріоритетів, спрощення функцій	2	1
Кодова надлишковість даних	дані / комунікації	коди виправлення помилок	2	1

Отримані результати формують підґрунтя для побудови інтегрованих рішень, у яких політики синтезуються та перевіряються у межах заданих ресурсно-часових обмежень із забезпеченням прозорих гарантій якості функціонування.

Список використаної літератури

- [1] Managing and Using Information Systems: A Strategic Approach. Wiley Sons, Inc., John, 2024.
- [2] О.Г. Додонов, О.В. Никифоров, В.Г. Путятін, В.О. Додонов, С.А. Куценко, А.П. Германюк Територіально-розподілені інформаційні комп'ютерні системи у єдиному інформаційному просторі: базові поняття та визначення. *Реєстрація, зберігання і обробка даних*, т. 26, № 1, с. 89-112. DOI: <https://doi.org/10.35681/1560-9189.2024.26.1.308647>.
- [3] О.Г. Додонов, Д.В. Ланде Мережева модель структурної живучості. *Реєстрація, зберігання і обробка даних*, т. 23, № 1, с. 15-22. DOI: <https://doi.org/10.35681/1560-9189.2021.23.1.235075>.
- [4] С.М. Лисенко, В.С. Харченко, К.Ю. Бобровнікова, Р.В. Щука. Резильєнтність комп'ютерних систем в умовах кіберзагроз: таксономія та онтологія. *Радіоелектронні і комп'ютерні системи*, № 1, с. 17-28. DOI: <https://doi.org/10.32620/reks.2020.1.02>.
- [5] А.А. Коваленко, Г.А. Кучук, В.М. Ткачов. Метод забезпечення живучості комп'ютерної мережі на основі VPN-тунелювання. *Системи управління, навігації та зв'язку. Збірник наукових праць*, т. 1, № 63, с. 90-95. DOI: <https://doi.org/10.26906/sunz.2021.1.090>.

UDC 004.41:658.8

IDENTIFYING NON-FUNCTIONAL REQUIREMENTS FOR A CRM SYSTEM

Rudenko M.O., Sotnik S.V.

(maksym.rudenko@nure.ua, svetlana.sotnik@nure.ua)

Kharkiv National University of Radio Electronics (Ukraine)

The article discusses the problem of defining non-functional requirements when designing CRM systems. The authors argue that the traditional approach to developing information systems often focuses primarily on functional requirements, while non-functional characteristics remain insufficiently