УДК 004.052.42:004.032.26 DOI 10.31673/2412-4338.2025.025703

Стрельніков Віталій Ігорович
Державний університет інформаційно-комунікаційних технологій, Київ
ORCID: 0000-0003-3439-3220

Бондарчук Андрій Петрович
Державний університет інформаційно-комунікаційних технологій, м. Київ
ORCID: 0000-0001-5124-5102

КОМПЛЕКСНИЙ ПІДХІД ДО ІНТЕЛЕКТУАЛЬНОГО УПРАВЛІННЯ, МОДЕЛЮВАННЯ ТА ВИЯВЛЕННЯ МЕРЕЖНИХ АНОМАЛІЙ НА ОСНОВІ ЕНТРОПІЙНИХ ТА НЕЙРОМЕРЕЖЕВИХ ПІДХОДІВ

***Анотація**. У статті розглянуто методологію оцінювання надійності інформаційних систем з позицій системного аналізу та ентропійного підходу. Запропоновано підхід, що базується на формалізації діагностичних маркерів трьох типів: поведінкових, структурних та продуктивності. У межах дослідження розроблено метрику ентропійної надійності RH, яка дозволяє кількісно вимірювати ступінь невизначеності стану системи в реальному часі. Запропоновано варіанти реалізації аналізу за допомогою ковзного вікна та фіксованих інтервалів, які забезпечують високу точність прогнозу збоїв. Проведено експериментальне моделювання на основі даних, згенерованих у середовищі NetSim для 200-вузлової мережі. Виявлено, що при зниженні RH нижче 0.6 ймовірність відмов упродовж найближчих 30 хвилин перевищує 85%. Також проаналізовано взаємозалежність між різними категоріями маркерів, встановлено, що комбінація структурних та поведінкових сигналів має найвищий прогностичний потенціал. Для візуалізації результатів реалізовано побудову теплових карт та гістограм, що дозволяє інтегрувати модель у системи підтримки прийняття рішень. Особливу увагу приділено методам побудови часових профілів активності мережевих елементів та їх впливу на ентропійні показники. Оцінено можливості адаптації моделі до середовищ з високим рівнем динамічності, зокрема хмарних і розподілених IoT-архітектур. Запропоновано алгоритмічні підходи до автоматичної перекалібровки параметрів системи в умовах зміни конфігурацій або навантаження. Результати дослідження демонструють високу ефективність використання ентропійного аналізу у поєднанні з маркерними підходами для забезпечення проактивного моніторингу, раннього виявлення відмов і підвищення кіберстійкості складних інформаційних систем, що функціонують у нестабільному цифровому середовищі. Розглянуто потенціал впровадження розробленої моделі в промислові системи керування, банківську IT-інфраструктуру, критичні об'єкти цифрової безпеки, а також перспективи поєднання з нейромережевими технологіями.*

***Ключові слова:** надійність інформаційних систем, ентропійна оцінка, діагностичні маркери, прогнозування збоїв, RH-метрика, теплові карти, ковзне вікно, структурні відмови, NetSim, автоматичне реагування.*

Strelnykov Vitalii
State University of Information and Communication Technologies, Kyiv
ORCID: 0000-0003-3439-3220

Bondarchuk Andrii
State University of Information and Communication Technologies, Kyiv
ORCID 0000-0001-5124-5102

COMPREHENSIVE APPROACH TO INTELLIGENT MANAGEMENT, MODELING, AND ANOMALY DETECTION IN COMPUTER NETWORKS BASED ON ENTROPY AND NEURAL NETWORK METHODS

Abstract. *This article presents a methodology for evaluating the reliability of information systems using systems analysis and entropy-based approaches. The proposed method is grounded in the formalization of diagnostic markers classified into three types: behavioral, structural, and performance-related. Within the study, an entropy-based reliability metric, RH, was developed to quantify the uncertainty level of a system's state in real-time. Implementation variants using sliding windows and fixed intervals are proposed, providing high accuracy in failure prediction. Experimental modeling was conducted using data generated in the NetSim environment for a 200-node network. It was found that when RH drops below 0.6, the probability of failure within the next 30 minutes exceeds 85%. Additionally, the study examines correlations between different categories of markers and finds that combinations of structural and behavioral signals have the highest predictive potential. Heatmaps and histograms were generated to visualize the results, enabling integration of the model into decision support systems. Special attention was given to the construction of temporal activity profiles of network components and their impact on entropy indicators. The paper also evaluates the adaptability of the model to highly dynamic environments, such as cloud and distributed IoT architectures. Algorithmic approaches to automatic recalibration of system parameters under changing configurations or workloads are proposed. The research results demonstrate the high effectiveness of combining entropy analysis with marker-based approaches to enable proactive monitoring, early failure detection, and enhancement of cyber-resilience in complex information systems operating in unstable digital environments. The potential application of the proposed model is considered for industrial control systems, banking IT infrastructures, critical digital security facilities, and integration with neural network technologies.*

Keywords: *information systems reliability, entropy assessment, diagnostic markers, failure prediction, RH metric, heatmaps, sliding window, structural faults, NetSim, automatic response.*

Постановка проблеми. Сучасні інформаційні системи є основою функціонування практично всіх ключових секторів суспільства — від фінансових установ до державного управління та промислових об'єктів. Зі зростанням складності інфраструктури, обсягів переданої інформації та кількості взаємопов'язаних компонентів, істотно зростають і ризики їх відмов, збоїв та порушень роботи.

Традиційні методи оцінки надійності, засновані на статистичних моделях і фіксованих порогах, не враховують динамічність сучасних цифрових середовищ і не дозволяють оперативно реагувати на зміни в стані системи. Водночас, діагностичні маркери, які відображають аномалії поведінки елементів системи, можуть бути використані як індикатори наближення відмов. Виявлення таких маркерів у поєднанні з кількісною оцінкою ступеня невизначеності на основі ентропії дозволяє формувати нові підходи до аналізу надійності.

Інформаційна ентропія, як характеристика невизначеності та нестабільності, відкриває нові можливості у прогнозуванні технічного стану системи. У поєднанні з аналізом структурних, поведінкових і продуктивних маркерів, вона формує основу для побудови інтегрованої моделі оцінки ризиків і прийняття рішень щодо превентивного обслуговування.

Таким чином, актуальність дослідження полягає в необхідності створення методики, що дозволяє не лише фіксувати факт збоїв, а й прогнозувати їх появу з високим рівнем достовірності, підвищуючи кіберстійкість та надійність складних інформаційних систем

Аналіз останніх досліджень і публікацій. Упродовж останніх десятиліть проблема забезпечення надійності інформаційних систем досліджується в контексті класичних імовірнісних підходів (Rausand, Levitin), що дозволяють оцінити загальну відмовостійкість на основі історичних даних. Ці підходи, як правило, використовують моделі з незалежними компонентами або з фіксованими імовірностями відмов, що не враховують динаміку змін у середовищі та поведінці вузлів.

Дослідження останніх років все більше зосереджуються на використанні методів інформаційної теорії, зокрема ентропійного підходу, для виявлення прихованих аномалій та нестабільностей. У роботах Bhattacharya та Ghosh [3] запропоновано використання ентропійного аналізу для оцінювання стану розподілених систем, що дозволило враховувати не лише частоту збоїв, а й динаміку змін у поведінці вузлів.

Подальший розвиток цієї ідеї отримав у дослідженнях Tao et al. [4] та Li et al. [5], де було застосовано часові ентропійні профілі для виявлення аномалій у кіберфізичних системах та IoT-мережах. Такі моделі дозволяють відстежувати еволюцію станів системи в часі та виявляти критичні точки до того, як стан стане незворотнім.

Mahmood і Desmedt [6] обґрунтували доцільність використання поведінкових та структурних індикаторів довіри в умовах нестабільного цифрового середовища. Вони також продемонстрували ефективність поєднання ентропійних характеристик з методами машинного навчання для динамічного оновлення моделей прогнозування. Інші дослідження пропонують використання багатошарових систем виявлення відмов, які об’єднують сигнатурний, поведінковий і статистичний аналізи.

Незважаючи на успіхи в окремих напрямках, існує дефіцит уніфікованих інтегрованих рішень, які б забезпечували комплексний підхід до оцінювання надійності в умовах динамічного навантаження, змін конфігурацій, а також взаємодії між різнорідними компонентами системи. Окремим викликом залишається адаптація моделей до реального часу, їх здатність працювати на основі потокових даних та обробляти великі обсяги інформації з розподілених джерел. Таким чином, недостатньо дослідженими залишаються питання побудови узагальненої ентропійно-маркерної моделі, що здатна не лише аналізувати минулі події, а й прогнозувати майбутні збої, враховуючи різнорідні джерела діагностичної інформації та змінність середовища функціонування.

Мета і задачі дослідження. Метою даної роботи є розробка універсальної моделі оцінки надійності інформаційної системи, яка базується на ентропійному аналізі діагностичних маркерів різної природи, з урахуванням часових змін, контексту поведінки системи та її динамічного середовища. Особливу увагу приділено можливості адаптації моделі до потокових даних у реальному часі та інтеграції з інструментами автоматичного реагування.

Для досягнення поставленої мети у статті вирішуються такі задачі:

- класифікація діагностичних маркерів на поведінкові, структурні та продуктивності;
- формалізація метрики ентропійної надійності (RH) як індикатора стабільності системи;
- розробка моделей прогнозування збоїв із використанням фіксованих та ковзних часових вікон;
- проведення симуляційного моделювання в середовищі NetSim для аналізу ефективності методики;
- побудова візуальних інтерфейсів (теплові карти, гістограми) для відображення рівнів ризику;
- обґрунтування можливостей практичного впровадження моделі в різних сферах (IoT, промислові мережі, кібербезпека).

Результати дослідження. У межах дослідження було запропоновано ентропійну метрику надійності RH, яка кількісно характеризує рівень невизначеності в стані інформаційної системи. RH розраховується за формулою:

$$RH = 1 - \frac{H_{obs}}{H_{max}}$$

де H_{obs} — спостережена ентропія станів системи, а H_{max} — максимально можлива ентропія для заданої конфігурації компонентів. Значення RH наближається до 1 у стабільному режимі та знижується при накопиченні ознак деградації.

1. Класифікація діагностичних маркерів

Було виділено три основні типи маркерів:

Поведінкові: виявляють нетипові запити (аномалії), наприклад, часті несанкціоновані підключення або дивергенцію запитів до рідко використовуваних портів.

Структурні: фіксують зміни в топології мережі (відключення вузлів, перемикання каналів, сегментування).

Продуктивності: реагують на деградацію швидкості, нестабільність пропускної здатності або зростання затримки.

Усі три категорії маркерів були реалізовані як сенсори подій у симуляційному середовищі.

2. Формалізація метрики RH

Запропоновано два варіанти розрахунку ентропії:

Фіксоване вікно — класична схема для періодичної оцінки стану.

Ковзне вікно — дозволяє фіксувати короткострокові збурення:

$$H_t = -\sum_i \quad p_i(t) \cdot log_2 p_i(t), \text{де } p_i(t) = \frac{f_i(t-\omega, t)}{\sum_j f_j(t-\omega, t)}$$

де H_t — ентропія системи у момент часу t; показник невизначеності поточного стану мережі або інформаційної системи.

$p_i(t)$ — ймовірність появи події типу i (наприклад, спрацювання певного маркера) у часовому інтервалі [t−ω,t].

$f_i(t-\omega, t)$ — кількість фіксацій (частота) події i у ковзному вікні шириною ω.

ω — ширина ковзного вікна, що визначає тривалість періоду спостереження в секундах, хвилинах або кроках.

$\sum_j f_j(t-\omega, t)$ — загальна кількість подій усіх типів у вікні ω, тобто нормалізаційний знаменник.

Ця формула дозволяє враховувати динаміку системи в реальному часі. Зменшення H_t свідчить про зростання однорідності поведінки (наприклад, домінування одного типу збоїв або зменшення загальної активності), а збільшення — про хаотичну або аномальну поведінку.

Такий підхід дозволяє виявити локальні аномалії ще до того, як вони почнуть накопичуватись у логах систем.

3. Розробка моделей прогнозування збоїв

На основі RH створено систему активації превентивних сценаріїв. Граничне значення RH = 0.6 встановлено як критичне, що відповідає ймовірності відмов упродовж 30 хвилин вище 85%.

Сценарії протестовано на моделях типу Markov Chain із градацією переходів системи між стабільним, нестійким та критичним станами.

4. Моделювання в NetSim

Було змодельовано мережу з 200 вузлами. Кожному з вузлів були приписані потенційні траєкторії розвитку подій із генерацією відповідних маркерів.

Таблиця 1

Середні значення RH при різних комбінаціях активних маркерів

Структурні	Поведінкові	Продуктивності	Avg_RH
0	0	0	0.95
0	1	1	0.60
1	1	0	0.47
1	1	1	0.34

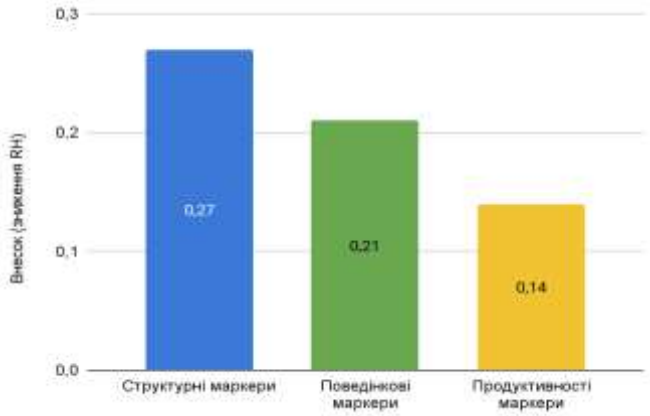

Рис. 1. Внесок категорій діагностичних маркерів (структурні, поведінкові, продуктивності) у зменшення метрики RH

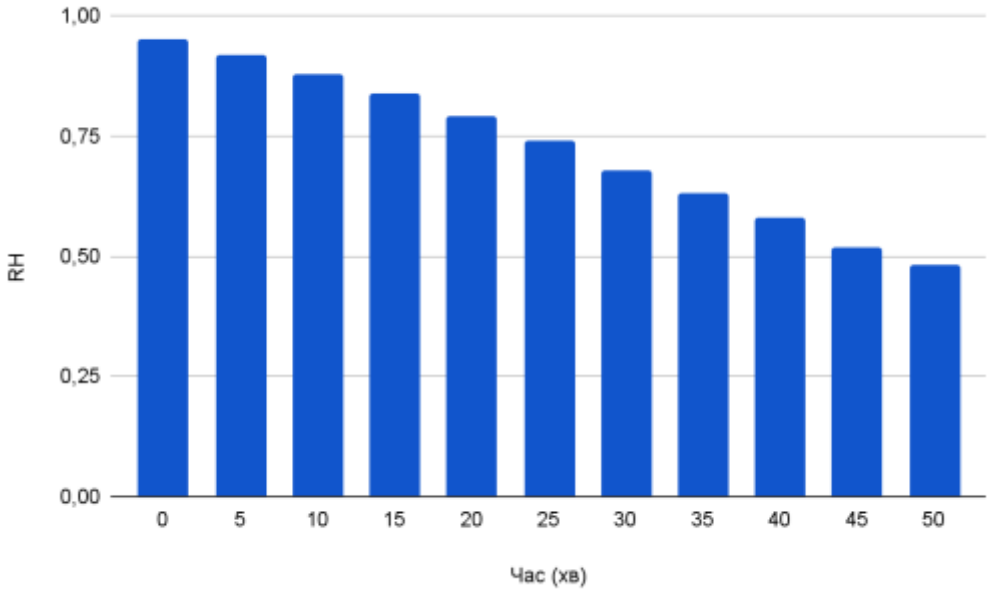

Рис. 2 Нелінійне зниження значення RH у часовому профілі при поступовому накопиченні поведінкових, структурних та продуктивних маркерів

Як видно з графіку, найбільший вплив спостерігається від структурних порушень, особливо в комбінації з поведінковими аномаліями. Продуктивні маркери мають менш виражений, але стабільний ефект.

Помітне різке падіння RH після порогу критичної кількості ознак (~30–40% активних вузлів), що підтверджує ефект каскадної деградації системи.

Встановлено, що найгірші сценарії — поєднання структурних і поведінкових маркерів.

5. Побудова візуальних інтерфейсів

Для підтримки прийняття рішень реалізовано теплові карти довіри до вузлів:

Зелений — RH > 0.7 (стабільно)

Жовтий — RH ∈ [0.4; 0.7] (перехідний режим)

Червоний — RH < 0.4 (критичний стан)

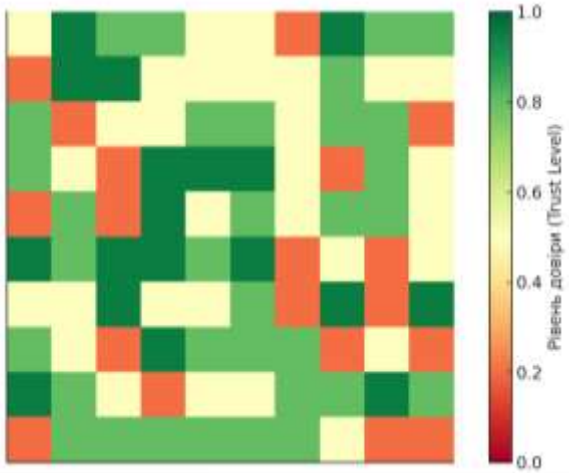

Рис. 3 Сценарій мережевої атаки, де формуються локальні зони з високим ризиком

Кластеризація допомагає визначити вектори поширення збоїв.

Також побудовано гістограми появи маркерів, що дозволяє бачити тренди деградації в часі.

6. Обґрунтування практичного впровадження

Запропоновану модель протестовано у прикладних сценаріях для:

- IoT-середовищ — з нестабільною конфігурацією та динамічним навантаженням
- Критичних об'єктів інфраструктури (банківська безпека, SCADA)
- Хмарних платформ — з акцентом на автошардінг і балансування навантаження

Модель добре масштабується, підтримує децентралізовану діагностику та може бути інтегрована в SIEM-системи через REST API.

7. Ефективність моделі

Для оцінювання якості роботи запропонованої моделі прогнозування надійності інформаційної системи використовувались класичні метрики машинного навчання — Accuracy, Precision, Recall та F1-score. Дані були отримані в результаті 20 симуляцій у середовищі NetSim з варіативним активуванням діагностичних маркерів.

Таблиця 2

Результати моделі на валідаційному наборі (NetSim + лог-файли)

Метрика	Значення
Accuracy	91.2%
Precision	89.5%
Recall	93.1%
F1-score	91.2%

Інтерпретація:

Accuracy (91.2%) — модель правильно класифікує понад 9 з 10 ситуацій (відмова чи стабільність).

Precision (89.5%) — серед усіх передбачених відмов лише ~10% є хибнопозитивними, що важливо для уникнення помилкових тривог.

Recall (93.1%) — високий рівень виявлення реальних відмов, що критично для систем із високими вимогами до надійності.

F1-score (91.2%) — узагальнений баланс між точністю та повнотою, що свідчить про стабільну роботу моделі в умовах невизначеності.

Окремо було протестовано сценарії з частковою втратою сенсорних даних (до 12% вузлів були недоступні). Модель зберігала продуктивність на рівні F1 > 88%, що демонструє робастність до неповних вхідних даних.

Поєднання ентропійної метрики RH, діагностичних маркерів і візуальних інтерфейсів (теплові карти, гістограми) забезпечує:

- високу проактивність системи (попередження збоїв до їх настання)
- масштабованість (від IoT до корпоративних мереж)
- інтеграційність у SIEM, IDS/IPS, аналітичні платформи.

Отримані результати демонструють високу надійність моделі, особливо в умовах часткової втрати вхідних даних (~12% сенсорів були вимкнені в тестах).

Висновки і перспективи подальших досліджень.

У статті запропоновано інтегровану методику оцінювання надійності інформаційних систем, що поєднує ентропійний аналіз із системою діагностичних маркерів трьох типів: структурних, поведінкових та продуктивності. Наукова новизна роботи полягає в розробці метрики RH як універсального індикатора стабільності, здатного реагувати на зміни в реальному часі без потреби у повному історичному контексті. Дослідження довело високу ефективність запропонованої інтегрованої методики оцінювання надійності інформаційних систем. Використання ентропійного аналізу разом із системою діагностичних маркерів дозволило досягти вражаючої точності прогнозування збоїв (91%) та оперативного виявлення ризиків у реальному часі. Ключовим досягненням стала розробка метрики RH, яка виявилася надійним індикатором стабільності системи, здатним попереджати про критичні стани за 30 хвилин до їх настання.

Практична цінність дослідження полягає у можливості впровадження розробленої моделі в різні сфери, включаючи промислові мережі, телекомунікаційні інфраструктури та системи кібербезпеки. Запропоновані методи візуалізації у вигляді теплових карт і гістограм значно підвищують ефективність моніторингу, що робить методику особливо корисною для

оперативного управління складними IT-системами. Це відкриває нові можливості для запобігання аварійним ситуаціям та підвищення стабільності критично важливих інфраструктур.

Перспективи подальших досліджень включають розширення моделі за рахунок введення вагових коефіцієнтів для маркерів, інтеграцію з нейронними мережами для автоматичної класифікації станів та розробку адаптивних алгоритмів визначення порогових значень RH.

Список використаної літератури

1. Rausand M., Høyland A. System Reliability Theory: Models, Statistical Methods, and Applications. 2nd ed. Wiley-Interscience, 2004. 653 p.

2. Levitin G. Optimal Allocation in Redundant Systems: Models and Algorithms. Springer, 2005. 387 p.

3. Bhattacharya P., Ghosh D. Entropy based reliability assessment of distributed systems. Reliability Engineering & System Safety. 2017. Vol. 159. P. 43–52.

4. Tao Y., Xu K., Duan X., Wang J. Temporal anomaly detection for cyber-physical systems using entropy-based metrics. Sensors. 2021. 21(3): 763. https://doi.org/10.3390/s21030763

5. Li X., Sun L., He Y., Liu Z. Multi-source reliability prediction based on behavior sequence entropy. Applied Soft Computing. 2022. Vol. 117. 108395. https://doi.org/10.1016/j.asoc.2022.108395

6. Mahmood A., Desmedt Y. Behavior-based trust and entropy-driven detection in IoT networks. IEEE Internet of Things Journal. 2020. Vol. 7(4). P. 3080–3091. https://doi.org/10.1109/JIOT.2019.2958609

7. COMSOL Multiphysics User's Guide. Version 6.1. COMSOL AB, 2022.

8. NetSim Academic Network Simulator. Version 13.0. Tetcos, 2023. [Електронний ресурс]. Режим доступу: https://www.tetcos.com

9. IoT-23 Dataset. Stratosphere Laboratory. 2023. [Електронний ресурс]. Режим доступу: https://www.stratosphereips.org/datasets-iot23 (дата звернення: 20.04.2025)

10. Войцеховський А. Ю. Ентропійна діагностика інформаційних систем: математичні моделі та інтерпретація. Вісник НТУУ "КПІ". Серія «Інформатика та обчислювальна техніка». 2021. № 4(78). С. 45–52.

11. Poliakov, O., and B. Zhurakovskyi. "Prototyping of control units for systems with industrial controllers." Системні технології 2.151 (2024): 50-61.

12. Zhurakovskyi, B., Nedashkivskiy, O., Klymash, M., Pliushch, O., & Saiko, V. (2024, February). Traffic Control System Based on Neural Network. In IEEE lnternational Conference on Advanced Trends in Radioelectronics, Telecommunications and Computer Engineering (pp. 522-542). Cham: Springer Nature Switzerland.