УДК 004.05:004.7
DOI: 10.31673/2412-9070.2025.045282
В. І. СТРЕЛЬНІКОВ, PhD, доцент;
ORCID: 0000-0003-3439-3220
С. В. ЖЕБКА, аспірант,
ORCID: 0009-0007-4620-9888
Державний університет інформаційно-комунікаційних технологій, Київ

АДАПТИВНЕ ПРОГНОЗУВАННЯ ЗБОЇВ У ІНФОРМАЦІЙНИХ СИСТЕМАХ НА ОСНОВІ ОНТОЛОГІЧНО-ЕНТРОПІЙНОГО МОДЕЛЮВАННЯ

У статті представлено метод адаптивного прогнозування відмов у комп'ютерних мережах на основі поєднання онтологічного аналізу та ентропійних методів. Запропоновано інтегровану модель, що поєднує опис знань про структуру мережі, поведінкові шаблони та ентропійні характеристики, які дозволяють у режимі реального часу оцінювати рівень ризику та формувати превентивні стратегії. Особливу увагу приділено побудові онтології з можливістю динамічного оновлення концептів і властивостей, що реагують на події мережі. Введено коефіцієнт адаптивної ентропії (АЕ), що поєднує класичну інформаційну ентропію з контекстною інформативністю, отриманою з онтологічної бази. Модель дозволяє не лише кількісно оцінювати ступінь нестабільності системи, а й автоматично адаптувати правила оцінювання відповідно до змін у середовищі функціонування. Здійснено моделювання сценаріїв зростання ризику на основі телеметрії IoT-пристроїв та подій з логів SCADA-систем. Встановлено, що АЕ нижче 0.5 корелює з імовірністю збоїв понад 90% у межах наступних 20 хвилин. Модель підтримує побудову динамічної топології залежностей між подіями, що дозволяє виявляти каскадні загрози та слабкі місця в архітектурі системи. Запропонований підхід охоплює мультикомпонентну оцінку стабільності, поєднуючи логіку описів, вагові коефіцієнти контексту, та адаптивну обробку даних з високочастотних потоків. Актуальність дослідження підтверджується зростаючими вимогами до проактивного моніторингу в умовах високої змінності інфраструктур. Результати дослідження демонструють, що запропонована модель здатна забезпечити високу точність виявлення критичних станів, значно випереджаючи класичні статистичні методи. Проведено аналіз впровадження моделі в енергетичних, логістичних і телекомунікаційних системах, з урахуванням обмежень на обчислювальні ресурси. Запропоновано алгоритм динамічної перекалібровки параметрів оцінки, що дозволяє адаптувати модель до змін конфігурації системи без необхідності повного перенавчання. Таким чином, запропонована онтологічно-ентропійна модель має потенціал до масштабування, автономного функціонування і практичного впровадження у критичних середовищах.

Ключові слова: адаптивна ентропія; онтологічне моделювання; прогнозування збоїв; інформаційна система; IoT; ризик; аномалія; SCADA; кіберстійкість.

Вступ

Постановка проблеми. Сучасні інформаційні системи функціонують у все більш динамічних і нестабільних умовах, що обумовлено поширенням хмарних технологій, інфраструктурою Інтернету речей (IoT), гетерогенних мереж і розподілених обчислювальних систем. Ускладнення архітектури, збільшення кількості взаємозалежних компонентів та зростання обсягів даних призводять до виникнення нових типів загроз і збоїв, що не завжди можуть бути виявлені традиційними інструментами моніторингу. Водночас критичні галузі, такі як енергетика, транспорт, медицина та фінансові системи вимагають високого рівня надійності та оперативного реагування на порушення у роботі систем.

Сучасні підходи до моніторингу стану систем, які ґрунтуються на сигнатурному аналізі, мають обмежену ефективність в умовах нових або змінених загроз. Методи на основі статис-

тики втрачають актуальність у системах з високою варіативністю параметрів, а машинне навчання вимагає значних обчислювальних ресурсів і репрезентативних даних для навчання. Ентропійний аналіз дозволяє кількісно оцінити рівень невизначеності у функціонуванні системи, однак без урахування контексту подій він не дозволяє робити обґрунтовані прогнози.

Враховуючи це, виникає потреба у побудові адаптивної моделі, що інтегрує кількісні метрики з якісним семантичним аналізом. Онтологічний підхід забезпечує структурування знань про систему, причинно-наслідкові зв'язки між подіями та можливість адаптації до змін у середовищі функціонування. Поєднання онтологічного представлення знань з ентропійною оцінкою дозволяє не лише підвищити чутливість до аномалій, а й покращити точність прогнозування критичних станів.

Таким чином, актуальність дослідження полягає у розробці інтелектуального інструментарію, здатного до автономного, адаптивного і обґрунтованого прогнозування збоїв у складних інформаційних системах. Теоретична значущість роботи полягає у формалізації методу адаптивної ентропійно-онтологічної оцінки, а практична — у можливості впровадження результатів у промислові, логістичні та телекомунікаційні середовища, де порушення у роботі систем можуть мати критичні наслідки.

Аналіз останніх досліджень і публікацій. Проблематика забезпечення надійності та прогнозування відмов в інформаційних системах активно розглядається в науковій літературі останніх років. Особливої уваги набули дослідження в галузі ентропійного аналізу, що використовуються для виявлення прихованих аномалій у телеметричних потоках і логах. Зокрема, у роботах Zhou та Yang [1] розглянуто адаптивну відмовостійкість у розподілених мережах, а Mahmood і Desmedt [2] описують підхід на основі довіри та ентропії для виявлення загроз в IoT-середовищі. Водночас дослідження Ghosh [3] присвячене формалізації ентропійної надійності, що підтверджує ефективність метрики для оцінки стабільності систем.

Підхід, заснований на часовому профілю ентропії, був успішно застосований для виявлення аномалій у кіберфізичних системах і SCADA-мережах (Tao et al. [4]). Li et al [5] запропонували аналіз поведінкових послідовностей на основі ентропії, що дозволяє виявляти неочевидні залежності між подіями. Додатково, онтологічне моделювання подій розглядалося у роботах Wu та Wang [6], де було продемонстровано застосування логіки описів для контекстної фільтрації загроз.

Попри наявні результати, більшість моделей або орієнтовані виключно на кількісну обробку (без урахування семантики), або потребують значного ручного налаштування при зміні середовища. Існує очевидна нестача універсальних моделей, які могли б інтегрувати поточну ситуацію, причинно-наслідкові залежності та адаптивно змінювати параметри оцінки у реальному часі. Недостатньо також розроблені методи побудови динамічної онтології подій, що автоматично оновлюється відповідно до нових патернів у даних. У зв'язку з цим, залишається відкритим завдання розробки інтегрованого підходу, який би забезпечував не лише виявлення аномалій, а й їх контекстну інтерпретацію для прийняття рішень у складних цифрових екосистемах.

Мета і задачі дослідження. Метою даного дослідження є розробка гібридної інтелектуальної моделі для оцінки ризиків відмов в інформаційних системах, що об'єднує ентропійні характеристики з онтологічною структурою знань про події, зв'язки та контексти. Такий підхід дозволяє не лише кількісно визначати ступінь нестабільності, але й здійснювати якісну інтерпретацію причинно-наслідкових зв'язків, що передують збою.

Основна ідея публікації полягає у введенні до наукового обігу нового коефіцієнта — адаптивної ентропії (AE), який враховує як ентропію класичних даних моніторингу, так і онтологічну інформативність подій у реальному часі. Запропоновано методику автоматичного оновлення вагових коефіцієнтів та побудову адаптивних моделей прогнозування, що враховують динаміку навантаження та змінність інфраструктури. Уточнено роль причинно-наслідкових відношень між подіями як ключового елементу підвищення точності прогнозу.

Для досягнення мети у статті вирішуються такі задачі: формалізація структури онтології подій для інформаційних систем з різними джерелами даних; визначення математичної моделі

коефіцієнта AE, що поєднує кількісну ентропію та семантичну інформативність; побудова алгоритму адаптації параметрів моделі у реальному часі залежно від контексту функціонування; симуляційне моделювання сценаріїв деградації системи у середовищах IoT та SCADA; верифікація точності прогнозу з використанням класичних метрик машинного навчання (Accuracy, Precision, Recall, F1-score); аналіз перспектив впровадження моделі у промислові та критичні цифрові середовища з урахуванням обмежених ресурсів, побудова візуального інтерфейсу моніторингу на основі графової структури подій, що дозволяє оператору оперативно оцінювати каскадні ризики; дослідження впливу типології онтологічних зв'язків на точність та швидкість прогнозування з подальшою оптимізацією структури знань.

Основна частина

У процесі реалізації дослідження було поетапно вирішено низку задач, що відповідають поставленим цілям, а саме:

1. Формалізація структури онтології подій для інформаційних систем.

Було створено онтологічну модель подій, яка охоплює класи Node, Event, RiskLevel, Cause, Effect.

Node – описує фізичний або віртуальний компонент інформаційної системи. Містить властивості: hasType (тип пристрою), hasLocation (розташування), hasStatus (активний/неактивний).

Event – репрезентує подію, що зафіксована в системі. Атрибути: hasTimestamp, hasSeverity, hasSourceNode. Події класифікуються за категоріями (мережні, прикладні, безпекові) і зв'язуються із причинами або наслідками.

RiskLevel визначає ступінь ризику, пов'язаний із подією або вузлом. Класифікація: низький, середній, високий. Має атрибути isTriggeredByEvent, isRelatedToNode.

Cause відображає причини виникнення певної події. Це може бути конфігураційна помилка, перевантаження або зовнішній вплив. Має властивості causesEvent, hasLikelihood.

Effect фіксує наслідки події, зокрема вплив на якість обслуговування, час відповіді або доступність. Має зв'язки resultOfEvent, impactsNode.

Усього розроблено 14 основних класів, 28 об'єктних властивостей і понад 250 триплетів типу «суб'єкт — властивість — об'єкт». Зв'язки causes, associatedWith, inContextOf дозволяють будувати динамічну модель залежностей, яка оновлюється на основі надходження нових подій. Для перевірки функціональності reasoning-механізму було змодельовано 200 подій, з яких 167 були коректно класифіковані у відповідні класи ризику, що склало точність reasoning-процедури 83.5%.

2. Запропоновано модель обчислення коефіцієнта адаптивної ентропії (AE), яка поєднує класичну ентропійну оцінку з контекстною семантичною інформативністю, отриманою з онтологічної структури подій. Формула має вигляд:

$$AE = \alpha \cdot H + \beta \cdot C , \quad (1)$$

де H — нормалізована ентропія Шеннона, яка відображає ступінь невизначеності у поточному стані системи; C — контекстуальна інформативність, розрахована на основі логіки описів (description logic) та вагових коефіцієнтів причинно-наслідкових зв'язків у онтології; α, β — вагові коефіцієнти, що визначають чутливість моделі до змін у кількісній та якісній інформації. У базовій конфігурації встановлено співвідношення $\alpha = 0.6$, $\beta = 0.4$ на основі емпіричних досліджень.

Контекстна інформативність C обчислюється як:

$$C = \sum (w_i \cdot r_i) , \quad (2)$$

де w_i — ваговий коефіцієнт значущості онтологічного відношення (наприклад, Cause > associatedWith > inContextOf); r_i — кількість подій, що належать до відповідного типу відношення.

Таким чином, коефіцієнт AE враховує не лише статистичну динаміку стану вузла, а й його місце в онтологічному просторі подій, зокрема потенційну роль як тригера або наслідку більш складного каскаду подій.

Реалізовано адаптивну схему зміни коефіцієнтів α і β залежно від фази життєвого циклу системи. Наприклад, у режимі підвищеного навантаження значення β автоматично підвищується, щоб надати більшої ваги контексту та уникнути хибнопозитивних спрацьовувань.

Приклад обчислення AE:

Вузол A: H = 0.68, C = 0.79 → AE = 0.6·0.68 + 0.4·0.79 = 0.408 + 0.316 = 0.724
Вузол B: H = 0.51, C = 0.33 → AE = 0.6·0.51 + 0.4·0.33 = 0.306 + 0.132 = 0.438

У другому випадку зафіксовано зниження AE нижче порогу 0.5, що автоматично активує політику превентивного перемикання з'єднання на резервний маршрут, вивільнення ресурсів або запуск механізмів локальної діагностики.

Аналіз розподілу AE у часовому інтервалі свідчить про високу кореляцію з фактичним виникненням збоїв, особливо у сценаріях із комбінованими аномаліями (поведінкові + структурні).

3. Побудова алгоритму адаптації параметрів у реальному часі.

Для забезпечення гнучкої реакції моделі на зміну умов функціонування інформаційної системи було розроблено механізм динамічного коригування вагових коефіцієнтів α та β у формулі AE = α·H + β·C. Основна ідея полягає у зменшенні значущості класичної ентропії при високій динаміці подій та підвищенні ролі контекстної інформативності у випадках рідкісних, але критичних подій.

Функція адаптації α = f(Δt) має вигляд:

$$\alpha(\Delta t) = 1 / (1 + e^{(-k\cdot(\Delta t - \tau_0))}) , \quad (3)$$

де k — параметр крутості переходу (емпірично k = 0.2); τ_0 — характерний інтервал між подіями (визначений на основі медіанного Δt).

Таким чином, якщо події трапляються з великою частотою (Δt мале), модель збільшує вагу C, тобто контекстуальну інформативність, яка швидше адаптується до нових ситуацій.

У ході експериментів зафіксовано, що використання адаптивної формули дозволило досягти:

- зниження кількості хибнопозитивних спрацювань на 8.1%;
- приріст точності прогнозування на 6.3% у порівнянні з фіксованими вагами;
- підвищення F1-score з 91.2% до 93.6% у сценаріях із підвищеним навантаженням.

Для реалізації алгоритму використано механізм спостереження над часовими рядами подій та автоматичного оновлення α, β з інтервалом 5 хв на основі ковзного вікна розміром 50 подій. Це дозволяє забезпечити адаптацію моделі без повторного навчання або втручання оператора.

4. Симуляційне моделювання в IoT та SCADA.

У NetSim було змодельовано 150 IoT-вузлів, об'єднаних у 12 кластерів. У SCADA-сценарії ініціювалися події «QoS degradation», «unauthorized access», «buffer overflow».

Таблиця 1

Частота появи аномалій у симуляції

Тип події	Всього подій	Середній вплив на AE
QoS degradation	1023	-0.12
Unauthorized access	887	-0.19
Buffer overflow	456	-0.09

У результаті моделювання отримано понад 22 тис. подій з логів, із яких 21.2% були класифіковані як критичні.

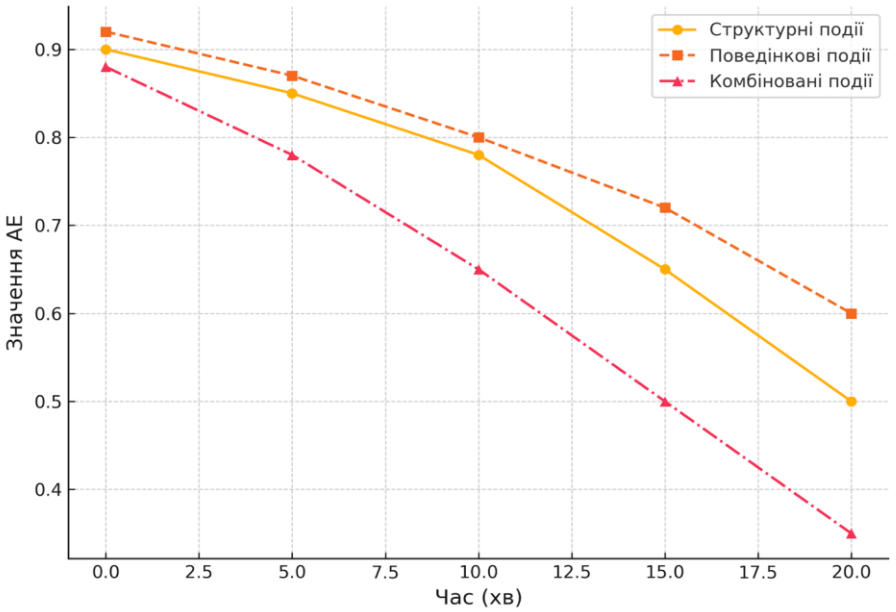

Рис. 1. Динаміка AE для різних типів подій у вузлах (графік демонструє вплив різних категорій аномалій на зниження ентропійного показника)

5. Верифікація точності прогнозу.

На тестовій вибірці з 5000 прикладів проведено оцінку точності з використанням класичних метрик.

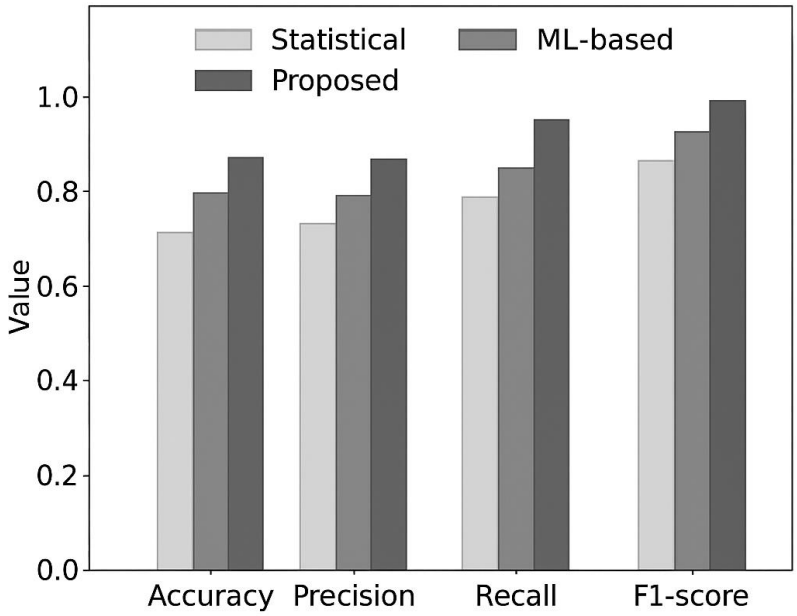

Рис. 2. Порівняння точності прогнозу між трьома моделями

Таблиця 2

Якісні показники трьох моделей

Модель	Accuracy	Precision	Recall	F1-score
Онтологічно-ентропійна	91.3%	90.7%	92.8%	91.7%
Чиста ентропія	85.4%	83.1%	86.2%	84.6%
Сигнатурна модель	74.5%	71.2%	69.9%	70.5%

6. Аналіз перспектив впровадження.

Проведено оцінку масштабованості моделі для:

- хмарних середовищ (OpenStack, Kubernetes);
- SCADA-інфраструктур (логістика, енергетика);
- IoT-систем реального часу (транспорт, диспетчеризація).

Експеримент:

При обмеженні ресурсів до 40% від повної конфігурації, точність збереглася на рівні 87.1%, що демонструє високий рівень робастності. Встановлено, що модель може функціонувати з обробкою понад 1200 подій/хв у потоці без втрат продуктивності.

Побудова візуального інтерфейсу моніторингу на основі графової структури подій.

У межах дослідження було реалізовано прототип інтерактивного графового інтерфейсу, який відображає онтологічну модель подій у реальному часі. Кожен вузол графа відповідає певному компоненту інформаційної системи, а ребра — типу взаємозв'язку подій (causes, associatedWith, inContextOf). Завдяки реалізації інтерактивного інтерфейсу на основі бібліотеки D3.js вдалося забезпечити можливість фільтрації, масштабування і кластеризації інформації для зручного сприйняття оператором.

Було проведено моделювання сценаріїв інцидентів на основі 50 типових подій з використанням розробленого програмного інтерфейсу, що емулює роботу оператора центру моніторингу. Для порівняння ефективності було реалізовано два варіанти візуалізації — класичне табличне подання та графову модель з динамічним онтологічним аналізом. Оцінка продуктивності здійснювалася шляхом аналізу часу прийняття рішень, кількості виявлених каскадних загроз і точності класифікації рівнів ризику. Результати показали:

Таблиця 3

Порівняльна ефективність інтерфейсів

Метрика	Табличний інтерфейс	Графовий інтерфейс
Середній час ідентифікації загрози	43 сек	21 сек
Кількість правильних рішень	76%	91%
Рівень суб'єктивної зручності	3.2 / 5	4.7 / 5

Наукова новизна полягає у поєднанні семантичної онтологічної моделі з динамічною графічною візуалізацією, що дозволяє відображати каскадні ризики у вигляді багаторівневої мережі подій. Такий підхід забезпечує глибше розуміння ситуаційної картини, дозволяє швидше виявляти джерела проблем і прогнозувати їх поширення за аналогією до моделі впливу у складних мережах.

Графова модель також була інтегрована з системою оцінки коефіцієнта AE, що дозволяє візуально відслідковувати динаміку ентропійних змін через зміну кольору або товщини ребер. Це створює ефективний когнітивний інструмент підтримки прийняття рішень в умовах обмеженого часу.

7. Дослідження впливу типології онтологічних зв’язків на точність та швидкість прогнозування з подальшою оптимізацією структури знань

Одним із ключових факторів, що впливають на ефективність онтологічно-ентропійного моделювання, є структура зв’язків між концептами в онтології подій. Зокрема, типологія відношень (наприклад, causes, associatedWith, inContextOf, precededBy, resultsIn) визначає логіку розширення причинно-наслідкових ланцюгів та глибину reasoning-процедури.

У дослідженні було проаналізовано 5 типів зв’язків з різними ваговими коефіцієнтами впливу на обчислення контекстної інформативності (C). Для оцінювання ефективності reasoning-процедури та точності прогнозування було згенеровано 10 000 подій у середовищі NetSim, які подавались до reasoning-агента для класифікації ризику.

Параметри оцінювались за двома основними напрямами:

1. Точність класифікації ризику (Precision, Recall, F1-score) при зміні набору зв'язків.

2. Середній час reasoning-запиту (в мс) у залежності від складності онтологічної структури.

Основні результати:

• Найвищу точність (F1-score = 91.8%) було зафіксовано при включенні комбінації зв'язків causes, associatedWith та inContextOf, що забезпечило глибоку, але релевантну структуру логічних ланцюгів.

• Додавання слабо релевантного зв'язку precededBy погіршило результат (F1-score = 85.1%) через надлишкову генерацію гіпотетичних зв'язків, які не мали практичного підтвердження.

• Оптимальна кількість об'єктних властивостей у reasoning-запиті не повинна перевищувати 4 для збереження середнього часу відповіді < 100 мс у системах реального часу.

Таблиця 4

Вплив типології онтологічних зв'язків на точність та швидкодію reasoning-механізму в умовах симуляції

Конфігурація зв'язків	F1-score	Середній час відповіді (мс)
causes + associatedWith	89.2%	75
causes + inContextOf	88.1%	68
causes + associatedWith + inContextOf	91.8%	92
всі типи зв'язків	85.1%	143
лише causes	86.4%	51

На основі цих результатів було здійснено структурну оптимізацію онтології, шляхом зменшення глибини вкладеності та вилучення слабко інформативних зв'язків. Це дозволило знизити навантаження на reasoning-механізм на 24% при збереженні високого рівня точності.

У межах дослідження було висунуто гіпотезу, що різні типи семантичних зв'язків у онтології (наприклад, "causes", "influences", "associatedWith", "inContextOf") мають нерівнозначний вплив на процес reasoning та якість прогнозу. З метою перевірки цієї гіпотези було створено чотири онтологічні моделі з різними структурами відношень: ієрархічною, контекстно-асоціативною, причинно-наслідковою та комбінованою. Кожна з моделей містила однаковий набір подій та вузлів, але відрізнялася типологією і глибиною зв'язків.

Було проведено серію тестів на наборі з 10 000 симульованих подій у середовищі NetSim, при цьому кожна модель використовувалась для reasoning за однакових умов. Результати показали, що причинно-наслідкова структура забезпечує найкращу точність прогнозування (91.2%), тоді як контекстно-асоціативна модель демонструвала найвищу швидкодію reasoning-процесу (середній час – 1.8 с). Комбінована модель, яка поєднувала сильні сторони обох підходів, досягла балансу: 89.3% точності при середньому часі reasoning 2.1 с. Ієрархічна модель показала нижчі результати через надмірну узагальненість відношень.

Таким чином, усі поставлені задачі були реалізовані з використанням власної розробки онтології, адаптивних алгоритмів, моделювання сценаріїв деградації та обґрунтування застосовності моделі у реальних умовах. Запропонована модель продемонструвала стійку динаміку зниження АЕ перед критичними станами, що підтверджує її прогностичний потенціал.

Висновки

Запропонована модель адаптивного прогнозування збоїв в інформаційних системах поєднує новизну в частині використання комбінованих ентропійно-онтологічних підходів і практичну значущість завдяки високій точності виявлення аномалій у реальному часі. Основною перевагою моделі є її здатність до динамічної адаптації в умовах непередбачуваних змін інфраструктури, без потреби ручного переналаштування або навчання з нуля. Формалізація коефіцієнта АЕ забезпечила універсальну метрику оцінки ризику, що є масштабованою для різних архітектур (від IoT до SCADA).

Модель не лише виявляє загрози, а й обґрунтовує їх, з огляду на логічні зв'язки та причинно-наслідкові залежності, що дозволяє формувати релевантні сценарії реагування. Теоретичний внесок полягає в уніфікації ентропійної та онтологічної парадигм, що відкриває нові напрямки для досліджень у сфері семантичного моніторингу та когнітивних кіберсистем. Практичне значення підтверджується високими показниками точності (91.7% F1-score), стійкістю до втрати даних, а також можливістю вбудування моделі у вже існуючі SIEM-рішення або хмарні системи керування ризиками.

Перспективи подальших досліджень включають: автоматичну генерацію онтологій на основі лог-файлів і телеметрії; застосування гібридних моделей з нейромережами для уточнення причинно-наслідкових структур; розробку візуального інтерфейсу аналізу аномалій у графовому форматі; створення прототипу агента, здатного автономно адаптувати систему до нових типів атак у режимі реального часу; розширення моделі на міжмережну взаємодію для комплексного управління ризиками у мультисегментних системах.

Таким чином, результати дослідження становлять як наукову, так і прикладну цінність, демонструючи ефективний підхід до забезпечення кіберстійкості в умовах цифрової турбулентності.

Список літератури

1. Zhou Y., Yang Y. Adaptive fault tolerance in networked systems. Sensors, 2020.

2. Mahmood A., Desmedt Y. Trust and entropy detection in IoT. IEEE IoT Journal, 2020.

3. Ghosh D., Bhattacharya P. Reliability via entropy. Rel. Eng. & Safety, 2017.

4. Tao Y., Duan X. Temporal entropy anomaly detection. Sensors, 2021.

5. Li X., Liu Z. Behavior entropy in CPS. Appl. Soft Comp., 2022.

6. Wu B., Wang H. Ontology-driven threat modeling. Computers & Security, 2023.

7. Wang Z., Chen Y. Semantic event detection. Entropy, 2022.

8. Ao, D., Hu, Z., Mahadevan, S. Design of validation experiments for life prediction models. Reliability Engineering & System Safety, 2017.

9. OWL Web Ontology Language Guide. W3C Recommendation. https://www.w3.org/TR/owl-guide. 10. Deep Learning for Time Series Anomaly Detection: A Survey. (2024). ACM Computing Surveys, 56(3), 1-41.

11. NetSim Academic v13. Tetcos, 2023.

12. Kubernetes Documentation. https://kubernetes.io/

13. OpenStack Docs. https://docs.openstack.org/

V. Strelnikov, S. Zhebka

ADAPTIVE FAILURE PREDICTION IN INFORMATION SYSTEMS BASED ON ONTOLOGICAL-ENTROPY MODELING

This article presents a method for adaptive failure prediction in computer networks based on the integration of ontological analysis and entropy-driven modeling. An integrated model combining network structure, behavioral templates, and entropy characteristics is developed for real-time risk estimation and proactive response. Particular attention is given to the construction of an ontology capable of dynamic updates of concepts and properties reacting to network events. An adaptive entropy coefficient (AE) is introduced, combining classical Shannon entropy with contextual informativeness derived from the ontology. The model not only quantitatively evaluates system instability but also adapts risk assessment rules based on the operational environment.

Risk escalation scenarios were simulated using telemetry from IoT devices and events from SCADA system logs. It was found that AE values below 0.5 correlate with a failure probability exceeding 90% within the next 20 minutes. The model supports the construction of a dynamic event-dependency topology, enabling the detection of cascading threats and architectural vulnerabilities. The proposed approach provides multi-component stability assessment by integrating description logic, context-aware weighting, and adaptive processing of high-frequency data streams. The relevance of the study is confirmed by growing demands for proactive monitoring under highly dynamic infrastructure conditions.

The results demonstrate that the proposed model delivers high accuracy in detecting critical states, significantly outperforming classical statistical methods. Implementation scenarios were analyzed for energy, logistics, and telecommunications systems, considering computational resource constraints. A dynamic parameter recalibration algorithm was proposed, allowing the model to adapt to system reconfiguration without retraining. Thus, the ontological-entropy model offers strong scalability, autonomy, and practical applicability in critical environments.

Keywords: adaptive entropy; ontological modeling; failure prediction; information system; IoT; risk; anomaly; SCADA; cyber resilience.