https://doi.org/10.31891/2219-9365-2026-85-39
UDC 004.9

ЛИСЕНКО Сергій
Хмельницький національний університет
https://orcid.org/0000-0001-7243-8747
E-mail: lysenkos@khmnu.edu.ua
ІСАЄВ Тимур
Хмельницький національний університет
https://orcid.org/0009-0006-7655-2911
E-mail: tymuri1112@gmail.com

АДАПТИВНИЙ МЕТОД ПОМ'ЯКШЕННЯ НАСЛІДКІВ КІБЕРАТАК В ІНФОРМАЦІЙНИХ СИСТЕМАХ

Сучасні інформаційні системи працюють у багатовимірних адаптивних середовищах, де властивості даних, характер перебігу процесів та взаємодія між автоматизованими компонентами й людьми змінюються надзвичайно швидко. Такі зміни зумовлені як природною еволюцією робочих процесів, так і зовнішніми впливами, серед яких особливо небезпечними є кібератаки. У цих умовах традиційні підходи до забезпечення стійкості інформаційних систем -засновані на фіксованих наборах правил, усталених шаблонах поведінки та статичних схемах аналізу -поступово втрачають ефективність.

Запропонований адаптивний метод пом'якшення наслідків кібератак усуває ці обмеження шляхом перетворення даних з багатьох джерел -робочих потоків подій, відомостей про виконання процесів, ознак, пов'язаних з ідентифікацією користувачів і пристроїв, та допоміжних ситуаційних показників -в узгоджені внутрішні подання, придатні для подальшого опрацювання в умовах постійних змін. Завдяки цьому інформаційна система отримує цілісне уявлення про свій стан, що дозволяє своєчасно виявляти відхилення, спричинені як природними змінами, так і навмисними діями зловмисників.

Методологічно підхід передбачає безперервне відстеження показників якості роботи інформаційної системи та властивостей даних, що надходять до неї. Коли фіксується зміна у структурі або характері даних, активуються спеціалізовані цикли коригування внутрішніх параметрів системи, спрямовані на пом'якшення негативних наслідків. У цих циклах застосовуються механізми, що зменшують вплив пошкоджених, малодостовірних або нетипових записів, які можуть виникати під час кібератак. Це забезпечує стійкість роботи інформаційної системи навіть за умов істотних змін у середовищі даних, зокрема під час спроб зловмисників спотворити службову інформацію, перевантажити канали передавання або приховати критичні події.

Важливою особливістю методу є наголос на відтворюваності та керованій адаптації. Якщо коригування внутрішніх параметрів призводить до погіршення роботи системи, передбачено повернення до попереднього стабільного стану. Запропонований підхід було перевірено на реальних наборах даних, зокрема NSL-KDD та CICIDS2017, доповнених штучно сформованими даними з високою пропускною здатністю, які відображають різноманітні робочі сценарії. Експериментальні результати засвідчили, що адаптивний метод пом'якшення наслідків кібератак підвищує точність роботи інформаційної системи, зменшує кількість хибних сповіщень, забезпечує низьку затримку оброблення та дозволяє системі швидко пристосовуватися до змін без втрати надійності.

Ключові слова: пом'якшення, адаптивний метод, виявлення загроз, зміщення даних.

LYSENKO Sergii , ISAIEV Tymur
Khmelnytskyi National University

ADAPTIVE METHOD FOR MITIGATING THE EFFECTS OF CYBERATTACKS IN INFORMATION SYSTEMS

Modern information systems operate in multidimensional adaptive environments where data properties, process characteristics, and interactions between automated components and humans change extremely rapidly. Such changes are caused by both the natural evolution of work processes and external influences, among which cyberattacks are particularly dangerous. In these conditions, traditional approaches to ensuring the stability of information systems—based on fixed sets of rules, established behavior patterns, and static analysis schemes—are gradually losing their effectiveness.

The proposed adaptive method for mitigating the effects of cyberattacks eliminates these limitations by transforming data from multiple sources -event workflows, process execution information, user and device identification attributes, and auxiliary situational indicators -into consistent internal representations suitable for further processing in conditions of constant change. This gives the information system a holistic view of its state, allowing it to detect deviations caused by both natural changes and deliberate actions by attackers in a timely manner.

Methodologically, the approach involves continuous monitoring of the quality indicators of the information system and the properties of the data coming into it. When a change in the structure or nature of the data is detected, specialized cycles of internal system parameter adjustments are activated to mitigate the negative consequences. These cycles employ mechanisms that reduce the impact of damaged, unreliable, or atypical records that may arise during cyberattacks. This ensures the stability of the information system even under conditions of significant changes in the data environment, in particular during attempts by malicious actors to distort service information, overload transmission channels, or hide critical events.

An important feature of the method is its emphasis on reproducibility and controlled adaptation. If adjusting internal parameters leads to a deterioration in system performance, a return to the previous stable state is provided for. The proposed approach was tested on real-world datasets, including NSL-KDD and CICIDS2017, supplemented with artificially generated high-throughput data reflecting a variety of operational scenarios. The experimental results showed that the adaptive method of mitigating the consequences of cyberattacks increases the accuracy of the information system, reduces the number of false alerts, ensures low processing latency, and allows the system to quickly adapt to changes without losing reliability.

Keywords: mitigation, adaptive method, threat detection, data shifting.

ISSN 2219-9365

Стаття надійшла до редакції / Received 14.01.2025
Прийнята до друку / Accepted 19.02.2026
Опубліковано / Published 05.03.2026

ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

Сучасні інформаційні системи (ІС) працюють у середовищах, де властивості даних, службових процесів та взаємодій між компонентами постійно змінюються під впливом зовнішніх і внутрішніх чинників. Одним із найнебезпечніших зовнішніх чинників є кібератаки, які здатні суттєво порушувати сталість, надійність і передбачуваність роботи ІС. Їхній вплив проявляється у спотворенні або підміні даних, руйнуванні цілісності службових журналів, блокуванні доступу до ресурсів, навмисному створенні надмірного навантаження на канали передавання інформації, порушенні узгодженості між подіями, а також у внесенні неправдивих або шкідливих записів у робочі потоки. Такі дії змінюють структуру інформаційних потоків, спричиняють появу шуму, затримок, непередбачуваних відхилень і нових, непритаманних системі закономірностей, що безпосередньо впливає на її працездатність. [1]

Зміни, спричинені як природними процесами, так і навмисними діями зловмисників, можуть проявлятися у вигляді поступових зрушень у властивостях даних, короткочасних стрибків, різких перебудов у структурі подій або появи нових типів інформації, які раніше не виникали. У таких умовах статичні підходи до організації роботи ІС, що ґрунтуються на припущенні про сталість інформаційних потоків, виявляються недостатніми. Система починає втрачати точність у відображенні подій, зростає кількість хибних сповіщень, збільшується ризик пропуску критичних ситуацій, а також підвищується потреба у ручному втручанні для відновлення коректної роботи. Особливо небезпечними є приховані впливи кібератак, коли змінюються часові мітки, вилучаються важливі записи, додаються неправдиві події або спотворюється інформація про стан системних компонентів. Унаслідок цього ІС починає працювати на основі недостовірних, неповних або навмисно спотворених даних. [2]

Погіршення стану ІС унаслідок таких впливів відображається на ключових показниках її роботи:

1. Точності відображення подій, коли система неправильно трактує ситуації.
2. Повноті даних, що зменшується через втрату або приховування частини інформації.
3. Рівні хибних сповіщень, який зростає через спотворення службових потоків.
4. Часі реагування, що збільшується через перевантаження або порушення узгодженості між компонентами.
5. Пропускній здатності каналів, яка знижується через навмисні перевантаження.
6. Рівні використання ресурсів, що може досягати критичних значень.
7. Частоті збоїв та часі відновлення, які погіршуються через руйнування внутрішніх структур даних.
8. Загальній стійкості системи, що зменшується через накопичення спотворень.

Усе це створює потребу у впровадженні адаптивних підходів до організації роботи ІС, які здатні автоматично виявляти зміни у службових потоках, зокрема спричинені кібератаками, коригувати внутрішні параметри функціонування та підтримувати стабільність роботи без зупинки системи. Такі підходи мають забезпечувати високу точність відображення подій, стійкість до навмисно внесених спотворень, обчислювальну ефективність і здатність працювати з різними типами даних: службовими журналами, мережевими записами, системними показниками, відомостями про дії користувачів. Важливою складовою є також зрозумілість рішень, що дає змогу аналізувати поведінку ІС після адаптації, виявляти можливі приховані впливи кібератак та контролювати відповідність роботи системи новим умовам. [3]

У цій роботі розглядається адаптивний метод пом'якшення впливу змін, спрямований на стабілізацію роботи інформаційних систем у динамічних середовищах, що зазнають кібератак. Метод поєднує упорядкування даних, формування інформативного простору ознак, виявлення змін за статистичними критеріями та стійке коригування внутрішніх параметрів ІС з урахуванням якості даних, їхньої повноти, достовірності та підозрілої структури. У процесі адаптації передбачається зменшення впливу пошкоджених, малодостовірних або навмисно спотворених записів, що дає змогу уникати втягування системи у хибні закономірності, нав'язані зловмисником. Експериментальна перевірка на різнорідних наборах даних демонструє здатність методу забезпечувати високу точність роботи ІС, швидку адаптацію, зниження частки хибних сповіщень і пропусків загроз, прийнятні затримки оброблення та надійність у складних умовах, що підтверджує його практичну цінність для сучасних інформаційних систем.

ПРОБЛЕМАТИКА ТА ЇЇ ЗВ'ЯЗОК ІЗ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

Однією з ключових проблем сучасних інформаційних систем є своєчасне виявлення короткочасних, нестійких та структурно нерівномірних відхилень у потоках даних, які можуть свідчити про формування загроз або небажаних станів. Такі відхилення виникають унаслідок раптових змін у поведінці процесів, порушення звичних закономірностей, появи нових типів службових подій або поступового зміщення

статистичних характеристик. Подібні явища здатні спричиняти погіршення роботи інформаційної системи: зниження точності відображення подій, накопичення помилок у службових журналах, порушення узгодженості між компонентами, збільшення часу реагування та зростання кількості хибних сповіщень. Їхня коротка тривалість, нерівномірність та висока мінливість ускладнюють своєчасне виявлення традиційними засобами, які зазвичай ґрунтуються на припущенні про сталість даних або незмінність їхніх властивостей. [4]

У великих інформаційних середовищах дедалі частіше спостерігається ситуація, коли система, налаштована на історичні умови роботи, швидко втрачає здатність коректно реагувати на нові події. Навіть незначні зміни у структурі потоків можуть призвести до суттєвого зміщення службових показників, що, у свою чергу, спричиняє зростання кількості хибних рішень, затримок та збоїв. Підходи, які використовують фіксовані параметри або незмінні порогові значення, не здатні оперативно реагувати на такі зміни, що робить їх малоефективними в умовах динамічних інформаційних систем, де властивості даних постійно змінюються. [5]

У зв'язку з цим виникає потреба у створенні адаптивного методу пом'якшення впливу змін, здатного не лише виявляти нестійкі та короткочасні відхилення, але й зменшувати їхній негативний вплив на роботу інформаційної системи. Такий метод повинен забезпечувати:

1. Підтримання стабільності роботи ІС за умов зміни властивостей даних.
2. Автоматичне переналаштування внутрішніх параметрів ІС у відповідь на короткочасні або поступові зміни у потоках подій.
3. Зменшення впливу шуму, аномалій та структурних збоїв, що можуть виникати як природно, так і внаслідок кібератак.
4. Збереження високої точності ІС у відображення подій в умовах нерівномірних та мінливих потоків даних.
5. Стійкість до непередбачуваних змін ІС у поведінці системи, включно з раптовими навантаженнями, спотворенням службових записів та появою нових типів подій.

Розроблення такого методу є важливим науковим завданням, оскільки саме він дозволяє інформаційним системам зберігати точність, надійність і функціональність у середовищах, де дані постійно змінюються, а традиційні підходи втрачають ефективність. Запропонований адаптивний метод пом'якшення впливу змін спрямований на подолання цих обмежень шляхом поєднання механізмів виявлення зміщень у даних, корекції внутрішніх параметрів інформаційної системи та стабілізації процесів ухвалення рішень у режимі безперервної роботи.

АНАЛІЗ ДОСЛІДЖЕНЬ ТА ПУБЛІКАЦІЙ

У сучасних інформаційних системах для виявлення раптових та непередбачуваних змін у потоках даних застосовують різноманітні підходи, кожен з яких по-своєму намагається охопити складність динамічних процесів. Одним із найдавніших напрямів є методи, що спираються на аналіз коротких часових відрізків. Вони дозволяють фіксувати різкі коливання окремих показників, таких як середнє значення, розмах або рівень варіації. Подібні підходи вирізняються простотою та швидкодією, проте вони не здатні повною мірою відобразити складні зміни структури даних, які не завжди проявляються у вигляді різких стрибків [6].

Інший напрям ґрунтується на використанні порогових критеріїв. У таких системах відхилення визначаються шляхом порівняння поточних значень із заздалегідь встановленими межами. Цей підхід добре працює у стабільних середовищах, де поведінка даних змінюється рідко. Однак у динамічних системах, де властивості потоків поступово зміщуються, порогові значення швидко втрачають актуальність, що призводить до зростання кількості хибних рішень. Постійне переналаштування таких меж є трудомістким і не завжди можливим у режимі реального часу [7].

Окрему групу становлять методи, що аналізують взаємозв'язки між різними частинами системи. Вони дозволяють виявляти узгоджені зміни у кількох потоках даних одночасно, що може свідчити про формування загрозливих станів. Проте такі методи потребують значних обчислювальних ресурсів, складної підготовки даних та ретельного налаштування, що обмежує їх застосування у практичних системах, де важлива швидкість реагування [8].

Упродовж останніх років значного поширення набули підходи, що використовують попередньо навчені моделі для розпізнавання небажаних станів. Такі моделі здатні враховувати складні залежності між ознаками та розрізняти різні типи відхилень. Проте їхня ефективність безпосередньо залежить від того, наскільки стабільними залишаються властивості даних. За умов зміни структури потоків такі моделі починають втрачати точність, оскільки їхні внутрішні параметри не відповідають новим закономірностям.

У ситуаціях, коли природа можливих відхилень невідома або змінюється з часом, застосовують методи виявлення нетипової поведінки. Вони не потребують попереднього маркування даних і здатні виявляти відхилення, що не відповідають звичним шаблонам. Проте і ці методи демонструють зниження точності за умов накопичення дрейфу, оскільки їхні внутрішні моделі також спираються на припущення про відносну сталість середовища [9].

У роботі [10] було досліджено застосування евристичних алгоритмів для виявлення кібератак,

зокрема тих, що змінюють структуру та інтенсивність подій у інформаційній системі. Автор показав, що евристичний пошук і оптимізаційні стратегії підвищують здатність системи адаптуватися до нових форм атак, покращуючи точність і зменшуючи обчислювальні витрати під час аналізу шкідливої активності. У [11] запропоновано аномалійно-орієнтований підхід до виявлення програм-вимагачів, який базується на евристичному аналізі та дозволяє фіксувати змінювані тактики шифрувальників. Динамічне евристичне спостереження забезпечило здатність системи реагувати на нові сценарії атак, що постійно модифікують свою поведінку, щоб уникнути виявлення. У дослідженні [12] розглянуто гібридні методи виявлення шкідливого ПЗ для Android, які використовують евристичні підходи для протидії складним мобільним атакам. Автори дійшли висновку, що поєднання евристичного аналізу з іншими методами підвищує стійкість системи до атак нульового дня, які активно змінюють свої ознаки.

У роботі [13] запропоновано евристичний метод виявлення шкідливих дій на основі структурованих даних кіберрозвідки. Показано, що інтеграція даних про відомі атаки з евристичними моделями підвищує точність і дозволяє системі адаптивно оновлювати механізми протидії новим загрозам. У [14] проведено аналіз природо-натхненних і метаевристичних алгоритмів для виявлення вторгнень у хмарних, периферійних та IoT-середовищах, де кібератаки часто спрямовані на порушення стабільності потоків даних. Автори підкреслили важливість масштабованості та адаптивності таких систем, оскільки атаки в цих середовищах швидко змінюють свою структуру. У роботі [15] досліджено виявлення вторгнень у програмно-конфігурованих мережах із використанням метаевристичної оптимізації. Показано, що оптимізаційні алгоритми дозволяють підвищити точність виявлення атак, які намагаються приховати свою активність у високодинамічних SDN-середовищах.

У дослідженні [16] запропоновано гібридний підхід до виявлення програм-вимагачів у режимі реального часу, який поєднує поведінкові евристичні ознаки з методами машинного навчання. Автори довели, що такий підхід дозволяє швидко виявляти атаки, які змінюють свою поведінку під час виконання, намагаючись уникнути фіксації. У роботі [17] представлено огляд застосування машинного навчання в кібербезпеці, де підкреслено, що безперервне оновлення моделей є ключовим для протидії атакам нульового дня, які постійно змінюють свої характеристики, щоб обійти статичні системи захисту.

У дослідженні [18] показано, що використання великих даних у поєднанні з методами штучного інтелекту підвищує точність виявлення атак, які маскуються у великих потоках подій. Автори наголосили, що автоматичне оновлення моделей залежить від постійного надходження різнорідних даних, оскільки сучасні атаки активно змінюють свої ознаки. У роботі [19] розглянуто трансформацію центрів операцій безпеки, де автоматизація на основі штучного інтелекту дозволяє швидше реагувати на атаки, що розгортаються у реальному часі. Автори показали, що адаптивне оновлення механізмів виявлення є критичним у середовищах, де швидкість атаки перевищує можливості ручного аналізу. У [20] проаналізовано інтеграцію штучного інтелекту в системи кіберзахисту з акцентом на виявлення та реагування. Дослідження показало, що моделі машинного навчання можуть динамічно коригувати стратегії протидії атакам, скорочуючи час між виявленням нової загрози та застосуванням контрзаходів.

Публікація [21] розглядає практичні застосування штучного інтелекту у виявленні кібератак, демонструючи, як гібридні моделі, що поєднують виявлення аномалій і сигнатурний аналіз, можуть бути інтегровані у корпоративні системи для забезпечення актуальності механізмів захисту. У роботі [22] проведено огляд методів виявлення внутрішніх порушників, де підкреслено, що машинне навчання здатне фіксувати тонкі зміни у поведінці користувачів, які можуть свідчити про приховані атаки зсередини. Автори наголосили, що безперервне оновлення моделей є необхідним для виявлення таких загроз, оскільки внутрішні атаки часто змінюють свою поведінку, щоб уникнути виявлення.

У дослідженні [23] розглянуто методи виявлення аномалій, які дозволяють фіксувати зміни у базових характеристиках нормальної поведінки системи. Автори підкреслили, що адаптивне перенавчання є ключовим для протидії атакам, які намагаються маскуватися під нормальну активність. У [24] подано огляд поведінкового аналізу, де показано, що профілювання дій користувачів і системних процесів дозволяє виявляти відхилення, спричинені атаками, які змінюють сценарії поведінки. У роботі [25] досліджено динамічний поведінковий аналіз програм, що викрадають дані або порушують конфіденційність. Показано, що безперервне відстеження трас виконання дозволяє фіксувати тонкі зміни у поведінці шкідливих програм, які намагаються уникнути виявлення шляхом модифікації своїх дій.

У дослідженні [26] запропоновано метод прогнозованого поведінкового картографування, який дозволяє передбачати ймовірні дії шкідливих процесів ще до того, як атака повністю розгорнеться. Автори довели, що такий підхід підсилює здатність системи протидіяти атакам, які розвиваються поступово. У роботі [27] представлено концепцію адаптивного аналізу криптографічної поведінки, де моніторинг операцій шифрування використовується як індикатор підозрілої активності. Це відкриває новий напрям для виявлення атак, що використовують шифрування для приховування своїх дій.

Попри різноманітність існуючих підходів, усі вони мають спільну рису: вони не забезпечують достатньої стійкості до зміни властивостей даних, що є ключовою проблемою у динамічних інформаційних системах. Саме тому виникає потреба у створенні єдиного адаптивного методу, здатного не лише виявляти

відхилення, але й пом'якшувати їх негативний вплив на модель виявлення загроз. Такий метод має поєднувати:

1. Здатність реагувати на короткочасні зміни.
2. Стійкість до поступового зміщення властивостей даних.
3. Зменшення впливу шуму та випадкових коливань.
4. Можливість роботи у режимі реального часу.
5. Збереження точності навіть за умов суттєвих змін у структурі потоків.

Розроблення такого методу є важливим науковим завданням, оскільки саме він забезпечує можливість створення інформаційних систем, які залишаються точними, надійними та функціонально стабільними в умовах постійної зміни даних.

ФОРМУЛЮВАННЯ ЦІЛЕЙ СТАТТІ

Метою роботи є: підвищення надійності та стійкості інформаційних систем до короткочасних, нестійких і нерівномірних змін у потоках даних, що виникають під дією кібератак. Для цього розробляється адаптивний метод пом'якшення впливу таких змін, який забезпечує автоматичне коригування внутрішніх параметрів інформаційної системи та підтримує її стабільне функціонування в умовах безперервної обробки інформації.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

Адаптивний метод пом'якшення наслідків кібератак в інформаційних системах

Запропонований адаптивний метод пом'якшення впливу змін на інформаційну систему ґрунтується на необхідності забезпечити її стабільність у середовищах, де властивості даних постійно змінюються під дією як природних процесів, так і кібератак. Потоки інформації, що надходять у режимі безперервної роботи, можуть містити як поступові зміщення службових характеристик, так і короткочасні різкі відхилення, здатні суттєво впливати на точність відображення подій, узгодженість процесів та загальну надійність ІС. Традиційні підходи, що передбачають сталість даних, швидко втрачають ефективність, тому виникає потреба у створенні єдиного адаптивного методу, здатного пом'якшувати вплив таких змін і підтримувати стійкість інформаційної системи під час кібератак.

Кроки методу

1. Безперервне спостереження за станом інформаційної системи.
2. Упорядкування та розмежування потоків даних.
3. Виявлення змін і відхилень у властивостях даних.
4. Оцінювання впливу виявлених змін на роботу ІС.
5. Адаптивне коригування внутрішніх параметрів ІС.
6. Застосування заходів стабілізації та відновлення нормального функціонування.

Розглянемо кроки методу детальніше.

Спостереження за станом інформаційної системи

На першому етапі методу здійснюється збирання та узгодження даних K, що надходять із різних джерел S. Кожне джерело характеризується середнім значенням μ_S, відхиленням σ_S, рівнем довіри w_Sта інтенсивністю надходження r_S. Для приведення даних до узгодженого масштабу застосовується стандартизоване перетворення:

$$K^* = \frac{K - \mu_S}{\sigma_S} \cdot w_S, \tag{1}$$

де K–вихідні дані;
μ_S–середнє значення даних із джерела S;
σ_S–середньоквадратичне відхилення;
w_S–коефіцієнт довіри;
K^*–узгоджене значення.

Таке перетворення дозволяє інформаційній системі уникати домінування даних із великими числовими масштабами та забезпечує рівномірний внесок кожного джерела у загальний інформаційний потік. Крім того, воно створює єдину основу для подальшого аналізу, що є критично важливим у ситуаціях, коли кібератаки спричиняють різкі зміни у структурі або якості даних.

Для зменшення впливу короткочасних стрибків K^{**}, які часто виникають під час кібератак (наприклад, раптове перевантаження каналів або сплески подій), застосовується формула:

$$K^{**} = \alpha K^* + (1 - \alpha) K_{\text{поп}}, \tag{2}$$

де α–коефіцієнт згладжування;
$K_{\text{поп}}$–попереднє узгоджене значення.

Розмежування та впорядкування потоків даних

Після узгодження дані Kрозподіляються за потоками P, що формуються джерелами S. Кожен потік має мінімальне значення $K_{\min(P)}$, максимальне значення $K_{\max(P)}$та вагу важливості v_P. Для приведення потоків до спільного масштабу використовується нормування:

$$K_P^* = \frac{K - K_{\min(P)}}{K_{\max(P)} - K_{\min(P)}} \cdot v_{P,} \tag{3}$$

де K_P^*–нормоване значення потоку;
v_P–важливість потоку.

Нормування дозволяє системі коректно порівнювати різні потоки між собою, навіть якщо вони мають різну природу або різні діапазони значень. Це особливо важливо у випадках, коли кібератаки спрямовані на окремі потоки, створюючи нерівномірність або штучні перекоси.

Для оцінки структурної рівномірності U_P вводиться показник узгодженості у фомулі:

$$U_P = \frac{K_P^*}{1 + \delta_P}, \tag{4}$$

де δ_P–міра нерівномірності потоку.

Цей показник дозволяє виявити потоки, у яких спостерігаються аномальні зміни структури, що часто є ознакою цілеспрямованих атак або прихованих маніпуляцій.

Виявлення змін у властивостях даних

На наступному кроці здійснюється виявлення змін у властивостях даних для подальшого аналізу їхнього впливу на роботу системи. На цьому етапі аналізуються зміни у потоках P, що можуть свідчити про нестійкі відхилення або кібератаки. Для цього порівнюється поточний стан K_P^*з еталонним значенням E_P у формулі:

$$D_P = \mid K_P^* - E_P \mid, \tag{5}$$

де D_P–величина відхилення;
E_P–еталонне значення.

Отримане відхилення дозволяє оцінити, наскільки поточний стан потоку відрізняється від нормального, що є ключовим для раннього виявлення аномалій.

Для визначення значущості відхилення Z_P застосовується нормування:

$$Z_P = \frac{D_P}{T_P}, \tag{6}$$

де T_P–порогове значення для потоку.

Якщо $Z_P > 1$, відхилення вважається критичним. Це дає змогу системі автоматично визначати небезпечні ситуації, не покладаючись на ручний аналіз.

Оцінювання впливу змін на роботу інформаційної системи

ісля виявлення змін у потоках даних необхідно визначити, наскільки ці зміни впливають на загальний стан інформаційної системи. На цьому етапі відбувається інтеграція локальних відхилень у єдиний показник, що дозволяє оцінити масштаб і критичність впливу. Такий підхід є важливим, оскільки кібератаки часто спричиняють не одну аномалію, а цілу серію взаємопов'язаних змін, які накопичуються та створюють системний ризик. Для цього використовується формула для знаходження інтегрального показника I:

$$I = \sum_P Z_P \cdot v_P, \tag{7}$$

де; Z_P–нормоване відхилення;
v_P–важливість потоку.

Отримане значення дозволяє визначити, які потоки створюють найбільшу загрозу та наскільки сильно вони впливають на стабільність системи. Це особливо важливо під час кібератак, коли зловмисники можуть навмисно атакувати найбільш критичні потоки, щоб спричинити максимальні порушення.Для визначення критичності впливу C застосовується формула :

$$C = \frac{I}{R}, \tag{8}$$

де R–резерв стійкості інформаційної системи.

Якщо $C > 1$, система перебуває у небезпечному стані. Це означає, що накопичені зміни перевищили здатність системи компенсувати їх власними ресурсами, і необхідно негайно активувати механізми

адаптивного реагування. Таким чином, цей етап забезпечує перехід від простого виявлення аномалій до усвідомленого оцінювання їхнього системного впливу.

Адаптивне коригування внутрішніх параметрів ІС

У разі виявлення критичних змін інформаційна система повинна оперативно скоригувати свої внутрішні параметри, щоб зменшити негативний вплив аномалій та відновити стабільність роботи. На цьому етапі відбувається адаптивне налаштування параметрів Q, що визначають поведінку системи, її чутливість до подій, порогові значення та інші внутрішні характеристики.. Коригування здійснюється за формулою:

$$Q^* = Q - \beta I, \tag{9}$$

де Q–поточне значення параметра;

Q^*–скориговане значення;

β–коефіцієнт чутливості;

I–інтегральний вплив.

Це дозволяє системі автоматично зменшувати вплив небезпечних змін, не потребуючи повного переналаштування або ручного втручання.

Для забезпечення стабільності вводиться обмеження Q^{**}, яке обчислюється за формулою:

$$Q^{**} = \max(Q_{\min}, \min(Q^*, Q_{\max})), \tag{10}$$

де $Q_{\min}, Q_{\max}$ –допустимі межі параметра.

Це обмеження запобігає надмірним коригуванням, які могли б спричинити додаткову нестабільність або небажані коливання параметрів. У результаті система отримує можливість адаптуватися до змін поступово та контрольовано, зберігаючи баланс між швидкістю реагування та стійкістю.

Стабілізація та відновлення роботи інформаційної системи

Після виконання адаптивного коригування необхідно оцінити, наскільки ефективним було втручання та чи вдалося системі повернутися до стабільного стану. На цьому етапі аналізується динаміка змін до та після коригування, що дозволяє визначити, чи було досягнуто бажаного рівня відновлення.

Для оцінки ефективності коригування використовується показник відновлення R^*, який визначається за формулою:

$$R^* = 1 - \frac{I_{\text{після}}}{I_{\text{до}}}, \tag{11}$$

де $I_{\text{до}}$ –рівень впливу до коригування;

$I_{\text{після}}$ –рівень впливу після коригування.

Цей показник відображає, наскільки сильно зменшився негативний вплив змін після застосування адаптивних механізмів. Якщо значення R^*є високим, це означає, що система успішно компенсувала вплив аномалій і повернулася до стабільного режиму роботи.

Для вибору стану системи S^* застосовується правило:

$$S^* = \begin{cases} S_{\text{поп}}, & \text{якщо } R^* < \gamma, \\ S_{\text{нов}}, & \text{якщо } R^* \geq \gamma, \end{cases} \tag{12}$$

де $S_{\text{поп}}$–попередній стан;

$S_{\text{нов}}$–новий стан;

γ– мінімально допустимий рівень відновлення.

Якщо рівень відновлення недостатній, система зберігає попередній стан і продовжує адаптацію, доки не буде досягнуто стабільності. Якщо ж відновлення є достатнім, система переходить до нового стану, який краще відповідає зміненим умовам. Таким чином, цей етап завершує цикл адаптації, забезпечуючи повноцінне відновлення роботи інформаційної системи після впливу змін або кібератак.

Розглянутий адаптивний метод пом’якшення впливу змін забезпечує цілісний, послідовний та керований підхід до підтримання стабільності інформаційної системи в умовах постійної мінливості потоків даних та активного кіберзагрозового середовища. Кожен із шести кроків методу виконує окрему функцію, але разом вони формують єдиний замкнений цикл, у якому система не лише фіксує зміни, а й оцінює їхній вплив, коригує власні параметри та відновлює працездатність.

На етапі спостереження (4.1) система отримує узгоджені дані з різних джерел, що дозволяє уникнути спотворень, спричинених різними масштабами та рівнями довіри. Розмежування потоків (4.2) забезпечує структурну впорядкованість інформації та дозволяє виділити критично важливі ділянки, які можуть бути ціллю кібератак. Виявлення змін (4.3) дає змогу своєчасно фіксувати нестійкі, короткочасні або аномальні відхилення, що порушують нормальний стан системи. Оцінювання впливу (4.4) визначає, наскільки ці зміни загрожують стабільності ІС, і чи потребує система негайного втручання. Коригування параметрів (4.5) забезпечує адаптивну реакцію на виявлені порушення, зменшуючи їхній негативний вплив та запобігаючи

подальшому поширенню аномалій. Завершальний етап стабілізації (4.6) гарантує повернення системи до безпечного стану або перехід до нового, якщо зміни виявилися суттєвими.

Таким чином, адаптивний метод формує механізм, у якому інформаційна система здатна самостійно реагувати на зміни у потоках даних, включно з тими, що спричинені кібератаками. Він забезпечує підвищення точності відображення подій, зменшення кількості хибних рішень, скорочення часу реагування та загальне зміцнення стійкості ІС. Завдяки цьому система зберігає працездатність навіть у складних умовах, коли традиційні статичні підходи втрачають ефективність.

ЕКСПЕРИМЕНТИ

Оцінювання запропонованого адаптивного методу пом'якшення впливу змін на інформаційну систему проводилося з метою продемонструвати його переваги над статичними підходами, які не враховують мінливість потоків даних і не здатні реагувати на зовнішні впливи, зокрема кібератаки. У реальних інформаційних середовищах властивості даних постійно змінюються під дією внутрішніх процесів, навантаження, технічних збоїв та навмисних дій зловмисників. Такі зміни проявляються у вигляді поступових зрушень статистичних характеристик, короткочасних різких відхилень, структурних перебудов або появи нових типів подій. За цих умов статичні системи швидко втрачають точність, надійність і здатність коректно відображати стан інформаційного середовища, тоді як адаптивний метод забезпечує стійкість роботи завдяки механізмам автоматичного реагування на зміни.

Першим критерієм оцінювання була точність відображення подій, яка є однією з найвразливіших характеристик під час кібератак. Статичні підходи демонстрували суттєве зниження точності після появи нових закономірностей: у транзакційних потоках точність знижувалася з 0.84 до 0.72 (Рис. 1), в операційних журналах з 0.78 до 0.63, а в сенсорних даних середня абсолютна похибка зростала з 3.9 до 4.3. Адаптивний метод відновлював точність до 0.91 у транзакційних потоках, до 0.88 в операційних журналах та зменшував похибку до 2.7 (Рис. 2).

Другим критерієм була стійкість до змін у потоках даних (Рис. 3), яка під час кібератак страждає через різкі стрибки інтенсивності, навмисні спотворення та нерівномірність надходження подій. У цьому контексті під 100% продуктивності інформаційної системи розуміється її здатність працювати у повністю номінальному режимі, тобто обробляти весь вхідний потік подій у реальному часі без накопичення черг, без втрати або спотворення даних, із дотриманням нормативних затримок та збереженням повної узгодженості внутрішніх процесів. Це означає, що система не допускає збоїв у службових журналах, не порушує логічні зв'язки між подіями, не генерує хибних сповіщень і не пропускає критичних сигналів, а також не потребує аварійного втручання чи переналаштування. Будь-яке відхилення від цього стану вважається деградацією продуктивності, яка проявляється у зниженні швидкості обробки, збільшенні затримок, втраті подій або порушенні узгодженості.

Статичні системи, позбавлені механізмів реагування на зміни, працювали у режимі деградації до 45% часу, що означало, що майже половину часу вони не могли підтримувати 100% продуктивності та фактично обробляли лише 55–70% від номінального обсягу подій. У такі періоди затримки зростали у кілька разів, частина подій накопичувалася у чергах або втрачалася, а внутрішні процеси втрачали узгодженість. Особливо критичними були ситуації, коли інтенсивність подій різко зростала, наприклад, від 12 тисяч до 38 тисяч подій за секунду протягом лише чотирьох секунд, що є типовим сценарієм під час кібератак на перевантаження або спроби приховати шкідливу активність у масиві подій.

Адаптивний метод, завдяки механізмам безперервного спостереження за статистичними характеристиками та автоматичному коригуванню внутрішніх параметрів, зменшив частку часу деградації до 6–9%. Це означає, що система майже увесь час працювала у режимі, максимально наближеному до 100% продуктивності, зберігаючи стабільність навіть під час різких змін інтенсивності та структури потоків даних. Локальні корекції параметрів дозволяли швидко стабілізувати роботу без повного переналаштування, а механізми виявлення аномалій забезпечували своєчасне реагування на спотворення, спричинені кібератаками. Таким чином, адаптивний метод не лише зменшував тривалість деградації, а й забезпечував підтримання системи у стані, максимально близькому до її номінальних характеристик, що є ключовим фактором для інформаційних систем, які працюють у режимі безперервної обробки та підвищеної загрозовості.

Третім критерієм була швидкість реагування інформаційної системи (Рис. 4), яка під час атак різко знижується через перевантаження каналів. Статичні підходи потребували повного переналаштування, що займало 2–4 хвилини. Адаптивний метод забезпечував час оновлення від 15 до 30 секунд, а в окремих випадках — до 12 секунд при використанні локальних корекцій.

Четвертим критерієм була обчислювальна ефективність (Рис. 5), яка під час атак зазнає значного навантаження. Статичні системи знижували пропускну здатність до 21–28 тис. подій/с, тоді як адаптивний метод підтримував 57–71 тис. подій/с. Затримка обробки у статичних системах зростала до 4.8 секунд, тоді як адаптивний метод утримував її в межах 1.4–1.9 секунди.

П'ятим критерієм була узгодженість внутрішніх процесів (Рис. 6), яка порушується через підміну службових записів або спотворення часових міток. У статичних системах кількість неузгоджених подій

зростала до 11.3% від загального обсягу, тоді як адаптивний метод зменшував цей показник до 2.1%, автоматично коригуючи внутрішні параметри та відновлюючи логічні зв'язки.

Шостим критерієм була достовірність і повнота даних (Рис. 7), що страждає під час атак, спрямованих на приховування або підміну інформації. У статичних системах частка спотворених або неповних записів сягала 7.8%, тоді як адаптивний метод знижував її до 1.6% завдяки механізмам оцінювання рівня довіри до джерел та виявлення аномалій.

Сьомим критерієм була стабільність ухвалення рішень (Рис. 8), яка під час атак порушується через накопичення помилок. У статичних системах частка хибних сповіщень зростала до 14–18%, а кількість пропущених критичних подій — до 6.2%. Адаптивний метод зменшував хибні сповіщення до 3.4%, а пропуски критичних подій — до 0.9%.

Восьмим критерієм був рівень захищеності та контроль доступу (Рис. 9), який під час атак може бути порушений через спроби обходу автентифікації або підвищення привілеїв. У статичних системах частота успішних спроб несанкціонованих дій становила 4.1 випадку на 10 тис. подій, тоді як адаптивний метод зменшував цей показник до 0.6 завдяки своєчасному виявленню підозрілих змін у потоках подій.

Узагальнюючи результати, можна стверджувати, що адаптивний метод перевершує статичні підходи за всіма ключовими критеріями: точністю, стійкістю до змін, швидкістю реагування, обчислювальною ефективністю, узгодженістю внутрішніх процесів, достовірністю даних, стабільністю ухвалення рішень та рівнем захищеності. Загальна точність роботи інформаційної системи після адаптації становила 97.08%, а аналіз за окремими категоріями показав майже безпомилкове відображення подій. Це підтверджує, що запропонований адаптивний метод є ефективним інструментом для підтримання стабільності інформаційних систем у динамічних умовах та здатний забезпечувати високу якість роботи незалежно від складності та мінливості середовища. Для наочного порівняння було сформовано зведену таблицю (Таблиця 1), яка демонструє переваги адаптивного методу над статичними підходами за всіма ключовими критеріями.

Таблиця 1

Порівняння ефективності інформаційної системи зі статичною моделлю та з адаптивним методом

Критерій оцінювання	**Статична система (без адаптивного методу)**	**Система з адаптивним методом пом'якшення впливу змін**
1. Точність відображення подій	Падіння точності: 0.84 → 0.72 (транзакції), 0.78 → 0.63 (журнали), похибка 3.9 → 4.3 (сенсори).	Відновлення точності: 0.91 (транзакції), 0.88 (журнали), похибка зменшена до 2.7 (сенсори).
2. Стійкість до змін у потоках даних	Деградація до 45% часу, різкі стрибки інтенсивності (12 → 38 тис. подій/с) призводять до збоїв.	Зменшення періодів деградації до 6–9%, стабільність навіть за різких змін інтенсивності.
3. Швидкість реагування	Повне переналаштування займає 2–4 хвилини, затримки накопичуються.	Оновлення за 15–30 с, у пікових умовах — до 12 с завдяки локальним корекціям.
4. Обчислювальна ефективність	Пропускна здатність падає до 21–28 тис. подій/с, затримка зростає до 4.8 с.	Пропускна здатність 57–71 тис. подій/с, затримка 1.4–1.9 с, без повного переналаштування.
5. Узгодженість внутрішніх процесів	Неузгоджені події: до 11.3% через спотворення міток часу та службових записів.	Зменшення неузгодженостей до 2.1%, автоматичне відновлення логічних зв'язків.
6. Достовірність і повнота даних	Спотворені або неповні записи: 7.8% після атак на журнали та канали передачі.	Зменшення спотворень до 1.6% завдяки оцінюванню довіри до джерел та виявленню аномалій.
7. Стабільність ухвалення рішень	Хибні сповіщення: 14–18%; пропущені критичні події: 6.2%.	Хибні сповіщення: 3.4%; пропущені критичні події: 0.9%.
8. Рівень захищеності та контроль доступу	Успішні несанкціоновані дії: 4.1 випадку на 10 тис. подій.	Зменшення до 0.6 випадку завдяки виявленню підозрілих змін у потоках.
Загальна ефективність системи	Низька стійкість, часті збої, залежність від ручного втручання.	Висока точність (97.08%), автономна адаптація, стабільність у динамічних умовах.

ISSN 2219-9365

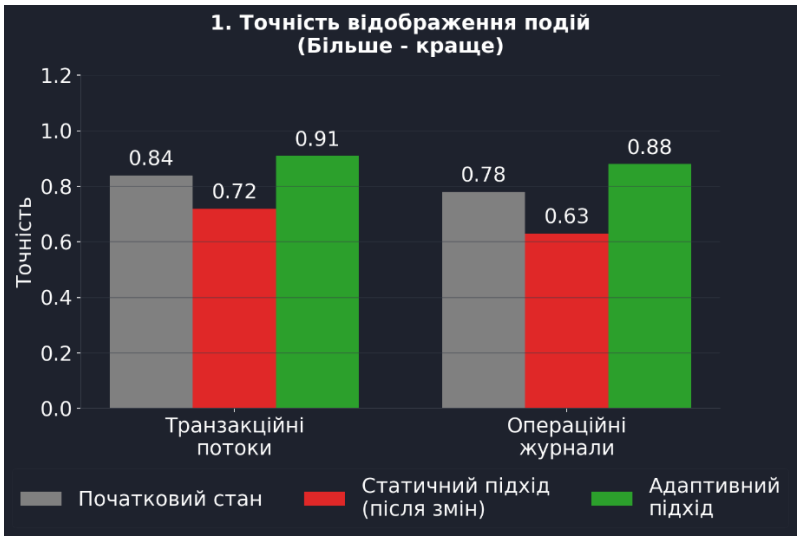

Рис. 1. Порівняння точності класифікації при зміні даних

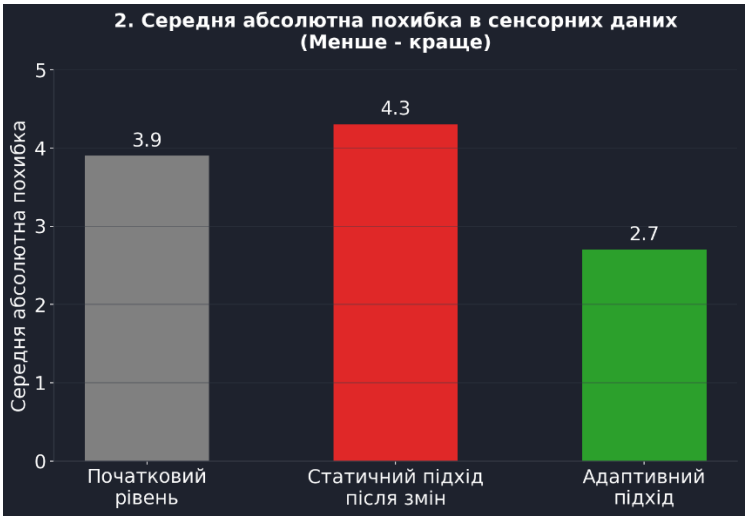

Рис. 2. Середня абсолютна похибка в сенсорних потоках

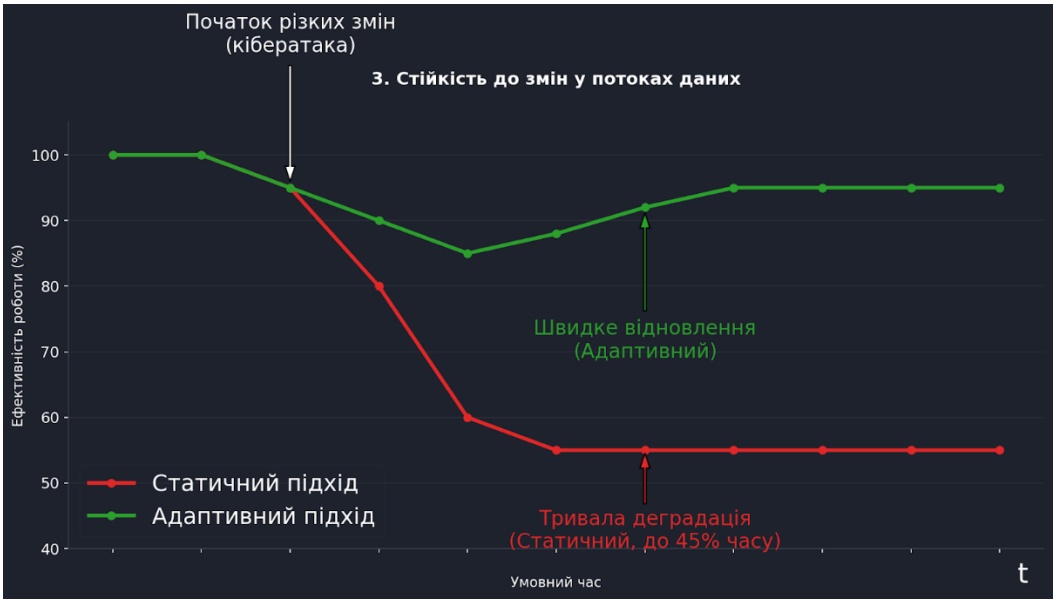

Рис. 3. Стабільність продуктивності моделі в часі

Рис. 4. Швидкість реагування системи

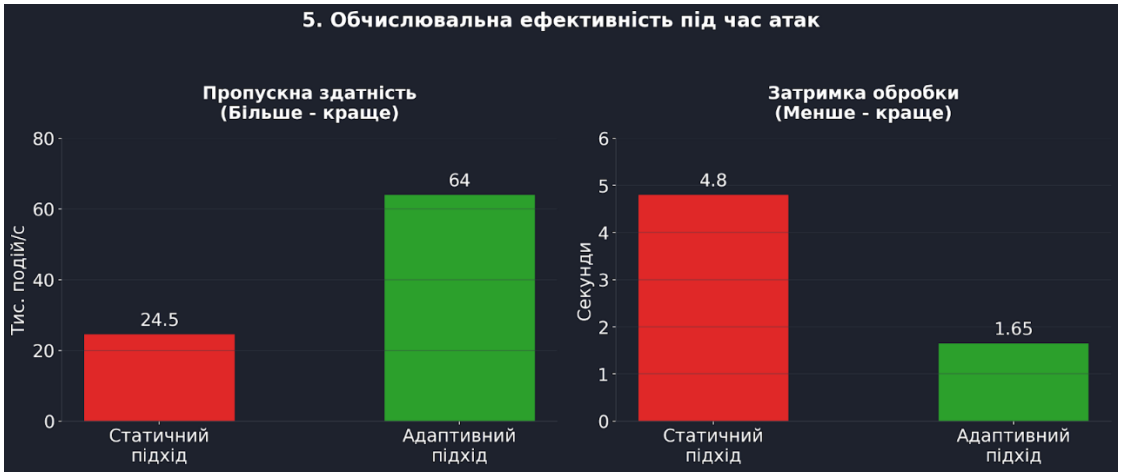

Рис. 5. Обчислювальна ефективніть під час атак

Рис. 6. Узгодженість процесів всередині ІС

ISSN 2219-9365

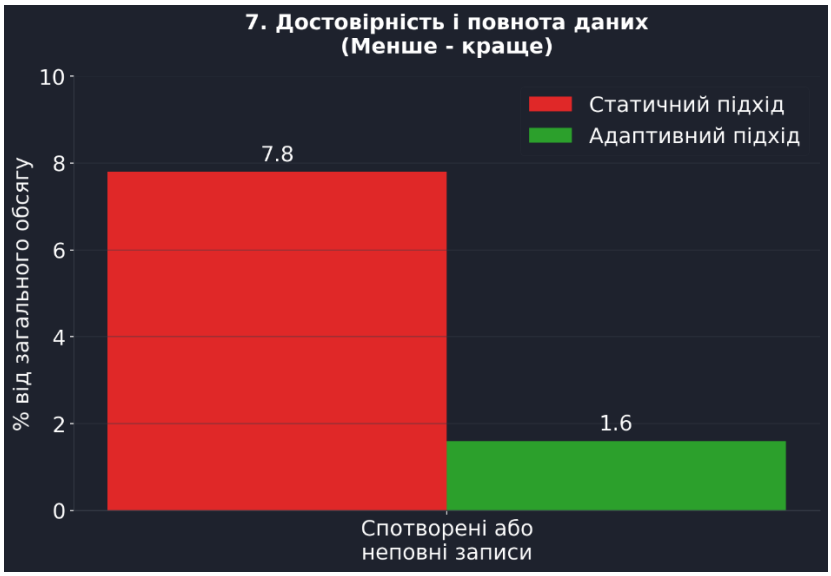

Рис. 7. Достовірність і повнота даних ІС

Рис. 8. Стабільність ухвалення рішень ІС

Рис. 9. Рівень захищеності ІС

ВИСНОВКИ З ДАНОГО ДОСЛІДЖЕННЯ І ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

У проведеному дослідженні було запропоновано та обґрунтовано адаптивний метод пом'якшення впливу змін, спрямований на забезпечення стабільності, стійкості та довготривалої актуальності роботи інформаційної системи в умовах кібератак і постійної мінливості потоків даних. Необхідність такого підходу зумовлена тим, що традиційні статичні системи швидко втрачають точність і надійність за умов дрейфу даних, появи нових закономірностей, структурних перебудов або навмисних спотворень, які є типовими наслідками шкідливих дій зловмисників. Запропонований метод долає ці обмеження завдяки поєднанню узгодження даних, формування інформативного простору ознак, виявлення змін за статистичними критеріями та адаптивного коригування внутрішніх параметрів, що дозволяє системі своєчасно реагувати на аномалії та підтримувати стабільність роботи.

Розроблений підхід продемонстрував здатність автономно адаптуватися до змін, викликаних як природними процесами, так і кібератаками, коригувати внутрішні параметри та підтримувати високу точність рішень без необхідності повного переналаштування. Експериментальні результати на трьох різнорідних потоках - транзакційних даних, журналах операційних подій та сенсорних вимірюваннях - підтвердили універсальність і надійність методу. У всіх випадках адаптивний підхід суттєво перевершив статичні системи за точністю, стійкістю до змін, швидкістю відновлення, обчислювальною ефективністю та здатністю працювати з різними структурами даних. Особливо показовими стали ситуації, у яких адаптивний метод відновлював або підвищував точність після появи нових закономірностей чи аномалій, тоді як статичні системи демонстрували тривалі періоди деградації та втрати продуктивності.

Порівняльний аналіз підтвердив, що адаптивний метод забезпечує не лише відновлення точності, а й коректну переорієнтацію вагових характеристик відповідно до нових умов, що підвищує інтерпретованість, стабільність і передбачуваність рішень. Інформаційна система продемонструвала здатність працювати у режимі реального часу, зберігаючи високу пропускну здатність і низьку затримку навіть за умов різких стрибків інтенсивності подій, характерних для кібератак. Це свідчить про те, що адаптивні підходи здатні забезпечити якісно новий рівень гнучкості, стійкості та надійності в інформаційних системах, які функціонують у середовищах із постійною зміною властивостей даних та активною загрозовою динамікою.

Отримані результати вказують на те, що впровадження адаптивних методів у архітектуру інформаційних систем суттєво підвищує їхню аналітичну стійкість, оперативність реагування та здатність до самостійного оновлення в умовах кібератак. Це відкриває перспективи для створення систем нового покоління, які не лише реагують на зміни, а й здатні підтримувати високу якість рішень у довгостроковій перспективі, незалежно від складності та мінливості загрозового середовища. Подальші дослідження можуть бути спрямовані на розширення адаптивних механізмів у напрямі роботи з розподіленими архітектурами, багаторівневими структурами знань та складними потоками подій, що дозволить ще більше підвищити ефективність, стійкість і гнучкість таких систем.

References

1. Kashtalian Antonina, Serhii Lysenko, et al. "Control and Decision-Making in Deceptive Multi-Computer Systems Based on Previous Experience for Cybersecurity of Critical Infrastructure." *Applied Sciences* Vol 15 P. 12286. https://doi.org/10.3390/app152212286
2. Denysiuk Dmytro, Oleg Savenko, Sergii Lysenko, Bohdan Savenko, Andrii Nicheporuk. "Detecting software implants using system decoys." (2024). https://ceur-ws.org/Vol-3899/paper25.pdf
3. Bokhonko Oleksandr, Sergii Lysenko, Piotr Gaj. "Development of the social engineering attack models." (2024). https://ceur-ws.org/Vol-3899/paper26.pdf
4. Adeosun, Omoshalewa Anike. "Enhancing financial cybersecurity in cloud engineering: A systematic review of threats, mitigation strategies and regulatory compliance." *Asian Journal of Research in Computer Science.* Vol. 18.5 2025. P. 244-256. 10.9734/ajrcos/2025/v18i5652
5. Ndibe, Ogochukwu Susan. "AI-driven forensic systems for real-time anomaly detection and threat mitigation in cybersecurity infrastructures." *International journal of research publication and reviews* Vol. 6.5. 2025. P. 389-411. https://shorturl.at/Q7Ze4
6. Gangineni, Venkataswamy Naidu, et al. "Preventing Phishing Attacks Using Advanced Deep Learning Techniques for Cyber Threat Mitigation." *Journal of Data Analysis and Information Processing.* Vol. 13.03. 2025. P.10-4236. https://doi.org/10.4236/jdaip.2025.133020
7. Kalla, Dinesh. Investigating the Impact of Heuristic Algorithms on Cyberthreat Detection. In: *2024 2nd International Conference on Advances in Computation, Communication and Information Technology (ICAICCIT)*. IEEE, 2024. p. 450-455. https://doi.org/10.1109/ICAICCIT64383.2024.10912106
8. Abiola, Olumide Bashiru, and M. O. Ijiga. "Implementing dynamic confidential computing for continuous cloud security posture monitoring to develop a zero trust-based threat mitigation model." *International Journal of Innovative Science and Research Technology (IJISRT) IJISRT25MAY587.* 2025. P. 69-83. https://doi.org/10.38124/ijisrt/25may587
9. Jain, Souratn. "Advancing cybersecurity with artificial intelligence and machine learning: Architectures, algorithms, and future directions in threat detection and mitigation." *World Journal of Advanced Engineering Technology and Sciences* Vol.14.1. 2025. P. 273-290. https://doi.org/10.30574/wjaets.2025.14.1.0022
10. Taylor, Theodore. Dynamic anomaly-driven detection for ransomware identification: An innovative approach based on heuristic analysis. *Authorea Preprints*, 2024. P. 1-5. https://doi.org/10.36227/techrxiv.173203089.97125949/v1
11. Yunmar, Rajif Agung. Hybrid Android malware detection: A Review of heuristic-based approach. *IEEe Access*, 2024, 12. P. 41255-41286. https://doi.org/10.1109/ACCESS.2024.3377658
12. Novak, Pavel, OUJEZSKY, Vaclav. Heuristic malware detection method based on structured cti data: A research study and proposal. In: *2024 International Conference on Software, Telecommunications and Computer Networks (SoftCOM)*. IEEE, 2024. p. 1-6. https://doi.org/10.23919/SoftCOM62040.2024.10721992

13. Hu, Wengui. A deep analysis of nature-inspired and meta-heuristic algorithms for designing intrusion detection systems in cloud/edge and IoT: state-of-the-art techniques, challenges, and future directions. *Cluster Computing*, 2024, 27.7. P. 8789-8815. https://doi.org/10.1007/s10586-024-04385-8

14. More, Sanjana A., KACHAVIMATH, Amit V. SDN Intrusion Detection using Meta-Heuristic Optimization and K-Nearest Neighbors Classifier. *Procedia Computer Science*, 2025, 260. P. 1137-1144. https://doi.org/10.1016/j.procs.2025.03.299

15. Fuller, Richard. A novel hybrid machine learning approach for real-time ransomware detection using behavior-driven heuristic features. 2024. P. 120-125 https://doi.org/10.22541/au.173161579.96102762/v1

16. Okoli, Ugochukwu Ikechukwu. Machine learning in cybersecurity: A review of threat detection and defense mechanisms. *World Journal of Advanced Research and Reviews*, 2024, 21.1. P. 2286-2295. https://doi.org/10.30574/wjarr.2024.21.1.0315

17. Kumar, Busireddy Hemanth. Big Data in Cybersecurity: Enhancing Threat Detection with AI and ML. *Metallurgical and Materials Engineering*, 2025, 31.3. P. 12-20. https://dx.doi.org/10.2139/ssrn.5201668

18. Mohammed, Anwar. Transforming SOC Operations: Harnessing the Power of AI and ML for Enhanced Threat Detection. *INTERNATIONAL JOURNAL OF RESEARCH CULTURE SOCIETY Monthly Peer-Reviewed, Refereed, Indexed*, 2024. P. 8. https://dx.doi.org/10.2139/ssrn.5197098

19. Katiyar, Nirvikar. AI and Cyber-Security: Enhancing threat detection and response with machine learning. *Educational Administration: Theory and Practice*, 2024, 30.4. P. 6273-6282. https://shorturl.at/7KFxt

20. Marimuthu, Oviya, RAVI, Priyadharshini, JANARTHANAN, Senthil. Application of AI and ML in Threat Detection. *Protecting and Mitigating Against Cyber Threats: Deploying Artificial Intelligence and Machine Learning*, 2025. P. 29. https://doi.org/10.1002/9781394305216.ch2

21. Alzaabi, Fatima Rashed, MEHMOOD, Abid. A review of recent advances, challenges, and opportunities in malicious insider threat detection using machine learning methods. *IEEE Access*, 2024, 12. P. 30907-30927. https://doi.org/10.1109/ACCESS.2024.3369906

22. Mizanur, Mohammad. Machine Learning-Based Anomaly Detection for Cyber Threat Prevention. *Journal of Primeasia*. 2025, 6.1. P. 1-8. https://doi.org/10.25163/primeasia.6110172

23. Subrahmanyam, Satya. Behavioral Analysis for Threat Detection. In: *Handbook of AI-Driven Threat Detection and Prevention*. CRC Press, 2025. P. 95-115. https://doi.org/10.1201/9781003521020-6

24. Ozturk, Mehmet. Dynamic behavioural analysis of privacy-breaching and data theft ransomware. 2024. https://doi.org/10.21203/rs.3.rs-4097219/v1

25. Dhanushkodi, Kavitha, and S. Thejas. "Ai enabled threat detection: Leveraging artificial intelligence for advanced security and cyber threat mitigation." *IEEE access* 12. 2024. P. 173127-173136. https://doi.org/10.1109/ACCESS.2024.3493957

26. Shanks, Gene. Innovative framework for ransomware detection using adaptive cryptographic behavior analysis. 2024. P. 10-14. https://doi.org/10.22541/au.173230401.11413813/v1

27. Dine, Faizal. "Cyber threat analysis and the development of proactive security strategies for risk mitigation." 2024. https://shorturl.at/8g0VP