DOI: https://doi.org/10.36910/6775-2524-0560-2025-60-34
УДК 004.056.57
**Фесьоха Віталій Вікторович**[1], доктор філософії, доцент
https://orcid.org/0000-0001-6612-1970
**Унтілова Олена Олексіївна**[1], ад'юнкт
https://orcid.org/0009-0003-8756-1889
**Чернявський Роман Геннадійович**[2]
https://orcid.org/0009-0000-3566-5350
[1]Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, м. Київ, Україна
[2]Центральний науково-дослідний інститут Збройних Сил України, м. Київ, Україна

# АНАЛІЗ ПІДХОДІВ ДО МІНІМІЗАЦІЇ ХИБНИХ РЕЗУЛЬТАТІВ У ПРОЦЕСІ ВИЯВЛЕННЯ АНОМАЛІЙ СИСТЕМАМИ КІБЕРЗАХИСТУ

**Фесьоха В.В., Унтілова О.О., Чернявський Р.Г. Аналіз підходів до мінімізації хибних результатів у процесі виявлення аномалій системами кіберзахисту.** У контексті дослідження проблеми виявлення невідомих (нових) кібератак на інформаційно-комунікаційні системи (ІКС) обґрунтовано доцільність застосування підходу на основі виявлення аномалій, який демонструє найбільший потенціал серед альтернативних методів. Розглянуто типи помилок, які виникають під час виявлення аномалій найбільш поширеними методами, а також причини їх виникнення: низька якість та неповнота даних, концепт-дрейф, дисбаланс класів, контекстні чинники експлуатації. Представлено порівняльний аналіз підходів, спрямованих на зменшення кількості хибних результатів у процесі виявлення аномалій системами кіберзахисту, описано їх переваги та недоліки. Запропоновано доменно-орієнтовану схему оцінювання загрозливості аномалій: подія аналізується у відповідності до релевантного домену (пам'ять, файлова система, мережа, доступ, база даних) із наперед визначеними пулами ознак Оцінюються три складові: прогнозна відповідність ланцюга подій (розбіжність між очікуваною та фактичною траєкторією), контекстна відповідність за архітектурою «суб'єкт-дія-об'єкт» і зміни стану ІКС до аномалії та після. Поєднання прогнозної, семантичної та інформації про стан системи дає змогу обґрунтовано відрізняти технічні збої від цілеспрямованих впливів і зменшувати ймовірність хибних висновків у сценаріях із невідомими кібератаками. Додатково підтримується контекстна історія підозрілих подій з метою відслідковування потенційних розподілених у часі кібератак. Запропонована схема розглядається як основа для формалізації критеріїв, алгоритмів вибору доменів і відповідних їм ознак, правил ухвалення рішень та процедур верифікації, спрямованих на розвиток інтелектуальних систем кіберзахисту критично важливих ІКС.
**Ключові слова:** невідомі кібератаки, виявлення аномалій, кіберзахист, хибні спрацювання, інформаційно-комунікаційні системи.

**Fesokha V., Untilova O., Cherniavskyi R. Analysis of approaches to minimize false results in the process of detecting anomalies by cyber defense systems**. In the context of researching the problem of detecting unknown (new) cyberattacks on information and communication systems (ICS), the feasibility of an anomaly detection approach, which demonstrates the greatest potential among alternative methods, is substantiated. The types of errors that occur during anomaly detection using the most common methods, as well as the causes of their occurrence, are examined: low data quality and incompleteness, concept drift, class imbalance, and contextual exploitation factors. A comparative analysis of approaches aimed at reducing the number of false results in the process of anomaly detection by cybersecurity systems is presented, and their advantages and disadvantages are described. A domain-oriented scheme for assessing the threat of anomalies is proposed: an event is analyzed according to a relevant domain (memory, file system, network, access, database) with predefined feature pools. Three components are evaluated: the predictive consistency of the event chain (the discrepancy between the expected and actual trajectory), contextual consistency based on the "subject-action-object" architecture, and changes in the ICS state before and after the anomaly. The combination of predictive, semantic, and system state information makes it possible to reasonably distinguish technical failures from targeted attacks and reduce the probability of false conclusions in scenarios involving unknown cyberattacks. Additionally, a contextual history of suspicious events is maintained to track potential cyberattacks distributed over time. The proposed scheme is considered a basis for formalizing criteria, algorithms for selecting domains and their corresponding features, decision-making rules, and verification procedures aimed at the development of intelligent cybersecurity systems for critically important ICS.
**Keywords:** unknown cyberattacks, anomaly detection, cybersecurity, false positives, information and communication systems.

**Постановка наукової проблеми.** Забезпечення надійного функціонування ІКС у різних сферах життєдіяльності держави значною мірою залежить від реалізації основних принципів кіберстійкості або кібербезпеки. Одним з основних і водночас найскладніших завдань в даному контексті є протидія новим (невідомим) кібератакам, які характеризуються високою ентропією та адаптивністю, що значно ускладнює їх виявлення та нейтралізацію [1]. До того ж, протягом останнього часу в Україні спостерігається зростання кількості складних та цілеспрямованих кібератак, що здійснюються із використанням раніше невідомих вразливостей, нетипових методів обходу засобів захисту та інструментів соціальної інженерії, що свідчить про постійну трансформацію парадигми кіберзагроз [2-5]. Зазначене актуалізує потребу у вдосконаленні підходів

до виявлення нових кібератак, а також підвищенні кіберстійкості ІКС в умовах відсутності апріорної інформації про властивості кібератак.

**Аналіз досліджень.** На основі аналізу наукових публікацій [6 - 15], присвячених виявленню невідомих (нових) кібератак, виокремлено основні підходи, порівняльний аналіз яких за критеріями: здатності виявляти невідомі кібератаки, залежності від навчальних даних, адаптивності та можливості верифікації прийнятих рішень наведено в таблиці 1. Вибір зазначених критеріїв порівняння обумовлено їх релевантністю до задачі виявлення невідомих кібератак в реальних умовах функціонування систем кіберзахисту.

Таблиця 1. Порівняння основних підходів до виявлення невідомих кібератак

| **Підхід** | **Здатність виявляти нові кібератаки** | **Потреба в попередньому навчанні** | **Адаптація** | **Верифікація рішень** |
|---|---|---|---|---|
| Методи прогнозування | Середня | Висока | Середня | Середня |
| Методи виявлення аномалій | Висока | Низька / немає | Висока | Середня |
| Біоінспіровані методи | Висока | Середня | Висока | Низька |
| Декларативні методи | Низька | Немає | Низька | Висока |

Так, найбільший потенціал у контексті протидії раніше невідомим кібератакам демонструють методи на основі виявлення аномалій у функціонуванні ІКС, оскільки дають змогу відстежувати підозрілу активність без потреби в попередніх знаннях про шаблон або сигнатуру кібератаки, забезпечують високий рівень адаптації до їхніх нових типів, а також мають прийнятний рівень верифікації [16]. У порівнянні з методами прогнозування [17,18], які потребують попереднього досвіду і демонструють середню здатність до виявлення нових кібератак, підхід виявлення аномалій дає змогу значно зменшити залежність від навчання та підвищити чутливість до нетипової поведінки процесів ІКС. Біоінспіровані методи [19], хоч і мають високу здатність до адаптації та виявлення нових кібератак, часто характеризуються складністю налаштування та низьким рівнем верифікації прийнятих рішень. Декларативні методи [20], навпаки, ефективні лише у разі відомих шаблонів кібератак, мають низьку гнучкість та не дозволяють оперативно реагувати на нові виклики.

Водночас, попри високу ефективність методів виявлення аномалій у функціонуванні ІКС, численні дослідження [21-23] вказують на проблематику хибних результатів, яка залишається невирішеною повністю. Зокрема, існують аномалії, що становлять реальну загрозу кібербезпеці ІКС, але можуть бути класифіковані системою як нормальний стан (хибнонегативний результат - False Negative, FN), що призводить до пропуску кібератак. З іншого боку, трапляються аномалії, які не мають відношення до кіберзагроз, наприклад, короткочасний збій драйвера мережевої карти або помилка апаратного контролера, але система класифікує їх як загрозливі (хибнопозитивний результат - False Positive FP), що призводить до перевантаження підсистеми прийняття рішень систем кіберзахисту, зниження ефективності реагування та потенційного пропуску реальних кібератак через розфокусування уваги на помилкових інцидентах.

У зв'язку з цим існує об'єктивна потреба в подальших наукових дослідженнях, спрямованих на підвищення ефективності виявлення аномалій та зменшення хибних результатів в системах кіберзахисту критично важливих ІКС.

**Мета роботи.** Метою дослідження є аналіз підходів до мінімізації хибних результатів у процесі виявлення аномалій системами кіберзахисту.

**Виклад основного матеріалу й обґрунтування отриманих результатів дослідження.** Під аномалією розумітимемо будь-яку незвичайну, неочікувану або підозрілу активність (діяльність) в ІКС, мережі або програмному (програмно-апаратному) забезпеченні, що не узгоджується з наперед визначеним профілем (шаблоном) нормальної поведінки та може свідчити про потенційні цілеспрямовані спроби порушення кібербезпеки зловмисниками [19]. Спираючись на зазначене, а також у відповідності до [24] аномалії в кібербезпеці класифікують за низкою критеріїв (рисунок 1).

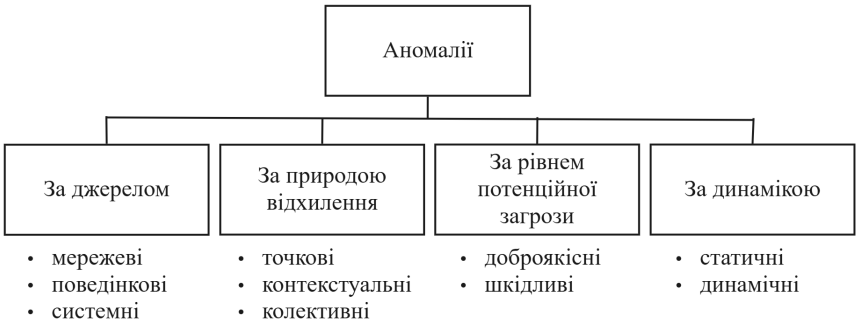


Рис 1. Класифікація аномалій в домені кібербезпеки

Наведена класифікація задає спільну рамку опису відхилень у різних доменах функціонування ІКС. У зв'язку з цим зазначимо джерела телеметрії, ключові метадані та часові вікна аналізу для кожної категорії аномалій, а також порядок їх обробки.

**За джерелом:** *мережеві* аномалії аналізують на рівні потоків і служб (NetFlow/Zeek, DNS, TLS-фінгерпринти, поля: bytes, duration, ports, SNI); *поведінкові* - за діями суб'єкта щодо об'єктів (послідовності входів, доступів, операцій над даними; журнали AD, VPN, DLP); *системні* - за артефактами ОС/ПЗ (Sysmon/EDR: створення процесів, зміни реєстру/конфігів, контроль цілісності, підписи).

**За природою відхилення:** *точкові* кіберінциденти зручно описувати як події з вектором ознак (час, джерело, атрибути); *контекстуальні* вимагають збагачення метаданими (роль, зона довіри, вікно обслуговування, топологія сегмента); *колективні* фіксуються як послідовності/графи взаємодій (ланцюги запитів, сесії, шляхи між вузлами).

**За рівнем потенційної загрози:** *доброякісні* ознаки часто мають легітимні джерела - календар змін, підписані пакети, відомі сервіси; *шкідливі* корисно співвідносити з відомими тактиками/техніками (MITRE ATT&CK), індикаторами компрометації (нетипові бінарі/скрипти, зовнішні напрями, артефакти ескалації).

**За динамікою:** *статичні* відхилення описують стан у момент часу (знімки, інваріанти конфігурації), тоді як *динамічні* потребують часових вікон і узгодження часу між джерелами (NTP, кореляція логів), бо спостерігаються як тренди/етапи (сканування, латеральні переміщення, повільне привласнення прав).

Таким чином, кожну аномалію формально можна описати кортежем виду ⟨джерело, природа відхилення від норми, рівень загрози, динаміка⟩, що надає специфікацію джерел спостереження й показників телеметрії, номенклатуру контекстних метаданих, параметри часової дискретизації, а також спосіб міждоменної кореляції подій. Наведені особливості підкреслюють потребу в подальшому розгляді процесу виявлення аномалій.

**Виявлення аномалій** - невід'ємна частина сучасної системи кіберзахисту, що має на меті ідентифікацію та класифікацію нетипових, непередбачуваних або підозрілих подій, послідовностей або станів, які можуть свідчити про здійснення деструктивного впливу, несанкціонований доступ чи іншу кіберзагрозу [25]. Ефективність даного процесу значною мірою визначається адаптивністю системи до умов динамічного середовища, де зазнають постійних змін як легітимні моделі поведінки, так і техніки, що застосовуються зловмисниками під час реалізації деструктивного впливу. У зв'язку з цим використовуються різноманітні підходи, серед яких широкого застосування знайшли статистичні методи, алгоритми (моделі) машинного навчання, а також комплексні гібридні (ансамблеві) підходи, що інтегрують кілька моделей для підвищення ефективності та точності аналізу [26-28]. З огляду на різноманітність зазначених підходів, доцільно провести їх порівняльний аналіз на предмет визначення притаманних їх чинників в модельних припущеннях і налаштуваннях, що породжують хибні результати. У таблиці 2 узагальнено порівняння методів виявлення аномалій [29-32] за критеріями, що безпосередньо впливають на виникнення хибнопозитивних і хибнонегативних спрацьовувань.

Таблиця 2. Порівняння методів виявлення аномалій

| Метод | Норма (припущення) | Гранулярність | Залежність від контексту | Чутливість до калібрування | Робастність до дрейфу | Типові FP | Типові FN |
|---|---|---|---|---|---|---|---|
| Статистичний | Стаціонарна, здебільшого лінійна; Незалежність ознак | Подія | Низька | Низька | Низька (без ковзних вікон) | Піки легітимних навантажень; періодичні / вікна; шум / сплески | Розподілені атаки, контекстно-залежні відхилення; колективні патерни |
| Машинне навчання | Нелінійна межа/ щільність; Норма стаціонарна без донавчання | Подія/сесія | Середня | Середня | Середня | Нові легітимні режими виглядають "рідкісно"; рідкі рееr-дії | Щільні колективні ланцюги; добре замасковані під розподіл навчання |
| Глибоке навчання | Високорозмірна нелінійна; часові залежності (для послідовних) | Подія / послідовність | Середня-Висока | Середня (пороги за скором) | Середня (потребує регулярного донавчання) | Нові легітимні патерни, не бачені на тренуванні; артефакти сенсорів | Короткі ізольовані кроки без історії; атаки, схожі на навчальні дані |
| Поведінковий | Профілі користувачів/ рееr-груп; рольова/ контекстна "норма" | Послідовність / сесія | Висока | Середня | Середня (чутливі до змін ролей) | Зміна ролі/розкладу; відрядження/нічні роботи; нові інструменти | Інсайдер, що мімікрує рееr-групу; повільна ескалація привілеїв |
| Семантичний | Детерміновані правила/ патерни; експертні припущення | Подія / патерн | Висока | Низька-Середня | Низька (правила швидко старіють) | Жорсткі умови без урахування контексту; поява нових легітимних дій | Нові техніки; варіації, не покриті правилами |
| Гібридний | Комбінація попередніх; логіка AND/OR/ваги | Багаторівнева (подія → послідовність → граф) | Висока | Висока (налаштування ваг/порогів) | Середня-Висока (якщо є адаптивні компоненти) | Дублювання сигналів - завищений ризик; конфлікти моделей; "кореляція ≠ причинність" | Несинхронізовані докази; слабкі сигнали губляться у прийнятті рішень; прогалини кореляції |

Порівняльний огляд методів виявлення аномалій показав не лише їхню відмінність за принципом дії, а й характером хибних спрацювань. Статистичні й порогові підходи дають прозорість і малу затримку, але припускають стаціонарність «норми», через що схильні до хибнопозитивних сигналів на періодичних і коротких легітимних сплесках, водночас пропускаючи розтягнуті у часі сценарії. Алгоритми машинного навчання значно краще моделюють багатовимірну норму, однак нові легітимні режими часто трактують як «рідкісні» - FP, тоді як колективні послідовності, схожі на навчальний розподіл, можуть залишатися непоміченими - FN. Глибоке навчання розкриває нелінійні та часові залежності, проте його помилки визначаються тренувальними даними: не бачені раніше легітимні патерни провокують FP, а кібератаки, подібні до навчальних прикладів - FN. Поведінкові методи критично залежать від коректного контексту ролей і спільних профілей: зміни функцій користувачів, графіків робіт чи інструментів дають FP, тоді як скомпрометований обліковий запис, що імітує групову норму призводить до FN. Семантичні підходи забезпечують пояснюваність і контроль, однак швидко втрачають актуальність відносно нових технік і варіацій кібератак: жорсткі умови без належної контекстуалізації множать FP, а невідомі або обфусковані прийоми формують FN. Гібридні рішення закривають «сліпі зони» окремих методів, але потребують уважного калібрування ваг і логіки: дублювання сигналів і розсинхронізація джерел легко ведуть до накопичення FP, тоді як слабкі, проте релевантні сигнали можуть «губитися», утворюючи FN.

У загальному випадку чітко простежуються спільні чинники хибних висновків [33-35]: невдала гранулярність представлення (аналіз окремих подій замість послідовностей/графів для колективних сценаріїв), хибна контекстуалізація (некоректне задання метаданих події - час/роль/зона, довіри/вікно обслуговування; помилки у формуванні референтних груп), крихкість порогів (глобальні, неперіодизовані пороги; несумірні скори різних моделей; невеликі зсуви розподілу різко змінюють кількість тривог), а також концепт-дрейф (повільна еволюція «норми» через релізи, періодичність, зміни ролей; без онлайн-адаптації профілі втрачають актуальність, накопичуючи FP або породжуючи FN). Додатково істотно впливають якість і повнота даних: пропуски, шум та неактуальні журнали спотворюють «норму» і зменшують варіативність легітимної поведінки, через що нові, але припустимі патерни маркуються як аномальні; брак або надлишок (і взаємна корельованість) ознак знижує роздільну здатність моделей. Нерівномірний класовий баланс робить рідкісні інциденти статистично «невигідними» для моделі, що проявляється падінням показників точності та повноти саме для цільового класу. Контекстні чинники експлуатації (час, роль, локація, політики доступу) визначають локальну «нормальність», і їх ігнорування породжує системні хибні спрацьовування. Нарешті, жорстко налаштовані або погано адаптовані алгоритми без урахування локальних політик, ролей і режимів схильні як до FP (через надто вузькі пороги), так і до FN (через надмірне згладжування сигналу).

Описавши причини та джерела хибних спрацьовувань, далі зосередимося на підходах, які покликані їх зменшувати. У таблиці 3 представлено порівняльний аналіз підходів до мінімізації хибних результатів у процесі виявлення аномалій системами кіберзахисту [33-38].

Таблиця 3. Аналіз підходів до мінімізації хибних результатів у процесі виявлення аномалій

| Підхід/Критерій | Зменшення FP | Зменшення FN | Адаптивність до змін | Обчислювальні ресурси | Пояснювальність | Складність впровадження | Залежність від якості даних | Гнучкість налаштувань |
|---|---|---|---|---|---|---|---|---|
| Концептуалізація поведінки | Високе | Середнє | Висока | Середні | Висока | Середня | Висока | Висока |
| Адаптивні пороги та самонавчання | Середнє | Високе | Висока | Низькі | Середня | Низька | Середня | Висока |
| Гібридні моделі | Високе | Високе | Висока | Високі | Середня | Висока | Середня | Висока |
| Очищення та балансування даних | Середнє | Середнє | Низька | Низькі | Висока | Низька | Висока | Низька |
| Глибокий аналіз залежностей ознак | Високе | Високе | Середня | Високі | Низька | Висока | Висока | Середня |
| Оцінка загрозливості для об'єкта захисту | Високе | Високе | Висока | Низькі | Висока | Середня | Середня | Висока |

Контекст (роль, peer-група, зона довіри, календар змін) різко зменшує хибнопозитивні висновки, бо «нестандартність» оцінюється відносно локальної норми. Слабке місце - скомпрометований обліковий запис, що імітує групову поведінку: хибнонегативні результати залишаються на помірному рівні. Метод добре адаптується, прозорий для аналітика, але критично залежить від якості й актуальності даних.

**Динамічні пороги у часових вікнах («періодизація» за годиною/днем) помітно скорочують пропуски, особливо для повільних зсувів поведінки, і майже не потребують ресурсів. Найкраще працює як швидкий перший шар: тригер → коротка контекстна перевірка.**

Гібридні моделі. Поєднання правил, статистики та машинного/глибокого навчання закриває сліпі зони окремих підходів і дає одночасне зниження FP/FN. Ціна - висока складність інтеграції, потреба в калібруванні порогів і ваг голосування, а також ризик дублювання сигналів і розсинхронізації джерел. Потребують дисципліни калібрування порогів і дедуплікації подій.

Очищення та балансування даних - не детектор, а лише обробка конвеєра: видалення артефактів логів, заповнення пропусків і робота з дисбалансом стабілізують усі наступні етапи, зменшуючи випадкові FP і «сліпі зони» FN. Процедури прозорі і не потребують значних обчислювальних ресурсів, але не замінюють адаптацію моделі у часі.

Моделі, здатні відловлювати нелінійні/послідовні взаємодії (від багатовимірної статистики до автокодувальників і рекурентних нейронних мереж), найкраще відрізняють складні відхилення й істотно зменшують обидва типи помилок. Водночас вони ресурсомісткі, менш пояснювані та потребують регулярного донавчання й контролю дрейфу з метою уникнення деградації балансу FP/FN.

Оцінка загрозливості аномалій. Зміщує рішення з площини «Чи є аномалія?» у площину «Наскільки це важливо тут і зараз?». Прив'язка до критичності активів, чутливості даних і можливого впливу дає подвійний ефект: по-перше, зменшує FP на малозначущих цілях (низький пріоритет навіть за помірного сигналу), по-друге, скорочує FN на критичних активах (навіть слабкі сигнали ескалюються, не губляться в шумі). Підхід ресурсно легкий і добре пояснюваний.

Таким чином, аналіз підходів до мінімізації хибних результатів у процесі виявлення аномалій показав, що жоден з них не є універсальним та повністю позбавленим недоліків. Поряд з цим, методи на основі оцінки загрозливості аномалій демонструють найбільшу ефективність, оскільки дають змогу не лише виявляти нетипові події, а й визначати їхній потенційний вплив на кібербезпеку інформаційної системи (мережі). На відміну від бінарного поділу «норма/аномалія», оцінка загрозливості враховує контекст подій, їхню історію, взаємозв'язки та потенційні наслідки,

що забезпечує підвищення точності виявлення кібератак навіть у випадках нелінійної сепарабельності класів.

Підсумовуючи, можна сказати, що аномалія не просто точка, що відхиляється від нормального профілю, а припущення про потенційний деструктивний вплив. Саме тому аномалію доцільно розглядати як семантичний кортеж ⟨джерело, природа відхилення від норми, рівень загрози, динаміка⟩, що надасть змогу змістити фокус від класифікації події до опису координат для її інтерпретації: що саме спостерігаємо, у якому контексті, як це розгортається в часі й чим це загрожує ІКС. Так, з урахуванням переваг підходу щодо оцінки загрозливості аномалій, типових помилок щодо гранулярності представлення та некоректної контекстуалізації запропоновано доменно-орієнтований підхід до оцінювання загрозливості аномалій, узагальнена функціональна схема якого представлено на рисунку 2.

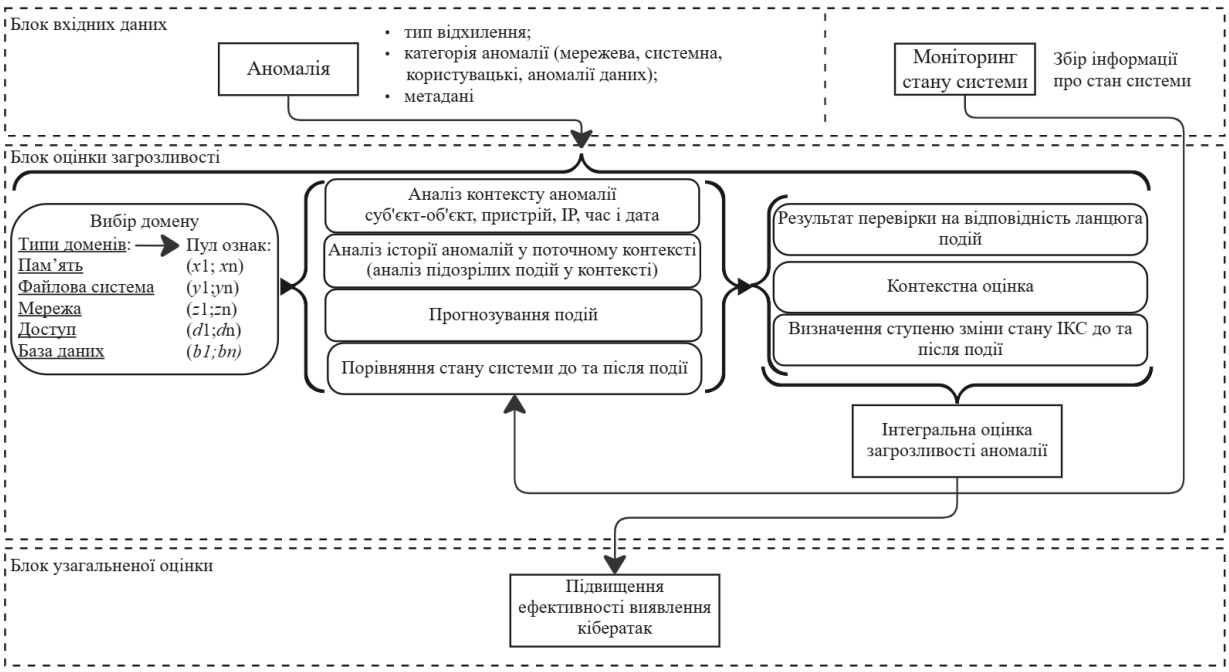


Рис 2. Узагальнена функціональна схема доменно-орієнтованого підходу до оцінювання загрозливості аномалій

У відповідності до запропонованого підходу вхідними даними є вже виявлена аномалія в системі з визначеним набором метаданих, що її описують (джерело, час, параметри події, категорія), а також вектор стану системи від модуля моніторингу на момент(и) до/після події. Мета - оцінити потенційну загрозливість поточної аномалії для ІКС.

В залежності від категорії аномалії активується підмножина доменів $D \subseteq$ {*пам'ять, файлова система, мережа, доступ, база даних*}, для кожного з яких визначено пул ознак (наприклад, для мережі - {bytes, duration, ports, SNI, JA3}; для доступу - {роль, групи, спосіб автентифікації}, що забезпечує коректну гранулярність представлення (розгляд послідовностей подій у релевантних доменах).

Наступним етапом є формування контексту аномалії (суб'єкт, подія, об'єкт, пристрій, IP-адреса, час/дата, зона довіри, політика доступу) на предмет відповідності подій локальній нормі ролі/сегмента у вказаний час/зоні. Додатково оцінюється історія підозрілих подій у поточному контексті, що дає змогу вивчати аномалії не окремо, а в рамках загальної динаміки, що в свою чергу підвищує ефективність виявлення потенційної прихованої активності зловмисників і протидії розподіленим у часі кібератакам.

На основі базових профілів (модель переходів/послідовностей для ролі/активу) обчислюється оцінка відповідності поточного ланцюга подій на предмет узгодження з очікуваним. Наприклад, звернення архіву до зовнішньої адреси після розпакування не є нормою, на відміну від створення теки з документами. Завдяки цьому можна виявляти приховані взаємозв'язки між, на перший погляд, незалежними інцидентами.

Наступним етапом є порівняння стану системи до і після виявленої аномалії на основі значень ознак релевантного домену. Якщо аномалія була короткочасною або не спричинила змін стану системи за визначеними ознаками, то з високою ймовірністю це технічний збій.

Інтегральну оцінку загрозливості аномалії формуємо з трьох незалежних технічних складових: контекстної відповідності, прогнозної відповідності ланцюга подій та зміни стану системи у релевантних доменах. Узагальнений показник отримуємо за правилом «2 із 3» - подія ескалується, якщо не менше двох оцінок перевищують пороги. Зазначений підхід зменшує FP (через локальну норму й вимогу фактичного впливу) та FN (через оцінку послідовностей). Саме на цьому етапі виявлена аномалія перетворюється на практичну інформацію, придатну для реагування.

Таким чином, запропонована схема реалізує багаторівневий підхід до оцінки загрозливості аномалій, який поєднує аналіз контексту, історії, причинно-наслідкових зв'язків і впливу на стан ІКС, що потенційно надасть змогу мінімізувати рівень хибних результатів у процесі виявлення аномалій системами кіберзахисту.

**Висновки.** Знання про аномалії є одним з фундаментальних аспектів сучасних систем кіберзахисту, особливо з огляду на зростаючу складність кібератак, зниження ефективності сигнатурних методів і важливість швидкого реагування на нові, раніше невідомі кібератаки.

Методи виявлення аномалій мають різний характер хибних спрацювань. Статистичні та порогові підходи схильні до хибнопозитивних спрацювань на легітимних, але нетипових сплесках. Алгоритми машинного та глибокого навчання часто помилково маркують нові, законні поведінкові патерни як аномалії через недостатнє покриття навчальними даними. Поведінкові методи генерують FP при зміні ролей користувачів, а семантичні - через жорсткі умови, які не враховують контекст. У гібридних системах FP можуть виникати через дублювання сигналів або їхню некоректну синхронізацію. Таким чином, проведений аналіз засвідчив, що проблема мінімізації хибних результатів у процесі виявлення аномалій залишається одним із ключових викликів для систем безпеки. Надмірна кількість хибнопозитивних спрацьовувань знижує ефективність реагування, перевантажує аналітиків і може призводити до ігнорування реальних кібератак, тоді як хибнонегативні результати створюють умови для прихованого проникнення зловмисників у критичні системи.

Розглянуті підходи до мінімізації хибних результатів демонструють різні переваги та обмеження у зниженні кількості помилок. Водночас жоден із підходів не забезпечує універсального вирішення зазначеної проблематики, що підкреслює необхідність комплексного застосування методів та адаптації моделей до конкретного домену й контексту аномалій.

Запропонована схема доменно-орієнтованого підходу до оцінювання загрозливості аномалій формує підґрунтя для створення більш точних систем кіберзахисту, здатних ефективніше реагувати на нові (невідомі) кібератаки з мінімальною кількістю хибних результатів.

Перспективним напрямком подальших наукових досліджень є розробка моделі оцінки загрозливості, зумовленої аномаліями у функціонуванні інформаційно-комунікаційних систем.

**Список бібліографічного опису**

1. Даник Ю.Г., Воробієнко П.П., Чернега В.М. Основи кібербезпеки та кібероборони. Одеса: ОНАЗ, 2019. 182-184 с.
2. CERT-UA минулого року опрацювала 4 315 кіберінцидентів. *Державна служба спеціального зв'язку та захисту інформації України.* URL:https://cip.gov.ua/ua/news/cert-ua-minulogo-roku-opracyuvala-4315-kiberincidentiv
3. Російські кібероперації: Аналітика за 1 півріччя 2024 року. *Державна служба спеціального зв'язку та захисту інформації України.* URL: https://docs.google.com/viewer?url=https://cip.gov.ua/services/cm/api/attachment/download?id=65897&embedded=true&a=bi
4. Sandworm Disrupts Power in Ukraine Using a Novel Attack Against Operational Technology. *Mandiant.* URL: https://cloud.google.com/blog/topics/threat-intelligence/sandworm-disrupts-power-ukraine-operational-technology/
5. Цільові кібератаки з використанням SuperOps RMM. *CERT-UA.* URL: https://cert.gov.ua/article/6279419
6. Кудін І. А. Структурні методи вивчення поверхні атак. Дипломна робота. Київ: Національний технічний університет ім. Ігоря Сікорського 2022р. 30-31 с.
7. A Novel Detection Approach of Unknown Cyber-Attacks for Intra-Vehicle NetworksUsing Recurrence Plots and Neural Networks. *SCRIBD.* URL: https://www.scribd.com/document/772182040/A-Novel-Detection-Approach-of-Unknown-Cyber-Attacks-for-Intra-Vehicle-Networks-Using-Recurrence-Plots-and-Neural-Networks
8. Cornell University/usfAD Based Effective Unknown Attack Detection Focused IDS Framework. *Cornell University.* URL:https://arxiv.org/abs/2403.11180

9. Detect Known and Unknown Cyberattacks – Better Together with Vectra NDR and Vectra Match. *Vectra AI.* URL: https://ww
w.vectra.ai/blog/detect-known-and-unknown-cyberattacks-better-together-with-vectra-ndr-and-vectra-match
10. Conditional Variational Auto-Encoder and Extreme Value Theory Aided TwoStage Learning Approach for Intelligent Fine-Grained Known/Unknown Intrusion Detection. *IEEE Xplore.* URL: https://ieeexplore.ieee.org/abstract/document/9439944
11. Robust detection of unknown DoS/DDoS attacks in IoT networks using a hybrid learning model. *ScienceDirect.* URL: https://
www.sciencedirect.com/science/article/abs/pii/ S2542660523001749
12. A review of Machine Learning-based zero-day attack detection: Challenges and future directions. *ScienceDirect.* URL: https:/
/www.sciencedirect.com/science/article/abs/pii/S01 40366422004248
13. A robust intelligent zero-day cyber-attack detection technique. *Springer Nature Link.* URL:https://link.springer.com/article/10
.1007/s40747-021-00396-9
14. From zero-shot machine learning to zero-day attack detection. *Springer Nature Link.* URL:https://link.springer.com/article/1
0.1007/s10207-023-00676-0
15. Predicting and mitigating cyber threats through data mining and machine learning. *ScienceDirect.* URL: https://www.science
direct.com/science/article/pii/S0140366424002962
16. І.В. Рубан, В.О. Мартовицький, С.О. Партика, Класифікація методів виявлення аномалій в ІС. Харків: ХНУР, 2016.
17. Повторацькй А.О., Виявлення аномалій для систем мережевого вторгнення. Львів: ЛНУ, 24-49 с.
18. М. Бешлей, А. Прислупський, М. Медвецький, Г. Бешлей, інтелектуальна система моніторингу та аналізу трафіку для виявлення атак у ПКМІ. Львів: НУЛП, 2022, 3 с.
19. Predicting and mitigating cyber threats through data mining and machine learning. *ScienceDirect.* URL: https://www.science
direct.com/science/article/pii/S0140366424002962
20. Artificial Immune Systems in Local and Network Cybersecurity: An Overview of Intrusion Detection Strategies. *NASK.* URL: https://www.acigjournal.com/Artificial-Immune-Systems-in-Local-and-Network-Cybersecurity-An-Overview-ofIntrusion,
184306,0,2.html
21. Insider Attack Identification and Prevention Using a Declarative Approach. *eScholarship.* URL: https://escholarship.org/uc/it
em/25d8k4p8
22. Anomaly detection optimization using big data and deep learning to reduce false-positive. *Cornell University.* URL:https://ar
xiv.org/abs/2209.13965
23. Behavior Anomaly Detection: Techniques and Best Practices. *Exabeam.* URL: https://www.exabeam.com/explainers/ueba/be
havior-anomaly-detection-techniques-and-best-practices/
24. How to Address IDS False Positives for Better Threat Detection Accuracy. *Fidelis Security.* URL: https://fidelissecurity.com/
cybersecurity-101/network-security/reducing-false-positives-in-intrusion-detection-systems/?utm_source=chatgpt.com
25. Combating the Challenges of False Positives in AI-Driven Anomaly Detection Systems and Enhancing Data Security in the Cloud. *ResearchGate.* URL: https://www.researchgate.net/publication/381303129_Combating_the_Challenges_of_False_Positiv
es_in_AI-Driven_Anomaly_Detection_Systems_and_Enhancing_Data_Security_in_the_Cloud
26. An overview of anomaly detection techniques: Existing solutions and latest technological trends. *ScienceDirect.* URL: https:/
/www.sciencedirect.com/science/article/abs/pii/S138912860700062X?utm_source=chatgpt.com
27. A Review on Machine Learning Approaches for Network Malicious Behavior Detection in Emerging Technologies. *MDPI.* URL: https://www.mdpi.com/1099-4300/23/5/529?utm_source=chatgpt.com
28. A Review of Machine Learning and Deep Learning Techniques for Anomaly Detection in IoT Data. *MDPI.* URL: https://ww
w.mdpi.com/2076-3417/11/12/5320?utm_source=chatgpt.com
29. Reducing False Positives in Real-Time Cyber Anomaly Detection by Fast Adaptation to Concept Drift. *Telosian.* URL: https:
//www.scitepress.org/Papers/2025/133205/133205.pdf
30. Intelligent approach to detecting online fraudulent trading with solution for imbalanced data in fintech forensics. *Scientific reports.* URL: https://www.nature.com/articles/s41598-025-01223-8
31. MDPI, Model Retraining upon Concept Drift Detection in Network Traffic Big Data URL: https://www.mdpi.com/1999-5903/17/8/328
32. Causes of False Positives. *Check point.* URL: https://www.checkpoint.com/cyber-hub/cyber-security/understanding-false-posi
tives-in-cybersecurity/

33. Chandola, V., Banerjee, A., & Kumar, V. Anomaly detection: A survey. *ACM Computing Surveys. 2009*.
34. Ahmed, M., Mahmood, A. N., & Hu, J. A survey of network anomaly detection techniques. *Journal of Network and Computer Applications.* 2016.
35. Javaid, A. et al. A deep learning approach for network intrusion detection system. *EAI Endorsed Transactions.* 2016.
36. Patcha, A., & Park, J. M. An overview of anomaly detection techniques: Existing solutions and latest technological trends. *Computer Networks.* 2007.
37. Kim, G., Lee, S., & Kim, S. A novel hybrid intrusion detection method integrating anomaly detection with misuse detection. *Expert Systems with Applications.* 2014.
38. Data-Driven Threat Hunting Using Sysmon. *ResearchGate.* https://www.researchgate.net/publication/325370335_Data-Driven_Threat_Hunting_Using_Sysmon

**References**

1. Danik, Y.H., Vorobiienko, P.P., Chernega, V.M. *Fundamentals of Cybersecurity and Cyber Defense*. Odesa: ONAZ, 2019.
2. CERT-UA processed 4,315 cyber incidents last year. State Service of Special Communications and Information Protection of Ukraine. URL: https://cip.gov.ua/ua/news/cert-ua-minulogo-roku-opracyuvala-4315-kiberincidentiv
3. Russian Cyber Operations: Analytics for the 1st Half of 2024. State Service of Special Communications and Information Protection of Ukraine. URL: https://docs.google.com/viewer?url=https://cip.gov.ua/services/cm/api/attachment/download?id=65897
4. Sandworm Disrupts Power in Ukraine Using a Novel Attack Against Operational Technology. Mandiant. URL: https://cloud.google.com/blog/topics/threat-intelligence/sandworm-disrupts-power-ukraine-operational-technology/
5. Targeted Cyber Attacks Using SuperOps RMM. CERT-UA. URL: https://cert.gov.ua/article/6279419
6. Kudin, I.A. *Structural Methods for Studying the Surface of Attacks*. Diploma thesis. Kyiv: National Technical University named after Igor Sikorsky, 2022, pp. 30-31.
7. A Novel Detection Approach of Unknown Cyber-Attacks for Intra-Vehicle Networks Using Recurrence Plots and Neural Networks. SCRIBD. URL: https://www.scribd.com/document/772182040/A-Novel-Detection-Approach-of-Unknown-Cyber-Attacks-for-Intra-Vehicle-Networks-Using-Recurrence-Plots-and-Neural-Networks
8. Cornell University / usfAD Based Effective Unknown Attack Detection Focused IDS Framework. Cornell University. URL: https://arxiv.org/abs/2403.11180
9. Detect Known and Unknown Cyberattacks – Better Together with Vectra NDR and Vectra Match. Vectra AI. URL: https://www.vectra.ai/blog/detect-known-and-unknown-cyberattacks-better-together-with-vectra-ndr-and-vectra-match
10. Conditional Variational Auto-Encoder and Extreme Value Theory Aided Two-Stage Learning Approach for Intelligent Fine-Grained Known/Unknown Intrusion Detection. IEEE Xplore. URL: https://ieeexplore.ieee.org/abstract/document/9439944
11. Robust Detection of Unknown DoS/DDoS Attacks in IoT Networks Using a Hybrid Learning Model. ScienceDirect. URL: https://www.sciencedirect.com/science/article/abs/pii/S2542660523001749
12. A Review of Machine Learning-Based Zero-Day Attack Detection: Challenges and Future Directions. ScienceDirect. URL: https://www.sciencedirect.com/science/article/abs/pii/S0140366422004248
13. A Robust Intelligent Zero-Day Cyber-Attack Detection Technique. Springer Nature Link. URL: https://link.springer.com/article/10.1007/s40747-021-00396-9
14. From Zero-Shot Machine Learning to Zero-Day Attack Detection. Springer Nature Link. URL: https://link.springer.com/article/10.1007/s10207-023-00676-0
15. Predicting and Mitigating Cyber Threats Through Data Mining and Machine Learning. ScienceDirect. URL: https://www.sciencedirect.com/science/article/pii/S0140366424002962
16. Ruban, I.V., Martovytskyi, V.O., Partika, S.O. *Classification of Anomaly Detection Methods in Information Systems*. Kharkiv: KhNUR, 2016.
17. Povtoratskyi, A.O. *Anomaly Detection for Network Intrusion Systems*. Lviv: LNU, pp. 24-49.
18. Beshliey, M., Prislupskiy, A., Medvetskyi, M., Beshliey, H. *Intelligent Traffic Monitoring and Analysis System for Detecting Attacks in PCMI*. Lviv: NULP, 2022, 3 pp.
19. Predicting and Mitigating Cyber Threats Through Data Mining and Machine Learning. ScienceDirect. URL: https://www.sciencedirect.com/science/article/pii/S0140366424002962
20. Artificial Immune Systems in Local and Network Cybersecurity: An Overview of Intrusion Detection Strategies. NASK. URL: https://www.acigjournal.com/Artificial-Immune-Systems-in-Local-and-Network-Cybersecurity-An-Overview-of-Intrusion,184306,0,2.html
21. Insider Attack Identification and Prevention Using a Declarative Approach. eScholarship. URL: https://escholarship.org/uc/item/25d8k4p8
22. Anomaly Detection Optimization Using Big Data and Deep Learning to Reduce False Positives. Cornell University. URL: https://arxiv.org/abs/2209.13965
23. Behavior Anomaly Detection: Techniques and Best Practices. Exabeam. URL: https://www.exabeam.com/explainers/ueba/behavior-anomaly-detection-techniques-and-best-practices/

24. How to Address IDS False Positives for Better Threat Detection Accuracy. Fidelis Security. URL: https://fidelissecurity.com/cybersecurity-101/network-security/reducing-false-positives-in-intrusion-detection-systems/?utm_source=chatgpt.com
25. Combating the Challenges of False Positives in AI-Driven Anomaly Detection Systems and Enhancing Data Security in the Cloud. ResearchGate. URL: https://www.researchgate.net/publication/381303129_Combating_the_Challenges_of_False_Positives_in_AI-Driven_Anomaly_Detection_Systems_and_Enhancing_Data_Security_in_the_Cloud
26. An Overview of Anomaly Detection Techniques: Existing Solutions and Latest Technological Trends. ScienceDirect. URL: https://www.sciencedirect.com/science/article/abs/pii/S138912860700062X?utm_source=chatgpt.com
27. A Review on Machine Learning Approaches for Network Malicious Behavior Detection in Emerging Technologies. MDPI. URL: https://www.mdpi.com/1099-4300/23/5/529?utm_source=chatgpt.com
28. A Review of Machine Learning and Deep Learning Techniques for Anomaly Detection in IoT Data. MDPI. URL: https://www.mdpi.com/2076-3417/11/12/5320?utm_source=chatgpt.com
29. Reducing False Positives in Real-Time Cyber Anomaly Detection by Fast Adaptation to Concept Drift. Telosian. URL: https://www.scitepress.org/Papers/2025/133205/133205.pdf
30. Intelligent Approach to Detecting Online Fraudulent Trading with Solution for Imbalanced Data in Fintech Forensics. Scientific Reports. URL: https://www.nature.com/articles/s41598-025-01223-8
31. MDPI, Model Retraining upon Concept Drift Detection in Network Traffic Big Data. URL: https://www.mdpi.com/1999-5903/17/8/328
32. Causes of False Positives. Check Point. URL: https://www.checkpoint.com/cyber-hub/cyber-security/understanding-false-positives-in-cybersecurity/
33. Chandola, V., Banerjee, A., & Kumar, V. *Anomaly Detection: A Survey*. ACM Computing Surveys, 2009.
34. Ahmed, M., Mahmood, A.N., & Hu, J. *A Survey of Network Anomaly Detection Techniques*. Journal of Network and Computer Applications, 2016.
35. Javaid, A., et al. *A Deep Learning Approach for Network Intrusion Detection System*. EAI Endorsed Transactions, 2016.
36. Patcha, A., & Park, J.M. *An Overview of Anomaly Detection Techniques: Existing Solutions and Latest Technological Trends*. Computer Networks, 2007.
37. Kim, G., Lee, S., & Kim, S. *A Novel Hybrid Intrusion Detection Method Integrating Anomaly Detection with Misuse Detection*. Expert Systems with Applications, 2014.
38. Data-Driven Threat Hunting Using Sysmon. ResearchGate. URL: https://www.researchgate.net/publication/325370335_Data-Driven_Threat_Hunting_Using_Sysmon