КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (34), 2026
ISSN 2663 – 4023
DOI 10.28925/2663-4023.2026.34.1249
УДК 004.056.5

**Лахно Валерій Анатолійович**
д.т.н., професор, професор кафедри комп'ютерних систем, мереж та кібербезпеки
Національний університет біоресурсів і природокористування України, Київ, Україна
ORCID:0000-0001-9695-4543
*lva964@nubip.edu.ua*

**Гладких Валерій Миколайович**
к.т.н., доцент, доцент кафедри комп'ютерних систем, мереж та кібербезпеки
Національний університет біоресурсів і природокористування України, Київ, Україна
ORCID:0000-0002-5868-9504
*v.hladkykh@nubip.edu.ua*

**Сагун Андрій Вікторович**
К.т.н., доцент, доцент кафедри комп'ютерних систем, мереж та кібербезпеки
Національний університет біоресурсів і природокористування України, Київ, Україна
ORCID:0000-0002-5151-9203
*a.sagun@nubip.edu.ua*

# АРХІТЕКТУРА БАГАТОРІВНЕВОГО ЗБОРУ ПОВЕДІНКОВИХ АРТЕФАКТІВ У ГЕТЕРОГЕННИХ МЕРЕЖАХ ДЛЯ ФОРМУВАННЯ ЦИФРОВИХ СЛІДІВ

**Анотація.** Об'єктом дослідження є процеси формування масиву цифрових доказів у гетерогенних інформаційно-комунікаційних системах в умовах постквантових кіберзагроз. Предметом дослідження є архітектурні рішення та методи багаторівневого збору поведінкових артефактів для систем підтримки прийняття рішень (СППР). Актуальність роботи зумовлена необхідністю розроблення альтернативних методів верифікації безпеки вузлів мережі у випадках, коли чинна криптографічна ідентифікація (TLS, PKI) може бути скомпрометована зловмисником із доступом до квантового ресурсу. На відміну від наявних методів, які зосереджені на аналізі окремих типів логів, у статті запропоновано концепцію сенсорної ієрархії, яка охоплює мережевий, системний та прикладний рівні інфраструктури. Наукова новизна отриманих результатів полягає у формалізації процедури перетворення розрізнених сирих подій безпеки у структуровані «цифрові сліди». Зокрема, розроблено архітектуру багаторівневого моніторингу, яка дозволить гнучко змінювати інтенсивність збору артефактів залежно від типу сегмента мережі та прогнозованого вектору атаки (EDoS-впливи, Supply Chain Attacks). Вперше описано методику зважування поведінкових ознак за їх інформативністю, що забезпечує мінімізацію обчислювальних витрат на опрацювання даних при збереженні високої достовірності формування вхідних параметрів для теоретико-ігрових моделей захисту. Практичне значення роботи полягає у розробленні структури програмних модулів для агрегації даних, які можна інтегрувати у діючи SIEM/IDS-платформи. Реалізація запропонованої архітектури засобами мови Python дозволила автоматизувати процес виявлення аномальних відхилень у поведінці вузлів, які формально зберігають валідність цифрових сертифікатів. Експериментальна апробація архітектури підтвердила її здатність забезпечувати цілісність інформаційного базису СППР навіть в умовах зміни топології гетерогенного середовища та значного рівня мережевого шуму.

**Ключові слова:** архітектура моніторингу, поведінкові артефакти, цифрові сліди, гетерогенні мережі, постквантова безпека, сенсорна ієрархія, агрегація даних.

## ВСТУП

Розвиток квантових обчислювальних систем та пов'язана з цим неминуча компрометація наявних асиметричних криптографічних протоколів сформували нову реальність для захисту гетерогенних інформаційних мереж. Сучасні гетерогенні середовища, що об'єднують хмарні обчислення, периферійні пристрої (IoT) та корпоративні сервери, зазвичай покладалися на такі криптосистеми, зокрема, RSA та алгоритми на еліптичних кривих, як на безальтернативний математичний фундамент цифрової довіри. У ситуації, коли зловмисник отримує можливість генерувати математично бездоганні підробки цифрових

сертифікатів, статичні механізми перевірки довіри втрачають свою ефективність. Відповідно, центр ваги у забезпеченні кібербезпеки (далі КБ) невідворотно зміститься у бік безперервного поведінкового аналізу. Замість одноразової криптографічної ідентифікації, системи захисту змушені спиратися на синхронну оцінку легітимності дій кожного вузла під час його функціонування. Незважаючи на загальне визнання необхідності переходу до парадигми нульової довіри, тобто Zero Trust та поведінкового моніторингу, практичне впровадження цієї концепції стикнулося із фундаментальними архітектурними перешкодами. Сучасні мережі є надзвичайно складними гетерогенними середовищами (ГС). В ГС одночасно функціонують хмарні сервіси, контейнеризовані додатки та класичні сервери. Чинні системи класу SIEM (Security Information and Event Management) або IDS (Intrusion Detection Systems) здебільшого орієнтовані на збір колосальних масивів «сирих» логів. Проте під час кібервпливів, зокрема, таких як атаки на ланцюги постачання (анг. Supply Chain Attacks – SCA), шкідливий код зловмисники майстерно маскують під штатні процеси оновлення. Аналогічну ситуацію спостерігаємо й при EDoS-впливах (анг. Economic Denial of Sustainability), коли атака розмита в часі. У результаті виникає проблема «інформаційного шуму». Тобто життєво важливі поведінкові аномалії губляться у терабайтах легітимного мережевого трафіку. Для розв'язання цієї проблеми недостатньо просто наростити пропускну здатність систем моніторингу. Необхідний концептуальний перехід від екстенсивного накопичення розрізнених подій до формування структурованих «цифрових слідів» (ЦС). В статті ЦС трактуємо як агреговані та зважені за рівнем інформативності докази компрометації. У попередніх дослідженнях багатьох авторів доведено ефективність використання обсягу накопичених ЦС як предиктивного маркера в теоретико-ігрових моделях керування захистом. Однак відкритим залишилося інженерне та алгоритмічне завдання. А саме як видобувати ці ЦС з гетерогенного середовища з мінімальними обчислювальними витратами. Отже існує нагальна потреба у синтезі спеціалізованої архітектури збору даних, яка б визначала, які саме програмні сенсори (тобто проби) та на яких рівнях інфраструктури (мережевому, системному, прикладному тощо) необхідно розгортати для наповнення математичних моделей адекватними вхідними даними. З огляду на це, метою даної статті є розробка архітектури багаторівневого збору та попереднього опрацювання поведінкових артефактів на основі концепції сенсорної ієрархії. Це дозволить подати алгоритмічний процес перетворення «сирих» подій безпеки у структуровані ЦС, необхідні для забезпечення цілісного інформаційного базису систем підтримки прийняття рішень (СППР) в умовах постквантових загроз.

Постановка проблеми. Поточний стан розвитку засобів кіберзахисту ГС характеризується глибокою суперечністю між зростаючою складністю об'єктів моніторингу та деградацією надійності чинних методів верифікації. У ГС, які інтегрують хмарні обчислення, IoT-сегменти та розподілені сервіси, архітектуру безпеки зазвичай будують на «периметральній» моделі та криптографічній автентифікації. Проте в умовах наближення до «квантового переходу», коли математична стійкість асиметричних шифрів опиниться під загрозою, довіра до статичних ідентифікаторів, як-от, сертифікатів чи підписів, перестане бути константою.

Основним проблемним аспектом є відсутність методики переходу від оперативного збору технічних логів до стратегічного формування доказової бази у вигляді цифрових слідів. Наявні методи збору інформації у системах класу SIEM наразі стикнулися з трьома бар'єрами. По-перше, це інформаційна асиметрія та надмірність. Зокрема, величезний обсяг «сирих» подій у ГС створив ефект зашумленості, за якого мікроаномалії, типові для атак на ланцюги постачання, тобто SCA, залишають непоміченими на фоні легітимного трафіку. По-друге, це відсутність ієрархічної кореляції. Так переважна більшість задіяних наразі засобів моніторингу функціонують ізольовано на мережевому або системному рівнях. Це не дозволяє вибудувати цілісний вектор атаки. Зокрема, це типово для у випадках EDoS-впливів, коли шкідлива активність розподілена між прикладними запитами та системними ресурсами. Й нарешті існує методологічний розрив у СППР. Так високорівневі теоретико-ігрові моделі прийняття рішень потребують структурованих вхідних параметрів, тобто обсягу та релевантності цифрових слідів. Проте, наявні архітектури збору ЦС досі не забезпечують їхнього оперативного видобування та синхронного зважування.

Аналіз останніх досліджень і публікацій. В умовах трансформації кіберзагроз, зокрема з урахуванням розвитку постквантових обчислень та зростання складності гетерогенних інформаційних середовищ, є стійка тенденція поступового переходу від сигнатурних методів захисту до поведінкових моделей аналізу.

Одним із пріоритетних напрямів є застосування методів класу User and Entity Behavior Analytics (UEBA). Так у [1] запропоновано використання поведінкових профілів користувачів та сутностей для виявлення аномалій у корпоративних мережах. Автори довели що ефективність виявлення загроз суттєво зросте завдяки аналізу відхилень від нормальної поведінки системи. Проте питання інтеграції багаторівневих джерел даних та їх узгодженої агрегації залишилося в [1] відкритим.

Фундаментальні аспекти кіберзагроз та перехід до нової парадигм захисту розглянуто у [2]. Автори обґрунтували релевантність зміщення акценту з периметральної безпеки до аналітичних механізмів. У свою чергу, у [3] проаналізовано сучасний стан політик інформаційної безпеки (ІБ), що підтвердило потребу формалізації процесів збору та інтерпретації подій безпеки.

Значний внесок у розвиток методів виявлення аномалій зроблено у роботах [4-17]. Автори систематизували методи синтезу систем виявлення вторгнень на основі різних методик та методів, зокрема машинного та глибинного навчання. У [4] наведено комплексний огляд IDS-систем, а у [14, 15] сформовано теоретичне підґрунтя для застосування алгоритмів виявлення аномалій у великих масивах даних. Водночас зазначені методи та моделі здебільшого орієнтовані на опрацювання вже агрегованих даних і не враховували специфіку їх первинного формування в ГС.

Окремий клас досліджень присвячений обробці великих потоків даних та подій у розподілених системах. У [5, 6] авторами розглянуто архітектури обробки даних у середовищах IoT та потокових системах. Зокрема автори [6] дослідили методи виявлення відхилень у часових послідовностях подій ІБ. Отримані результати підтвердили можливість ефективного опрацювання великих обсягів телеметрії, проте не вирішили задачі семантичної інтерпретації подій у розрізі ІБ ГС. У [7] досліджено питання виявлення аномалій у хмарних середовищах із використанням методів штучного інтелекту та моделей довіри. Автори підкреслили важливість синхронного оцінювання поведінки вузлів, що є близьким до концепції формування цифрових слідів, однак не пропонують механізму їх ієрархічної агрегації.

Концептуальний перехід до моделі нульової довіри (Zero Trust) відображено у [8, 9]. Автори обґрунтували потребу безперервної верифікації дій суб'єктів у системі незалежно від їхнього розташування. Цей метод фактично передбачає використання поведінкових характеристик як основного джерела довіри. Це узгоджено з ідеєю формування ЦС.

Зазначимо, що релевантним наразі є захист ланцюгів постачання програмного забезпечення. У [10] та [11] визначені головні ризики та методи їх мінімізації, зокрема обґрунтовано потребу комплексного моніторингу поведінки компонентів систем. Проте зазначені концепції здебільшого зосереджені на організаційних та процедурних аспектах, залишив відкритим питання автоматизованого формування доказової бази компрометації.

Проблематика постквантової безпеки розглядалась у [12, 13]. Автори підкреслили ризики компрометації сучасних криптографічних механізмів та необхідність синтезу альтернативних методів забезпечення довіри. Це додатково обґрунтовує доцільність переходу до поведінкового аналізу як незалежного джерела інформації про стан безпеки.

Окремо слід відзначити дослідження у сфері цифрової криміналістики [16, 17], де ЦС розглядають як елемент доказової бази. Проте зазвичай їх формування відбувається постфактум. А діючи системи ІБ потребують їхнього оперативного та синхронного формування.

Отже, аналіз наукових джерел довів, що наявні дослідження охоплюють окремі аспекти задачі, зокрема, виявлення аномалій, обробку великих даних, Zero Trust архітектури та безпеку ланцюгів постачання. Водночас відсутня модель, яка б забезпечувала інтеграцію багаторівневого збору поведінкових артефактів, їх зважування за інформативністю та формування структурованих ЦС як вхідних параметрів для СППР. Це і визначило актуальність та наукову новизну даного дослідження.

Мета та завдання дослідження. Мета статті – розробка багаторівневої архітектури збору та попередньої обробки поведінкових артефактів у гетерогенних середовищах (ГС), яка забезпечує формування структурованого вектору цифрових слідів (ЦС) для систем підтримки прийняття рішень в умовах постквантових кіберзагроз.

Для досягнення поставленої мети необхідно розв'язати наступні задачі:

– систематизувати та класифікувати класи поведінкових артефактів на мережевому, системному та прикладному рівнях ГС, визначивши їхні питомі ваги інформативності для виявлення аномалій, притаманних атакам на ланцюги постачання та EDoS-впливам;

– розробити архітектуру ієрархічного моніторингу та відповідний математичний алгоритм агрегації розрізнених подій безпеки у структуровані ЦС, провівши оцінку ефективності запропонованого рішення шляхом обчислювального експерименту в середовищі PyCharm із використанням засобів мови Python.

## РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Перехід до поведінкового аналізу вимагає математичного опису процесу ідентифікації та накопичення ЦС. У [17] подано модель накопичення доказів $F_t$. Проте для синтезу модуля моніторингу необхідно декомпозувати процес збору, деталізувавши механізм перетворення сирих логів гетерогенної мережі на структурований вектор ЦС.

Нехай ГС має множину вузлів $N = \{1, 2, \dots, n\}$. Кожен вузол ГС генерує потік подій або артефактів поведінки. Систему збору представимо у вигляді багаторівневої сенсорної ієрархії. (БСІ). У БСІ артефакти реєструють на трьох базових рівнях. Це відповідно, мережевій ($Net$), системний ($Sys$) та прикладний ($App$).

Тоді загальний вектор сирих подій $E_t$, зафіксованих системою моніторингу в момент часу $t$, представимо так:

$$E_t = \bigcup_{i=1}^{n} \left( E_{i,t}^{Net} \cup E_{i,t}^{Sys} \cup E_{i,t}^{App} \right) \tag{1}$$

За умов постквантових атак на ланцюги постачання, зловмисник прагне мінімізувати аномальність своїх дій. Тому переважна більшість подій у множині $E_t$ є легітимним трафіком. Щоб виділити інформативні ознаки компрометації, введемо функцію фільтрації та зважування Ф. Ця функція зіставляє кожній події $e \in E_t$ її питому вагу інформативності $w_e \in [0,1]$, яка відображає ймовірність того, що подія є наслідком шкідливої активності. До прикладу атипова затримка TLS-хендшейку або нетипове завантаження CPU.

Відповідно, приріст ЦС від одного вузла $i$ за малий проміжок часу $\Delta t$ визначаємо як зважену сума інформативних артефактів:

$$\Delta f_{i,t} = \sum_{e \in E_{i,t}} \Phi(e) \cdot w_e \cdot \delta(e) \tag{2}$$

де $\delta(e)$ – індикаторна функція, що дорівнює 1, якщо подія $e$ класифікована сенсором як атипова, тобто перевищує встановлений поріг відхилення від еталонного профілю, і 0 в іншому випадку.

Для агрегації даних на рівні всієї мережі врахуємо інтенсивність захисних зусиль щодо збору та аналізу логів $u_t$, яка виступає керуючим параметром у СППР. Ще доведено у [17]. Тоді загальна швидкість накопичення структурованих ЦС $\frac{dF_t}{dt}$ набуває вигляду:

$$\frac{dF_t}{dt} = \kappa \cdot u_t \cdot \sum_{i \in N_{comp}} \Delta f_{i,t} - \lambda F_t \tag{3}$$

де $\kappa$ – коефіцієнт загальної ефективності архітектури збору визначаємо пропускною здатністю сенсорів та точністю налаштування функції Ф; $N_{comp}$ – підмножина скомпрометованих вузлів; $\lambda$ – швидкість «застарівання» або релевантності ЦС з часом.

Рівняння (3) є технологічною декомпозицією макроскопічного процесу. Воно доводить, що для підвищення швидкості формування бази доказів і, як наслідок, пришвидшення активації предиктивного маркера необхідно не лише наростити обчислювальні зусилля $u_t$, але й оптимізувати процес фільтрації Ф, відкидаючи «порожні» події ще на етапі сенсорів. Отже, така математична постановка задачі вимагає розробки відповідної архітектури програмних засобів, здатних розраховувати ваги $w_e$ без надмірного перевантаження гетерогенної інфраструктури.

Для ефективної роботи функції фільтрації Ф та коректного обчислення ваги інформативності $w_e$, що фігурують у рівнянні швидкості накопичення ЦС (3), необхідно розробити чітку таксономію джерел сирих подій. В умовах постквантових загроз, коли криптографічний захист на рівні з'єднання потенційно можна скомпрометований підробкою цифрового сертифіката, система моніторингу повинна агрегувати аномалії паралельно з кількох рівнів інфраструктури. Це дозволить нівелювати «сліпі зони» окремих сенсорів та виявити зловмисника навіть за умови успішного обходу ним механізмів автентифікації.

Згідно із запропонованою архітектурою, процес видобування подій $e \in E_t$ розподіляємо на три взаємопов'язані ієрархічні рівні:

1. Мережевий рівень ($Net$) забезпечує збір телеметрії трафіку та метаданих з'єднань (NetFlow, PCAP-статистика, параметри сесій). В умовах компрометації TLS, зловмисник із квантовим ресурсом потенційно здатен підробити підпис, однак він не завжди бездоганно відтворює фізичні та часові характеристики легітимного криптографічного хендшейку. Це, наприклад, затримка на обчислення або розмір пакетів обміну ключами.

2. Системний рівень ($Sys$) охоплює метрики продуктивності та життєдіяльності окремих вузлів. Зокрема це завантаження CPU/RAM, дискова активність, системні виклики ядра операційної системи.

Цей рівень є принциповим для ідентифікації EDoS-впливів, коли зловмисник намагається економічно виснажити хмарну інфраструктуру через генерацію зовні легітимних, але ресурсоємних фонових мікротранзакцій.

3. Прикладний рівень ($App$) реєструє логіку роботи додатків, ланцюжки викликів API, запити до баз даних або виклики методів смарт-контрактів. Моніторинг цього рівня є основним для виявлення атак на ланцюги постачання (тобто SCA), оскільки впроваджений шкідливий код, навіть діючи від імені валідного процесу, рано чи пізно ініціює нетипові для еталонної поведінки прикладні операції.

Кожному виявленому артефакту $e$ система присвоює питому вагу інформативності $w_e$, яка віддзеркалює ступінь достовірності того, що дана подія є наслідком компрометації. У Таблиці 1 наведено класифікацію базових артефактів із відповідними орієнтовними ваговими коефіцієнтами.

Значення $w_e$ не є статичними і можуть бути налаштовані алгоритмами машинного навчання під час стадії профілювання конкретної мережі. Основний принцип визначення ваги зводиться до такого – чим вищими є обчислювальні або організаційні витрати зловмисника на «якісну» імітацію легітимної поведінки за конкретною метрикою, тим вищою є вага $w_e$ цього артефакту для формування загального обсягу доказів $F_t$. Відповідно, обробка подій із високим показником $w_e$ дозволяє СППР значно швидше досягти критичної маси ЦС, коли тіньова ціна $\lambda_F$ змінить знак, сигналізуючи про необхідність активації ізоляції вузла.

На рисунку 1 наведено архітектуру розробленої СППР для протидії постквантовим атакам на ланцюги постачання ПЗ. Запропонована СППР здійснює інтеграцію методів поведінкового аналізу та диференціально-ігрового моделювання для адаптивного керування процесом ізоляції скомпрометованих вузлів.

*Таблиця 1*

**Класифікація поведінкових артефактів та їх вагових коефіцієнтів для формування ЦС (Складено авторами)**

| Рівень ієрархії | Тип артефакту (Подія $e$) | Основний вектор загрози | Питома вага $w_e$ | Обґрунтування ваги інформативності |
|---|---|---|---|---|
| Мережевий ($E^{Net}$) | Мікроаномалії затримки (latency) під час TLS-handshake | Постквантова компрометація (MitM-підробка) | 0,70-0,85 | Складно точно імітувати мережеві таймінги під час використання гібридних крипто-алгоритмів. |
| Мережевий ($E^{Net}$) | Відхилення у співвідношенні обсягів Rx/Tx трафіку | Виток даних (Data Exfiltration)/C2-комунікація | 0,40-0,60 | Може бути наслідком легітимного резервного копіювання, тому потребує кореляції з іншими рівнями. |
| Системний ($E^{Sys}$) | Асиметричні сплески завантаження CPU/RAM на типові запити | EDoS-атаки на хмарні сервіси | 0,80-0,95 | Висока ймовірність ресурсної атаки, яку маскують під штатне навантаження. |
| Системний ($E^{Sys}$) | Ініціація нетипових дочірніх процесів легітимним ПЗ | SCA (етап закріплення) | 0,85-0,95 | Пряма ознака виконання стороннього коду в контексті довіреного процесу. |
| Прикладний ($E^{App}$) | Відхилення графа викликів (Call Graph) до внутрішніх API | Експлуатація прихованих бекдорів | 0,65-0,85 | Зміна бізнес-логіки додатка після «легітимного» оновлення компонента. |
| Прикладний ($E^{App}$) | Нетипові патерни виклику методів смарт-контрактів / БД | Фішинг/Компрометація прикладного рівня | 0,75-0,90 | Спроба масового виведення активів або підміни даних авторизованим користувачем. |

На відміну від наявних, головним елементом архітектури СППР є модуль багаторівневого збору поведінкових артефактів у гетерогенних мережах, який забезпечує формування цифрових слідів як узагальненого представлення аномальної активності. Система отримує дані з різнорідних джерел, включаючи мережевий трафік, журнали безпеки (IDS/IPS, EDR), події CI/CD, а також телеметрію з хмарних та IoT/OT-систем. На основі цих даних модуль багаторівневого збору виконує агрегацію поведінкових артефактів на таких рівнях: мережевому (NetFlow, DNS, TLS, HTTP); хостовому (процеси,

системні виклики, файлові операції); прикладному (журнали застосунків, API-виклики); інфраструктурному (контейнери, віртуальні машини, сервіси); фізичному/IoT-рівні.

Результатом роботи модуля є формування сирих ЦС, які далі проходять етап нормалізації, кореляції та фільтрації шуму.

На основі опрацьованих даних обчислюємо фазові змінні моделі. А саме $x(t)$ – частка скомпрометованих вузлів; $y(t)$ – обсяг накопичених цифрових слідів. Ці змінні є вхідними параметрами для математичного ядра СППР.


*Рисунок 1. Архітектура СППР для протидії постквантовим атакам на ланцюги постачання з модулем багаторівневого збору поведінкових артефактів та предиктивним маркером ЦС*

Центральним компонентом СППР є модуль розв'язання антагоністичної диференціальної гри з використанням методу прямого та зворотного проходу (FBSM). У межах цього модуля: інтегруємо рівняння стану, які описують процес компрометації та накопичення ЦС; спряжені змінні $\lambda1(t), \lambda2(t)$, які інтерпретуємо як тіньові ціни; визначаємо оптимальні стратегії захисника та атакуючого.

Модуль предиктивного аналізу реалізує основний параметр СППР – використання предиктивного маркера, яким є зміна знаку тіньової ціни $\lambda2(t)$: при $\lambda2(t) < 0$ система перебуває у фазі накопичення доказів (інвестиційна фаза); при $\lambda2(t) > 0$ – у фазі готовності до активної ізоляції; момент $\lambda2(t) = 0$ визначає точку переходу та виступає сигналом до зміни стратегії. Отже, предиктивний маркер дозволить СППР виявити момент, коли подальше накопичення ЦС втрачає сенс і необхідно переходити до активних дій.

На основі сигналів предиктивного модуля СППР здійснює гнучке керування порогом ізоляції $\theta$. У разі виявлення переходу система: знижує поріг $\theta$; переводить систему захисту з пасивного (спостережного) режиму в активний; ініціює процедури ізоляції.

Рішення, сформовані СППР, передаємо далі до виконавчого рівня, де реалізуємо наступні дії – ізоляція та блокування вузлів; сегментація мережі; посилення механізмів IDS/IPS та EDR; перегляд політик безпеки; запуск поглибленого аналізу поведінкових артефактів.

Функціонування системи дозволить: зменшити частку скомпрометованих вузлів; локалізувати розповсюдження атак; мінімізувати сукупні втрати.

Для верифікації ефективності запропонованої архітектури, див. рис. 1, та математичної моделі збору ЦС проведено обчислювальний експеримент. Симуляцію виконано засобами мови програмування Python із використанням бібліотек наукових обчислень для генерації та аналізу стохастичних процесів у гетерогенних мережах. Сценарій експерименту передбачав імітацію функціонування корпоративного сегмента мережі протягом умовного часу $T = 100$. У нормальному режимі роботи вузли системи генерували значний обсяг легітимного фонового трафіку, відповідно мережеві запити, фонові процеси ОС, штатні виклики API тощо, який моделювався як нормальний розподіл із заданою дисперсією. У

момент часу $t = 40$ проведена умовна постквантова атака на ланцюг постачання ПЗ. Відповідно зловмисник, використовуючи підроблений цифровий сертифікат, впроваджував шкідливе оновлення ПЗ та починав генерувати мікроаномалії на мережевому, системному та прикладному рівнях інфраструктури, див. таблицю 1.

Мета експерименту – порівняти чинний сценарій моніторингу коли реалізована суцільна агрегація сирих подій без зважування та розроблену ієрархічну архітектуру, див рис. 1. Остання, використовує функцію фільтрації та вагові коефіцієнти інформативності ($w_{net} = 0{,}75,\ w_{sys} = 0{,}90,\ w_{app} = 0{,}85$). Загальний обсяг накопичених доказів $F(t)$ розраховано за диференціальним рівнянням із врахуванням швидкості застарівання слідів $\lambda$. Зміни показників наведено на рисунку 2.

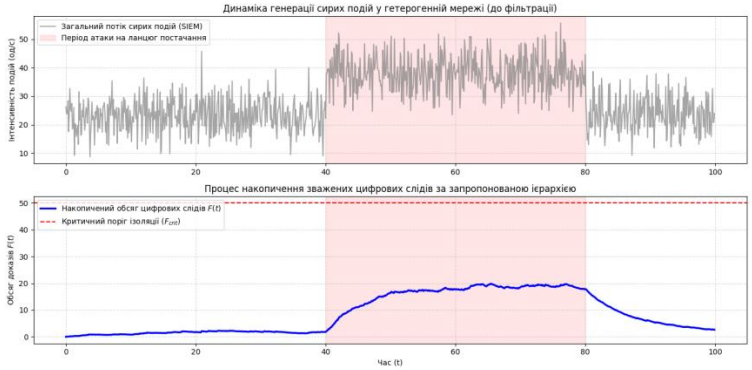


*Рисунок 2. Результати обчислювального експерименту*

Наведені на рис. 2 графічні залежності віддзеркалили недоліки чинних систем збору логів та переваги запропонованої концепції СППР.

Верхня панель графіка відображає загальний потік сирих подій у мережі. Як видно з результатів симуляції, активність зловмисника в період від $t = 40$ до $t = 80$, яку виділено зоною атаки та позначено рожевим кольором є високоорганізованою та низькоінтенсивною. Вектор шкідливих дій генерує мікроаномалії. Ці мікроаномалії фактично розмиваються у загальному масиві легітимного «шумового» трафіку гетерогенної мережі. У подібних умовах типова SIEM-система, яка оперує пороговими значеннями інтенсивності сирих подій, скоріше за все виявиться нездатною зафіксувати аномалію без генерування неприйнятно високої кількості хибних спрацювань.

Нижня панель демонструє результати роботи запропонованого математичного апарату попередньої фільтрації та зваженої агрегації. До початку атаки (на інтервалі $t < 40$) система успішно відсіює легітимний фоновий шум. Тобто обсяг сформованих ЦС $F(t)$ коливався поблизу нульової позначки завдяки механізму «забування» ЦС $\lambda$. Однак із початком шкідливого впливу, коли корельовані аномалії починали одночасно фіксуватися на мережевому, системному та прикладному рівнях, функція фільтрації виділяла корисний сигнал. Обсяг структурованих доказів$F(t)$ починав зростати. У момент часу $t \approx 50$ накопичений обсяг ЦС потенційно подолає встановлений поріг $F_{crit} = 50$ (для наведеного графіку). З практичної точки зору це означає, що розроблена архітектура здатна не лише виявити факт компрометації обходу криптографічного захисту, але й забезпечити СППР достовірним предиктивним маркером. Своєчасне досягнення порога $F_{crit}$ ініціює зміну знака тіньової ціни слідів. Це є математично обґрунтованим тригером для активації процедури ізоляції скомпрометованого сегмента ще до моменту настання незворотних деструктивних наслідків для мережі. Відповідно, запропонована модель дозволить знизити обчислювальне навантаження на аналітичні модулі СППР за рахунок відсікання «порожніх» подій безпосередньо на рівні сенсорів.

## ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

У статті розв’язано релевантну науково-прикладну задачу синтезу архітектури багаторівневого збору поведінкових артефактів у гетерогенних мережах для формування цифрових слідів (ЦС). Отримані результати дозволяють зробити наступні висновки:

1. Обґрунтовано необхідність переходу від статичних криптографічних методів захисту гетерогенних середовищ (ГС) до безперервного поведінкового моніторингу в умовах постквантових загроз. Доведено, що в ситуації потенційної компрометації PKI-інфраструктури достовірним джерелом інформації про стан безпеки вузла ГС є його ЦС.

2. Розроблено концепцію сенсорної ієрархії, яка, на відміну від наявних рішень, охопила три рівні інфраструктури. Це, відповідно, мережевий, системний та прикладний. Це дозволяє здійснювати перехресну кореляцію подій та виявляти складні атаки, зокрема, EDoS, SCA, які зловмисники маскують під легітимну активність на окремих рівнях.

3. Запропоновано математичну процедуру агрегації ЦС через введення функції фільтрації та вагових коефіцієнтів інформативності $w_e$. Це забезпечило перехід від екстенсивного накопичення «сирих» логів до формування структурованого вектору доказів $F_t$.

4. Експериментальна апробація запропонованої архітектури засобами мови Python підтвердила її обчислювальну ефективність. Результати симуляції продемонстрували, що зважений збір артефактів потенційно дозволяє ідентифікувати атипову активність у ГС та досягти порога ізоляції скомпрометованого сегмента значно раніше, ніж це можливо при використанні наявних SIEM, в умовах високого рівня мережевого шуму.

5. Показано, що практичне значення роботи полягає у можливості інтеграції запропонованих алгоритмів у діючі системи виявлення вторгнень. Це дозволить автоматизувати процес формування бази доказів, наприклад, для теоретико-ігрових моделей захисту, мінімізуючи при цьому навантаження на ресурси ГС.

Перспективи подальших досліджень полягають у застосуванні методів машинного навчання для налаштування вагових коефіцієнтів $w_e$ залежно від зміни релевантних загроз.

## СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Khan, M. Z. A., Khan, M. M., & Arshad, J. (2022). Anomaly detection and enterprise security using user and entity behavior analytics (UEBA). In *2022 3rd International Conference on Innovations in Computer Science & Software Engineering (ICONICS)* (pp. 1-9).
2. Singer, P. W., & Friedman, A. (2013). *Cybersecurity and cyberwar: What everyone needs to know*. Oxford University Press.
3. Paananen, H., Lapke, M., & Siponen, M. (2020). State of the art in information security policy development. *Computers & Security, 88*, 101608. https://doi.org/10.1016/j.cose.2019.101608
4. Ahmad, Z., Khan, A. S., Shiang, C. W., Abdullah, J., & Ahmad, F. (2021). Network intrusion detection system: A systematic study of machine learning and deep learning approaches. *Transactions on Emerging Telecommunications Technologies, 32*(1), e4150. https://doi.org/10.1002/ett.4150
5. Keshavarzian, A., Sharifian, S., & Seyedin, S. (2019). Modified deep residual network architecture deployed on serverless framework of IoT platform based on human activity recognition application. *Future Generation Computer Systems, 101*, 14-28. https://doi.org/10.1016/j.future.2019.06.009
6. Li, H., Li, Z., Peng, S., Li, J., & Tungom, C. E. (2020). Mining the frequency of time-constrained serial episodes over massive data sequences and streams. *Future Generation Computer Systems, 110*, 849-863. https://doi.org/10.1016/j.future.2019.11.008
7. Qureshi, K. N., Jeon, G., & Piccialli, F. (2021). Anomaly detection and trust authority in artificial intelligence and cloud computing. *Computer Networks, 184*, 107647. https://doi.org/10.1016/j.comnet.2020.107647
8. Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero trust architecture* (NIST Special Publication 800-207). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-207
9. Ashfaq, S., Patil, S. A., Borde, S., Chandre, P., Shafi, P. M., & Jadhav, A. (2023). Zero trust security paradigm: A comprehensive survey and research analysis. *Journal of Electrical Systems, 19*(2).
10. Boyens, J., Paulsen, C., Moorthy, R., & Bartol, N. (2022). *Supply chain risk management practices for federal information systems and organizations* (NIST Special Publication 800-161 Revision 1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-161r1
11. Reichert, B. M., & Obelheiro, R. R. (2024). Software supply chain security: A systematic literature review. *International Journal of Computers and Applications, 46*(10), 853-867. https://doi.org/10.1080/1206212X.2024.2390978
12. Chen, L., Jordan, S., Liu, Y.-K., Moody, D., Peralta, R., Perlner, R., & Smith-Tone, D. (2016). *Report on post-quantum cryptography* (NIST Interagency/Internal Report 8105). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8105
13. Joseph, D., Misoczki, R., Manzano, M., Tricot, J., Pinuaga, F. D., Lacombe, O., ... Hansen, R. (2022). Transitioning organizations to post-quantum cryptography. *Nature, 605*(7909), 237-243. https://doi.org/10.1038/s41586-022-04623-2

14. Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. *ACM Computing Surveys*, *41*(3), Article 15. https://doi.org/10.1145/1541880.1541882
15. Pang, G., Shen, C., Cao, L., & van den Hengel, A. (2021). Deep learning for anomaly detection: A review. *ACM Computing Surveys*, *54*(2), Article 38. https://doi.org/10.1145/3439950
16. Casey, E. (2011). *Digital evidence and computer crime: Forensic science, computers, and the Internet* (3rd ed.). Academic Press.
17. Lakhno, V., Voloshyn, S., Mamchenko, S., Kulinich, O., & Kasatkin, D. (2024). Cluster analysis for studying digital traces of students in educational institutions. Cybersecurity: Education, Science, Technique, 3(23), 31-41. https://doi.org/10.28925/2663-4023.2024.23.3141

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 2 (34), 2026
ISSN 2663 – 4023

**Valerii Lakhno**
Doctor of Technical Sciences, Professor, Professor of Department of Computer Systems and Networks
National University of Life and Environmental Sciences of Ukraine, Kyiv, Ukraine
ORCID: 0000-0001-9695-4543
*lva964@nubip.edu.ua*

**Valerii Hladkykh**
Associated Professor, Department of Computer Systems and Networks,
National University of Life and Environmental Sciences of Ukraine, Kyiv, Ukraine
ORCID: 0000-0002-5868-9504
*v.hladkykh@nubip.edu.ua*

**Andrii Sahun**
Associated Professor, Department of Computer Systems and Networks,
National University of Life and Environmental Sciences of Ukraine, Kyiv, Ukraine
ORCID: 0000-0002-5151-9203
*a.sagun@nubip.edu.ua*

## MULTILEVEL ARCHITECTURE FOR BEHAVIORAL ARTIFACT COLLECTION IN HETEROGENEOUS NETWORKS TO FORM DIGITAL FOOTPRINTS

**Abstract.** The object of research is the process of generating a digital evidence array within heterogeneous information and communication systems under post-quantum cyber threats. The subject of research encompasses architectural solutions and methods for the multilevel collection of behavioral artifacts for decision support systems (DSS). The relevance of this work stems from the need to develop alternative security verification methods for network nodes in cases where current cryptographic identification (TLS, PKI) may be compromised by an adversary with access to quantum resources. Unlike existing methods focused on analyzing individual log types, this paper proposes the concept of a sensor hierarchy covering the network, system, and application levels of the infrastructure. The scientific novelty of the results lies in the formalization of the procedure for transforming disparate raw security events into structured "digital footprints." Specifically, a multilevel monitoring architecture has been developed, enabling flexible adjustments to the intensity of artifact collection depending on the network segment type and the predicted attack vector (EDoS impacts, Supply Chain Attacks). For the first time, a methodology for weighting behavioral features based on their informativeness is described, ensuring the minimization of computational costs for data processing while maintaining high reliability in forming input parameters for game-theoretic security models. The practical significance of the work lies in the development of software module structures for data aggregation that can be integrated into existing SIEM/IDS platforms. The implementation of the proposed architecture using the Python language has enabled the automation of detecting anomalous deviations in node behavior, even when digital certificates formally remain valid. Experimental validation of the architecture confirmed its ability to ensure the integrity of the DSS information base, even under conditions of changing heterogeneous environment topology and significant network noise levels.

**Keywords:** monitoring architecture, behavioral artifacts, digital footprints, heterogeneous networks, post-quantum security, sensor hierarchy, data aggregation.

### REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Khan, M. Z. A., Khan, M. M., & Arshad, J. (2022). Anomaly detection and enterprise security using user and entity behavior analytics (UEBA). In *2022 3rd International Conference on Innovations in Computer Science & Software Engineering (ICONICS)* (pp. 1-9).
2. Singer, P. W., & Friedman, A. (2013). *Cybersecurity and cyberwar: What everyone needs to know*. Oxford University Press.
3. Paananen, H., Lapke, M., & Siponen, M. (2020). State of the art in information security policy development. *Computers & Security, 88*, 101608. https://doi.org/10.1016/j.cose.2019.101608

4. Ahmad, Z., Khan, A. S., Shiang, C. W., Abdullah, J., & Ahmad, F. (2021). Network intrusion detection system: A systematic study of machine learning and deep learning approaches. *Transactions on Emerging Telecommunications Technologies, 32*(1), e4150. https://doi.org/10.1002/ett.4150
5. Keshavarzian, A., Sharifian, S., & Seyedin, S. (2019). Modified deep residual network architecture deployed on serverless framework of IoT platform based on human activity recognition application. *Future Generation Computer Systems, 101*, 14-28. https://doi.org/10.1016/j.future.2019.06.009
6. Li, H., Li, Z., Peng, S., Li, J., & Tungom, C. E. (2020). Mining the frequency of time-constrained serial episodes over massive data sequences and streams. *Future Generation Computer Systems, 110*, 849-863. https://doi.org/10.1016/j.future.2019.11.008
7. Qureshi, K. N., Jeon, G., & Piccialli, F. (2021). Anomaly detection and trust authority in artificial intelligence and cloud computing. *Computer Networks, 184*, 107647. https://doi.org/10.1016/j.comnet.2020.107647
8. Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero trust architecture* (NIST Special Publication 800-207). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-207
9. Ashfaq, S., Patil, S. A., Borde, S., Chandre, P., Shafi, P. M., & Jadhav, A. (2023). Zero trust security paradigm: A comprehensive survey and research analysis. *Journal of Electrical Systems, 19*(2).
10. Boyens, J., Paulsen, C., Moorthy, R., & Bartol, N. (2022). *Supply chain risk management practices for federal information systems and organizations* (NIST Special Publication 800-161 Revision 1). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-161r1
11. Reichert, B. M., & Obelheiro, R. R. (2024). Software supply chain security: A systematic literature review. *International Journal of Computers and Applications, 46*(10), 853-867. https://doi.org/10.1080/1206212X.2024.2390978
12. Chen, L., Jordan, S., Liu, Y.-K., Moody, D., Peralta, R., Perlner, R., & Smith-Tone, D. (2016). *Report on post-quantum cryptography* (NIST Interagency/Internal Report 8105). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.IR.8105
13. Joseph, D., Misoczki, R., Manzano, M., Tricot, J., Pinuaga, F. D., Lacombe, O., ... Hansen, R. (2022). Transitioning organizations to post-quantum cryptography. *Nature, 605*(7909), 237-243. https://doi.org/10.1038/s41586-022-04623-2
14. Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. *ACM Computing Surveys, 41*(3), Article 15. https://doi.org/10.1145/1541880.1541882
15. Pang, G., Shen, C., Cao, L., & van den Hengel, A. (2021). Deep learning for anomaly detection: A review. *ACM Computing Surveys, 54*(2), Article 38. https://doi.org/10.1145/3439950
16. Casey, E. (2011). *Digital evidence and computer crime: Forensic science, computers, and the Internet* (3rd ed.). Academic Press.
17. Lakhno, V., Voloshyn, S., Mamchenko, S., Kulinich, O., & Kasatkin, D. (2024). Cluster analysis for studying digital traces of students in educational institutions. Cybersecurity: Education, Science, Technique, 3(23), 31-41. https://doi.org/10.28925/2663-4023.2024.23.3141

Отримано редакцією журналу / Received: 16.01.26
Прорецензовано / Revised: 02.02.26
Схвалено до друку / Accepted: 24.09.26