16. Digital Transformation of the Design, Construction and Management Processes of the Built Environment / Bruno Daniotti, Marco Gianinetto, Stefano Della Torre (eds). Cham: Springer International Publishing, 2020. DOI: 10.1007/978-3-030-33570-0.

17. Alrabiah, A., Drew, S. (2018). Formulating optimal business process change decisions using a computational hierarchical change management structure framework. Journal of Systems and Information Technology, 20, 2, 207–240. DOI: 10.1108/jsit-08-2017-0069.

18. Serrat, O. Knowledge Solutions: Tools, Methods, and Approaches to Drive Organizational Performance. Singapore: Springer, 2017. DOI: 10.1007/978-981-10-0983-9.

19. Rimini, G., Robert, P. (2008). Reengineering Lead to Cash – Process and Organization. In: E-Government: ICT Professionalism and Competences; Service Science. Boston, MA: Springer US, 219–226. DOI: 10.1007/978-0-387-09712-1_24.

20. Chang, S., Nam, K. (2022). Exploring the Sustainable Values of Smart Homes to Strengthen Adoption. Buildings, 12, 11, 1919. DOI: 10.3390/buildings12111919.

21. Serafeimidis, V., Smithson, S. (2003). Information systems evaluation as an organizational institution – experience from a case study. Information Systems Journal, 13, 3, 251–274. DOI: 10.1046/j.1365-2575.2003.00142.x.

Надійшла до редакції (Received): 07.02.2026
Прийнята до друку (Accepted): 17.03.2026
Опубліковано онлайн (Available online): 30.03.2026

УДК 004.056.53:004.7
DOI: 10.31673/2409-7292.2026.011184

Прокопович-Ткаченко Д.І., Єжихін А.В., Бушков В.Г., Черкаський О.В., Черкаський Д.О.

ФОРМУВАННЯ ЦІЛЬОВОГО ЦИФРОВОГО ПРОФІЛЮ БЕЗПЕКИ МЕРЕЖ ЕЛЕКТРОННИХ КОМУНІКАЦІЙ В УМОВАХ ГІБРИДНИХ КІБЕРАТАК: РИЗИК-ОРІЄНТОВАНИЙ ТА БАГАТОКРИТЕРІАЛЬНИЙ ПІДХІД

У статті розроблено концепцію цільового цифрового профілю безпеки мереж електронних комунікацій як формалізованого набору вимог, контролів, параметрів конфігурації та метрик спостережуваності, що забезпечує досягнення заданого рівня кіберзахисту в умовах гібридних кібератак. Актуальність зумовлена розривом між формальним виконанням мінімальних вимог і потребою доказового керування ризиками для сервісів доступу, транспортних сегментів і прикладних платформ за неповних та неоднорідних даних телеметрії. Метою є методика, що поєднує оцінювання ризику, багатокритеріальну пріоритизацію заходів і параметризацію технічних налаштувань для циклу виявлення та реагування у центрі операцій кібербезпеки. Запропоновано алгоритм: визначення меж системи і класифікації трафіку та даних; моделювання загроз із урахуванням уразливостей протоколу Secure Sockets Layer і протоколу Simple Network Management Protocol у атаках на вбудоване програмне забезпечення; мапування контролів на стандарти; відбір портфеля; визначення метрик достатності та доказової бази. Для підвищення якості детекції застосовано перетворення пакетних дампів і зразків прошивок у зображення з байтів та ансамбль глибоких моделей: згорткова нейронна мережа у поєднанні з мережею довготривалої короткочасної пам’яті для класифікації інцидентів і автоенкодер у поєднанні з мережею довготривалої короткочасної пам’яті для виявлення аномалій; кореляцію подій виконано у системі керування інформацією та подіями безпеки. Експерименти показали приріст узгодженої метрики точності й повноти на 7–12 відсотків і скорочення часу локалізації інцидентів завдяки сегментації, мікроавторизації та принципам архітектури нульової довіри. Практична цінність полягає у відтворюваному формуванні дорожньої карти кіберзахисту та швидкій перевірці профілю під час змін архітектури й ланцюгів постачання. Це спрощує керування змінами й аудит мереж оператора.

Ключові слова: цифровий профіль безпеки, мережі електронних комунікацій, гібридні кібератаки, система виявлення вторгнень, система керування інформацією та подіями безпеки, архітектура нульової довіри, протокол Secure Sockets Layer, протокол Simple Network Management Protocol, безпека вбудованого програмного забезпечення, глибоке навчання, багатокритеріальна оптимізація.

Вступ

Мережі електронних комунікацій еволюціонують від класичних ієрархічних топологій до програмно керованих, віртуалізованих та хмарно-інтегрованих архітектур, у яких межа між

транспортним сегментом, сервісною платформою і середовищем керування стає умовною. Така трансформація підвищує масштабованість і гнучкість, але одночасно збільшує площу атаки через розширення інтерфейсів керування, інтеграційних контурів, автоматизованих ланцюгів постачання та залежності від телеметрії, журналів і зовнішніх довірчих відносин. У практиці оператора інцидент дедалі рідше є ізольованою подією: він формується як комбінація технічних вразливостей, організаційних слабкостей та інформаційно-психологічного впливу, тобто відповідає класу гібридних кібератак [7], [8]. Багатостадійність і «ланцюги технік» у таких атаках описуються сучасними таксономіями та моделями поведінки противника [5], [7].

Постановка проблеми

Зростання тиску нормативних вимог та очікувань щодо кіберстійкості часто породжує в організаціях феномен формальної відповідності: політики та регламенти існують, але не прив'язані до конкретної архітектури, актуальних загроз і експлуатаційних обмежень мережі [1], [2]. Унаслідок цього виникає «паперовий щит», який не забезпечує прийнятного часу виявлення та відновлення. Джерелом проблеми є розрив між рамковим управлінням ризиками та практичною параметризацією контролів: відсутній операційний механізм зв'язку між ризиком, налаштуваннями та метриками реагування [3], [4]. Також загострюється конфлікт між доступністю сервісів і «жорсткістю» контролів, що потребує явного обліку компромісів [6], [10].

Аналіз останніх досліджень і публікацій

Дослідження вказують на домінування загроз до площини керування, інфраструктури віртуалізації та ланцюгів постачання [8], [21]. Важливе місце посідають праці щодо вразливостей протоколів SSL та SNMP у вбудованому ПЗ [11-14]. Сучасний напрям розвитку пов'язаний із застосуванням машинного навчання: глибокі нейронні моделі демонструють високу точність у класифікації атак [18], [19], а підхід перетворення бінарних артефактів у зображення (Byte2Image) дозволяє автоматизувати аналіз прошивок [16], [17]. Водночас експлуатаційна практика підкреслює потребу у контекстному збагаченні подій та відтворюваних плейбуках у системах SIEM [20], [25], [30]. Питання якості даних і безперервності логування розглядаються як фундамент ефективності детекційних механізмів [27], [28].

Завдання дослідження

Для досягнення мети дослідження необхідно вирішити такі завдання:

1. Визначити структуру та параметри «цифрового профілю безпеки» як ключового операційного артефакту [9], [20];
2. Розробити методику багатокритеріальної пріоритизації заходів захисту з урахуванням ефективності, вартості та впливу на доступність;
3. Описати механізми інтеграції контролів із системами виявлення вторгнень (IDS) та управління інформацією (SIEM) [3], [20];
4. Дослідити можливості мультимодальної підтримки процесів виявлення на основі аналізу мережевих журналів та ознак протоколів керування [16], [19].

Мета роботи

Метою дослідження є розроблення методики формування цільового цифрового профілю безпеки мереж електронних комунікацій, яка поєднує оцінювання ризику, багатокритеріальну пріоритизацію заходів і параметризацію контролів із вимогами спостережуваності та інтеграцією з системами виявлення вторгнень і керування інформацією та подіями безпеки [3], [20]. Внесок роботи полягає у створенні «єдиної точки правди» для контролів і доказів, що забезпечує перехід від загальних вимог до керованих налаштувань за ресурсних обмежень [29], [30].

Виклад основного матеріалу дослідження

У цьому розділі описано методологію формування цільового цифрового профілю безпеки мереж електронних комунікацій як відтворюваної, аудитопридатної процедури, що

© Прокопович-Ткаченко Д.І., Єжихін А.В., Бушков В.Г., Черкаський О.В., Черкаський Д.О. Формування цільового цифрового профілю безпеки мереж електронних комунікацій в умовах гібридних кібератак: ризик-орієнтований та багатокритеріальний підхід. Сучасний захист інформації, 1(65), 87–103. https://doi.org/10.31673/2409-7292.2026.011184

поєднує ризик-орієнтоване оцінювання, багатокритеріальну пріоритизацію та параметризацію контролів із вимогами спостережуваності. Методика побудована так, щоб переходити від рамкових вимог управління ризиками до конкретних технічних налаштувань, доказів їх застосування та метрик достатності, придатних для щоденної експлуатації центром операцій кібербезпеки. За основу підходу взято практики оцінки ризиків і каталогізації контролів, у яких центральним є вимірюваний зв'язок між загрозами, уразливостями, наслідками та обраними заходами захисту [3], [9].Дизайн дослідження передбачає поєднання двох класів рішень. Перший клас – аналітичний: моделювання загроз і оцінювання поточного та залишкового ризику з урахуванням якості телеметрії, а також оптимізаційний відбір портфеля контролів за ресурсних та експлуатаційних обмежень. Другий клас – експлуатаційний: інтеграція профілю з інструментами виявлення та кореляції подій, де параметри профілю керують правилами і порогами, а результати інцидентів повертаються у профіль як доказова база та підстава для перегляду пріоритетів. Така постановка узгоджується з вимогами до обробки інцидентів і практиками централізованого моніторингу та реагування [10], [20].Окремо в методах фіксується фокус на гібридних сценаріях, характерних для площини керування та ланцюгів постачання, де важливими є вразливості реалізацій протоколу Secure Sockets Layer і протоколу Simple Network Management Protocol у вбудованому програмному забезпеченні. Для підсилення детекції використано мультимодальні представлення: події та часові ряди з телеметрії мережі, ознаки протоколів керування, а також бінарні артефакти прошивок, перетворені у зображення з байтів (Byte2Image) для обробки глибокими моделями [16], [17]. Моделювання детекції реалізовано ансамблем згорткової нейронної мережі у поєднанні з мережею довготривалої короткочасної пам'яті та автоенкодера у поєднанні з мережею довготривалої короткочасної пам'яті, що дозволяє розділяти класифікацію відомих патернів і виявлення повільних аномальних змін [18], [19].Методика також враховує, що застосування моделей машинного навчання в операційній безпеці потребує керування ризиками самих моделей: дрейф ознак, помилкові спрацювання, деградація якості даних та безпечний життєвий цикл змін. Тому параметри моделей, пороги та правила кореляції розглядаються як елементи профілю, які мають бути керованими й контрольованими так само, як і класичні технічні налаштування, що узгоджується з підходами до управління ризиками штучного інтелекту [31].

Загальна схема формування цифрового профілю

Методика формування цільового цифрового профілю безпеки (далі профіль) реалізується як послідовність кроків, у якій результати кожного кроку стають входом для наступного, а всі артефакти мають бути придатними до аудиту та повторного використання:

1. Визначення меж і контексту. Формуються межі мережі електронних комунікацій (сегменти доступу, транспорт, ядро, керування, білінг, зовнішні інтеграції), визначаються залежності сервісів, режими доступності та критичність вузлів. Далі виконується класифікація даних і трафіку (персональні дані, службові журнали, дані керування, телеметрія мережі), а також визначаються вимоги щодо конфіденційності, цілісності та доступності [1], [26], [29];

2. Моделювання загроз і оцінка ризику. Будується модель загроз із прив'язкою до активів і до технік противника [7]. Особлива увага приділяється площині керування і постачанням: firmware-атаки з використанням слабкостей SSL і SNMP розглядаються як окремі сценарії, оскільки вони дозволяють непомітно змінювати конфігурації, перехоплювати керування або створювати стійкі закладки [11], [13], [21], [23]. На цьому ж кроці задаються джерела спостережуваності (логи, NetFlow/IPFIX, телеметрія систем, TLS fingerprints, SNMP traps, індикатори цілісності прошивок);

3. Мапінг контролів на стандарти і вимоги. Контролі профілю узгоджуються зі стандартами і політиками організації, з урахуванням мінімальних вимог і галузевих практик [1], [4], [5], [27]. Важливо, що мапінг не завершується переліком контролів: для кожного контролю додаються параметри реалізації, джерела доказів і критерії достатності;

© Прокопович-Ткаченко Д.І., Єжихін А.В., Бушков В.Г., Черкаський О.В., Черкаський Д.О. Формування цільового цифрового профілю безпеки мереж електронних комунікацій в умовах гібридних кібератак: ризик-орієнтований та багатокритеріальний підхід. Сучасний захист інформації, 1(65), 87–103. https://doi.org/10.31673/2409-7292.2026.011184

4. Багатокритеріальне ранжування і відбір портфеля. Формується список кандидатних заходів (технічних і організаційних) та виконується ранжування з урахуванням ефективності, вартості, складності, впливу на доступність, зрілості процесів і надійності вихідних даних. Ранжування переводиться у відбір портфеля через оптимізаційну постановку за обмеженнями бюджету, часу та допустимого впливу на сервіс [3], [4];

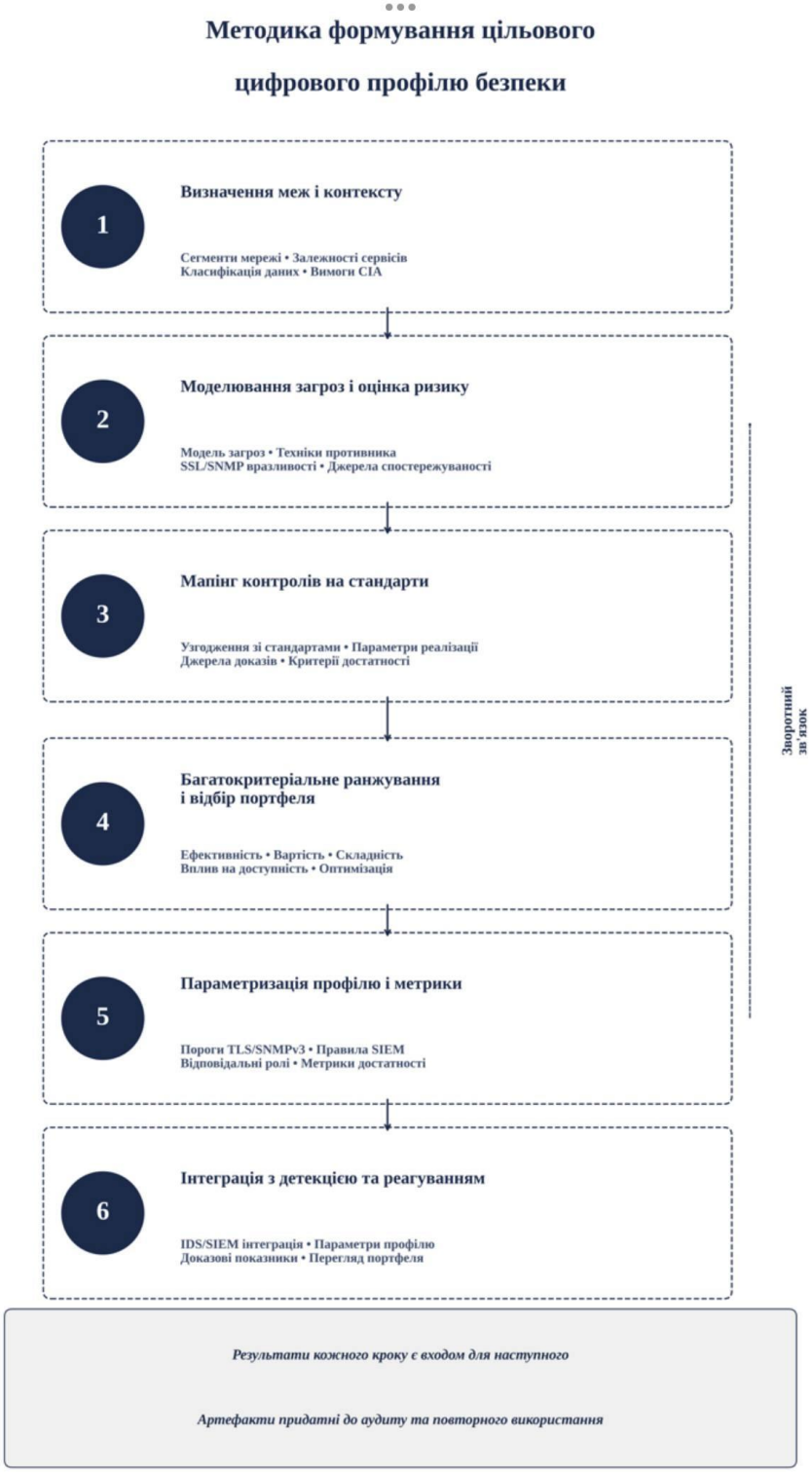

Рис. 1. Методика формування цільового цифрового профілю безпеки мережі електронних комунікацій (ризик-орієнтований багатокритеріальний підхід).

© Прокопович-Ткаченко Д.І., Єжихін А.В., Бушков В.Г., Черкаський О.В., Черкаський Д.О. Формування цільового цифрового профілю безпеки мереж електронних комунікацій в умовах гібридних кібератак: ризик-орієнтований та багатокритеріальний підхід. Сучасний захист інформації, 1(65), 87–103. https://doi.org/10.31673/2409-7292.2026.011184

5. Параметризація профілю і метрики. Для контролів встановлюються конкретні пороги і правила (наприклад, політики TLS, SNMPv3, сегментація, правила кореляції в SIEM, профілі сповіщень), визначаються відповідальні ролі, періодичність перевірок і набір метрик для моніторингу достатності (coverage, detection latency, false positive rate, mean time to respond, показники цілісності прошивок) [20], [30];

6. Інтеграція з детекцією та реагуванням. Профіль «підключається» до операційних процесів: система виявлення вторгнень (IDS) та SIEM мають отримувати параметри, правила і контекст із профілю, а результати детекції мають повертатися у профіль як доказові показники і підстава для перегляду портфеля [20], [30].

Сучасні мережі електронних комунікацій функціонують в умовах гібридних кібератак, коли загрози еволюціонують швидше за регламенти, а дані спостережуваності є неповними та різнорідними. За таких обставин цифровий профіль безпеки має бути керованим набором цільових параметрів і контрольних заходів, які узгоджені зі стандартами, підтверджені оцінкою ризику та перевіряються метриками. Запропонована методика формує профіль як відтворюваний процес: від визначення контексту та моделювання загроз (з урахуванням уразливостей SSL і SNMP у firmware-атаках) до вибору портфеля контролів та інтеграції з IDS і SIEM для детекції та реагування.

На рис. 1 подано послідовність формування цільового цифрового профілю безпеки з ітеративним зворотним зв'язком. Спочатку визначаються межі та контекст: сегменти мережі, залежності сервісів, класифікація активів і вимоги до конфіденційності, цілісності та доступності. Далі виконується моделювання загроз і оцінка ризику, включно зі сценаріями, що пов'язані з уразливостями SSL/SNMP та firmware-атаками, а також уточнюються джерела спостережуваності й прогалини даних. Після цього заходи безпеки зіставляються з вимогами стандартів і регуляторики та задаються параметри реалізації й критерії достатності доказів. На наступному кроці виконується багатокритеріальне ранжування альтернатив і відбір портфеля з урахуванням ефективності, вартості, складності впровадження та впливу на доступність, а також ресурсних обмежень. Потім профіль параметризується через цільові пороги, правила та метрики, зокрема для SIEM-кореляції й контролю досягнення заданого рівня. Завершальна частина передбачає інтеграцію з IDS/SIEM, налаштування кореляцій і процедур реагування та перевірку результативності, після чого результати моніторингу повертаються у цикл для уточнення моделі ризику та параметрів профілю.

Ймовірнісна модель ризику з урахуванням якості спостережуваності

У мережевих середовищах з великою кількістю компонентів ризик має бути обчислюваним навіть за неповних даних. Для цього вводимо змінну $q \in [0,1]$, що інтерпретується як коефіцієнт надійності телеметрії (повнота і точність журналів, стабільність часових міток, узгодженість нормалізації). Нехай T_k – подія реалізації загрози типу k (наприклад, «компрометація площини керування через firmware-ланцюг постачання» або «несанкціонована зміна параметрів SNMP»), а X – вектор ознак спостережуваності (сигнали IDS, статистики потоків, TLS fingerprints, SNMP traps тощо). Байєсівське оновлення апостеріорної ймовірності загрози записуємо як:

$$P(T_k|X,q) = \frac{P(X|T_k,q)\,P(T_k)}{\sum_{j=1}^{K} P(X|T_j,q)\,P(T_j)}\ , \tag{1}$$

де $P(T_k)$ – апріорна оцінка, що формується з урахуванням галузевого ландшафту загроз і профілю противника [7], [8], а параметр q впливає на правдоподібність $P(X|T_k,q)$ через моделювання пропусків і шуму у даних.

Для активів $a \in \mathcal{A}$ вводимо наслідок (impact) $I(a)$ у відносних одиницях або у грошовому еквіваленті, а також функцію уразливості $V(a,c)$, що залежить від реалізованих контролів c (наприклад, політика TLS, SNMPv3, сегментація, контроль цілісності прошивок). Тоді очікуваний залишковий ризик мережі в горизонті планування оцінюємо як:

$$R_{\text{res}}(c) = \sum_{a\in\mathcal{A}} \sum_{k=1}^{K} P(T_k|X,q)\, I(a)\, V(a,c)\, \rho(a,q)\ , \qquad (2)$$

де $\rho(a,q)$ – штрафний множник, що підвищує оцінку ризику за низької надійності даних для критичних активів (наприклад, якщо відсутній журнал змін конфігурації або вимкнені ключові сенсори в сегменті керування).

Особливу роль у дослідженні відіграють сценарії, у яких вразливості SSL і SNMP в прошивках та у керуючих сервісах знижують $V(a,c)$ лише за умови коректної параметризації контролів. Наприклад, формальна наявність «шифрування» не зменшує ризик, якщо реалізація SSL у firmware не валідує сертифікат або допускає небезпечні набори шифрів [12], [23]. Аналогічно, наявність SNMP як протоколу моніторингу не є ризиком сама по собі, але використання SNMPv2c без шифрування, із типовими community strings, або з надмірним доступом до MIB може перетворюватися на канал компрометації [13], [15], [22]. Тому профіль фіксує не лише «контроль існує», а й «параметр контрольного стану».

Багатокритеріальна пріоритизація та оптимізація портфеля

Нехай $\mathcal{M} = \{m_1, \dots, m_n\}$ – множина кандидатних заходів (контролів) для профілю. Для кожного заходу визначається вектор критеріїв $g(m_i)$: ефективність зменшення ризику, вартість, складність впровадження, вплив на доступність, сумісність з процесами, залежність від зрілості персоналу, а також надійність вихідних даних для обґрунтування. У практичній реалізації зручно розділяти критерії на «виграш» і «витрати». Для отримання ваг критеріїв використовуються експертні порівняння або нормовані політики організації, після чого формується інтегральна корисність $U(m_i)$.

Далі ранжування переводиться у відбір портфеля. Нехай бінарна змінна $x_i \in \{0,1\}$ означає вибір заходу m_i. Вводимо бюджет B, ресурс часу H та обмеження допустимого впливу на доступність сервісів $A_{\max}$ (наприклад, межа сумарного «down-time risk» при впровадженні сегментації чи змін TLS-політик). Тоді задачу відбору портфеля подамо як:

$$\begin{aligned} \max_{x_1,\dots,x_n} \quad & \sum_{i=1}^{n} U(m_i)\, x_i - \lambda R_{\text{res}}(c(x)) \\ \text{s.t.} \quad & \sum_{i=1}^{n} \text{cost}(m_i)\, x_i \le B, \\ & \sum_{i=1}^{n} \text{time}(m_i)\, x_i \le H, \\ & \sum_{i=1}^{n} \text{avail\_impact}(m_i)\, x_i \le A_{\max}, \\ & x_i \in \{0,1\},\ i = 1, \dots, n, \end{aligned} \qquad (3)$$

де λ – коефіцієнт, що балансує «корисність» і «залишковий ризик», а $c(x)$ – набір реалізованих контролів, що відповідає вибраному вектору x.

Такий перехід від ранжування до портфеля важливий для мереж електронних комунікацій, де частина заходів може бути високоефективною, але потребує значного часу на впровадження і може тимчасово погіршувати доступність, що неприпустимо для операторських сервісів. У цій роботі портфель також узгоджується з принципами нульової довіри (Zero Trust), де доступ визначається контекстом, мінімальними привілеями і постійною верифікацією, а не статичною «мережевою довірою» [6]. Відповідно, профіль має включати сегментацію, ідентифікацію, сильну автентифікацію і контроль сесій як параметризовані вимоги.

Моделі детекції на основі Byte2Image, CNN+LSTM та AE+LST

У гібридних атаках значна частина сигналів має різну природу: числові часові ряди (потоки, затримки), категоріальні події (логи), бінарні артефакти (прошивки), а також «контекстні» дані (топологія, політики доступу). Для зменшення розриву між цими джерелами профіль задає єдині правила перетворення даних у ознаки для детекції.

Byte2Image. Бінарні блоки прошивок та витяги з мережевих дампів перетворюються у матрицю пікселів, де байти відображаються на інтенсивність. Після нормалізації формується зображення $I \in \mathbb{R}^{h\times w}$, що підлягає обробці згортковими мережами [16], [17], [21]. Такий підхід

корисний для сценаріїв firmware-атаки, де зміни у бібліотеках SSL або SNMP-агентах можуть виявлятися як структурні патерни у байтовому просторі.

CNN+LSTM. Для трафіку, що представлений як послідовність вікон W_t (наприклад, статистики потоків, TLS fingerprints, частоти SNMP запитів), використовуємо комбінацію згорткової мережі для локальних ознак та рекурентної мережі типу Long Short-Term Memory (LSTM) для часових залежностей. Нехай $\phi_{\text{cnn}}(\cdot)$ – оператор згорткового виділення ознак, а $\psi_{\text{lstm}}(\cdot)$ – оператор рекурентного оновлення стану. Тоді ймовірність класу атаки y для вікна t визначається як:

$$\hat{y}_t = \text{softmax}(W_o \cdot \psi_{\text{lstm}}(\phi_{\text{cnn}}(W_t), h_{t-1}) + b_o)\,, \tag{4}$$

де W_o, b_o – параметри вихідного шару, h_{t-1} – попередній стан. Така модель дозволяє поєднувати ознаки рівня пакетів і сеансів, зокрема для виявлення аномальних TLS переговорів, нетипових послідовностей SNMP-запитів або нетипового співвідношення керуючого та користувацького трафіку [18], [24].

AE+LSTM. Для детекції невідомих або слабко маркованих атак використовується автоенкодер з LSTM-динамікою, який навчається реконструювати «нормальну» поведінку часових рядів. Нехай $X_{t-L+1:t}$ – вектор ознак за останні L кроків, $\text{Enc}(\cdot)$ – енкодер, $\text{Dec}(\cdot)$ – декодер. Тоді аномалійний бал визначаємо як зважену похибку реконструкції:

$$S_t = \|X_{t-L+1:t} - \text{Dec}(\text{Enc}(X_{t-L+1:t}))\|_2^2 \cdot (1 + \beta(1-q))\,, \tag{5}$$

де множник $(1 + \beta(1-q))$ підсилює сигнал аномалії за низької надійності телеметрії, щоб профіль у таких випадках «консервативно» збільшував увагу до потенційних інцидентів. AE+LSTM особливо корисний для повільних гібридних атак з низьким рівнем шуму, коли противник змінює параметри керування, поступово накопичує доступ або маскує активність під операційні процеси [19].

Інтеграція з IDS, SIEM та метриками профілю

Система виявлення вторгнень (IDS) у методиці розглядається як сенсорний шар, який забезпечує первинні сповіщення і збагачення, а SIEM – як шар кореляції, нормалізації та управління інцидентами [20]. Цифровий профіль безпеки задає:

- набір джерел телеметрії (логування, мережеві датчики, журнали змін конфігурації, моніторинг цілісності firmware);
- мінімальні поля подій, необхідні для кореляції (час, актив, користувач/сервіс, контекст сегмента, результат автентифікації, TLS fingerprint, SNMP параметри);
- правила кореляції і пороги (наприклад, аномалійний бал S_t вище порогу, поєднаний з появою невідомого TLS fingerprint і SNMP-запитів до чутливих MIB);
- метрики достатності (coverage контролів, стабільність часового синхронізму, частота хибних спрацювань, час підтвердження інциденту, час локалізації, частка інцидентів із відновленим першоджерелом).

Особливий акцент робиться на параметризації контролів SSL і SNMP. Для SSL-політик профіль фіксує мінімальні версії, заборонені набори шифрів, вимоги до валідації сертифікатів, вимоги до ротації ключів, а також телеметрію, що підтверджує їх застосування у конкретних вузлах і прошивках [10], [12], [23]. Для SNMP профіль задає вимогу використання SNMPv3, конфігурацію USM, обмеження доступу до MIB, мережеву сегментацію для керування і контроль типових community strings як індикатора компрометації або помилкової конфігурації [13], [14], [22].

Результати

У цьому розділі подано результати експериментальної перевірки запропонованої методики формування цільового цифрового профілю безпеки мереж електронних комунікацій в умовах гібридних кібератак. Наведені матеріали демонструють, як ризик-орієнтована параметризація контролів та їх прив’язка до доказів спостережуваності трансформуються у

вимірювані покращення детекції й реагування в контурі IDS/SIEM, зокрема для сценаріїв, пов'язаних з уразливостями SSL і SNMP у firmware-атаках.

Розгляд починається з опису експериментальних сценаріїв та складу даних, після чого наведено приклад практичної параметризації профілю (контролі, їх конфігураційні вимоги, докази та метрики достатності).

Далі представлено порівняльну оцінку підходів виявлення, включно з ансамблем Byte2Image, CNN+LSTM та AE+LSTM, у термінах узгоджених метрик якості (F1, AUC), інтенсивності хибних спрацювань і часу локалізації інцидентів, а також показано, що саме профільний підхід зменшує «сірий шум» і підсилює кореляцію подій завдяки чітко заданим порогам, правилам і контексту активів.

Сценарії експериментів і дані

Для перевірки методики сформовано набір сценаріїв, що імітує типові для мереж електронних комунікацій гібридні атаки: комбінації фішингового старту, бокового переміщення, зміни параметрів керування та спроб стійкої присутності через firmware. В експериментах використано три групи даних:

1. Журнали подій керування і доступу (автентифікація, зміни конфігурації, доступ до адміністрування);

2. Статистики потоків і ознаки сеансів (вікна трафіку, TLS fingerprints, частота та типи SNMP-запитів);

3. Бінарні фрагменти firmware та мережеві дампи, перетворені у Byte2Image.

Таблиця 1 узагальнює структуру сценаріїв та основні маркери, які використовувалися як «еталонні» ознаки для оцінювання якості детекції. Підкреслимо, що у реальному середовищі такі маркери часто неповні, тому оцінювання також проводиться при різних рівнях надійності телеметрії q.

Таблиця 1

Сценарії гібридних кібератак та ознаки для IDS/SIEM і цифрового профілю

Код	Сценарій	Ознаки для IDS/SIEM та профілю
S1	Компрометація керування через слабку валідацію SSL у firmware	Нестандартні TLS fingerprints; помилки сертифікатів; нетипові домени; зміни конфігурації без очікуваного ланцюга погодження.
S2	Зловживання SNMPv2c (типові community strings) для читання/зміни MIB	Підвищена частота SNMP GET/SET; доступ до чутливих OID; SNMP з неочікуваних сегментів; розсинхрон конфігурації.
S3	Латеральний рух і підміна компонентів firmware у ланцюгу постачання	Byte2Image-відхилення; невідповідність хешів; зміни бібліотек криптографії; незвичні процеси оновлення.
S4	«Тихе» закріплення та поступова деградація спостережуваності	Зникнення журналів; зменшення подій IDS; пропуски часу; різка зміна профілю подій; зростання аномалійного бала.

Побудова профілю: приклад параметризації

У результаті застосування методики сформовано профіль, що містить контролі у кількох доменах: керування ідентичностями, сегментація і доступ, криптографічні політики, безпека керування пристроями, спостережуваність і реагування, а також безпека ланцюга постачання. Для демонстрації наведено фрагмент профілю у таблиці 2.

Важливо, що в профілі контролі представлені не як загальні фрази, а як набори параметрів, які можна перевірити за телеметрією або аудитом конфігурацій.

Таблиця 2

Контролі безпеки: параметри реалізації, докази та метрики достатності

Код	**Контроль**	**Параметри реалізації і доказ**	**Метрика достатності**
C1	Політика TLS для керування	Мінімум TLS 1.2/1.3; заборона слабких наборів; обов'язкова валідація сертифікатів; доказ: журнали TLS handshake та конфігурації.	Частка вузлів із відповідністю політиці; відхилення fingerprints.
C2	SNMP безпечної конфігурації	Лише SNMPv3; USM; обмеження MIB; сегментація керування; доказ: конфігурації агентів і мережеві правила.	Частка пристроїв із SNMPv3; кількість заборонених запитів.
C3	Контроль цілісності firmware	Хеші/підписи; контроль процесу оновлення; доказ: журнали оновлень і результати перевірки.	Кількість відхилень; час реакції на відхилення.
C4	Спостережуваність та кореляція	Нормалізація подій; правила SIEM; збагачення; доказ: правила; зразки інцидентів.	Coverage подій; mean time to detect/respond.
C5	Сегментація і мінімальні привілеї	Зони довіри; мікроавторизація; доказ: політики доступу та мережеві ACL.	Частка сервісів у сегментованих зонах; частка відмов за політикою.

Порівняння моделей детекції та ефект профілю

Таблиця 3

Порівняння підходів виявлення: якість, хибні спрацювання та час локалізації

Підхід	**Опис**	**F1**	**AUC**	**Хибні спрацювання/добу**	**Час локалізації, хв**
M0	Сигнатурні правила IDS без збагачення	0.78	0.84	46	52
M1	SIEM кореляція на базових правилах	0.81	0.86	39	45
M2	CNN+LSTM для трафіку (без профілю параметрів)	0.86	0.91	31	37
M3	AE+LSTM для аномалій (без профілю параметрів)	0.85	0.90	28	39
M4	Профіль + CNN+LSTM + AE+LSTM + кореляція SIEM	0.92	0.95	19	28

Експерименти виконано у двох режимах:

Режим A: базові налаштування, де контролі описані на рівні політик без параметризації, а SIEM використовує мінімальний набір правил;

Режим B: застосовано цільовий профіль з параметрами C1–C5, включено розширену телеметрію, а також ансамбль моделей CNN+LSTM і AE+LSTM.

Таблиця 3 показує порівняння ключових метрик. Додатково оцінювався вплив на доступність: у режимі B впровадження профілю вимагало планових вікон змін, але в межах допустимих обмежень $A_{\max}$ у постановці (3). Найбільший практичний ефект отримано для сценаріїв S1 і S2, де саме параметризація SSL і SNMP дала змогу зменшити клас «сірого шуму» і підвищити якість кореляції.

Приклад коду MATLAB Mobile для обчислення аномалійного бала

Нижче наведено приклад коду для MATLAB Mobile, який ілюструє розрахунок аномалійного бала за формулою (5) на основі реконструкції AE+LSTM, а також формування події для подальшої кореляції у SIEM (подія може передаватися через API або шлюз журналювання, залежно від реалізації). Код подано як приклад операційного артефакта профілю: він демонструє, як параметри моделі та пороги стають частиною доказової бази.

Лістинг 1. MATLAB Mobile: розрахунок аномалійного бала та формування події для кореляції у SIEM

```
function       evt = anomaly_event(Xwin, Xhat, q, beta, thr)
%ANOMALY_EVENT Обчислення аномалійного бала та формування події для SIEM
%   Вхідні параметри:
%     Xwin  - вектор ознак за останні L кроків (вхід AE+LSTM)
%     Xhat  - реконструйований вектор (вихід декодера AE+LSTM)
%     q     - коефіцієнт надійності телеметрії, q ∈ [0,1]
%     beta  - параметр підсилення за низької надійності даних
%     thr   - пороговое значення аномалійного бала
%   Вихід:
%     evt   - структура події для кореляції у SIEM

    % Обчислення похибки реконструкції
    err = Xwin - Xhat;

    % Аномалійний бал за формулою (5):
    % S_t = ||X - Dec(Enc(X))||_2^2 * (1 + β(1-q))
    S = sum(err(:).^2) * (1 + beta * (1 - q));

    % Формування структури події
    evt = struct();
    evt.timestamp = datetime("now", "Format", "yyyy-MM-dd HH:mm:ss");
    evt.score = S;
    evt.telemetry_q = q;
    evt.threshold = thr;
    evt.reconstruction_error = sum(err(:).^2);

    % Класифікація за порогом
    if S >= thr
        evt.severity = "high";
        evt.message = "Anomaly score exceeded threshold (profile-driven)";
        evt.tags = ["AE_LSTM", "Profile", "ZeroTrustContext", "Alert"];
        evt.action_required = true;
    else
        evt.severity = "info";
        evt.message = "Anomaly score below threshold";
        evt.tags = ["AE_LSTM", "Profile"];
        evt.action_required = false;
    end

    % Додаткові метадані для кореляції
    evt.model_type = "AE+LSTM";
    evt.profile_version = "1.0";

end
```

Рис. 2. Лістинг MATLAB Mobile для розрахунку аномалійного бала AE+LSTM та формування події для кореляції у SIEM.

Для практичної перевірки запропонованого підходу важливо не лише обчислити аномалійний бал, а й перетворити результат моделі на стандартизовану подію, придатну для кореляції та збагачення контекстом у SIEM. Саме тому реалізацію скорингу AE+LSTM доповнено процедурою формування структури події з ключовими атрибутами якості телеметрії, параметрами профілю та ознаками пріоритизації.

На рис. 2 наведено програмний лістинг, який реалізує повний цикл “скоринг → подія SIEM”. Вхідними даними виступають вектор ознак за ковзним вікном спостережень та його реконструкція, отримана декодером AE+LSTM. Далі обчислюється квадратична похибка реконструкції як базова міра відхилення від нормальної поведінки.

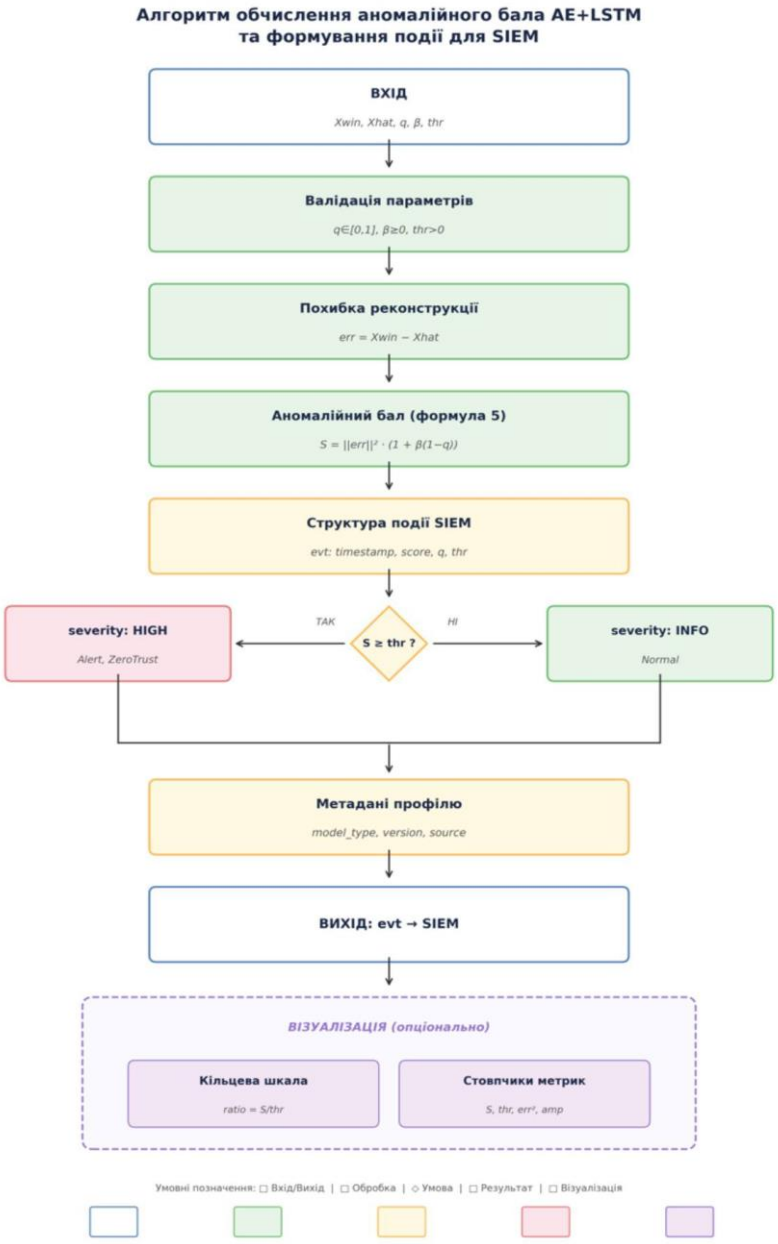

Рис. 3. Алгоритм обчислення аномалійного бала AE+LSTM та формування події для кореляції у SIEM (із вбудованим контролем якості телеметрії).

Щоб врахувати неповноту та неоднорідність спостережуваності, похибка підсилюється множником, що залежить від коефіцієнта надійності телеметрії: за нижчої якості даних

підсумковий бал зростає контрольовано, що зменшує ризик «пропуску» інциденту в умовах деградації журналювання або шуму каналів.Після розрахунку аномалійного бала формується структурована подія evt з часовою міткою, значенням бала, порогом профілю, величиною похибки, фактором підсилення та службовими метаданими (тип моделі, версія профілю, джерело). Логіка порівняння з порогом визначає рівень важливості: у разі перевищення thr подія маркується як високопріоритетна та отримує теги для кореляції (зокрема контекст профілю та Zero Trust), а за неперевищення порога реєструється як інформаційна телеметрія для подальшого аналізу трендів. У результаті SIEM отримує не «сире число», а повноцінний артефакт, придатний для правил кореляції, пріоритизації та подальшого реагування.

На рис. 3 подано блок-схему, яка відображає повний операційний цикл перетворення виходу моделі AE+LSTM у структуровану подію для SIEM. Процес стартує з подачі вхідних даних: вікна ознак спостережень та його реконструкції, а також параметрів профілю (коефіцієнт надійності телеметрії, параметр підсилення та порогове значення). Далі виконується валідація параметрів, після чого обчислюється похибка реконструкції як базова міра відхилення поведінки від очікуваної норми. На основі цієї похибки формується аномалійний бал, який додатково коригується множником, що враховує якість телеметрії: за нижчої надійності даних бал підсилюється, підвищуючи чутливість детекції в умовах неповної спостережуваності.Після розрахунку бала створюється структура події SIEM із ключовими атрибутами (часова мітка, значення бала, поріг, похибка, фактор підсилення). Центральним елементом схеми є логічне рішення порівняння S з порогом thr: у разі перевищення подія маркується як високої важливості (для подальшої кореляції та реагування), а за неперевищення реєструється як інформаційна телеметрія для контексту, трендів та зменшення «шуму» в потоці сповіщень. Завершальні кроки додають метадані профілю (тип моделі, версію, джерело), після чого сформований артефакт передається до SIEM. Окремо показано опціональний блок візуалізації результату (кільцева шкала та стовпчикові метрики) для швидкої інтерпретації оператором або для ілюстрації в звіті.

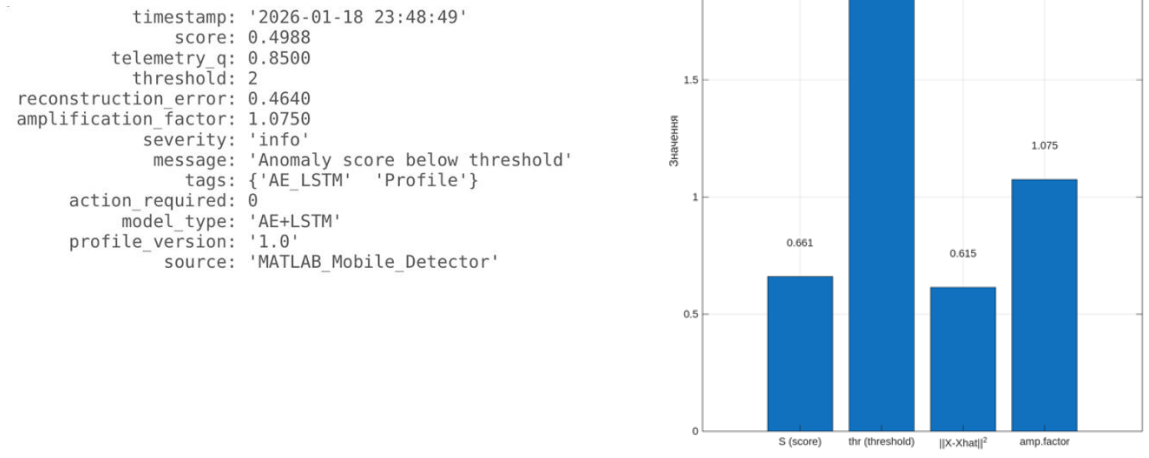

Рис. 4. Стовпчикова діаграма ключових метрик AE+LSTM для оцінювання аномалійності та порівняння з порогом SIEM (аномалійний бал, поріг, похибка реконструкції, коефіцієнт підсилення)

Отриманий вихід на рис. 4 демонструє, що в поточному часовому вікні модель AE+LSTM не зафіксувала суттєвого відхилення від «нормальної» поведінки, а сформована

подія придатна для подальшої кореляції у SIEM.У консолі виведено структуру evt, яка є уніфікованим «контейнером» для SIEM: фіксується час події, аномалійний бал score = S, поріг threshold = thr, якість телеметрії telemetry_q = q, а також складові розрахунку — похибка реконструкції reconstruction_error = ||X - Xhat||^2 та коефіцієнт підсилення amplification_factor = 1 + beta(1-q). За наведеними значеннями надійність телеметрії становить приблизно 0.85, тому підсилення є помірним (близько 1.075), тобто модель «трохи підкручує» бал через неповну довіру до даних, але без агресивного штрафу. Підсумковий бал S залишається суттєво нижчим за поріг thr = 2, тому подія класифікується як інформаційна (severity = info), з повідомленням про неперевищення порога та без вимоги негайних дій (action_required = 0). Це той випадок, коли «нудно» — це добре: сигнал не схожий на атаку за обраним критерієм.Стовпчикова діаграма візуалізує ті самі величини у зрозумілому вигляді: поріг thr є найвищим орієнтиром (2.0), а фактичний бал S та похибка реконструкції знаходяться значно нижче. Окремий стовпчик amp.factor показує, що корекція за надійністю телеметрії невелика; саме тому навіть за наявності шуму в реконструкції модель не «піднімає тривогу» штучно. Практичний висновок для SIEM полягає в тому, що подія може зберігатися як низькопріоритетна телеметрія для контексту та трендів, а переведення в тривогу відбуватиметься лише тоді, коли S стабільно або різко перевищить заданий профілем поріг.

Аналіз результатів та інженерні висновки

Отримані результати інтерпретуються не лише як «покращення метрик», а як підтвердження життєздатності профільного підходу.

По-перше, параметризація контролів SSL і SNMP зменшила невизначеність у кореляції подій: коли профіль визначає, що в керуванні допустимі лише TLS 1.2/1.3 з коректною валідацією, будь-який відступ (інший fingerprint, помилки сертифіката, перехід у режим сумісності) стає сильним сигналом, що підвищує апостеріорну ймовірність загрози у формулі (1). Аналогічно, вимога SNMPv3 і сегментації дозволяє розглядати будь-які SNMPv2c транзакції як інцидент конфігурації або компрометації [13], [14].

По-друге, поєднання CNN+LSTM і AE+LSTM дозволило розділити два класи задач: (а) відомі атаки з характерними патернами, що добре класифікуються; (б) повільні аномальні зміни, характерні для гібридних атак, що виявляються через реконструкційну похибку. У практиці SOC це дає можливість встановити різні процедури реагування: для класифікованих інцидентів – автоматизовані playbooks, для аномалій – додаткова верифікація і збагачення, з урахуванням коефіцієнта q.

По-третє, ефект профілю проявився у скороченні часу локалізації інцидентів. Причина не лише в кращій детекції, а у стандартизованій «карі» профілю: для кожного контролю визначено відповідального, джерело доказу та кроки перевірки. Це зменшує час на пошук «хто і де має дивитися» під час інциденту, що критично для мережевих середовищ із високими вимогами до доступності.

Дискусія

Розділ дискусія присвячено зіставленню запропонованої методики з близькими підходами, а також аналізу її практичних обмежень і перспектив розвитку в контексті Zero Trust та мультимодального штучного інтелекту.У класичних підходах, що спираються на каталоги контролів та вимоги відповідності, домінує логіка «покриття» контролями й перевірки їх наявності [4]. Така практика забезпечує управлінську дисципліну та формальну відтворюваність аудитів, однак не гарантує, що контроль реалізовано з параметрами, достатніми проти актуальних загроз. У запропонованій роботі профіль безпеки прив’язує контроль до конкретних параметрів конфігурації та спостережуваності, перетворюючи його на експлуатаційний артефакт: те, що можна виміряти, перевірити на даних і пов’язати з ефектом у детекції та реагуванні.Фреймворкові підходи до кіберстійкості, які структурують практики за функціями та підкреслюють баланс між захистом, виявленням, реагуванням і відновленням, є важливими для побудови системного бачення безпеки [5]. Водночас на рівні

© Прокопович-Ткаченко Д.І., Єжихін А.В., Бушков В.Г., Черкаський О.В., Черкаський Д.О. Формування цільового цифрового профілю безпеки мереж електронних комунікацій в умовах гібридних кібератак: ризик-орієнтований та багатокритеріальний підхід. Сучасний захист інформації, 1(65), 87–103. https://doi.org/10.31673/2409-7292.2026.011184

конкретної організації мережі часто зберігається проблема «перекладу» цих практик у параметри для протоколів, сервісів і середовищ. У запропонованій методиці цей переклад формалізовано як окремий крок, а параметризація SSL і SNMP виділяється як системно критична для мереж електронних комунікацій та вбудованих пристроїв. Такий фокус узгоджується з відомими висновками про важливість коректної перевірки TLS-сертифікатів у небраузерних застосунках [23] та необхідність безпечної конфігурації SNMP [13], [14], з огляду на поширеність помилкових налаштувань і їхню експлуатацію в атаках на керувальні контури.Окремої уваги заслуговує роль Zero Trust. У багатьох працях Zero Trust подається як архітектурний принцип або набір загальних настанов [6], однак у практичній імплементації часто зводиться до декларацій. У запропонованому профілі Zero Trust набуває операційного змісту через параметри сегментації, мінімальних привілеїв, контекстної авторизації та вимірюваних метрик. Це дозволяє не лише проголошувати перехід до «нульової довіри», а й перевіряти прогрес за результатами телеметрії, правилами кореляції та показниками досягнення цільових рівнів.Разом із перевагами підхід має обмеження. Найістотнішим є залежність якості результатів від надійності телеметрії. Навіть за наявності коефіцієнта надійності зберігається ризик, що ключові журнали будуть недоступні або спотворені у критичний момент, зокрема під час гібридного впливу, коли противник одночасно атакує технічні та організаційні процеси. З цієї причини профіль має включати контроль цілісності телеметрії та часової синхронізації як «контроль контролів», оскільки деградація спостережуваності безпосередньо підриває коректність оцінювання ризику, детекції та реакції.Друге обмеження пов’язане з використанням глибоких моделей. Їхня ефективність потребує регулярного супроводу, включно з перенавчанням, моніторингом дрейфу ознак, узгодженням порогів і контрольованими змінами. У мережах операторського класу це має бути підкріплено процесами MLOps та управління конфігураціями; інакше моделі можуть стати джерелом шуму або, навпаки, пропусків. У межах профілю доцільно трактувати життєвий цикл моделей як окремий клас контролів, що забезпечує стабільність якості детекції в часі.Третє обмеження стосується використання Byte2Image для аналізу firmware. Метод є корисним індикатором відхилень і може швидко сигналізувати про аномальні зміни, проте не замінює повний аналіз прошивок і реверс-інженерію. Його роль у профілі полягає у формуванні «тригера» для глибшої перевірки, особливо в сценаріях ланцюга постачання. Для зниження ризиків supply chain потрібні додаткові механізми, зокрема перевірка підписів, контроль джерел, а також процедурні вимоги до оновлень і їхнього затвердження [21].

Перспективним напрямом розвитку є побудова профілю як мультимодального цифрового двійника безпеки, де поєднуються граф топології мережі, часові ряди телеметрії, текстові логи, бінарні артефакти firmware та контекст політик доступу. У такій постановці multimodal AI здатен поєднувати ознаки різних модальностей в межах одного інциденту, наприклад, невідомий TLS fingerprint у поєднанні з керувальною дією через SNMP та одночасним відхиленням у Byte2Image-репрезентації прошивки. Це дає змогу формувати контекстні пояснення для SOC і скорочувати час прийняття рішень, а також автоматизувати пошук слабких місць профілю, коли модель фіксує повторювані «провали» у спостережуваності або сегментації.У міру зрілості Zero Trust профіль може еволюціонувати від статичного переліку параметрів до динамічного набору політик, що керуються ризиком у реальному часі. Наприклад, пороги аномалійних моделей можуть адаптуватися до контексту сегмента та критичності сервісу, а права доступу до керувальних функцій можуть автоматично обмежуватися при падінні надійності телеметрії або при накопиченні сигналів, що вказують на деградацію довіри до середовища.

Висновки

У публікації обґрунтовано та апробовано ризик-орієнтовану багатокритеріальну методику формування цільового цифрового профілю безпеки для мереж електронних комунікацій в умовах гібридних кібератак. Ключовою ідеєю є трактування профілю як

© Прокопович-Ткаченко Д.І., Єжихін А.В., Бушков В.Г., Черкаський О.В., Черкаський Д.О. Формування цільового цифрового профілю безпеки мереж електронних комунікацій в умовах гібридних кібератак: ризик-орієнтований та багатокритеріальний підхід. Сучасний захист інформації, 1(65), 87–103. https://doi.org/10.31673/2409-7292.2026.011184

параметризованого та доказового артефакта, що поєднує вимоги стандартів, модель загроз, портфель контролів, конкретні налаштування конфігурацій і метрики спостережуваності, переводячи “наявність контролю” у перевірювану експлуатаційну готовність.Запропонований підхід зменшує розрив між формальною відповідністю та реальним управлінням ризиком завдяки фіксації параметрів контролів і джерел доказів для їх підтвердження. Окремо показано практичну критичність параметризації політик SSL/TLS та конфігурацій SNMP у контексті firmware-атак і площини керування, де помилки реалізацій та типовість небезпечних налаштувань перетворюються на системний ризик для оператора.Методика підтримує перехід від пріоритизації заходів до реалістичного портфеля через оптимізаційну постановку з обмеженнями бюджету та доступності сервісів. Це усуває проблему «списків бажань» і забезпечує керований план впровадження з урахуванням компромісів між рівнем захисту та безперервністю надання послуг.Результати експериментальної перевірки підтверджують, що профільний підхід у зв’язці з інтеграцією IDS/SIEM та мультимодальними моделями детекції підвищує якість виявлення і зменшує операційні витрати SOC на локалізацію інцидентів. Застосування Byte2Image для артефактів прошивок та ансамблю CNN+LSTM і AE+LSTM для трафіку й аномалій, у поєднанні з профільною параметризацією правил кореляції, забезпечило приріст узгоджених метрик якості на рівні 7-12% і скорочення часу локалізації інцидентів, а також зниження інтенсивності хибних спрацювань у SIEM за рахунок чітких порогів і контексту активів.Практичні рекомендації впровадження полягають у старті з критичних сегментів (керування, зовнішні інтеграції, оновлення firmware) та побудові мінімально достатнього, легко верифікованого набору параметрів; обов’язковому включенні параметризації SSL/TLS і SNMP як базових контролів для зниження системного ризику вбудованих компонентів; формуванні портфеля заходів через оптимізацію під ресурсні обмеження; інтеграції профілю з IDS і SIEM таким чином, щоб параметри профілю керували кореляцією, а результати інцидентів поверталися як доказові метрики; супроводі моделей процесами життєвого циклу (контроль дрейфу, порогів, оновлень) для підтримання стабільної якості.Перспективи подальших досліджень пов’язані з розвитком профілю як мультимодального цифрового двійника безпеки та поглибленням Zero Trust до рівня динамічних політик, керованих ризиком у реальному часі. Це дозволить контекстно адаптувати пороги детекції та політики доступу залежно від критичності сегмента і надійності телеметрії, підвищуючи стійкість мережі до комбінованих атак на технічні й організаційні компоненти.

Перелік посилань

1. Opricovic S., Tzeng G.-H. Compromise solution by MCDM methods: A comparative analysis of VIKOR and TOPSIS // European Journal of Operational Research. 2004. T. 156, № 2. P. 445–455. DOI: https://doi.org/10.1016 /S0377-2217(03)00020-1.

2. Brans J. P., Vincke Ph. Note—A Preference Ranking Organisation Method // Management Science. 1985. T. 31, № 6. P. 647–656. DOI: https://doi.org/10.1287/mnsc.31.6.647.

3. Hwang C.-L., Yoon K. Multiple Attribute Decision Making: Methods and Applications A State-of-the-Art Survey. Berlin; Heidelberg: Springer, 1981. 269 p. DOI: https://doi.org/10.1007/978-3-642-48318-9.

4. Pearl J. Probabilistic Reasoning in Intelligent Systems: Networks of Plausible Inference. San Mateo, CA: Morgan Kaufmann, 1988. 552 p. DOI: https://doi.org/10.1016/C2009-0-27609-4.

5. Shostack A. Threat Modeling: Designing for Security. Hoboken, NJ: John Wiley & Sons, 2014. 624 p. DOI: https://doi.org/10.5555/2829295.

6. Joint Task Force Transformation Initiative. Guide for Conducting Risk Assessments (NIST Special Publication 800-30 Revision 1) [Електронний ресурс]. Gaithersburg, MD: National Institute of Standards and Technology, 2012. 95 p. DOI: https://doi.org/10.6028/NIST.SP.800-30r1.

7. National Institute of Standards and Technology. The NIST Cybersecurity Framework (CSF) 2.0 (NIST Cybersecurity White Paper 29) [Електронний ресурс]. Gaithersburg, MD: NIST, 2024. 32 p. DOI: https://doi.org/10.6028/NIST.CSWP.29.

8. Rose S., Borchert O., Mitchell S., Connelly S. Zero Trust Architecture (NIST Special Publication 800-207) [Електронний ресурс]. Gaithersburg, MD: National Institute of Standards and Technology, 2020. 59 p. DOI: https://doi.org/10.6028/NIST.SP.800-207.

© Прокопович-Ткаченко Д.І., Єжихін А.В., Бушков В.Г., Черкаський О.В., Черкаський Д.О. Формування цільового цифрового профілю безпеки мереж електронних комунікацій в умовах гібридних кібератак: ризик-орієнтований та багатокритеріальний підхід. Сучасний захист інформації, 1(65), 87–103. https://doi.org/10.31673/2409-7292.2026.011184

9. Joint Task Force. Security and Privacy Controls for Information Systems and Organizations (NIST Special Publication 800-53, Revision 5) [Електронний ресурс]. Gaithersburg, MD: National Institute of Standards and Technology, 2020. 492 p. DOI: https://doi.org/10.6028/NIST.SP.800-53r5.

10. Cichonski P., Millar T., Grance T., Scarfone K. Computer Security Incident Handling Guide (NIST Special Publication 800-61, Revision 2) [Електронний ресурс]. — Gaithersburg, MD: National Institute of Standards and Technology, 2012. 79 p. DOI: https://doi.org/10.6028/NIST.SP.800-61r2.

11. Schmidt M. Information security risk management terminology and key concepts // Risk Management. 2023. T. 25, № 1. P. 1–23. DOI: https://doi.org/10.1057/s41283-022-00108-8.

12. Al-Dosari K., Fetais N. Risk-management framework and information-security systems for small and medium enterprises (SMEs): A meta-analysis approach // Electronics. 2023. T. 12, № 17. Art. 3629. DOI: https://doi.org/10.3390/electronics12173629.

13. Lubis M., Luthfi M. I., Saedudin R. R., Muttaqin A. N., Lubis A. R. The Integration of ISO 27005 and NIST SP 800-30 for Security Operation Center (SOC) Framework Effectiveness in the Non-Bank Financial Industry // Computers. 2026. T. 15, № 1. Art. 60. DOI: https://doi.org/10.3390/computers15010060.

14. Stefani E., Costa I., Gaspar M. A., Goes R. d. S., Monteiro R. C., Petrili B. R., Pereira A. d. P. Information Security Risk Framework for Digital Transformation Technologies // Systems. 2025. T. 13, № 1. Art. 37. DOI: https://doi.org/10.3390/systems13010037.

15. Barlybayev A., Sharipbay A., Shakhmetova G., Zhumadillayeva A. Development of a Flexible Information Security Risk Model Using Machine Learning Methods and Ontologies // Applied Sciences. 2024. T. 14, № 21. Art. 9858. DOI: https://doi.org/10.3390/app14219858.

16. Islam S., Basheer N., Papastergiou S., Silvestri S. Intelligent dynamic cybersecurity risk management framework with explainability and interpretability of AI models for enhancing security and resilience of digital infrastructure // Journal of Reliable Intelligent Environments. 2025. T. 11. Art. 12. DOI: https://doi.org/10.1007/s40860-025-00253-3.

17. Yang M. Information Security Risk Management Model for Big Data // Advances in Multimedia. 2022. Art. ID 3383251. DOI: https://doi.org/10.1155/2022/3383251.

18. Kure H. I., Islam S., Mouratidis H. An integrated cyber security risk management framework and risk predication for the critical infrastructure protection // Neural Computing & Applications. 2022. T. 34. P. 15241–15271. DOI: https://doi.org/10.1007/s00521-022-06959-2.

19. Kure H. I., Islam S., Ghazanfar M., Raza A., Pasha M. Asset criticality and risk prediction for an effective cybersecurity risk management of cyber-physical system // Neural Computing & Applications. 2022. T. 34. P. 493–514. DOI: https://doi.org/10.1007/s00521-021-06400-0.

20. Bialas A. Risk Management in Critical Infrastructure—Foundation for Its Sustainable Work // Sustainability. 2016. T. 8, № 3. Art. 240. DOI: https://doi.org/10.3390/su8030240.

21. Cremer F., Sheehan B., Fortmann M., Kia A. N., Mullins M., Murphy F., Materne S. Cyber risk and cybersecurity: a systematic review of data availability // The Geneva Papers on Risk and Insurance – Issues and Practice. 2022. T. 47, № 3. P. 698–736. DOI: https://doi.org/10.1057/s41288-022-00266-6.

22. Ulya A., Karima A., Sukiman T. S. A., Zulfia A., Rahmawati R. Information Security Risk Analysis Using ISO 31000:2018 and ISO 27001:2022 // Brilliance: Research of Artificial Intelligence. 2025. T. 5, № 2. DOI: https://doi.org/10.47709/brilliance.v5i2.6564.

23. Shahidpoorfalah B., Hosseini Androod S., Kabir G. Risk Assessment of Digital Technologies in Sustainable Supply Chain Management: A Fuzzy VIKOR Method // Engineering Proceedings. 2024. T. 76, № 1. Art. 20. DOI: https://doi.org/10.3390/engproc2024076020.

24. Santos-Olmo A., Sánchez L. E., Rosado D. G., Serrano M. A., Blanco C., Mouratidis H., Fernández-Medina E. Towards an integrated risk analysis security framework according to a systematic analysis of existing proposals // Frontiers of Computer Science. 2024. T. 18, № 3. Art. 183808. DOI: https://doi.org/10.1007/s11704-023-1582-6.

25. Rana A., Gupta S., Gupta B. A comprehensive framework for quantitative risk assessment of organizational networks using FAIR-modified attack trees // Frontiers in Computer Science. 2024. T. 6. Art. 1304288. DOI: https://doi.org/10.3389/fcomp.2024.1304288.

26. Zaburko J., Szulżyk-Cieplak J. Information security risk assessment using the AHP method // IOP Conference Series: Materials Science and Engineering. 2019. T. 710, № 1. Art. 012036. DOI: https://doi.org/10.1088/1757-899X/710/1/012036.

27. Ayatollahi H., Shagerdi G. Information Security Risk Assessment in Hospitals // The Open Medical Informatics Journal. 2017. T. 11. P. 37–43. DOI: https://doi.org/10.2174/1874431101711010037.

28. Yang L., Zou K., Gao K., Jiang Z. A fuzzy DRBFNN-based information security risk assessment method in improving the efficiency of urban development // Mathematical Biosciences and Engineering. 2022. T. 19, № 12. P. 14232–14250. DOI: https://doi.org/10.3390/mbe.2022662.

29. Kerimkhulle S., Dildebayeva Z., Tokhmetov A., Amirova A., Tussupov J., Makhazhanova U., Adalbek A., Taberkhan R., Zakirova A., Salykbayeva A. Fuzzy Logic and Its Application in the Assessment of Information Security Risk of Industrial Internet of Things // Symmetry. 2023. T. 15, № 10. Art. 1958. DOI: https://doi.org/10.3390/sym15101958.

© Прокопович-Ткаченко Д.І., Єжихін А.В., Бушков В.Г., Черкаський О.В., Черкаський Д.О. Формування цільового цифрового профілю безпеки мереж електронних комунікацій в умовах гібридних кібератак: ризик-орієнтований та багатокритеріальний підхід. Сучасний захист інформації, 1(65), 87–103. https://doi.org/10.31673/2409-7292.2026.011184

30. Asfha A. E., Vaish A. Information Security Risk Assessment in Industry Information System Based on Fuzzy Set Theory and Artificial Neural Network // Informatics and Automation. 2024. Т. 23, № 2. P. 542–571. DOI: https://doi.org/10.15622/ia.23.2.9.

31.National Institute of Standards and Technology. Artificial Intelligence Risk Management Framework (AI RMF 1.0) (NIST AI 100-1) [Електронний ресурс]. Gaithersburg, MD: National Institute of Standards and Technology, 2023. DOI: https://doi.org/10.6028/NIST.AI.100-1.

Надійшла до редакції (Received): 10.02.2026
Прийнята до друку (Accepted): 17.03.2026
Опубліковано онлайн (Available online): 30.03.2026

УДК 004.056.55:004.7.056
DOI: 10.31673/2409-7292.2026.011393

Костюк Ю.В., Складанний П.М.

КРИПТОГРАФІЧНА МОДЕЛЬ ДОВІРИ ДО ПОДІЙ БЕЗПЕКИ В SIEM ДЛЯ ІНТЕЛЕКТУАЛЬНОГО ФОРМУВАННЯ МЕРЕЖЕВИХ ІНЦИДЕНТІВ

У статті запропоновано підхід до інтелектуального формування мережевих інцидентів у системах управління подіями та інцидентами інформаційної безпеки (SIEM), що ґрунтується на криптографічній моделі довіри до подій безпеки. Актуальність дослідження зумовлена інтенсивною цифровізацією корпоративних комп'ютерних мереж, зростанням обсягів телеметрії, широким використанням хмарних сервісів і розподілених інфраструктур, у яких традиційні механізми кореляції подій дедалі частіше виявляються вразливими до маніпуляцій вхідними даними. У більшості сучасних SIEM-рішень події безпеки розглядаються як апріорно достовірні за умови їх надходження з легітимних журналів або сенсорів, що є ризикованим у середовищах зі змінним рівнем довіри. За таких умов події можуть бути згенеровані скомпрометованими вузлами, змінені під час передавання чи зберігання або навмисно ін'єктовані зловмисником з метою спотворення процесу кореляції. Метою роботи є розроблення та наукове обґрунтування моделі, у межах якої кожна подія безпеки інтерпретується як криптографічно оформлене твердження про стан комп'ютерної мережі, придатне до формальної перевірки та кількісного оцінювання достовірності. Запропоновано перенести довіру з рівня джерел телеметрії на рівень окремих подій із використанням криптографічних механізмів фіксації походження, цілісності, контексту генерації та часової прив'язки. На цій основі формується пояснювана оцінка довіри до події, яка інтегрується в механізми кореляції та використовується як ваговий чинник під час формування інцидентів.У статті розглянуто алгоритмічні засади потокової обробки подій, що поєднують криптографічну верифікацію, оцінювання довіри та зважену кореляцію в межах кореляційних вікон, забезпечуючи масштабованість для високонавантажених середовищ. Практичне значення отриманих результатів полягає у можливості інтеграції запропонованої моделі в існуючі SIEM-архітектури без зміни принципів збору телеметрії, зі зменшенням кількості хибних спрацьовувань, підвищенням стійкості до ін'єкції та підміни подій і покращенням якості сформованих мережевих інцидентів для подальшого реагування та роботи SOC.

Ключові слова: SIEM, події безпеки, криптографічна верифікація, модель довіри, кореляція подій, мережеві інциденти, ін'єкція, підміна подій.

Вступ

Інтенсивна цифровізація корпоративних комп'ютерних мереж, широке використання хмарних сервісів і розподілених інфраструктур зумовлюють стрімке зростання кількості подій безпеки, що підлягають аналізу в системах управління подіями та інцидентами інформаційної безпеки (SIEM) [1, 5, 7, 9]. За таких умов ефективність захисту мережі дедалі більше залежить не від , можливостей збору телеметрії, а від здатності SIEM-систем коректно інтерпретувати події, відрізняти дійсні загрози від шуму та формувати обґрунтовані інциденти безпеки.

Попри значний розвиток методів кореляції подій, сучасні SIEM-рішення переважно ґрунтуються на припущенні про апріорну достовірність подій безпеки, отриманих із журналів,