

**Гринкевич Ганна Олександрівна**

доктор технічних наук, професор кафедри інформаційної та кібернетичної безпеки імені професора Володимира Бурячка

Київський столичний університет імені Бориса Грінченка, м. Київ, Україна

ORCID ID 0000-0003-1922-5165

ggrynkevych@ukr.net

**Василенко Володимир Вікторович**

кандидат технічних наук, доцент, доцент кафедри комп'ютерних наук

Державного університету інформаційно-комунікаційних технологій, м. Київ, Україна

ORCID ID 0000-0001-8465-6178

oknelisavvova172@gmail.com

**Рудін Дмитро Геннадійович**

Platform Engineer

Capital One, Плейно, Техас, США

ORCID ID 0009-0007-4171-4973

itelecombox@gmail.com

### МОДЕЛЬ ЗАМІНИ КОМЕРЦІЙНИХ EDR/XDR-РІШЕНЬ ЛОКАЛЬНОЮ OPEN-SOURCE АРХІТЕКТУРОЮ З AI-ПІДТРИМКОЮ SOC-ПРОЦЕСІВ

**Анотація.** У статті розглядається підхід до побудови локальної системи моніторингу та реагування на інциденти кібербезпеки, який може виступати альтернативою або доповненням до комерційних EDR/XDR-рішень. Актуальність дослідження обумовлена зростанням кількості кінцевих точок у корпоративних інфраструктурах та значними витратами, пов'язаними з використанням ліцензійних моделей сучасних платформ безпеки. У вступній частині обґрунтовується необхідність пошуку економічно ефективних рішень, здатних забезпечити належний рівень виявлення загроз, зберігання та аналізу подій безпеки.

У роботі сформульовано проблему обмеженості традиційних підходів до впровадження EDR/XDR у середовищах із великою кількістю пристроїв та визначено зв'язок цієї проблеми з практичними завданнями забезпечення кіберстійкості організації. Проведено аналіз функціональних можливостей сучасних систем моніторингу безпеки, а також окреслено їхні ключові переваги та недоліки з точки зору вартості, масштабованості та залежності від постачальника.

Метою дослідження є розроблення моделі локальної open-source архітектури, яка поєднує функції збору, індексації та зберігання подій безпеки з можливостями аналітичної обробки за допомогою локального штучного інтелекту. У розділі результатів описано запропоновану архітектуру, що включає використання Wazuh як платформи моніторингу кінцевих точок, систем індексації подій, централізованого сховища логів та окремого AI-шару для підтримки процесів SOC. Розглянуто апаратну конфігурацію системи, параметри обробки та зберігання даних, а також підходи до забезпечення відмовостійкості та масштабованості. Побудовано математичну модель системи, яка пов'язує кількість кінцевих точок з потоком подій, обсягами зберігання, складом обчислювальних вузлів, навантаженням на аналітиків SOC та сукупною вартістю володіння, і наведено архітектурну схему рішення.

Окрему увагу приділено техніко-економічному аналізу запропонованого рішення, який включає оцінку початкових витрат на інфраструктуру, експлуатаційних витрат та порівняння з традиційними підписними моделями. Також визначено обмеження та ризики, пов'язані з впровадженням open-source підходу, зокрема необхідність додаткового налаштування, відсутність повністю автоматизованого реагування та підвищені вимоги до кваліфікації персоналу. Кількісне оцінювання за моделлю показало, що на п'ятирічному горизонті запропонована архітектура стає економічно доцільнішою за комерційне рішення починаючи приблизно з 450 кінцевих точок, а для інфраструктури з 1 000 точок забезпечує економію близько 40 % за терміну окупності близько 1,2 року.

У висновках узагальнено результати дослідження та підтверджено доцільність використання локальної open-source архітектури у сценаріях, де критичним є контроль витрат та збереження даних у межах організації. Запропоновано подальші напрями досліджень, зокрема проведення пілотного впровадження та оцінювання ефективності системи в реальних умовах.

**Ключові слова:** кібербезпека, EDR, XDR, SIEM, Wazuh, open-source, штучний інтелект, SOC, математична модель, сукупна вартість володіння.

**Ganna Grynkevych**

Doctor of Technical Sciences, Professor in the Professor Volodymyr Buryachko Department of Information and Cyber Security

Boris Grinchenko Kyiv Metropolitan University, Kyiv, Ukraine

ORCID ID 0000-0003-1922-5165

ggrynkevych@ukr.net

© 2026 Гринкевич Г.О., Василенко В.В., Рудін Д.Г. Цей матеріал ліцензовано за умовами

CC BY 4.0.

<https://creativecommons.org/licenses/by/4.0/>

**Volodymyr Vasylenko**

PhD, Associate Professor, Associate Professor of the Department of Computer Science  
State University of Information and Communication Technologies, Kyiv, Ukraine  
ORCID ID 0000-0001-8465-6178  
oknelisavvoval72@gmail.com

**Dmytro Rudin**

Platform Engineer  
Capital One, Plano, Texas, USA  
ORCID ID 0009-0007-4171-4973  
itelecombox@gmail.com

**MODEL FOR REPLACING COMMERCIAL EDR/XDR SOLUTIONS WITH A LOCAL OPEN-SOURCE ARCHITECTURE WITH AI SUPPORT FOR SOC PROCESSES**

**Abstract.** The article considers an approach to building a local system for monitoring and responding to cybersecurity incidents that can serve as an alternative or complement to commercial EDR/XDR solutions. The relevance of the study is driven by the growing number of endpoints in corporate infrastructures and the significant costs associated with subscription-based security platforms. The introduction substantiates the need to find cost-effective solutions capable of ensuring an appropriate level of threat detection, event storage, and analysis.

The paper formulates the problem of limitations inherent in traditional approaches to implementing EDR/XDR in environments with a large number of devices and establishes its connection with practical tasks of ensuring organizational cyber resilience. An analysis of the functional capabilities of modern security monitoring systems is carried out, along with identification of their key advantages and limitations in terms of cost, scalability, and vendor dependency.

The purpose of the study is to develop a model of a local open-source architecture that combines functions of event collection, indexing, and storage with analytical processing capabilities using a local artificial intelligence layer. The results section describes the proposed architecture, which includes the use of Wazuh as an endpoint monitoring platform, event indexing systems, centralized log storage, and a dedicated AI layer to support SOC processes. The hardware configuration, data processing and storage parameters, as well as approaches to ensuring scalability and system resilience are also considered. A mathematical model of the system is constructed that links the number of endpoints to the event stream, storage volumes, the number of processing nodes, SOC analyst workload and total cost of ownership, and an architectural diagram of the solution is presented.

Particular attention is paid to the technical and economic analysis of the proposed solution, including the evaluation of initial infrastructure investments, operational costs, and comparison with traditional subscription models. The study also identifies limitations and risks associated with the open-source approach, including the need for additional configuration, absence of fully automated response mechanisms, and increased requirements for staff expertise. Quantitative evaluation with the model shows that over a five-year horizon the proposed architecture becomes more cost-effective than a commercial solution starting from approximately 450 endpoints, and for an infrastructure of 1,000 endpoints it yields savings of about 40% with a payback period of about 1.2 years.

The conclusions summarize the research findings and confirm the feasibility of using a local open-source architecture in scenarios where cost control and data ownership are critical. Further research directions are proposed, including pilot implementation and evaluation of system performance under real-world conditions.

**Keywords:** cybersecurity, EDR, XDR, SIEM, Wazuh, open-source, artificial intelligence, SOC, mathematical model, total cost of ownership.

**1. Вступ**

Сучасні корпоративні інформаційні системи функціонують в умовах постійного зростання кількості кінцевих пристроїв, інтенсивності мережевої взаємодії та обсягів подій безпеки. У таких середовищах традиційні підходи до захисту інформації, що базуються переважно на превентивних механізмах, вже не забезпечують належного рівня контролю та своєчасного виявлення загроз. Це зумовлює необхідність використання систем, орієнтованих на моніторинг поведінки, аналіз подій та оперативне реагування на інциденти [2].

У практиці кібербезпеки широкого застосування набули рішення класу EDR та XDR, які дозволяють здійснювати безперервний контроль за станом кінцевих точок, виявляти аномальну активність і формувати рекомендації або автоматизовані дії у відповідь на інциденти [7], [8], [9]. Такі рішення зазвичай інтегруються із системами централізованого збору та аналізу подій, що забезпечує побудову єдиного середовища моніторингу безпеки на рівні організації.

Разом із тим впровадження комерційних платформ цього класу пов'язане зі значними витратами, особливо у випадках, коли інфраструктура налічує сотні або тисячі пристроїв. Підписна модель ліцензування створює постійне фінансове навантаження, яке зростає разом із масштабуванням системи. Це обмежує можливості довгострокового розвитку інфраструктури безпеки та ускладнює оптимізацію витрат.

Альтернативним напрямом є використання локальних рішень, побудованих на основі open-source компонентів, які дозволяють зберігати контроль над даними, гнучко налаштовувати систему та зменшувати залежність від зовнішніх постачальників [4], [5]. Додаткові можливості з'являються завдяки використанню локальних інструментів штучного інтелекту, які можуть застосовуватися для підтримки аналітичних процесів, обробки великих обсягів подій та підвищення ефективності роботи аналітиків безпеки [10], [11].

У даній роботі розглядається підхід до побудови локальної системи моніторингу та реагування на інциденти кібербезпеки, що базується на open-source інструментах і передбачає використання AI для підтримки процесів SOC. Основна увага приділяється архітектурі системи, її ресурсним характеристикам, а також можливості зниження витрат при збереженні ключових функцій сучасних рішень класу EDR/XDR.

## 2. Постановка проблеми

У сучасних організаціях із розвинутою IT-інфраструктурою кількість кінцевих точок може досягати кількох сотень або більше, що суттєво ускладнює забезпечення належного рівня кібербезпеки. Використання комерційних EDR/XDR-рішень у таких умовах дозволяє централізувати процеси моніторингу, виявлення загроз та реагування на інциденти, однак супроводжується значними експлуатаційними витратами, що прямо залежать від кількості пристроїв.

Підписна модель ліцензування, яка використовується більшістю постачальників, формує постійні витрати, що мають тенденцію до зростання разом із масштабуванням інфраструктури. У довгостроковій перспективі це створює фінансові обмеження для організацій та ускладнює впровадження комплексних підходів до моніторингу безпеки. Крім того, використання таких рішень часто супроводжується залежністю від постачальника, що обмежує гнучкість у виборі інструментів та підходів до обробки даних.

З іншого боку, сучасні open-source платформи дозволяють реалізувати базові функції моніторингу подій безпеки, включаючи збір, кореляцію та зберігання даних. Однак їх використання вимагає додаткових зусиль щодо інтеграції, налаштування та побудови повноцінної аналітичної інфраструктури. Це особливо актуально для організацій, які прагнуть поєднати економічну ефективність із високим рівнем контролю над даними та процесами безпеки.

Водночас розвиток технологій штучного інтелекту відкриває нові можливості для підтримки процесів аналізу подій безпеки, зокрема для автоматизації узагальнення інформації, виявлення взаємозв'язків між подіями та формування рекомендацій для аналітиків. Використання локальних AI-рішень дозволяє зберігати дані в межах організації та зменшувати залежність від зовнішніх сервісів.

Таким чином, виникає науково-практична проблема, яка полягає у необхідності розроблення моделі побудови локальної системи моніторингу та реагування на інциденти кібербезпеки, що забезпечує функціональність, наближену до комерційних EDR/XDR-рішень, але водночас дозволяє зменшити витрати, підвищити гнучкість та забезпечити контроль над даними. Розв'язання цієї проблеми має важливе значення для підвищення ефективності забезпечення кібербезпеки організацій та оптимізації використання ресурсів.

## 3. Аналіз останніх досліджень і публікацій

Сучасні дослідження у сфері кібербезпеки значною мірою зосереджені на розвитку систем виявлення та реагування на інциденти, зокрема рішень класу EDR, XDR та SIEM. Значний внесок у формування підходів до виявлення загроз зроблено в рамках MITRE ATT&CK® Framework, який систематизує тактики та техніки атак і використовується як основа для побудови сучасних систем моніторингу безпеки [1]. Крім того, стандарти NIST визначають вимоги до організації контролів безпеки та управління подіями, що є базою для впровадження комплексних систем захисту інформації [2], [3].

У сучасних комерційних рішеннях класу XDR реалізовано інтеграцію функцій моніторингу кінцевих точок, аналізу мережевої активності та централізованої обробки подій. Такі платформи, як Cortex XDR, SentinelOne Singularity та CrowdStrike Falcon, забезпечують автоматизоване виявлення загроз, кореляцію подій та часткову автоматизацію реагування [7], [8], [9]. Водночас ці рішення характеризуються високим рівнем інтеграції та зручністю використання, що досягається за рахунок централізованої архітектури та використання власних аналітичних механізмів.

Паралельно розвиваються open-source рішення, які дозволяють реалізувати функції моніторингу безпеки без прив'язки до конкретного постачальника. Зокрема, платформа Wazuh забезпечує збір та аналіз подій із кінцевих точок, контроль цілісності файлів та виявлення аномалій, тоді як OpenSearch використовується для індексації, зберігання та пошуку великих обсягів даних [4], [5]. Подібні рішення часто доповнюються іншими компонентами, що дозволяє створювати гнучкі та масштабовані системи моніторингу.

Окремий напрям досліджень пов'язаний із використанням штучного інтелекту для аналізу подій безпеки. Зокрема, сучасні підходи передбачають застосування великих мовних моделей для узагальнення інформації, виявлення прихованих залежностей між подіями та підтримки процесу прийняття рішень аналітиками [10], [11]. Такі рішення дозволяють зменшити навантаження на персонал та підвищити ефективність обробки великих обсягів даних.

Незважаючи на значну кількість досліджень та існуючих рішень, залишається невирішеною проблема забезпечення економічно ефективної та водночас функціонально повноцінної системи моніторингу безпеки для організацій із великою кількістю кінцевих точок. Комерційні платформи забезпечують високий рівень автоматизації, однак супроводжуються значними витратами та залежністю від постачальника. Open-source рішення, у свою чергу, потребують додаткової інтеграції та налаштування, що ускладнює їх використання у складних середовищах.

Таким чином, існує потреба у розробленні підходу, який поєднує переваги open-source інструментів із можливостями сучасних AI-технологій та дозволяє забезпечити необхідний рівень функціональності при

зниженні витрат і збереженні контролю над інфраструктурою. Саме вирішенню цієї задачі присвячене дане дослідження.

#### 4. Мета і задачі дослідження

Метою даного дослідження є розроблення та обґрунтування моделі побудови локальної системи моніторингу та реагування на інциденти кібербезпеки на основі open-source компонентів із застосуванням локального штучного інтелекту для підтримки SOC-процесів, яка може виступати альтернативою або доповненням до комерційних EDR/XDR-рішень у середовищах із великою кількістю кінцевих точок.

Для досягнення поставленої мети визначено такі задачі дослідження:

1. Проаналізувати сучасні підходи до побудови систем моніторингу кібербезпеки, зокрема рішення класу EDR, XDR та SIEM.
2. Визначити обмеження використання комерційних платформ з точки зору вартості, масштабованості та залежності від постачальника.
3. Розробити архітектурну модель локальної open-source системи, що забезпечує збір, індексацію та зберігання подій безпеки.
4. Обґрунтувати доцільність використання локального AI-шару для підтримки аналітичних процесів SOC, включаючи узагальнення подій, кореляцію інцидентів та формування рекомендацій.
5. Оцінити ресурсні характеристики запропонованої системи, зокрема апаратні вимоги, обсяги зберігання даних та енергоспоживання.
6. Провести техніко-економічне порівняння різних підходів до впровадження систем моніторингу безпеки, включаючи повну заміну, гібридну модель та використання комерційних рішень.
7. Визначити обмеження та ризики запропонованого підходу, а також сформулювати критерії оцінювання ефективності на етапі пілотного впровадження.

#### 5. Результати дослідження

У даному розділі представлено результати розроблення моделі локальної системи моніторингу та реагування на інциденти кібербезпеки, яка базується на використанні open-source компонентів та локального штучного інтелекту. Запропонований підхід орієнтований на забезпечення функціональності, наближеної до комерційних EDR/XDR-рішень, із одночасним зниженням витрат та підвищенням контролю над інфраструктурою.

##### 5.1. Архітектура запропонованого рішення

Основу запропонованої системи становить багаторівнева архітектура, яка включає компоненти збору, обробки, зберігання та аналізу подій безпеки. Центральним елементом є платформа Wazuh, яка забезпечує моніторинг кінцевих точок, виявлення аномалій та збір телеметрії.

Архітектура системи передбачає такі основні компоненти:

- агенти на кінцевих точках для збору подій;
- кластер менеджерів Wazuh для обробки та кореляції подій;
- систему індексації та пошуку даних на базі OpenSearch;
- централізоване сховище логів на базі NAS;
- локальний AI-шар для аналітичної обробки подій.

Запропонований підхід дозволяє розподілити навантаження між компонентами та забезпечити масштабованість системи відповідно до кількості кінцевих точок.

Узагальнену архітектуру запропонованої системи наведено на рис. 1. Вона є чотирирівневою: рівень збору даних (агенти Wazuh на кінцевих точках та syslog-джерела), рівень обробки та кореляції (кластер менеджерів Wazuh за балансувальником навантаження), рівень індексації та зберігання (кластер OpenSearch для оперативних даних і NAS-сховище для середньострокового та архівного зберігання) та рівень аналітики, що поєднує локальний AI-шар і робоче місце аналітика SOC. Потік даних є односпрямованим від кінцевих точок до сховища, тоді як AI-шар отримує лише сповіщення підвищеного рівня критичності та повертає аналітику результату узагальнення й рекомендації, не виконуючи автоматичних дій на кінцевих точках.

Для AI-шару обрано компактні вузли Apple Mac Mini M4 Pro з уніфікованою пам'яттю, що дозволяє виконувати локальні великі мовні моделі розміром 8–14 млрд параметрів (у квантованому вигляді) за допомогою середовищ виконання llama.cpp або Ollama з енергоспоживанням порядку 40 Вт на вузол. Вузли працюють за API-шлюзом, який реалізує чергу запитів, формування контексту (RAG на основі бази знань правил Wazuh і матриці MITRE ATT&CK) та шаблони запитів до моделі.

##### 5.2. Математична модель запропонованої системи

Для кількісного обґрунтування архітектури та порівняння сценаріїв впровадження побудовано математичну модель, яка пов'язує кількість кінцевих точок з навантаженням на систему, обсягами зберігання, складом обчислювальних вузлів, навантаженням на аналітиків SOC та сукупною вартістю володіння (TCO). Модель складається з чотирьох взаємопов'язаних підмоделей: потоку подій та зберігання, обчислювальних ресурсів, аналітичної продуктивності та вартості.

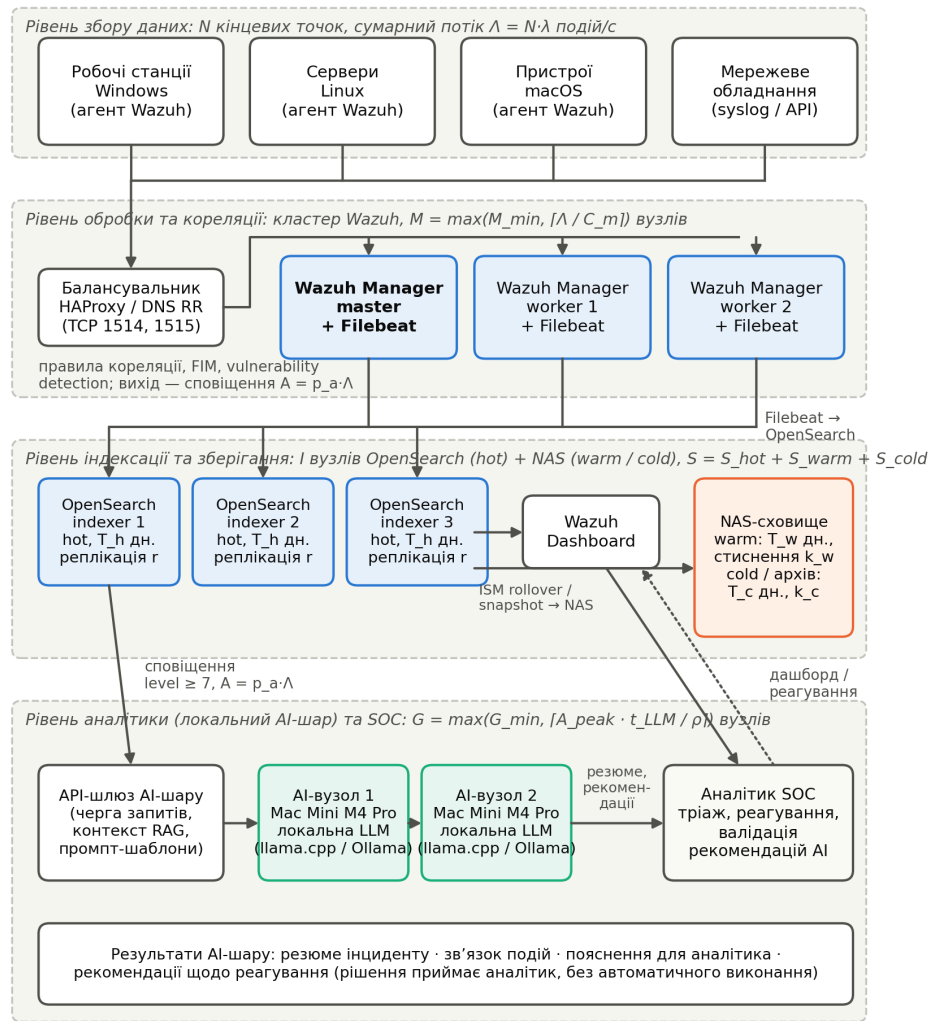


Рис. 1. Архітектура запропонованої локальної open-source системи моніторингу та реагування з AI-підтримкою SOC-процесів

Нехай  $N$  – кількість кінцевих точок,  $\lambda$  – середня інтенсивність генерування подій однією кінцевою точкою (подій/с),  $s$  – середній розмір збереженої події (КБ). Сумарний потік подій, що надходить до кластера менеджерів Wazuh, становить

$$\Lambda = N \cdot \lambda. \quad (1)$$

Лише частка  $p_a$  подій після кореляції перетворюється на сповіщення, які потребують уваги аналітика (у термінах Wazuh – сповіщення рівня 7 і вище). Середня та пікова інтенсивність сповіщень визначаються як

$$A = p_a \cdot \Lambda, \quad A_{peak} = k_p \cdot A, \quad (2)$$

де  $k_p$  – коефіцієнт нерівномірності (відношення пікової інтенсивності до середньої).

Багаторівнева модель зберігання (п. 5.4) описується періодами зберігання  $T_h$ ,  $T_w$ ,  $T_c$  (діб) для оперативного (hot), середньострокового (warm) та архівного (cold) рівнів, коефіцієнтами стиснення  $k_h$ ,  $k_w$ ,  $k_c$  та коефіцієнтом реплікації  $r$  оперативного рівня. Сумарний обсяг зберігання дорівнює

$$S = \Lambda \cdot s \cdot 86400 \cdot \left( \frac{r T_h}{k_h} + \frac{T_w}{k_w} + \frac{T_c}{k_c} \right) = S_{hot} + S_{warm} + S_{cold}. \quad (3)$$

Кількість вузлів кожного типу визначається як найменше ціле, що задовольняє обмеження продуктивності та вимоги відмовостійкості. Для кластера менеджерів Wazuh з продуктивністю одного вузла  $C_m$  (подій/с)

$$M = \max \left( M_{min}, \lceil \frac{\Lambda}{C_m} \rceil \right), \quad (4)$$

для кластера індексації OpenSearch з продуктивністю індексування  $C_i$  та обсягом дискового простору одного вузла  $D_i$

$$I = \max\left(I_{\min}, \left[\max\left(\frac{\Lambda}{C_i}, \frac{S_{hot}}{D_i}\right)\right]\right), \quad (5)$$

де  $M_{\min} = 2$  та  $I_{\min} = 3$  – мінімальна кількість вузлів, необхідна для відмовостійкості та кворуму кластера.

AI-шар розглядається як система масового обслуговування з  $G$  обслуговуючими пристроями, кожен з яких обробляє одне сповіщення за середній час  $t_{LLM}$  (с). За умови обмеження коефіцієнта завантаження вузла величиною  $\rho < 1$  (для збереження прийняттого часу очікування у черзі) необхідна кількість AI-вузлів у піковому режимі становить

$$G = \max\left(G_{\min}, \left[\frac{A_{peak} \cdot t_{LLM}}{\rho}\right]\right). \quad (6)$$

Навантаження на аналітиків SOC оцінюється через добову кількість сповіщень, що потребують тріажу,  $A_d = N \cdot a$ , де  $a$  – кількість таких сповіщень на одну кінцеву точку за добу, та середній час обробки одного сповіщення  $\tau$ . AI-шар скорочує час тріажу на частку  $\alpha$  за рахунок автоматичного узагальнення, збагачення контекстом і формування рекомендацій. Необхідна чисельність аналітиків (у еквіваленті повної зайнятості, FTE) дорівнює

$$F = \frac{A_d \cdot \tau}{W \cdot u}, \quad \tau = \tau_0(1 - \alpha), \quad (7)$$

де  $\tau_0$  – час тріажу без AI-підтримки,  $W$  – тривалість робочого дня (хв),  $u$  – частка робочого часу, що використовується продуктивно.

Початкові витрати на open-source архітектуру складаються з вартості обчислювальних вузлів, мережевого сховища, мережевої інфраструктури та одноразових витрат на інтеграцію:

$$CAPEX_{oss} = Mc_m + Ic_i + Gc_g + c_{nas} + c_{tb}(S_{warm} + S_{cold}) + c_{net} + c_{impl}, \quad (8)$$

де  $c_m$ ,  $c_i$ ,  $c_g$  – вартість вузлів менеджера, індексера та AI-вузла відповідно,  $c_{nas}$  – базова вартість NAS,  $c_{tb}$  – вартість 1 ТБ корисної ємності,  $c_{net}$  – мережеве обладнання,  $c_{impl}$  – вартість впровадження. Річні експлуатаційні витрати включають електроенергію, обслуговування та запасні частини (частка  $f_{maint}$  вартості обладнання  $C_{hw}$ ), а також додаткові трудовитрати на супровід платформи порівняно з комерційним рішенням:

$$OPEX_{oss} = P_{\Sigma} \cdot 8760 \cdot e + f_{maint} \cdot C_{hw} + (\varphi_0 + \varphi_1 N)c_{FTE}, \quad (9)$$

де  $P_{\Sigma}$  – сумарна споживана потужність вузлів (кВт),  $e$  – вартість 1 кВт·год,  $\varphi_0 + \varphi_1 N$  – додаткова трудомісткість супроводу (FTE),  $c_{FTE}$  – річна вартість одного спеціаліста.

Сукупна вартість володіння за горизонт  $T$  років для трьох сценаріїв, розглянутих у п. 5.6, визначається виразами

$$TCO_{com}(N, T) = C_0 + NpT, \quad (10)$$

$$TCO_{oss}(N, T) = CAPEX_{oss}(N) + OPEX_{oss}(N) \cdot T, \quad (11)$$

$$TCO_{hyb}(N, T) = CAPEX_{oss}((1 - h)N) + C_{int} + [OPEX_{oss}((1 - h)N) + hNp]T, \quad (12)$$

де  $p$  – річна вартість ліцензії комерційного EDR/XDR на одну кінцеву точку,  $C_0$  – витрати на його розгортання,  $h$  – частка кінцевих точок, які у гібридній моделі залишаються під комерційним рішенням,  $C_{int}$  – додаткові витрати на інтеграцію двох платформ.

З рівнянь (10)–(12) впливають два ключові показники економічної ефективності: термін окупності інвестицій в open-source архітектуру

$$T^* = \frac{CAPEX_{oss} - C_0}{Np - OPEX_{oss}}, \quad Np > OPEX_{oss}, \quad (13)$$

та порогова кількість кінцевих точок  $N^*$ , за якої на заданому горизонті  $T$  виконується умова  $TCO_{oss}(N^*, T) = TCO_{com}(N^*, T)$ ; для  $N > N^*$  open-source архітектура є економічно доцільнішою.

Для узагальненої оцінки, яка враховує не лише вартість, а й функціональну повноту рішення, введено інтегральний показник ефективності

$$E = \Phi \cdot \frac{TCO_{com}}{TCO_{oss}}, \quad \Phi = \sum_{j=1}^n w_j f_j, \quad \sum_{j=1}^n w_j = 1, \quad (14)$$

де  $\Phi$  – коефіцієнт функціонального покриття,  $f_j \in [0; 1]$  – ступінь реалізації  $j$ -ї функції класу EDR/XDR (моніторинг кінцевих точок, контроль цілісності, виявлення вразливостей, кореляція, автоматизоване реагування тощо),  $w_j$  – вагові коефіцієнти, що визначаються експертно відповідно до пріоритетів організації. Значення  $E > 1$  за умови  $\Phi \geq \Phi_{\min}$  свідчить про доцільність переходу до запропонованої моделі.

Числові значення параметрів моделі, використані для розрахунків у п. 5.7, наведено в табл. 2. Вони мають ілюстративний характер і базуються на публічних рекомендаціях щодо розмірності компонентів Wazuh та

OpenSearch [4], [5], публічних цінових пропозиціях виробників обладнання й постачальників EDR/XDR-рішень, а також на експертній оцінці авторів; уточнення параметрів є одним із завдань пілотного впровадження (п. 5.9).

Таблиця 2

Параметри математичної моделі (ілюстративні значення)

| Параметр                                                    | Позначення                    | Значення                  | Обґрунтування                                     |
|-------------------------------------------------------------|-------------------------------|---------------------------|---------------------------------------------------|
| Інтенсивність подій на кінцеву точку                        | $\lambda$                     | 0,5 подій/с               | типова для агента Wazuh із увімкненим аудитом [4] |
| Середній розмір події                                       | s                             | 1,2 КБ                    | JSON-документ сповіщення в OpenSearch             |
| Частка подій, що стають сповіщеннями                        | $p_a$                         | 0,03                      | сповіщення рівня $\geq 7$                         |
| Коефіцієнт нерівномірності                                  | $k_p$                         | 5                         | пікове навантаження в робочі години               |
| Періоди зберігання hot / warm / cold                        | $T_h / T_w / T_c$             | 30 / 90 / 365 діб         | вимоги розслідування інцидентів та аудиту         |
| Стиснення hot / warm / cold                                 | $k_h / k_w / k_c$             | 1 / 3 / 8                 | без стиснення; стиснені індекси; архів            |
| Реплікація оперативного рівня                               | r                             | 2                         | одна репліка кожного шарда                        |
| Продуктивність менеджера Wazuh / індексера                  | $C_m / C_i$                   | 1 500 / 3 000 подій/с     | рекомендації документації [4], [5]                |
| Дисковий простір індексера                                  | $D_i$                         | 4 ТБ                      | SSD-масив вузла                                   |
| Мінімальна кількість вузлів M / I / G                       | $M_{min} / I_{min} / G_{min}$ | 2 / 3 / 2                 | відмовостійкість, кворум                          |
| Час обробки сповіщення LLM                                  | $t_{LLM}$                     | 20 с                      | модель 8–14 млрд параметрів на Mac Mini M4 Pro    |
| Допустиме завантаження AI-вузла                             | $\rho$                        | 0,6                       | обмеження часу очікування в черзі                 |
| Сповіщення для тріажу на кінцеву точку                      | a                             | 0,1 за добу               | після налаштування правил                         |
| Час тріажу без AI / скорочення з AI                         | $\tau_0 / \alpha$             | 10 хв / 0,45              | експертна оцінка                                  |
| Робочий день / продуктивна частка                           | W / u                         | 480 хв / 0,7              | –                                                 |
| Вартість вузлів: менеджер / індексер / AI                   | $c_m / c_i / c_g$             | 2 500 / 4 000 / 2 200 USD | публічні ціни серверів 1U та Mac Mini M4 Pro      |
| NAS: базова вартість / 1 ТБ                                 | $c_{nas} / c_{tb}$            | 2 500 / 150 USD           | публічні ціни                                     |
| Мережеве обладнання / впровадження                          | $c_{net} / c_{impl}$          | 2 000 / 15 000 USD        | комутація 10GbE; трудовитрати інтеграції          |
| Споживана потужність вузлів                                 | –                             | 150 / 250 / 40 / 200 Вт   | менеджер / індексер / AI-вузол / NAS              |
| Вартість електроенергії                                     | e                             | 0,15 USD/кВт·год          | середнє значення для комерційних споживачів       |
| Частка витрат на обслуговування                             | $f_{maint}$                   | 0,10 на рік               | запасні частини, оновлення                        |
| Додаткова трудомісткість супроводу                          | $\varphi_0 + \varphi_1 N$     | 0,1 + N/5000 FTE          | експертна оцінка                                  |
| Вартість спеціаліста                                        | $c_{FTE}$                     | 80 000 USD/рік            | –                                                 |
| Ліцензія EDR/XDR на кінцеву точку                           | p                             | 60 USD/рік                | нижня межа публічних цін [7]–[9]                  |
| Розгортання комерційного рішення                            | $C_0$                         | 5 000 USD                 | –                                                 |
| Частка точок під комерційним рішенням (гібрид) / інтеграція | h / $C_{int}$                 | 0,2 / 5 000 USD           | критичні сервери                                  |

### 5.3. Апаратна конфігурація системи

Для реалізації системи передбачається використання окремих обчислювальних вузлів для різних функціональних задач. Зокрема, кластер Wazuh формується з декількох серверів, що забезпечують відмовостійкість та балансування навантаження. Для обробки AI-запитів використовуються окремі вузли, оптимізовані для виконання моделей штучного інтелекту.

Основні елементи апаратної конфігурації включають:

- сервери для обробки подій безпеки;
- вузли для виконання AI-аналізу;
- мережеве сховище для довготривалого зберігання логів;
- мережеву інфраструктуру для забезпечення передачі даних.

Такий підхід дозволяє гнучко масштабувати систему шляхом додавання нових вузлів без необхідності повної перебудови архітектури.

### 5.4. Обробка та зберігання подій безпеки

Система передбачає централізований збір подій із кінцевих точок із подальшою їх обробкою та індексацією. Обсяг даних, що генерується, залежить від кількості пристроїв та рівня деталізації логування. Для оптимізації використання ресурсів застосовується багаторівнева модель зберігання даних, яка включає:

- оперативне зберігання для швидкого доступу до актуальних подій;
- середньострокове зберігання для аналізу інцидентів;
- довгострокове архівування для відповідності вимогам аудиту.

Такий підхід дозволяє забезпечити баланс між швидкістю системи та обсягами зберігання даних.

### 5.5. Використання штучного інтелекту в SOC-процесах

Важливою складовою запропонованої моделі є використання локального AI для підтримки аналітичних процесів. На відміну від повністю автоматизованих систем, запропонований підхід передбачає використання AI як інструменту підтримки прийняття рішень.

Основні функції AI-шару включають:

- узагальнення великої кількості подій безпеки;
- виявлення взаємозв'язків між інцидентами;
- формування текстових пояснень для аналітиків;
- генерацію рекомендацій щодо реагування.

Такий підхід дозволяє зменшити навантаження на аналітиків та підвищити швидкість обробки інцидентів.

### 5.6. Техніко-економічний аналіз

Одним із ключових результатів дослідження є порівняння різних підходів до побудови систем моніторингу безпеки. Для цього розглянуто три основні сценарії:

- використання виключно комерційного EDR/XDR-рішення;
- повна заміна на open-source архітектуру;
- гібридний підхід.

Таблиця 1

Порівняння підходів до побудови системи моніторингу безпеки

| Підхід              | Початкові витрати | Операційні витрати | Гнучкість | Залежність від постачальника |
|---------------------|-------------------|--------------------|-----------|------------------------------|
| Комерційний EDR/XDR | низькі            | високі             | обмежена  | висока                       |
| Open-source рішення | середні           | низькі             | висока    | низька                       |
| Гібридна модель     | середні           | середні            | середня   | середня                      |

Отримані результати свідчать, що open-source підхід дозволяє суттєво зменшити довгострокові витрати при збереженні необхідного рівня функціональності.

### 5.7. Оцінювання ефективності запропонованої моделі

Оцінювання ефективності запропонованої моделі виконано за допомогою математичної моделі (п. 5.2) з параметрами табл. 2 для діапазону від 100 до 1 000 кінцевих точок, що відповідає інфраструктурам середніх та великих організацій. Оцінювання здійснюється за чотирма групами критеріїв: економічна ефективність (сукупна вартість володіння, порогова кількість кінцевих точок  $N^*$  та термін окупності  $T^*$ ), масштабованість (обсяги зберігання та склад вузлів), продуктивність SOC-процесів (навантаження на аналітиків) та функціональна повнота (коефіцієнт  $\Phi$ ). Оскільки параметри моделі мають ілюстративний характер, наведені нижче числові результати слід розглядати як оцінку порядку величин та характеру залежностей, а не як точний прогноз для конкретної організації.

Залежність сукупної вартості володіння за п'ятирічний горизонт від кількості кінцевих точок для трьох сценаріїв впровадження наведено на рис. 2. Витрати на комерційне EDR/XDR-рішення зростають лінійно та пропорційно кількості ліцензій, тоді як витрати на open-source архітектуру визначаються переважно фіксованою складовою (мінімальна відмовостійка конфігурація з двох менеджерів, трьох індексів та двох AI-вузлів) і зростають значно повільніше – за рахунок обсягу сховища та трудомісткості супроводу. Криві перетинаються за

порогового значення  $N^* \approx 450$  кінцевих точок: для менших інфраструктур вигіднішою залишається підписна модель, оскільки фіксовані витрати на власну платформу не компенсуються економією на ліцензіях, а для більших – open-source архітектура. Гібридна модель через збереження фіксованої складової та частини ліцензій стає вигіднішою за комерційне рішення лише за  $N \approx 590$  і в усьому діапазоні поступається повній заміні; її доцільність визначається не економічними, а ризиковими міркуваннями – збереженням автоматизованого реагування для критичних серверів.

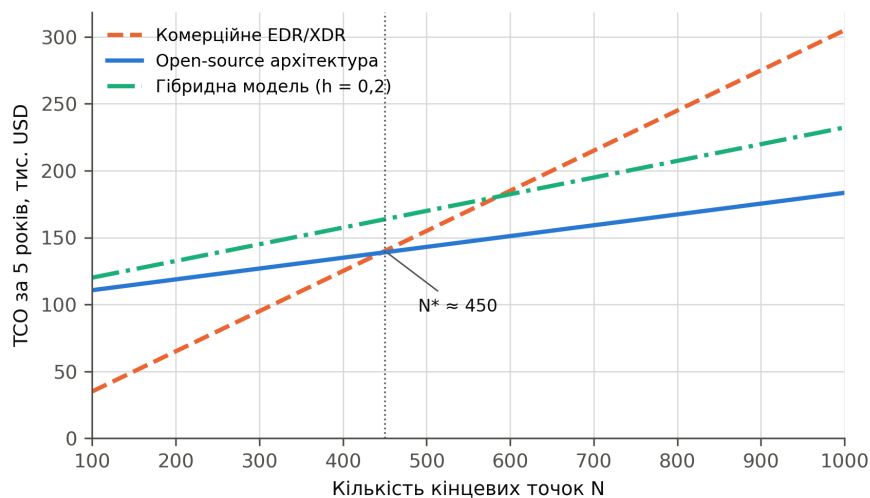


Рис. 2. Сукупна вартість володіння за 5 років залежно від кількості кінцевих точок для трьох сценаріїв впровадження

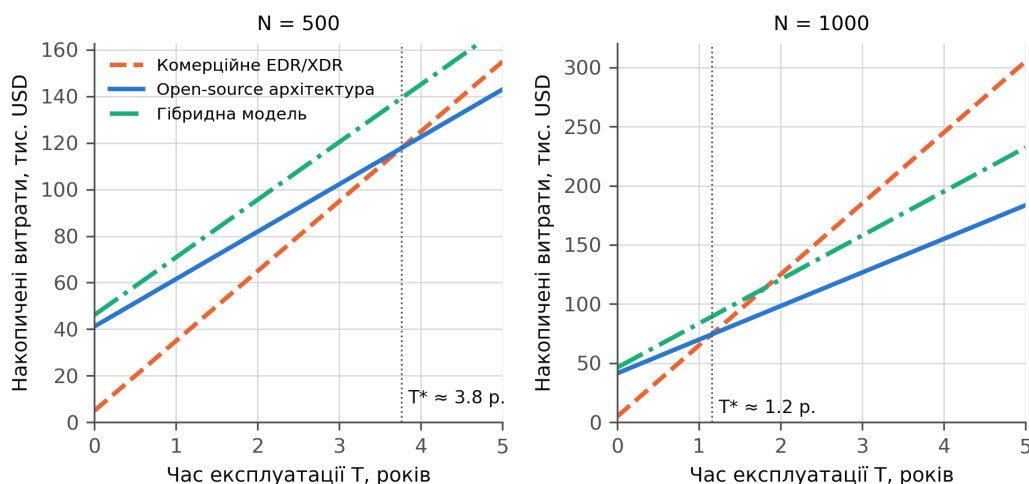


Рис. 3. Накопичені витрати за сценаріями впровадження та термін окупності  $T^*$  для інфраструктур із 500 (а) та 1 000 (б) кінцевих точок

Результати оцінювання масштабованості наведено на рис. 4. Сумарний обсяг зберігання зростає лінійно і становить близько 3,5 ТБ для 500 та 7,0 ТБ для 1 000 кінцевих точок, з яких на оперативний рівень (індексери з реплікацією) припадає 44 %, тоді як 56 % даних за рахунок стиснення розміщуються на значно дешевшому NAS-сховищі. Це підтверджує доцільність багаторівневої моделі зберігання (п. 5.4). Мінімальна відмовостійка конфігурація вузлів ( $M = 2$ ,  $I = 3$ ,  $G = 2$ ) є достатньою в усьому діапазоні до 1 000 кінцевих точок; додаткові індексери потрібні лише починаючи приблизно з 4 000 точок, коли обмежувальним фактором стає дисковий простір оперативного рівня, а додаткові менеджери – з 6 000 точок. Важливо, що AI-шар не є вузьким місцем системи: навіть за пікової інтенсивності сповіщень двох вузлів Mac Mini достатньо для інфраструктури з 10 000 кінцевих точок, оскільки один вузол за обраного часу обробки здатний опрацювати близько 2 600 сповіщень за добу. Вартість AI-шару становить лише близько 11 % початкових витрат.

Вплив AI-шару на продуктивність SOC-процесів ілюструє рис. 5. За прийнятого скорочення часу тріажу  $\alpha = 0,45$  необхідна чисельність аналітиків для інфраструктури з 1 000 кінцевих точок зменшується з 3,0 до 1,6 FTE, тобто вивільняється близько 1,3 FTE, що за річної вартості спеціаліста 80 тис. USD є співмірним із самою економією на ліцензіях. Аналіз чутливості (рис. 5, б) показує, що ефект зберігається в широкому діапазоні  $\alpha$ : навіть за консервативної оцінки  $\alpha = 0,2$  вивільнення становить 0,6 FTE для  $N = 1000$ . Цей ефект свідомо не включено до розрахунку TCO, оскільки сучасні комерційні платформи також містять AI-асистенти [11], і його коректне порівняння потребує експериментальних даних пілотного впровадження.

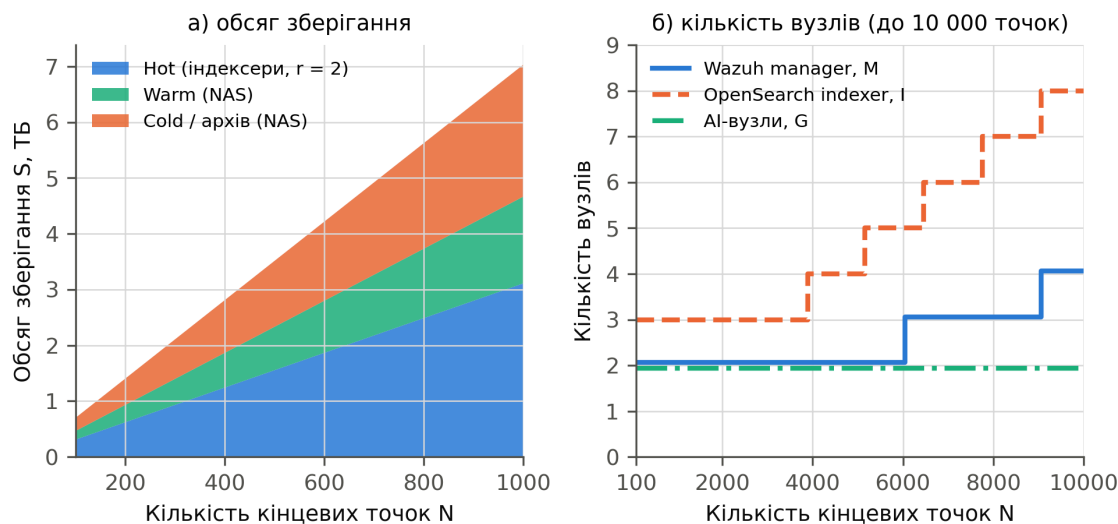


Рис. 4. Масштабованість запропонованої архітектури: а) обсяг зберігання за рівнями; б) необхідна кількість вузлів

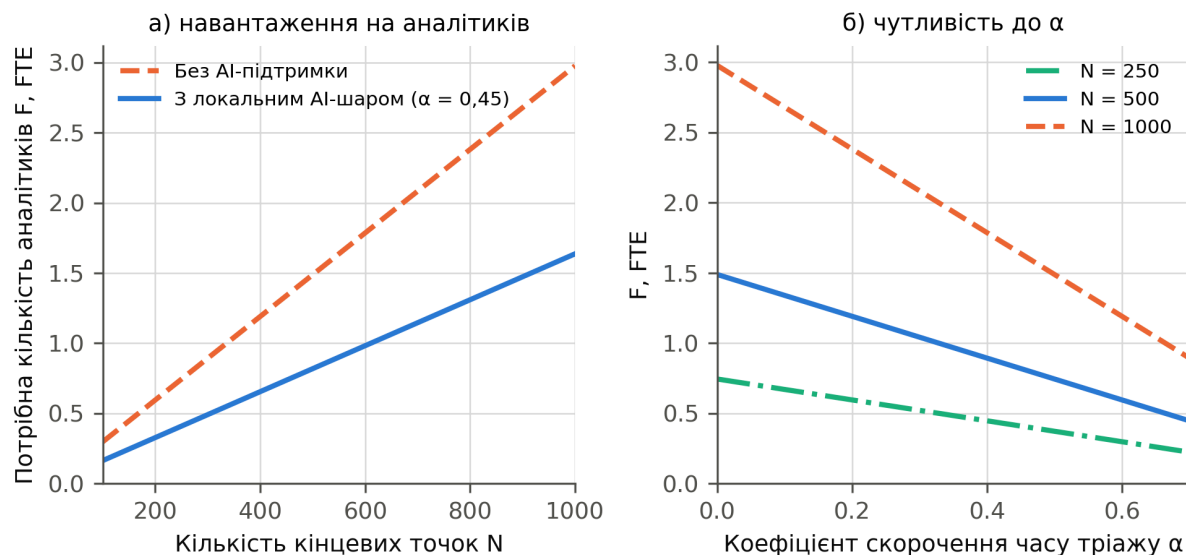


Рис. 5. Навантаження на аналітиків SOC: а) необхідна чисельність аналітиків з AI-підтримкою та без неї; б) чутливість до коефіцієнта скорочення часу тріажу  $\alpha$

Узагальнені результати оцінювання для трьох характерних масштабів інфраструктури наведено в табл. 3.

Таблиця 3

Результати оцінювання ефективності запропонованої моделі ( $T = 5$  років)

| Показник                                       | $N = 250$             | $N = 500$             | $N = 1\,000$          |
|------------------------------------------------|-----------------------|-----------------------|-----------------------|
| Сумарний потік подій $\Lambda$ , подій/с       | 125                   | 250                   | 500                   |
| Обсяг зберігання $S$ (hot / warm / cold), ТБ   | 1,8 (0,8 / 0,4 / 0,6) | 3,5 (1,6 / 0,8 / 1,2) | 7,0 (3,1 / 1,6 / 2,4) |
| Склад вузлів $M / I / G$                       | 2 / 3 / 2             | 2 / 3 / 2             | 2 / 3 / 2             |
| $CAPEX_{oss}$ , тис. USD                       | 41,0                  | 41,2                  | 41,5                  |
| $OPEX_{oss}$ , тис. USD/рік                    | 16,4                  | 20,4                  | 28,4                  |
| $TCO_{com} / TCO_{oss} / TCO_{hyb}$ , тис. USD | 80,0 / 122,8 / 138,8  | 155,0 / 143,0 / 169,9 | 305,0 / 183,5 / 232,3 |
| Економія відносно комерційного рішення, %      | -54                   | 8                     | 40                    |
| Термін окупності $T^*$ , років                 | не досягається        | 3,8                   | 1,2                   |
| Аналітики SOC без AI / з AI, FTE               | 0,74 / 0,41           | 1,49 / 0,82           | 2,98 / 1,64           |

Аналіз чутливості порогового значення  $N^*$  до найбільш невизначених параметрів показує, що воно змінюється від 820 кінцевих точок за вартості ліцензії 40 USD/рік до 310 за 80 USD/рік та 230 за 100 USD/рік, а

зростання трудомісткості супроводу з 0,1 до 0,2 FTE підвищує  $N^*$  до 630. Подовження горизонту планування з 3 до 7 років знижує  $N^*$  з 560 до 400. Отже, для інфраструктур із 500 і більше кінцевих точок економічна доцільність запропонованої моделі є стійкою до варіації параметрів, а для інфраструктур із 250–500 точок рішення слід приймати на основі фактичних значень вартості ліцензій та наявних компетенцій персоналу.

Щодо функціональної повноти, запропонована архітектура забезпечує реалізацію основних функцій класу EDR/XDR – моніторинг кінцевих точок, контроль цілісності файлів, виявлення вразливостей, кореляцію подій, зберігання та пошук, аналітичну підтримку – за винятком повністю автоматизованого реагування, що відображено в обмеженнях (п. 5.8). За експертної оцінки коефіцієнт функціонального покриття  $\Phi$  становить 0,8–0,9 залежно від вагових коефіцієнтів, що за  $N = 1000$  дає значення інтегрального показника ефективності  $E \approx 1,3 \dots 1,5$ , тобто перехід до запропонованої моделі є доцільним. Експериментальне визначення  $\Phi$ , а також параметрів  $a$ ,  $\tau_0$  та  $\alpha$  є завданням пілотного впровадження.

Таким чином, запропонована модель має потенціал забезпечити баланс між економічною ефективністю, функціональністю системи та якістю аналітичної підтримки процесів кібербезпеки, а побудована математична модель дозволяє кількісно обґрунтувати рішення щодо доцільності її впровадження для конкретної організації.

### 5.8. Обмеження та ризики

Незважаючи на переваги, запропонована модель має ряд обмежень:

- відсутність повністю автоматизованого реагування;
- необхідність додаткового налаштування та інтеграції;
- підвищені вимоги до кваліфікації персоналу;
- потенційно вищий рівень хибнопозитивних спрацювань.

Ці фактори необхідно враховувати при прийнятті рішення щодо впровадження системи.

### 5.9. Пілотне впровадження та оцінювання ефективності

Для перевірки ефективності запропонованої моделі доцільно провести пілотне впровадження, яке включає тестування системи в реальному середовищі. Основними критеріями оцінювання можуть бути:

- точність виявлення інцидентів;
- рівень хибнопозитивних спрацювань;
- швидкість обробки подій;
- витрати на обслуговування системи.

Результати пілотного впровадження дозволяють оцінити доцільність масштабування системи та її використання в корпоративному середовищі.

## 6. Висновки та перспективи подальших досліджень

У результаті проведеного дослідження було розроблено модель побудови локальної системи моніторингу та реагування на інциденти кібербезпеки, яка базується на використанні open-source компонентів та локального штучного інтелекту. Запропонований підхід дозволяє поєднати функціональні можливості сучасних систем класу EDR/XDR із підвищеним рівнем контролю над інфраструктурою та зниженням залежності від зовнішніх постачальників.

У ході дослідження встановлено, що використання open-source інструментів, зокрема платформ моніторингу кінцевих точок та систем індексації подій, забезпечує можливість побудови масштабованої та гнучкої архітектури. При цьому застосування локального AI-шару дозволяє підвищити ефективність аналітичних процесів, зменшити навантаження на персонал та покращити якість обробки інцидентів.

Проведений техніко-економічний аналіз показав, що запропонована модель має потенціал для зниження довгострокових витрат у порівнянні з використанням виключно комерційних EDR/XDR-рішень. Особливо це актуально для організацій із великою кількістю кінцевих точок, де витрати на ліцензування мають тенденцію до зростання.

Побудована математична модель дозволила кількісно оцінити запропоноване рішення. За ілюстративних значень параметрів на п'ятирічному горизонті порогова кількість кінцевих точок, починаючи з якої open-source архітектура є вигіднішою за комерційне EDR/XDR-рішення, становить близько 450; для інфраструктури з 1 000 кінцевих точок економія сягає 40 % за терміну окупності близько 1,2 року, мінімальна відмовостійка конфігурація з семи вузлів залишається достатньою до кількох тисяч кінцевих точок, а AI-шар скорочує необхідну чисельність аналітиків SOC приблизно на 45 %. Для інфраструктур із меншою кількістю кінцевих точок доцільність впровадження визначається фактичною вартістю ліцензій та наявними компетенціями персоналу.

Разом із тим визначено, що впровадження такої моделі супроводжується рядом обмежень, зокрема необхідністю додаткового налаштування системи, відсутністю повністю автоматизованого реагування та підвищеними вимогами до кваліфікації спеціалістів. Це обумовлює доцільність використання поетапного підходу до впровадження, зокрема через пілотне тестування.

Перспективи подальших досліджень пов'язані з практичною реалізацією запропонованої моделі у реальному середовищі та проведенням її експериментальної оцінки. Доцільним є дослідження ефективності

системи за різними метриками, включаючи точність виявлення інцидентів, рівень хибнопозитивних спрацювань та швидкість реагування. Окремим напрямом є вдосконалення AI-компонента, зокрема адаптація моделей до специфіки організаційної інфраструктури та розширення функцій підтримки аналітиків SOC.

**Внесок авторів.** Гринкевич Ганна Олександрівна – концептуалізація; методика; формування загальної архітектури дослідження; визначення підходів до побудови телекомунікаційної інфраструктури; аналіз джерел; підготовка огляду літератури та теоретичних основ дослідження; узагальнення результатів дослідження; підготовка основного тексту статті. Василенко Володимир Вікторович – розроблення підходів до забезпечення кібербезпеки; визначення функціональних вимог до систем класу EDR/XDR; аналіз сучасних рішень у сфері моніторингу безпеки; формування підходів до виявлення та реагування на інциденти; участь у розробленні архітектури системи з точки зору безпеки; емпіричне дослідження та перевірка практичних аспектів застосування. Dmytro Rudin – програмне забезпечення; реалізація технічної частини архітектури; оцінювання апаратних та інфраструктурних рішень; техніко-економічний аналіз; побудова математичної моделі та розрахунки за нею; підготовка архітектурної схеми та графічних матеріалів; розрахунок ресурсних параметрів системи; збір і перевірка емпіричних даних; участь у моделюванні сценаріїв впровадження.

#### **Декларація про штучний інтелект**

Під час підготовки статті інструменти штучного інтелекту використовувалися обмежено для допоміжних задач, зокрема для перевірки граматики, стилістичного оформлення та покращення якості формулювань. Усі основні ідеї, підходи, результати дослідження та висновки сформульовані авторами самостійно.

#### **Конфлікт інтересів**

Автор заявляє про відсутність конфлікту інтересів та підтверджує, що під час підготовки цієї роботи не існувало жодних комерційних, фінансових чи інших взаємовідносин, які могли б бути розцінені як такі, що здатні вплинути на результати дослідження або їх інтерпретацію. Робота виконана відповідно до принципів академічної доброчесності, етичних норм проведення наукових досліджень та вимог редакційної політики щодо запобігання конфлікту інтересів.

#### **Список використаної літератури**

1. MITRE Corporation. MITRE ATT&CK® Framework. 2024. URL: <https://attack.mitre.org> (date of access: 27.03.2026).
2. National Institute of Standards and Technology (NIST). Security and Privacy Controls for Information Systems and Organizations (SP 800-53 Rev. 5). Gaithersburg, MD, 2022. URL: <https://doi.org/10.6028/NIST.SP.800-53r5> (date of access: 27.03.2026).
3. National Institute of Standards and Technology (NIST). Guide to Cyber Threat Information Sharing (SP 800-150). Gaithersburg, MD, 2023. URL: <https://doi.org/10.6028/NIST.SP.800-150> (date of access: 27.03.2026).
4. Wazuh Inc. Wazuh Documentation. 2024. URL: <https://documentation.wazuh.com> (date of access: 27.03.2026).
5. OpenSearch Project. OpenSearch Documentation. 2024. URL: <https://opensearch.org/docs> (date of access: 27.03.2026).
6. Elastic N.V. Elastic Security Overview. 2023. URL: <https://www.elastic.co/security> (date of access: 27.03.2026).
7. Palo Alto Networks. Cortex XDR: Technical Overview. 2023. URL: <https://www.paloaltonetworks.com/cortex/cortex-xdr> (date of access: 27.03.2026).
8. SentinelOne. Singularity XDR Platform Overview. 2024. URL: <https://www.sentinelone.com/platform> (date of access: 27.03.2026).
9. CrowdStrike. CrowdStrike Falcon Platform Overview. 2024. URL: <https://www.crowdstrike.com/platform> (date of access: 27.03.2026).
10. Bommasani R., Hudson D. A., Adeli E. et al. On the Opportunities and Risks of Foundation Models. 2023. URL: <https://arxiv.org/abs/2108.07258> (date of access: 27.03.2026).
11. Microsoft. Security Copilot: AI for Cybersecurity. 2024. URL: <https://www.microsoft.com/security/copilot> (date of access: 27.03.2026).

**Надійшла до редакції: 10.05.2026**

**Прийнята до друку: 15.09.2026**

**Опубліковано: 30.09.2026**