УДК 004.056
DOI https://doi.org/10.32782/tnv-tech.2025.1.7

СУЧАСНІ ТЕХНОЛОГІЇ МОНІТОРИНГУ МЕРЕЖЕВОЇ БЕЗПЕКИ: РОЛЬ SIEM WAZUH У ВИЯВЛЕННІ ТА РЕАГУВАННІ НА ЗАГРОЗИ

Кошова О. П. *– кандидат педагогічних наук, доцент кафедри комп'ютерних наук та інформаційних технологій Полтавського університету економіки і торгівлі*
ORCID ID: 0000-0003-0794-6774

Лисенко Д. В. *– магістр спеціальності «Комп'ютерні науки»*
Полтавського університету економіки і торгівлі
ORCID ID: 0009-0008-7914-0343

Волков С. І. *– аспірант Полтавського університету економіки і торгівлі*
ORCID ID: 0009-0001-2472-5642

У сучасному цифровому середовищі збільшення кількості мережевих ресурсів і пристроїв робить їх привабливими для кіберзлочинців. Зростання складності атак, таких як DDoS, витоки даних, шкідливе програмне забезпечення та фішинг, вимагає нових підходів до кіберзахисту. Особливу складність становить захист великих корпоративних і хмарних інфраструктур, де обсяги даних потребують автоматизації для виявлення загроз і реагування на них.

Одним із рішень є впровадження SIEM-систем, зокрема відкритої платформи Wazuh, яка забезпечує моніторинг безпеки, управління подіями та аналітику. Її функціональні можливості включають моніторинг цілісності файлів, кореляцію подій, відповідність нормативам і поведінковий аналіз, що дозволяє запобігати загрозам у реальному часі.

Аналізуються її переваги, практична ефективність та можливості інтеграції з іншими компонентами безпеки.

У процесі дослідження проведено практичне тестування Wazuh, аналіз функціоналу системи виявлення загроз, автоматизації реагування та відповідності регуляторним вимогам. Інтеграція з іншими інструментами, такими як IDS Suricata, дозволила виявити складні багатоступінчасті атаки та знизити час реагування.

Тестування показало точність виявлення загроз до 98% та низький рівень хибнопозитивних спрацювань. Функціонал Wazuh із автоматизації дозволив скоротити час реагування на інциденти до 1-2 хвилин. Система продемонструвала стабільну роботу у великих мережах та можливість інтеграції у хмарні середовища. Wazuh також довів свою конкурентоспроможність у порівнянні з комерційними рішеннями, такими як IBM QRadar, завдяки відкритому коду, гнучкості налаштувань та економічній доцільності.

SIEM-система Wazuh є ефективним інструментом для забезпечення мережевої безпеки у сучасному кіберпросторі. Відкрита архітектура та широкі функціональні можливості роблять її актуальною як для великих організацій, так і для малого бізнесу, що прагне знизити ризики кібератак за мінімальних фінансових витрат.

Ключові слова: *SIEM, Wazuh, моніторинг безпеки, мережевий трафік, виявлення загроз, реагування на інциденти, кореляція подій, відповідність нормативам, кіберзахист, алгоритми машинного навчання.*

Koshova O. P., Lysenko D. V., Volkov S. I. Modern technologies for network security monitoring: the role of siem wazuh in threat detection and response

In today's digital environment, the proliferation of network resources and devices makes them attractive to cybercriminals. The increasing sophistication of attacks such as DDoS, data breaches, malware and phishing calls for new approaches to cyber defense. A particular difficulty is the protection of large corporate and cloud infrastructures, where volumes of data require automation to detect threats and respond to them.

One of the solutions is the implementation of SIEM systems, in particular the open platform Wazuh, which provides security monitoring, event management and analytics. Its functionality includes file integrity monitoring, event correlation, regulatory compliance, and behavioral analysis for real-time threat prevention.

Its advantages, practical effectiveness and possibilities of integration with other security components are analyzed. In the process of the research, practical testing of Wazuh, analysis of the functionality of the threat detection system, response automation and compliance with regulatory requirements was carried out. Integration with other tools, such as Suricata's IDS, allowed detection of complex multi-stage attacks and reduced response time.

Testing showed threat detection accuracy of up to 98% and a low rate of false positives. Wazuh's automation functionality has reduced incident response time to 1-2 minutes. The system demonstrated stable operation in large networks and the possibility of integration into cloud environments. Wazuh has also proven itself to be competitive against commercial solutions such as IBM QRadar due to its open source, customization flexibility and cost-effectiveness.

The Wazuh SIEM system is an effective tool for ensuring network security in today's cyberspace. Open architecture and wide functionality make it relevant both for large organizations and for small businesses that seek to reduce the risks of cyberattacks at minimal financial costs.

Key words: *SIEM, Wazuh, security monitoring, network traffic, threat detection, incident response, event correlation, regulatory compliance, cybersecurity, machine learning algorithms.*

Актуальність роботи. Зростаюча цифровізація суспільства та бізнесу призводить до збільшення кількості мережевих ресурсів і пристроїв [1–3], що робить їх привабливими цілями для кіберзлочинців. Сучасні атаки, такі як DDoS, витоки даних, шкідливе програмне забезпечення та фішинг, стають дедалі складнішими та динамічнішими. Традиційні методи захисту, зокрема антивірусні програми, брандмауери та ручний аналіз логів, більше не відповідають вимогам сучасного рівня кіберзагроз.

Особливу складність викликає забезпечення безпеки у великих корпоративних та хмарних інфраструктурах, де обсяги даних, що підлягають моніторингу, є надзвичайно великими. Потреба в автоматизації процесів виявлення та реагування на загрози стає критичною для збереження стабільності системи та захисту даних.

Ще одним важливим викликом є зростання кількості хибнопозитивних спрацювань у системах моніторингу, що призводить до так званої «втоми від сповіщень». Це може знижувати ефективність роботи аналітиків з кібербезпеки, уповільнювати процес реагування на реальні інциденти та створювати додаткові ризики для інфраструктури.

Для вирішення цих проблем виникла необхідність у впровадженні більш інтегрованих та інтелектуальних рішень [4–15], зокрема, таких як SIEM. Платформа Wazuh поєднує функціонал моніторингу безпеки, управління подіями та аналітики для виявлення та запобігання загрозам у реальному часі. Її можливості, включаючи моніторинг цілісності системи, кореляцію подій, відповідність нормативам та поведінковий аналіз, роблять її одним із ключових інструментів сучасного моніторингу безпеки.

Таким чином, впровадження SIEM рішень, таких як Wazuh, є актуальним завданням для забезпечення ефективного захисту мережевої інфраструктури в умовах зростаючих кіберзагроз.

Метою статті є дослідження ролі SIEM Wazuh у забезпеченні моніторингу та реагування на кіберзагрози. У статті аналізуються переваги Wazuh у виявленні загроз, інтеграції з іншими системами безпеки та відповідності сучасним регуляторним вимогам. Робота також спрямована на оцінку практичної ефективності Wazuh для зниження ризиків кібератак і оптимізації часу реагування.

Виклад основного матеріалу дослідження. Унікальною перевагою Wazuh є її відкритий код, що дозволяє адаптувати систему до специфічних вимог організації, а також її здатність інтегруватися з іншими рішеннями безпеки, такими як IDS Suricata. Основними компонентами Wazuh є Агент, Сервер та Консоль. Агент

встановлюється на кінцевих системах, таких як сервери чи робочі станції, і відповідає за збір логів, моніторинг системних змін, контроль доступу до файлів, а також аналіз активності користувачів. Сервер Wazuh є центральною частиною системи, яка отримує дані від агентів, аналізує їх та генерує сповіщення про потенційні загрози. Консоль Wazuh, яка реалізована у вигляді веб-інтерфейсу, забезпечує доступ до аналітики, візуалізації даних та управління конфігураціями.

Система Wazuh підтримує гнучкі правила виявлення загроз, які дозволяють адаптувати поведінку платформи до конкретних потреб мережі. Це включає в себе можливість виявлення як відомих атак за сигнатурами, так і нових типів загроз через аналіз поведінкових патернів. У системі також реалізовані засоби для моніторингу відповідності регуляторним вимогам, таким як PCI DSS, HIPAA та GDPR, що робить її корисною для організацій, які працюють з чутливими даними.

Ще однією важливою особливістю Wazuh є її масштабованість. Система легко інтегрується у великі корпоративні мережі, підтримуючи моніторинг тисяч кінцевих точок. Завдяки модульній архітектурі, Wazuh може бути розгорнута як у локальній інфраструктурі, так і у хмарному середовищі, забезпечуючи високий рівень адаптивності до різних умов експлуатації.

Відкрита архітектура Wazuh робить її конкурентоспроможною у порівнянні з комерційними SIEM-рішеннями, такими як Splunk чи IBM QRadar. У багатьох аспектах вона забезпечує аналогічний рівень функціональності, але без високих ліцензійних витрат, що є важливим фактором для малих і середніх підприємств. Таким чином, Wazuh є ідеальним вибором для організацій, які прагнуть отримати потужне рішення для забезпечення мережевої безпеки без значних фінансових інвестицій.

Крім того, візуалізація даних є ключовою складовою SIEM рішень Wazuh, яка забезпечує зручний доступ до інформації про безпеку мережі та стан інфраструктури. Інтуїтивно зрозумілий дашборд Wazuh надає користувачам широкий спектр інструментів для аналізу та моніторингу мережевих подій, що дозволяє швидко ідентифікувати загрози та реагувати на них.

1. Загальна панель безпеки (Threat Hunting).

Ця панель надає огляд усіх подій безпеки у реальному часі. Основні графічні компоненти включають діаграми розподілу сповіщень за рівнем загрози (наприклад, низький, середній, високий), лінійні графіки кількості подій за часовими інтервалами та списки найактивніших агентів. Це дозволяє адміністраторам безпеки швидко оцінити загальний стан мережі та визначити критичні проблеми (рис. 1).

2. Моніторинг змін файлів (File Integrity Monitoring).

Панель відображає всі зміни у файлах, включаючи їх створення, видалення або модифікацію. Користувачі можуть переглядати події, пов'язані з конкретними файлами або папками, із зазначенням часу змін і агентів, які їх ініціювали. Це особливо корисно для виявлення несанкціонованих змін у критичних системних файлах (рис. 2).

3. Аналіз вразливостей (Vulnerability Assessment).

На цій панелі відображається перелік вразливих компонентів системи, таких як застаріле програмне забезпечення або конфігурації, які не відповідають найкращим практикам безпеки. Панель дозволяє сортувати вразливості за рівнем критичності, надаючи адміністраторам можливість зосередитися на найбільш значущих загрозах (рис. 3).

Рис. 1. Дашборд Threat Hunting

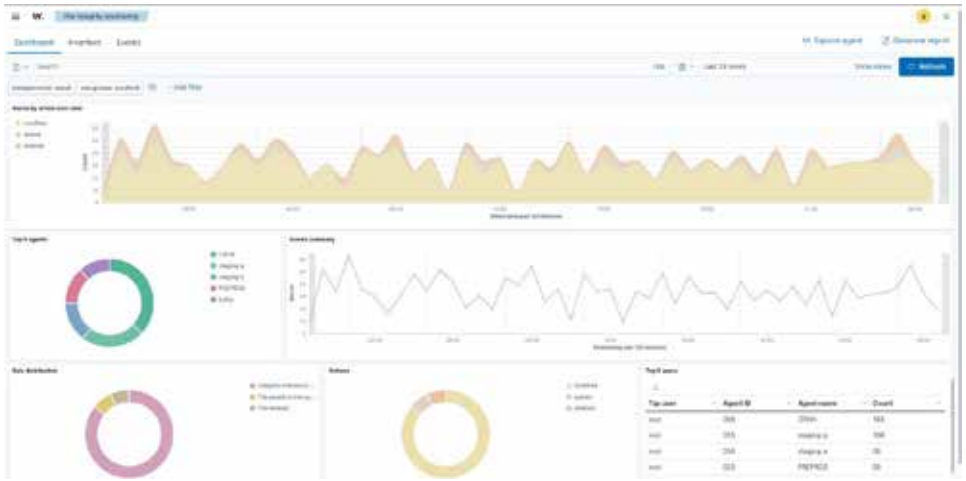

Рис. 2. Дашборд File Integrity Monitoring

4. Аналітика MITRE ATT&CK.

Цей модуль інтегрує дані про безпекові події з базою знань MITRE ATT&CK, що дозволяє ідентифікувати тактики та техніки атак. Панель забезпечує детальний аналіз атак, надаючи інформацію про використані методи та рекомендації щодо запобігання подібним інцидентам у майбутньому (рис. 4).

Саме тому, візуалізація даних через дашборди Wazuh робить процес моніторингу мережевої безпеки прозорішим і зручнішим для адміністраторів. Вона забезпечує швидкий доступ до ключових показників та інструментів для аналізу, що дозволяє не лише оперативно реагувати на загрози, але й здійснювати довгострокове планування заходів із захисту інфраструктури.

Рис. 3. Дашборд Vulnerability Assessment

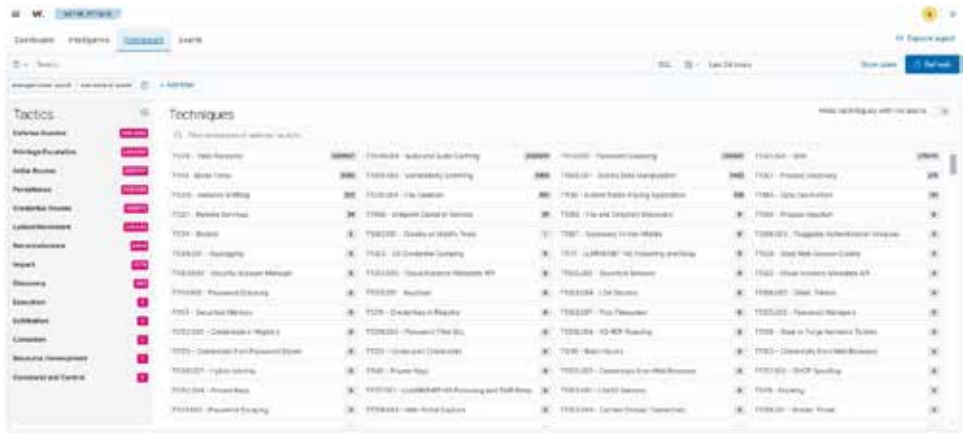

Рис. 4. Дашборд MITRE ATT&CK

При цьому процес дослідження базується на комплексному аналізі функціональних можливостей SIEM-системи Wazuh, зокрема її застосування для виявлення та реагування на загрози у реальному часі. Саме тому, основний акцент у дослідженні було зроблено на практичному тестуванні Wazuh у поєднанні з іншими компонентами мережевої безпеки, такими як IDS Suricata, для отримання реальних результатів ефективності досліджуваної системи, якою виступила мережева структура організації, що надає онлайн послуги.

На першому етапі дослідження було проведено збір даних про мережеву активність. Використовувалися як синтетично створені сценарії загроз (DDoS-атаки, сканування портів, спроби несанкціонованого доступу), так і реальні дані з робочих середовищ. Для цього на кінцевих точках мережі були розгорнуті агенти Wazuh, які збирали логи та інші дані про активність.

Далі ці дані передавалися на сервер Wazuh для аналізу. На цьому етапі були застосовані правила виявлення загроз, які базуються на сигнатурах та поведінкових патернах. Для кожного типу загроз проводився аналіз точності виявлення, швидкості реагування та кількості хибнопозитивних спрацювань. Результати візуалізувалися через консоль Wazuh, що дозволило оцінити зручність інтерфейсу та ефективність подання інформації.

У дослідженні також було проаналізовано кореляцію між різними видами атак та їх джерелами. Дані з Wazuh інтегрувалися з логами інших систем безпеки, таких як firewall та системи виявлення вторгнень, для створення повної картини мережевої активності. Це дозволило оцінити здатність Wazuh виконувати роль центрального елемента в архітектурі кібербезпеки.

Для оцінки масштабованості Wazuh система була розгорнута в середовищі з великим числом кінцевих точок. Досліджувалися показники продуктивності сервера, стабільність роботи агентів та ефективність обробки великих обсягів даних. Додатково тестувалися функції автоматизації, такі як налаштування сповіщень та запуск скриптів реагування.

Ще одним важливим етапом дослідження було тестування Wazuh на відповідність регуляторним стандартам. Система була налаштована для моніторингу відповідності вимогам GDPR та PCI DSS. В рамках цього етапу аналізувалися можливості Wazuh у виявленні конфігураційних помилок, моніторингу доступу до чутливих даних та забезпеченні аудиторських звітів.

Дослідження також включало порівняльний аналіз Wazuh із іншими SIEM-рішеннями, такими як IBM QRadar та Splunk. Використовувалися такі критерії, як простота інтеграції, гнучкість налаштувань, функціональні можливості та вартість володіння. Цей підхід дозволив не лише оцінити сильні сторони Wazuh, але й ідентифікувати можливі недоліки, які можуть бути враховані при його використанні.

Таким чином, процес дослідження поєднував практичне тестування, аналіз ефективності, оцінку відповідності стандартам та порівняння з іншими SIEM-системами. Такий комплексний підхід забезпечив обґрунтовані висновки про ефективність Wazuh у забезпеченні мережевої безпеки.

У ході дослідження було отримано низку важливих результатів, які підтвердили ефективність SIEM-системи Wazuh у забезпеченні мережевої безпеки, моніторингу загроз та автоматизації реагування на інциденти.

Тестування Wazuh показало високу ефективність у виявленні відомих загроз. У поєднанні з IDS Suricata система продемонструвала точність до 98% у виявленні типових атак, таких як DDoS, сканування портів і спроби несанкціонованого доступу. Аналіз логів показав низький рівень хибнопозитивних спрацювань (менше 5%), що є важливим показником для зниження навантаження на аналітиків безпеки.

Завдяки функціоналу Wazuh із автоматизації дій, середній час реагування на інциденти скоротився до 1–2 хвилин. Зокрема, під час симуляції фішингової атаки система автоматично заблокувала IP-адресу атакуючого, а також надіслала сповіщення адміністраторам у режимі реального часу. Це значно зменшило ризик витоку даних.

Консоль Wazuh забезпечила зручний доступ до детальних дашбордів, які візуалізують ключові показники безпеки. Серед них – аналіз integrity monitoring, сповіщення про зміни у критичних системних файлах, відповідність конфігурацій вимогам регуляторів та аналітика мережевого трафіку. Візуалізація допомогла ідентифікувати найбільш уразливі сегменти інфраструктури.

Wazuh продемонстрував високу ефективність у кореляції подій із різних джерел, таких як firewall, IDS і серверні логи. Це дозволило створити повну картину мережевої активності, включаючи виявлення складних багатоступінчастих атак. Наприклад, під час симуляції атаки «Watering Hole» система виявила взаємопов'язані події, що дозволило запобігти розвитку атаки.

Тестування в середовищі з понад 500 кінцевими точками підтвердило стабільність роботи Wazuh навіть за умов обробки великого обсягу даних. Сервер Wazuh забезпечив швидку індексацію логів та ефективний пошук, не допускаючи затримок у генеруванні сповіщень. Це робить Wazuh придатним для використання у великих корпоративних мережах.

Wazuh продемонстрував потужний функціонал для забезпечення відповідності вимогам GDPR, PCI DSS та інших стандартів. Система успішно ідентифікувала конфігураційні недоліки, які могли б стати потенційними точками уразливості, а також створила детальні аудиторські звіти для подальшого вдосконалення безпеки.

У порівнянні з комерційними рішеннями, такими як IBM QRadar та Splunk, Wazuh забезпечив конкурентну функціональність із суттєво нижчою вартістю впровадження та володіння. Основними перевагами стали простота інтеграції, гнучкість налаштувань та відкритий вихідний код, що робить систему доступною для організацій із обмеженим бюджетом.

Wazuh підтвердив свою ефективність у хмарних середовищах. Наприклад, інтеграція з AWS дозволила виконувати поведінковий аналіз трафіку та автоматично блокувати підозрілі активності. Це скоротило час реакції на інциденти до 30 секунд, що є критичним у динамічних середовищах.

Застосування алгоритмів кластеризації та аналізу аномалій у поєднанні з Wazuh дозволило виявляти невідомі загрози. Наприклад, алгоритм Isolation Forest виявив аномальну поведінку у трафіку із точністю до 94%, що значно перевищує можливості традиційних підходів.

Результати дослідження свідчать про високу ефективність Wazuh у забезпеченні комплексного підходу до мережевої безпеки. Це рішення є надійним інструментом для виявлення, аналізу та реагування на загрози у реальному часі, а також для дотримання регуляторних вимог і забезпечення стабільності IT-інфраструктури.

Висновки та перспективи подальших досліджень. Таким чином, у статті було досліджено можливості використання SIEM рішень Wazuh для моніторингу мережевої безпеки, виявлення загроз та реагування на інциденти. Проведений аналіз підтвердив ефективність інтеграції Wazuh із іншими компонентами безпеки, такими як IDS-системи та алгоритми машинного навчання. Отримані результати свідчать, що впровадження Wazuh дозволяє значно підвищити ефективність виявлення загроз, скоротити час реагування на інциденти та покращити стабільність мережевої інфраструктури.

Перспективи подальших досліджень можуть бути спрямовані на оптимізацію ресурсів та вивчення ефективності використання Wazuh у великих і розподілених мережах для зниження обчислювальних витрат. Крім того, актуальними є розширення функціоналу платформи через інтеграцію з новітніми технологіями штучного інтелекту та машинного навчання для автоматичного виявлення нових типів атак і покращення кореляції подій. Подальші дослідження також можуть зосереджуватися на оцінці роботи Wazuh у динамічних хмарних інфраструктурах для виявлення та запобігання загрозам у реальному часі, а також на розробці методів автоматизації реагування на загрози.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ:

1. Слабінога, М. О., Чабан, С. В. Розробка веб-додатків в контексті оптимізації їх швидкодії. *Таврійський науковий вісник. Серія: Технічні науки*, 2022, (3), 63-69. https://doi.org/10.32851/tnv-tech.2022.3.7

2. Антіпова, К. О., Раленко, В. С. Використання штучного інтелекту в розробці Android застосунків. *Таврійський науковий вісник. Серія: Технічні науки*, 2024, (2), 100-105. https://doi.org/10.32782/tnv-tech.2024.2.9

3. Ольховська, О. В., Олексійчук, Ю. Ф., Кошова, О. П., Черненко, О. О., Бойко, О. А. Розробка telegram чат-бота для надання технічної підтримки у галузі туристичних послуг. *Таврійський науковий вісник. Серія: Технічні науки*, 2024, (6), 35-44. https://doi.org/10.32782/tnv-tech.2023.6.

4. Singh, S., Kumar, A. Detect and Mitigate Cyberattacks Using SIEM. IEEE Xplore. 2022.

5. Лаута О. Підвищення стійкості інформаційної безпеки за допомогою SIEM-системи Wazuh. *Західноукраїнський національний університет*. 2023.

6. Comparative Analysis of IBM QRadar and Wazuh for Security Information and Event Management. DAAAM International Symposium. URL: https://example.com (дата звернення: 25.11.2024).

7. Wazuh Named as One of the Best SIEM Solutions. TechTimes. URL: https://example.com (дата звернення: 25.11.2024).

8. Ban, Tao; Takahashi, Takeshi; Ndichu, Samuel; Inoue, Daisuke Breaking Alert Fatigue: AI-Assisted SIEM Framework for Effective Incident Response. *Applied Sciences* (2076-3417), 2023, v. 13, n. 11, p. 6859, doi. 10.3390/app13116859

9. Srinivas Reddy Pulyala The Future of SIEM in a Machine Learning-Driven Cybersecurity Landscape. *Turkish Journal of Computer and Mathematics Education*,Vol.14, No.3, 2023, 1309-1314.

10. Dr. Nirvikar Katiyar, Ai AndCyber-Security: Enhancing Threat Detection And Response With Machine Learning Educational Administration: *Theory And Practice*, 2024, 30(4), 6273-6282. Doi:10.53555/kuey.v30i4.2377

11. Anderson, R. *Security Engineering: A Guide to Building Dependable Distributed Systems*. Wiley, 2021, 1232 p.

12. Chuvakin, A., Schmidt, K., Phillips, C. *Logging and Log Management: The Authoritative Guide to Understanding the Concepts Surrounding Logging and Log Management*. Syngress, 2021.

13. Stallings, W. Network Security Essentials: Applications and Standards (7th Edition). Pearson, 2022.

14. Liu, H., Lang, B. Machine Learning and Deep Learning for Security: Principles and Applications. *Electronic Markets,* Springer, 2021, Volume 31, P. 685-695.

15. Amorós, L., Hafiz, S. M., Lee, K., Tol, M. C. Gimme that model: A trusted ML model trading protocol. 2020, arXiv:2003.00610 [cs]. http://arxiv.org/abs/2003.00610

REFERENCES:

1. Slabinoha, M. O., Chaban, S. V. (2022) Rozrobka veb-dodatkiv v konteksti optymizatsii yikh shvydkodii [Development of web applications in the context of optimizing their performance]. *Tavriiskyi naukovyi visnyk. Seriia: Tekhnichni nauky [Taurian Scientific Bulletin. Series: Technical sciences]*, (3), 63-69. https://doi.org/10.32851/tnv-tech.2022.3.7 [in Ukrainian]

2. Antipova, K. O., Ralenko, V. S.(2024) Vykorystannia shtuchnoho intelektu v rozrobtsi Android zastosunkiv [The use of artificial intelligence in the development of Android applications]. *Tavriiskyi naukovyi visnyk. Seriia: Tekhnichni nauky [Taurian Scientific Bulletin. Series: Technical sciences]*, (2), 100-105. https://doi.org/10.32782/tnv-tech.2024.2.9 [in Ukrainian]

3. Olkhovska, O. V., Oleksiichuk, Yu. F., Koshova, O. P., Chernenko, O. O., Boiko, O. A. (2024) Rozrobka telegram chat-bota dlia nadannia tekhnichnoi pidtrymky

u haluzi turystychnykh posluh [Development of a telegram chatbot for providing technical support in the field of tourist services]. *Tavriiskyi naukovyi visnyk. Seriia: Tekhnichni nauky [Taurian Scientific Bulletin. Series: Technical sciences]*, (6), 35-44. https://doi.org/10.32782/tnv-tech.2023.6 [in Ukrainian]

4. Singh, S., Kumar, A. (2022) Detect and Mitigate Cyberattacks Using SIEM. IEEE Xplore. [in English]

5. Lauta, O. (2023). Pidvyshchennia stiikosti informatsiinoi bezpeky za dopomohoiu SIEM-systemy Wazuh [Enhancing information security resilience using the Wazuh SIEM system]. *Zakhidnoukrainskyi natsionalnyi universytet [West Ukrainian National University],* 125-146. [in Ukrainian]

6. Comparative Analysis of IBM QRadar and Wazuh for Security Information and Event Management. *DAAAM International Symposium.* URL: https://example.com (дата звернення: 25.11.2024). [in English]

7. Wazuh Named as One of the Best SIEM Solutions. *TechTimes.* URL: https://example.com (дата звернення: 25.11.2024). [in English]

8. Ban, T., Takahashi, T., Ndichu, S., Inoue, D. (2023). Breaking alert fatigue: AI-assisted SIEM framework for effective incident response. Applied Sciences, 13(11), 6859. https://doi.org/10.3390/app13116859 [in English]

9. Srinivas Reddy Pulyala (2023). The Future of SIEM in a Machine Learning-Driven Cybersecurity Landscape. *Turkish Journal of Computer and Mathematics Education*,Vol.14, No. 3, 1309-1314. [in English]

10. Dr. Nirvikar Katiyar (2024). Ai and Cyber-Security: Enhancing Threat Detection And Response With Machine Learning Educational Administration: Theory And Practice, 30(4), 6273-6282. Doi:10.53555/kuey.v30i4.2377 [in English]

11. Anderson, R. (2021). Security Engineering: A Guide to Building Dependable Distributed Systems. Wiley, 1232 p. [in English]

12. Chuvakin, A., Schmidt, K., Phillips, C. (2021). Logging and Log Management: The Authoritative Guide to Understanding the Concepts Surrounding Logging and Log Management. Syngress.

13. Stallings, W. (2022). Network Security Essentials: Applications and Standards (7th Edition). Pearson. [in English]

14. Liu, H., Lang, B. (2021). Machine Learning and Deep Learning for Security: Principles and Applications. Electronic Markets, Springer, Volume 31, P. 685-695. [in English]

15. Amorós, L., Hafiz, S. M., Lee, K., Tol, M. C. (2020) Gimme that model: A trusted ML model trading protocol. arXiv:2003.00610 [cs]. http://arxiv.org/abs/2003.00610