УДК 004.056.53

Ящук В. І.,
valentina.lender@gmail.com, ORCID ID: 0000-0003-2651-4918,
Researcher ID: F-9466-2019,
к.е.н., доц., доцент кафедри управління інформаційною безпекою, Львівський державний університет безпеки життєдіяльності, м. Львів

Фединець Н. І.,
nataliafedynets@gmail.com, ORCID ID: 0000-0001-6811-3720,
Researcher ID: P-3237-3596,
к.е.н., доц., доцент кафедри менеджменту, Львівський торговельно-економічний університет, м. Львів

ІНТЕГРАЦІЯ АВТОМАТИЗОВАНИХ РІШЕНЬ У СИСТЕМУ МЕНЕДЖМЕНТУ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ НА ОСНОВІ ЗАСТОСУВАННЯ SIEM-ТЕХНОЛОГІЙ

Анотація. *Розглянуто теоретичні, науково-методичні та організаційно-функціональні основи використання SIEM-систем в управлінні інформаційною безпекою. Визначено сучасні підходи до управління інформаційною безпекою та розслідування інцидентів. Наведено методичні підходи до формування концепції функціонування SIEM-систем в управлінні інформаційною безпекою. Запропоновано етапи вирішення науково-практичної проблеми, пов'язаної з підвищенням рівня захищеності інформаційних систем за допомогою SIEM-систем в управлінні інформаційною безпекою. У сучасних умовах стрімкого розвитку цифрових технологій та глобальної цифровізації питання гарантування інформаційної безпеки набуває особливої актуальності. З кожним роком зростає кількість кіберзагроз, які стають дедалі складнішими, скоординованішими та цілеспрямованішими, що, своєю чергою, створює нові виклики для підприємств, державних установ і приватного сектору. У такому контексті формування ефективної системи менеджменту інформаційної безпеки (СУІБ) є не лише технічною, але й стратегічною необхідністю для будь-якої організації. СУІБ побудована відповідно до міжнародних стандартів, зокрема ISO/IEC 27001, забезпечує цілісну політику управління ризиками, контролює доступ до критичних інформаційних активів і дозволяє формувати культуру безпеки в організаційному середовищі. Разом з тим, традиційні підходи до організації інформаційної безпеки все частіше виявляються недостатньо ефективними в умовах динамічного ландшафту загроз. Однією з головних проблем є фрагментованість засобів захисту, що призводить до втрати цілісної картини подій безпеки в організації. Затримки в реагуванні на інциденти, обумовлені переважно ручною обробкою інформації, а також ризики, пов'язані з людським фактором (помилки, упередженість, недогляди), значно знижують ефективність системи захисту. Тому зростає потреба в інтеграції автоматизованих рішень, які здатні забезпечити своєчасне виявлення, аналіз і реагування на кіберзагрози з мінімальним залученням людини. У цьому контексті все більшого поширення набувають SIEM-технології (Security Information and Event Management), які поєднують функціональність збору, нормалізації, кореляції та аналізу подій інформаційної безпеки з можливістю виявлення аномалій та автоматизованого реагування на інциденти. Інтеграція SIEM у систему менеджменту інформаційної безпеки дозволяє створити єдиний інформаційно-аналітичний центр, що забезпечує безперервний моніторинг та контроль за станом безпеки в реальному часі. Мета статті полягає у дослідженні можливостей інтеграції автоматизованих рішень на основі SIEM-технологій у СУІБ з урахуванням актуальних викликів, практичних аспектів реалізації та потенційних переваг такого підходу. У межах дослідження проаналізовано архітектурні та функціональні особливості SIEM-систем, визначено їх роль у зменшенні впливу людського фактору та пришвидшенні процесів виявлення і реагування на інциденти, а також розглянуто перспективи подальшого розвитку SIEM у поєднанні з технологіями штучного інтелекту та автоматизованими платформами SOAR (Security Orchestration, Automation and Response). Стаття спрямована на розкриття інноваційного потенціалу автоматизації в галузі інформаційної безпеки та обґрунтування доцільності впровадження таких рішень в організаціях різного масштабу.*

Ключові слова: *інформаційна безпека, SIEM, менеджмент безпеки, автоматизація, моніторинг, інциденти, IT-ризики, стандарти ISO/IEC.*

Yashchuk V. E.,
valentina.lender@gmail.com, ORCID ID: 0000-0003-2651-4918,
Researcher ID: F-9466-2019,
Ph.D., Associate Professor, Associate Professor of the Department of Information Security Management, Lviv State University of Life Safety, Lviv

Fedynets N. I.,
nataliafedynets@gmail.com, ORCID ID: 0000-0001-6811-3720,
Researcher ID: P-3237-3596,
Ph.D., Associate Professor, Associate Professor of the Department of Management, Lviv University of Trade and Economics, Lviv

INTEGRATION OF AUTOMATED SOLUTIONS INTO THE INFORMATION SECURITY MANAGEMENT SYSTEM BASED ON THE APPLICATION OF SIEM TECHNOLOGIES

Abstract. *The theoretical, scientific-methodological and organizational-functional foundations of the use of SIEM systems in information security management are considered. Modern approaches to information security management and incident investigation are determined. Methodological approaches to the formation of the concept of the functioning of SIEM systems in information security management are presented. The stages of solving the scientific and practical problem associated with increasing the level of security of information systems using SIEM systems in information security management are proposed. In modern conditions of rapid development of digital technologies and global digitalization, the issue of ensuring information security is becoming particularly relevant. Every year, the number of cyber threats is increasing, becoming more complex, coordinated and targeted, which, in turn, creates new challenges for enterprises, government agencies and the private sector. In this context, the formation of an effective information security management system (ISMS) is not only a technical but also a strategic necessity for any organization. An ISMS, built in accordance with international standards, in particular ISO/IEC 27001, provides a holistic risk management policy, controls access to critical information assets and allows you to form a security culture in the organizational environment. At the same time, traditional approaches to organizing information security are increasingly proving to be insufficiently effective in the conditions of a dynamic threat landscape. One of the main problems is the fragmentation of protection measures, which leads to the loss of a holistic picture of security events in the organization. Delays in responding to incidents, caused mainly by manual processing of information, as well as risks associated with the human factor (errors, bias, oversights), significantly reduce the effectiveness of the protection system. Therefore, there is a growing need to integrate automated solutions that are able to ensure timely detection, analysis and response to cyber threats with minimal human involvement. In this context, SIEM technologies (Security Information and Event Management) are becoming increasingly widespread, combining the functionality of collecting, normalizing, correlating and analyzing information security events with the ability to detect anomalies and automated response to incidents. The integration of SIEM into the information security management system allows you to create a single information and analytical center that provides continuous monitoring and control of the security status in real time. The purpose of the article is to study the possibilities of integrating automated solutions based on SIEM technologies into the ISMS, taking into account current challenges, practical aspects of implementation and potential advantages of such an approach. The study analyzed the architectural and functional features of SIEM systems, determined their role in reducing the impact of the human factor and accelerating the processes of detecting and responding to incidents, and also considered the prospects for further development of SIEM in combination with artificial intelligence technologies and automated SOAR (Security Orchestration, Automation and Response) platforms. The article is aimed at revealing the innovative potential of automation in the field of information security and substantiating the feasibility of implementing such solutions in organizations of various scales.*

Keywords: *information security, SIEM, security management, automation, monitoring, incidents, IT risks, ISO/IEC standards.*

JEL Classification: M15, O33, D83, L86
DOI: https://doi.org/10.32782/2522-1205-2025-84-31

Постановка проблеми. У сучасних умовах цифрової трансформації суспільства та стрімкого розвитку інформаційних технологій підприємства стикаються з постійним зростанням кількості та складності кіберзагроз. Традиційні методи гарантування інформаційної безпеки, які ґрунтуються

переважно на ручному моніторингу, реагуванні та аналізі інцидентів, вже не здатні ефективно протистояти актуальним викликам, особливо в умовах масштабованих та динамічних IT-інфраструктур. Це зумовлює потребу у впровадженні автоматизованих підходів до управління інформаційною безпекою, зокрема шляхом інтеграції спеціалізованих програмно-апаратних рішень.

Повномасштабне вторгнення росії в Україну спричинило значне зростання кібератак. За даними Державної служби спеціального зв'язку та захисту інформації України, кількість кіберінцидентів у 2023 році збільшилась на 38% порівняно з 2022 роком. Найпоширенішими типами кібератак сьогодні є DDoS-атаки (розподілені атаки відмови в обслуговуванні), фішингові атаки, атаки на вебсайти, шкідливе програмне забезпечення.

Ручне реагування на кіберінциденти стає все більш складним і трудомістким, тому виникає необхідність автоматизації цих процесів за допомогою, наприклад, SIEM-систем. SIEM-системи дозволяють автоматизувати багато процесів менеджменту інформаційної безпеки, таких як: збір даних про безпеку з різних джерел; виявлення та аналіз кіберінцидентів; реагування на кіберінциденти; створення звітів про кібербезпеки.

Аналізуючи статистику кібератак в Україні [1–2], можна зробити висновок, що у 2023 році спостерігалося зростання кількості кіберінцидентів до 38%, зафіксовано 2372 кібератаки на органи державної влади, 1046 кібератак на об'єкти критичної інфраструктури. У другому півріччі 2023 року було зареєстровано 342 кібератаки, у середньому 57 зареєстрованих інцидентів на місяць та 1-2 на добу. Водночас за 6 місяців у першому півріччі 2024 року зареєстрованих кібератак вже було 762, у середньому 128 на місяць та 4-5 на добу.

У III кварталі 2024 р. кількість зареєстрованих кіберінцидентів зросла на 46% [1-2], зафіксовано 1834 кібератаки за перші 6 місяців. Окрім цього, протягом III кварталу 2024 року зафіксовано 202 кібератаки, ініційовані проросійськими хакерськими угрупованнями, що на 26% менше, ніж у другому кварталі поточного року. У III кварталі 2024 року зареєстровано 355 кіберінцидентів, що на 46% вище, ніж у другому кварталі 2024 року [1-2].

За даними урядової команди реагування на комп'ютерні надзвичайні події CERT-UA [1-2], 347 кібератак зафіксовано на уряд та урядові організації, 276 – на місцеві органи влади, 175 – на організації у секторі безпеки та оборони, 127 – комерційні організації. Ще 92 рази було атаковано енергетичний сектор, 81 – телеком, 38 – освітні установи, 32 – транспортну галузь, 30 – фінансовий сектор, 25 – IT-сектор, 15 – ЗМІ, 12 – медичні установи.

Сучасні інформаційні системи та мережі все більше уразливі до різноманітних загроз, таких як несанкціонований доступ, розкрадання інформації, DDoS-атаки, інвазії шкідливого програмного забезпечення та інші. Ці загрози стають все більш складними і витонченими, що ускладнює їх виявлення та запобігання. Підприємства використовують складні інформаційні системи та мережі, які охоплюють різноманітні пристрої, додатки та протоколи. Для забезпечення ефективного управління інформаційною безпекою необхідно мати всебічний огляд всіх компонентів інформаційної системи. Управління інформаційною безпекою є складним і трудомістким завданням, яке вимагає постійного моніторингу та аналізу великої кількості даних. SIEM системи дозволяють автоматизувати багато завдань безпеки, що звільняє персонал для виконання інших важливих завдань.

SIEM-технології, які поєднують функції збору, кореляції, аналізу подій безпеки та управління інцидентами, стають ключовими інструментами для створення ефективної системи менеджменту інформаційної безпеки. Проте на практиці впровадження таких рішень часто супроводжується низкою проблем: високою вартістю, складністю налаштування та експлуатації, нестачею кваліфікованого персоналу, а також фрагментарністю існуючих підходів до інтеграції SIEM у загальну архітектуру інформаційної безпеки підприємства. Крім того, бракує уніфікованих методичних підходів до оцінювання ефективності та результативності таких систем із точки зору стратегічного управління ІБ.

Відтак, постає проблема наукового обґрунтування та розроблення комплексного підходу до інтеграції автоматизованих рішень на основі SIEM-технологій у систему менеджменту інформаційної безпеки організацій із урахуванням сучасних нормативних вимог, ризик-орієнтованих моделей та принципів безперервного вдосконалення. Її вирішення сприятиме підвищенню стійкості IT-інфраструктури до загроз, зменшенню часу реагування на інциденти та оптимізації процесів управління ІБ.

Аналіз останніх досліджень і публікацій. Питаннями, які охоплюють різні аспекти менеджменту інформаційної безпеки, займалися багато дослідників сучасності. У своїх роботах вони висвітлюють широкий спектр проблем, пов'язаних із формуванням політик безпеки, ризик-менеджментом, упровадженням систем контролю та реагування на інциденти.

Окрему увагу сучасні дослідження приділяють питанням впровадження та адаптації SIEM-систем у структуру інформаційної безпеки організацій. Так, у працях Uetz R., Herzog M., Hackländer L., Schwarz S., Henze M., Shukla A., Gandhi P. A., Elovici Y., Shabtai A., Kremer R., Wudali P. N., Momiyama S., Araki T., Furukawa J., Pulyala S. R. [3-14] розглядаються можливості підвищення ефективності виявлення загроз із використанням штучного інтелекту, автоматизованої кореляції подій та обробки великих обсягів журналів безпеки. Пропонуються моделі інтеграції SIEM із системами класу SOAR, а також підходи до розробки адаптивних правил виявлення аномальної активності.

Разом з тим, більшість наявних робіт зосереджені переважно на технічних аспектах функціонування SIEM-рішень або на окремих прикладах їх впровадження без урахування повної інтеграції у систему менеджменту інформаційної

безпеки згідно з вимогами міжнародних стандартів (ISO/IEC 27001, ISO/IEC 15408). Недостатньо розкритими залишаються питання методологічної уніфікації процесу впровадження SIEM-технологій із погляду управлінської ефективності, оцінювання ризиків, стратегічного планування та безперервного вдосконалення системи ІБ.

Отже, продовжує залишатися актуальною необхідність у подальших дослідженнях низки питань щодо формування уніфікованого підходу до інтеграції автоматизованих рішень на основі SIEM-технологій у комплексну систему менеджменту інформаційної безпеки організацій. Проблеми, перераховані вище, та їхня актуальність зумовили вибір теми статті, визначили її мету та завдання.

Постановка завдання. Метою статті є визначення методичних підходів до інтеграції автоматизованих рішень у систему менеджменту інформаційної безпеки на основі застосування SIEM-технологій, що є основою оптимізації архітектури управління кіберзагрозами, підвищення адаптивності організацій до сучасних викликів інформаційного середовища, забезпечення безперервності бізнес-процесів, а також створення умов для зміцнення цифрової довіри, зниження рівня ризиків та підвищення стійкості інформаційних систем до внутрішніх і зовнішніх загроз.

Виклад основного матеріалу дослідження. SIEM-система – це система управління інформаційною безпекою та розслідуванням інцидентів (Security Information and Event Management). Вона призначена для збору, консолідації, зберігання, аналізу та візуалізації даних безпеки з різних джерел, таких як мережеві пристрої, сервери, робочі станції, програмне гарантування безпеки тощо. SIEM-системи використовуються для виявлення, реагування та розслідування інцидентів безпеки, а також для гарантування відповідності вимогам безпеки. SIEM-система (Security Information and Event Management) – це програмне забезпечення, яке збирає, обробляє та аналізує дані про події безпеки з різних джерел, таких як мережеві пристрої, сервери, додатки та кінцеві точки. SIEM-системи використовують для виявлення, реагування та запобігання загрозам інформаційній безпеці.

Роботу SIEM-системи можна розділити на чотири основних етапи: збір даних; консолідація та зберігання даних; аналіз даних; розроблення звітів та сповіщень. Окрім цих основних етапів, SIEM-система може виконувати також інші функції, такі як: менеджмент відповідей на інциденти – допомога в реагуванні на виявлені інциденти; аналіз поведінки користувачів – виявлення аномалій у поведінці користувачів; відстеження відповідності вимогам – гарантування відповідності вимогам безпеки. Етапи роботи SIEM-системи можуть бути адаптовані до конкретних потреб організації. Наприклад, організація, яка має обмежений бюджет, може зосередитися на основних етапах, таких як збирання, консолідація та зберігання даних. А організація, яка має високий рівень ризику, може використовувати більш складні функції, такі як аналіз поведінки користувачів або управління відповідями на інциденти.

SIEM-системи збирають дані з різних джерел, таких як: мережеві пристрої, наприклад брандмауери, маршрутизатори, комутатори тощо; сервери, такі як веб-сервери, файлові сервери, бази даних тощо; робочі станції, наприклад, комп'ютери, ноутбуки, планшети тощо; програмне гарантування безпеки, таке як антивірусні програми, системи виявлення вторгнень (IDS), системи управління вразливостями тощо. SIEM-системи можуть збирати дані в різних форматах, таких як текстові файли, XML, JSON, CSV тощо. SIEM-система повинна мати можливість обробляти та перетворювати дані в єдиний формат для подальшого аналізу.

SIEM-системи можуть збирати дані кількома способами, такими як: пряме підключення – SIEM-система може підключатися безпосередньо до джерела даних і отримувати дані в реальному час; сервер повідомлень – SIEM-система може отримувати дані з сервера повідомлень, який збирає дані з різних джерел; автоматичне завантаження – SIEM-система може автоматично завантажувати дані з локальних або віддалених файлів. Вибір методу збору даних залежить від конкретного джерела даних і потреб організації.

Основними функціями SIEM-систем є збір даних, обробка даних, фільтрація, кореляція, аналіз, виявлення аномалій, виявлення вторгнень, виявлення загроз, генерація рішень, повідомлення про загрози, автоматичне реагування. Сьогодні на світовому ринку представлено широкий спектр SIEM-систем, які пропонують різні функції та можливості. Наведемо деякі з найпопулярніших сучасних SIEM-систем:

– IBM QRadar. Комплексна SIEM-система, яка пропонує широкий спектр функцій, включаючи виявлення вторгнень, аналіз загроз, управління інцидентами та реагування на них.

– Splunk Enterprise Security. SIEM-система, яка спеціалізується на аналізі великих обсягів даних.

– Microsoft Sentinel. SIEM-система, яка інтегрована з іншими продуктами Microsoft, такими як Azure Monitor та Azure Security Center.

– Siemplify. SIEM-система, яка пропонує простий і зручний інтерфейс.

– LogRhythm. SIEM-система, яка пропонує широкий спектр функцій та можливостей для великих організацій.

Автоматизація в системі управління інформаційною безпекою (СУІБ) за допомогою технологій SIEM (Security Information and Event Management) є ключовим етапом трансформації процесів гарантування кібербезпеки в умовах постійного зростання кількості загроз та обсягів даних, що потребують обробки. SIEM-системи забезпечують централізований моніторинг інформаційної інфраструктури в реальному часі, збираючи, нормалізуючи та корелюючи події з різних джерел (серверів, мережевого обладнання, прикладного програмного забезпечення тощо). Такий підхід дозволяє не лише виявляти аномальні або потенційно небезпечні дії, а й оперативно оцінювати їх контекст та критичність.

Однією з основних функціональних переваг SIEM є автоматичне виявлення підозрілих дій на основі заздалегідь визначених кореляційних правил, сценаріїв або з використанням методів машинного навчання. Це дозволяє значно прискорити і підвищити точність виявлення інцидентів безпеки. Подальший розвиток цієї функціональності полягає в інтеграції SIEM із платформами SOAR (Security Orchestration, Automation and Response), що забезпечує автоматизовану оркестрацію дій реагування на виявлені інциденти. Завдяки попередньо налаштованим сценаріям (playbooks) система може самостійно вживати відповідних заходів – від блокування доступу до ізоляції вузлів та інформування відповідальних осіб.

Ще одним важливим аспектом автоматизації в СУІБ є формування звітності, необхідної для аудитів та забезпечення відповідності нормативним вимогам (наприклад, ISO/IEC 27001, GDPR, NIS2). SIEM-системи дозволяють генерувати структуровані звіти, які містять детальну інформацію про інциденти, активність користувачів, зміни конфігурації та інші аспекти, що мають значення для контролю безпеки та прийняття управлінських рішень.

Автоматизація процесів за допомогою SIEM має низку суттєвих переваг. По-перше, значно скорочується час реагування на інциденти, що критично важливо для мінімізації шкоди та уникнення ескалації загроз. По-друге, зменшується ризик людських помилок, що особливо актуально в умовах високої інтенсивності подій та навантаження на фахівців із безпеки. По-третє, зростає загальна ефективність роботи Центру операцій безпеки (SOC), оскільки автоматизовані процеси зменшують рутинне навантаження та дозволяють аналітикам зосередитись на більш складних загрозах і стратегічних завданнях.

Архітектура інтеграції системи управління інформаційною безпекою (СУІБ) із SIEM-технологіями (Security Information and Event Management) є критичним чинником для побудови ефективної, масштабованої та адаптивної системи захисту інформаційних активів. Така архітектура передбачає взаємодію кількох функціональних компонентів, які спільно забезпечують моніторинг, аналіз, реагування та документування інцидентів інформаційної безпеки у рамках загальної стратегії управління ризиками.

У типовій інтеграційній архітектурі першим шаром виступають джерела логів – елементи інформаційної інфраструктури, з яких збираються дані про події. До таких джерел належать мережеве обладнання (маршрутизатори, комутатори, міжмережеві екрани), сервери, бази даних, системи управління доступом, програмне забезпечення користувачів, вебсервери тощо. Наприклад, з міжмережевого екрану збираються логи про блокування трафіку, з контролера домену – події автентифікації, з БД – спроби несанкціонованого доступу або SQL-ін’єкції.

Центральною ланкою архітектури є сама SIEM-система, яка виконує роль аналітичного ядра. Вона нормалізує вхідні логи, корелює події з різних джерел, виявляє аномалії та генерує попередження про потенційні інциденти. Наприклад, якщо SIEM отримує з різних вузлів інформацію про неуспішні спроби входу в систему протягом короткого періоду, вона може виявити атаку перебором паролів (brute force) та ініціювати відповідні заходи реагування.

Ефективність SIEM значно підвищується при її інтеграції з іншими компонентами СМІБ. Зокрема, з системами управління ідентифікацією та доступом (IAM), які дозволяють визначати, хто саме виконав підозрілу дію. Інтеграція з базами конфігураційного обліку (CMDB) забезпечує контекст для розуміння критичності активів, на які спрямована атака. Використання модулів контролю витоку даних (DLP) дозволяє фіксувати спроби несанкціонованого копіювання або передавання конфіденційної інформації. Інтеграція з системами виявлення та реагування на загрози на кінцевих пристроях (EDR) дає змогу отримувати інформацію про поведінку шкідливого програмного забезпечення на робочих станціях і серверах, що дозволяє швидше локалізувати інцидент.

Типовими сценаріями інтеграції є, зокрема: централізований збір логів про доступ користувачів до критичних ресурсів із подальшою аналітикою SIEM; використання SIEM для виявлення спроб передання персональних даних через незашифровані канали, що ініціює реакцію DLP-модуля; автоматизована перевірка змін у конфігурації систем із порівнянням до політик, згенерованих в IAM чи CMDB.

Ключовим технологічним інструментом реалізації такої інтеграції є API (Application Programming Interface), що дозволяє обмінюватись даними між SIEM і зовнішніми системами. Наприклад, REST API використовується для запиту даних про інциденти з SIEM до зовнішньої системи управління ризиками, або навпаки – для передання контекстної інформації в SIEM з інших джерел. Автоматичні скрипти на мові Python дають змогу реалізувати кастомізовані сценарії – наприклад, автоматично блокувати облікові записи після виявлення підозрілої активності. У поєднанні з технологіями SOAR (Security Orchestration, Automation and Response) це забезпечує автоматизоване виконання playbook’ів – наборів дій для типових інцидентів (наприклад, перевірка хешу файлу в сторонньому репозиторії, ізоляція хосту, сповіщення відповідального аналітика тощо).

На рис 1. наведемо типову архітектуру інтеграції системи виявлення та реагування (SIEM) із засобами розширеного захисту кінцевих точок (EDR) та платформою автоматизації безпеки (SOAR) у системі менеджменту інформаційної безпеки (СУІБ).

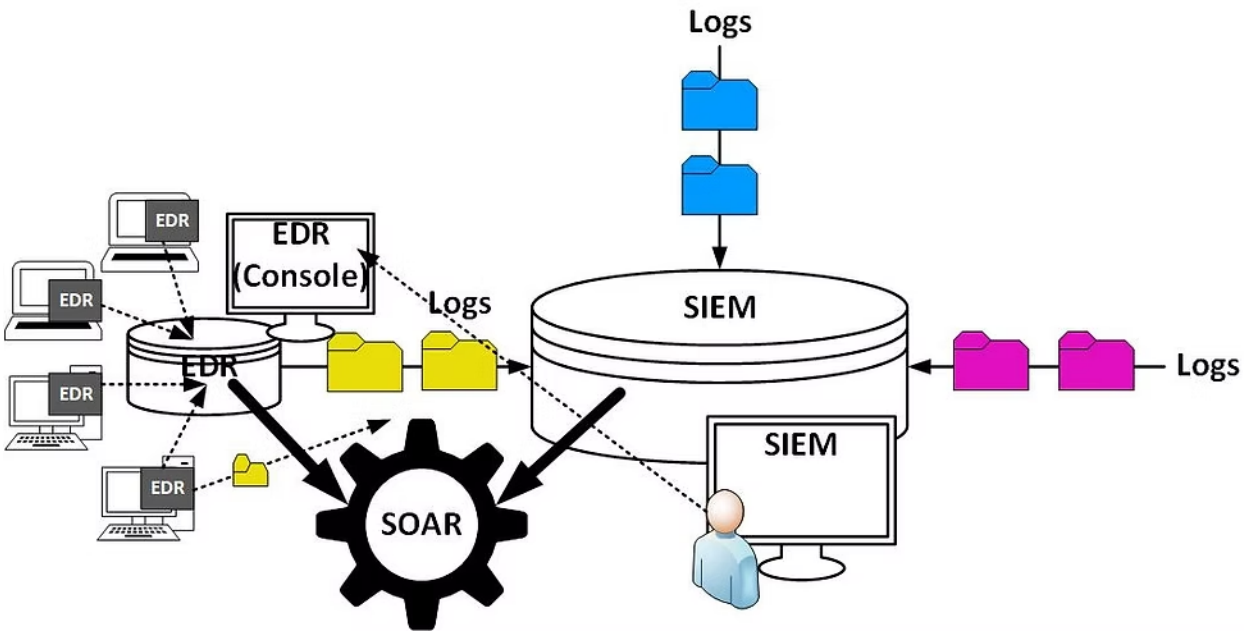

Рис. 1. Підхід до побудови адаптивної, автоматизованої та ефективної системи управління інформаційною безпекою

Клієнтські пристрої з установленими агентами EDR збирають телеметрію, поведінкові дані та журнали подій. Ці дані надсилаються до централізованої EDR-консолі, яка агрегує логі, виконує попередній аналіз загроз і передає зібрану інформацію далі. Жовті папки представляють файли журналів (logs), які від EDR надходять до SIEM-системи. SIEM-сервер є основним вузлом збору, зберігання, кореляції та аналізу подій інформаційної безпеки. До нього також надходять журнали подій із інших джерел – зображені сині та рожеві папки, – що символізують інші категорії логів: наприклад, журнали мережевого обладнання, баз даних, серверів чи прикладного ПЗ. Інтерфейс взаємодії аналітика дозволяє отримувати попередження, аналітичні зведення та проводить розслідування інцидентів.

Інтеграція з платформою SOAR дає можливість отримати сигнали від EDR та SIEM для автоматизації процесів реагування. SOAR виконує сценарії (playbooks), які можуть ініціювати блокування облікових записів, ізоляцію хостів, створення тікетів у системах обслуговування тощо. Цей елемент візуально об'єднує всі джерела в єдиний механізм реагування.

Отже, такий підхід забезпечує повноцінну інтеграційну архітектуру СМІБ, у якій реалізовано багатоджерельний моніторинг, централізовану аналітику подій через SIEM, автоматизовану відповідь на інциденти через SOAR, а також постійне збагачення даних за рахунок EDR-модулів на кінцевих точках. Ця архітектура є прикладом сучасного підходу до побудови адаптивної, автоматизованої та ефективної системи управління інформаційною безпекою.

Отож архітектура інтеграції SIEM у СМІБ передбачає створення взаємопов'язаної екосистеми, де дані з усіх рівнів інформаційної інфраструктури об'єднуються, аналізуються і трансформуються в аналітичну інформацію, що використовується для ефективного реагування на загрози. Такий підхід дозволяє перейти від фрагментарного контролю до цілісного управління безпекою на основі даних, автоматизації та адаптивності.

Використання SIEM-систем (систем управління інформаційною безпекою та подіями) забезпечує низку переваг, серед яких ключовими є підвищення ефективності менеджменту інформаційної безпеки, скорочення часу реагування на кіберінциденти, зниження ризиків реалізації кібератак, а також загальне підвищення рівня захисту інформації в організації. Завдяки централізованому збору, зберіганню, аналізу та кореляції журналів подій із різноманітних джерел, SIEM-системи дозволяють своєчасно виявляти потенційні загрози та оперативно реагувати на них. Під час вибору конкретного рішення варто враховувати низку важливих чинників, зокрема розмір організації, типи даних, які підлягають моніторингу, а також перелік функцій і можливостей, що відповідають потребам безпеки. SIEM-системи сприяють забезпеченню відповідності нормативно-правовим вимогам у сфері інформаційної безпеки, покращують загальну ситуаційну обізнаність та оптимізують процеси управління інцидентами, що робить їх важливим компонентом сучасної архітектури кіберзахисту. Загалом застосування SIEM у контексті автоматизації СУІБ дозволяє досягти вищого рівня зрілості процесів інформаційної безпеки, забезпечити проактивне управління ризиками та сприяти стійкості організацій до сучасних кіберзагроз.

Висновки і перспективи подальших досліджень у даному напрямі. Інтеграція систем EDR, SIEM та SOAR забезпечує підвищення ефективності управління інцидентами інформаційної безпеки за рахунок автоматизації виявлення,

аналізу та реагування на загрози в режимі реального часу. Представлена архітектура демонструє потенціал для побудови адаптивних і масштабованих систем захисту в умовах зростаючої складності кіберзагроз.

Перспективи подальших досліджень передбачають удосконалення методів кореляції даних із різнорідних джерел, розвиток інтелектуальних механізмів прийняття рішень у SOAR-платформах, а також впровадження машинного навчання для підвищення точності прогнозування та мінімізації хибнопозитивних спрацювань.

ЛІТЕРАТУРА

1. Про CERT-UA. Державна служба спеціального зв'язку та захисту інформації України, 2023. URL: https://cert.gov.ua.
2. Про Національний координаційний центр кібербезпеки. *Верховна Рада України*. 2016. URL: https://zakon.rada.gov.ua/laws/show/242/2016#Text.
3. Uetz R., Herzog M., Hackländer L., Schwarz S., Henze M. You Cannot Escape Me: Detecting Evasions of SIEM Rules in Enterprise Networks. *arXiv*. 2023. URL: https://arxiv.org/abs/2302.08128.
4. Shukla A., Gandhi P. A., Elovici Y., Shabtai A. RuleGenie: SIEM Detection Rule Set Optimization. *arXiv*. 2025. URL: https://arxiv.org/abs/2504.05678.
5. Kremer R., Wudali P. N., Momiyama S., Araki T., Furukawa J., Elovici Y., Shabtai A. IC SECURE: Intelligent System for Assisting Security Experts in Generating Playbooks for Automated Incident Response. *arXiv*. 2023. URL: https://arxiv.org/abs/2306.04593.
6. Advancing Cyber Resilience through the Convergence of SIEM, SOAR, and AI Technologies. *ResearchGate*. 2025. URL: https://www.researchgate.net/publication/378741231.
7. Pulyala S. Reddy. From Detection to Prediction: AI powered SIEM for Proactive Threat Hunting and Risk Mitigation. *Turkish Journal of Computer and Mathematics Education.* 2024. Vol. 15, No. 3. P. 112-119. URL: https://www.turcomat.org/index.php/ turkbilmat/article/view/5214.
8. TechScience Review. AI/ML in Security Orchestration, Automation and Response: Future Research Directions. *TechScience*. 2025. URL: https://www.techscience.com/cmc/v76n1/59053.
9. Miller D. Security Information and Event Management (SIEM) – Implementation Guide. Boca Raton: CRC Press, 2020. 358 p.
10. Pitis A. SIEM: Trends and Best Practices for Operations and Development. Apress, 2020. 242 p.
11. Коробейнікова Т. І., Федорченко В. В. Системний моніторинг мережевої безпеки в тріаді SIEM-EDR-NDR. *International scientific journal «Grail of Science»*. 2023. №3 (31) (May, 2023). С. 354-360.
12. Коробейнікова Т. І., Федорченко В. В. Системний моніторинг мережевої безпеки в тріаді SIEM-EDR-NDR. *International periodical scientific journal «SWorldJournal»*. 2023. № 19 (part 1) (May, 2023). С. 33-39.
13. Кошара А., Бакало Б. Підвищення захищеності державного сектору на основі SIEM-систем. *Інфокомунікаційні та комп'ютерні технології*. 2023. Т. 2, № 4. С. 128–133. URL: https://doi.org/10.36994/2788-5518-2022-02-04-14.
14. Драб Ю., Ящук В. Основні підходи до побудови системи управління інформаційною безпекою. *Інформаційна безпека та інформаційні технології: збірник тез доповідей V Всеукраїнської науково-практичної конференції молодих учених, студентів і курсантів*, м. Львів, 26 листопада 2021 року. Львів: ЛДУ БЖД, 2021. С. 29-32.
15. Yashchuk V., Ivanusa A., Maslova N., Tkachuk R., Brych T. INTEGRATION OF VULNERABILITY DATABASES INTO ISMS – A PATH TO ENHANCING CYBER RESILIENCE OF CRITICAL SYSTEMS. *Resilient Systems: Secure Digital Technologies and Critical Infrastructure: Proceedings of 1st International Scientific and Practical Conference.* Drohobych: Donetsk National Technical University, 2025. 184 p. P. 60-66.
16. Top SIEM Use Cases for Correlation and SIEM Alerts Best Practices. *DNSstuff*. 2020. URL: https://www.dnsstuff.com/common-siem-alerts.
17. Computer Networking and Cybersecurity: A Guide to Understanding Communications Systems, Internet Connections, and Network Security Along with Protection from Hacking and Cyber Security Threats. 2020. 242 p.

REFERENCES

1. Pro CERT-U (2023), *Derzhavna sluzhba spetsial'noho zv"yazku ta zakhystu informatsiyi Ukrayiny*, available at: https://cert.gov.ua.
2. Pro Natsional′nyy koordynatsiynyy tsentr kiberbezpeky. Verkhovna Rada Ukrayiny. 2016, available at: https://zakon.rada.gov.ua/laws/show/242/2016#Text.
3. Uetz, R., Herzog, M., Hackländer, L., Schwarz, S. and Henze, M. (2023), You Cannot Escape Me: Detecting Evasions of SIEM Rules in Enterprise Networks, *arXiv*, available at: https://arxiv.org/abs/2302.08128.
4. Shukla, A., Gandhi, P. A., Elovici, Y. and Shabtai, A. (2025), RuleGenie: SIEM Detection Rule Set Optimization, *arXiv*, available at: https://arxiv.org/abs/2504.05678.
5. Kremer, R., Wudali, P. N., Momiyama, S., Araki, T., Furukawa, J., Elovici, Y. and Shabtai, A. IC SECURE: Intelligent System for Assisting Security Experts in Generating Playbooks for Automated Incident Response, *arXiv*. available at: https://arxiv.org/abs/2306.04593.
6. Advancing Cyber Resilience through the Convergence of SIEM, SOAR, and AI Technologies (2025), *ResearchGate*, available at: https://www.researchgate.net/publication/378741231.
7. Pulyala, S. Reddy 2024, From Detection to Prediction: AI powered SIEM for Proactive Threat Hunting and Risk Mitigation, *Turkish Journal of Computer and Mathematics Education*, Vol. 15, No. 3, p. 112-119, available at: https://www.turcomat.org/index.php/turkbilmat/article/view/5214.

8. TechScience Review. AI/ML in Security Orchestration, Automation and Response: Future Research Directions (2025), *TechScience*, available at: https://www.techscience.com/cmc/v76n1/59053.

9. Miller, D. (2020), Security Information and Event Management (SIEM) – Implementation Guide, CRC Press, Boca Raton, 358 p.

10. Pitis, A. (2020), SIEM: Trends and Best Practices for Operations and Development, Apress, 242 p.

11. Korobeynikova, T. I. and Fedorchenko, V. V. (2023), Systemnyy monitorynh merezhevoyi bezpeky v triadi SIEM-EDR-NDR, *International scientific journal «Grail of Science»,* № 3 (31), s. 354-360.

12. Korobeynikova, T. I. and Fedorchenko, V. V. (2023), Systemnyy monitorynh merezhevoyi bezpeky v triadi SIEM-EDR-NDR, *International periodical scientific journal «SWorldJournal»,* № 19 (part 1), s. 33-39.

13. Koshara, A. and Bakalo, B. (2023), Pidvyshchennya zakhyshchenosti derzhavnoho sektoru na osnovi SIEM-system, *Infokomunikatsiyni ta komp"yuterni tekhnolohiyi*, t. 2, № 4. s. 128-133, available at: https://doi.org/10.36994/2788-5518-2022-02-04-14.

14. Drab, Yu. and Yashchuk, V. (2021), Osnovni pidkhody do pobudovy systemy upravlinnia informatsiinoiu bezpekoiu, *Informatsiina bezpeka ta informatsiini tekhnolohii: zbirnyk tez dopovidei V Vseukrainskoi naukovo-praktychnoi konferentsii molodykh uchenykh, studentiv i kursantiv*, m. Lviv, 26 lystopada 2021 roku, LDU BZhD, Lviv, s. 29-32.

15. Yashchuk, V., Ivanusa, A., Maslova, N., Tkachuk, R. and Brych, T. (2025), INTEGRATION OF VULNERABILITY DATABASES INTO ISMS – A PATH TO ENHANCING CYBER RESILIENCE OF CRITICAL SYSTEMS. *Resilient Systems: Secure Digital Technologies and Critical Infrastructure: Proceedings of 1st International Scientific and Practical Conference*, Donetsk National Technical University, Drohobych, 184 p.

16. Top SIEM Use Cases for Correlation and SIEM Alerts Best Practices (2020), *DNSstuff*, available at: https://www.dnsstuff.com/common-siem-alerts.

17. Computer Networking and Cybersecurity: A Guide to Understanding Communications Systems, Internet Connections, and Network Security Along with Protection from Hacking and Cyber Security Threats (2020), 242 p.

Стаття надійшла: 06.10.2025
Стаття прийнята: 17.11.2025
Стаття опублікована: 30.12.2025