Скочко П. А., магістрант
Шелуха О.О., к.т.н. , доцент
Державний університет «Житомирська політехніка»

СУЧАСНІ ЗАСОБИ МОНІТОРИНГУ ТА РЕАГУВАННЯ НА ІНЦИДЕНТИ КІБЕРБЕЗПЕКИ В ІНФОРМАЦІЙНИХ СИСТЕМАХ

Сучасні інформаційні системи постійно зазнають впливу кіберзагроз, рівень складності яких невпинно зростає. Методи атак стають дедалі витонченішими, зловмисники активно застосовують автоматизовані засоби та техніки обходу традиційних механізмів захисту. Збільшення кількості атак на корпоративні мережі та інформаційні ресурси організацій зумовлене розвитком технологій, які одночасно відкривають нові можливості для захисту та створюють додаткові вразливості. Традиційні методи кібербезпеки, такі як антивірусні програми, міжмережеві екрани та системи управління доступом, залишаються важливими компонентами захисту, проте вони не завжди можуть забезпечити комплексний підхід до протидії загрозам. Різноманітність атак, включаючи DDoS, фішингові кампанії, експлуатацію вразливостей програмного забезпечення та інсайдерські загрози, потребує застосування більш гнучких та адаптивних засобів моніторингу та аналізу подій безпеки. Крім того, значні обсяги логів, що генеруються в межах корпоративних мереж, ускладнюють виявлення аномальних дій і потребують застосування автоматизованих методів аналізу, здатних здійснювати моніторинг безпекових подій у режимі реального часу.

Впровадження SIEM-систем дозволяє вирішити зазначені проблеми, забезпечуючи централізований збір, аналіз та кореляцію подій безпеки в масштабах всієї організації. SIEM-системи забезпечують централізований моніторинг подій безпеки та ефективний аналіз даних із різних джерел, включно з мережевими пристроями, серверами, додатками й базами даних. Вони виконують не лише збір і кореляцію інформації про інциденти, а й застосовують аналітичні механізми для виявлення загроз. Сучасні рішення, такі як Splunk, IBM QRadar, ArcSight і Graylog, використовують алгоритми машинного навчання, що дає змогу розпізнавати нетипові дії в мережі та мінімізувати кількість хибнопозитивних спрацювань. Автоматизація процесів аналізу подій безпеки суттєво скорочує час реагування на загрози та знижує навантаження на фахівців із кібербезпеки.

Впровадження SIEM-систем у корпоративні мережі не лише підвищує рівень ситуаційної обізнаності щодо подій безпеки, а й сприяє дотриманню вимог регуляторних органів. Чинні стандарти, такі як ISO/IEC 27001, GDPR та NIST, передбачають наявність механізмів для збору та аналізу логів, що робить SIEM критично важливим компонентом інформаційної безпеки організацій, які прагнуть відповідати міжнародним нормам [1-3]. Крім того, SIEM-системи інтегруються з іншими засобами захисту, зокрема системами автоматизації реагування на інциденти та рішеннями для розширеного виявлення і реагування, забезпечуючи комплексний підхід до управління кібербезпекою.

Дослідження ефективності SIEM-рішень демонструють їхню значущу роль у підвищенні рівня безпеки мережевої інфраструктури. Наприклад, за даними Ponemon Institute, використання SIEM-систем у поєднанні з автоматизованими засобами реагування дозволяє знизити фінансові втрати від кібератак на 30–40%, а середній час реагування на інциденти скорочується в 2–3 рази порівняно з традиційними методами обробки подій [4]. Дослідження Gartner підтверджують, що підприємства, які інтегрують SIEM у свої інфраструктури, демонструють вищий рівень відповідності стандартам безпеки та ефективніше запобігають витокам даних. Крім того, звіт Exabeam SIEM Productivity Study вказує на те, що використання сучасних SIEM-рішень підвищує продуктивність команд безпеки та забезпечує швидше виявлення й усунення загроз [5]. Водночас впровадження SIEM вимагає значних ресурсів і правильної конфігурації, оскільки некоректні налаштування можуть призвести до перевантаження системи через надмірну кількість хибнопозитивних спрацювань.

З урахуванням зростання складності кіберзагроз та обсягів мережевого трафіку, SIEM-системи є ключовими технологіями для організацій, що прагнуть забезпечити ефективний моніторинг і своєчасне реагування на інциденти. Завдяки автоматизації аналізу подій і можливості інтеграції з іншими технологіями кіберзахисту, SIEM сприяє підвищенню рівня інформаційної безпеки та мінімізації ризиків, пов'язаних із кібератаками.

Список використаних джерел:

1. Kent K., Souppaya M. Guide to Computer Security Log Management. *NIST Special Publication 800-92*. 2006. URL: https://csrc.nist.gov/publications/detail/sp/800-92/final (дата звернення: 21.03.2025).
2. Menges F., et al. Towards GDPR-compliant data processing in modern SIEM systems. *Computers & Security*. 2020.
3. Tóth T. ISO 27001:2022 and NIS2 requirements and applicability of SIEM solutions. 2024.
4. Ponemon Institute LLC. Exabeam SIEM Productivity Study. 2019. 43 p.
5. Schneider M., Davies A., Ahlm E. Critical Capabilities for Security Information and Event Management. 2024.