ІНТЕГРАЦІЯ SOC ТА ISMS ЧЕРЕЗ AI

Іванський І.О., Нехороших Д.М.
Харківський національний університет радіоелектроніки, Харків, Україна

Управління інформаційною безпекою щороку стає складнішим зі зростанням вимог стандартів, зокрема ISO/IEC 27001. Традиційні підходи із базою ручного зіставлення контролів та перевірці підтверджуючих документів, вже не відповідають сучасним потребам. Такі процеси є повільними, вони створюють значне навантаження для всіх учасників та є недостатньо впорядкованими.

Традиційні методи управління інцидентами часто передбачають використання ручних процесів та обмежену автоматизацію, і саме через це вони не здатні впоратися зі складністю сучасних кібератак.

Зростаюча складність загроз у сфері кібербезпеки зумовила нагальну необхідність застосування більш інтелектуальних і динамічних механізмів захисту [1, 2].

Впровадження модулів на базі штучного інтелекту (ШІ) розглядається не лише як спосіб підвищення ефективності, а також як інструмент оптимізації витрат.

У довгостроковій перспективі дане рішення може сприяти здешевленню впровадження та підтримки рішень інформаційної безпеки, роблячи їх більш доступними для організацій з обмеженими ресурсами.

Метою доповіді є дослідження можливостей інтеграції операційних систем кібербезпеки (SOC) та систем управління інформаційною безпекою (ISMS) із використанням технологій штучного інтелекту, а також обґрунтування доцільності застосування ШІ-модулів для автоматизації процесів аудиту, управління ризиками та контролю відповідності стандартам з метою підвищення ефективності та зниження витрат на забезпечення інформаційної безпеки.

SOC AI – це система, розроблена для вдосконалення реагування на інциденти за допомогою автоматизації та передових технологій штучного інтелекту [1].

AI SOC описується як центр операцій з безпеки, в якому штучний інтелект виконує роботи з розслідування, сортування та кореляції, які в іншому випадку виконували б аналітики 1-го та 2-го рівнів. Подібна модель описується так, де ШІ допомагає визначати пріоритетність сповіщень, розслідувати інциденти, запускати сценарії реагування та генерувати докази, готові до аудиту.

Обидва описи вказують на одну й ту саму основну зміну: ШІ більше не використовується лише всередині окремих інструментів, а як рівень міркування, що працює у всьому середовищі [3].

ISO заявляє, що ISO 27001 є найвідомішим стандартом для систем управління інформаційною безпекою. ШІ може створювати нові моделі ризиків, але це не робить класифікацію даних, контроль доступу, управління

постачальниками, реагування на інциденти або управління активами менш важливими. Це робить їх ще важливішими [3].

Оптимізований процес, впроваджений в компанії Oplium, має на меті представити нову процедуру SOC, яка дозволяє ефективно реагувати на інциденти та підвищити продуктивність команди з безпеки при роботі зі складними загрозами.

З метою інтеграції SOC AI з провідними інструментами, що забезпечують комплексне виявлення загроз, такими як Rapid7 InsightIDR, та надійне управління квитками, такими як Jira, Oplium розробила добре інтегровану процедуру для автоматизації та підвищення якості на кількох етапах управління інцидентами.

Цей процес працює на віртуальній машині, розміщеній на Oracle Cloud Infrastructure.

Налаштування віртуальної машини використовує всі 24 ГБ оперативної пам'яті, доступні в безкоштовному тарифі, і тому ідеально підходить для роботи SOC [1].

Контейнеризація робить систему масштабованою, модульною та простішою в управлінні.

Ця віртуальна машина працює за дуже суворими правилами безпеки, які дозволяють отримати доступ до інфраструктури SOC лише користувачам, підключеним через VPN.

Така конфігурація гарантує, що лише авторизовані користувачі, які безпечно підключені, можуть взаємодіяти з проектом, тим самим підвищуючи безпеку середовища, конфіденційних даних SOC та запущених процесів [1].

Процес роботи центру реагування на інциденти (SOC) компанії Oplium складається з п’яти основних етапів:

1) виявлення інциденту та створення запиту;

2) класифікація та розслідування інциденту;

3) аналіз інциденту та реагування;

4) закриття інциденту;

5) аналіз після інциденту та постійне вдосконалення.

Впровадження SOC AI демонструє, що використання штучного інтелекту дозволяє автоматизувати та інтегрувати процеси реагування на інциденти, підвищуючи ефективність SOC, зменшуючи навантаження на аналітиків і забезпечуючи більш швидке та якісне управління кіберзагрозами.

З огляду на те, що такі стандарти, як ISO/IEC 27001 та SOC 2, встановлюють дедалі вищі вимоги, ручне зіставлення контрольних заходів та перевірка доказів просто не встигають за ними: ці процеси повільні та хаотичні.

Водночас управління системою управління інформаційною безпекою (ISMS) – супроводжується значними обсягами документації, збором доказів, зіставленням політик із усіма цілями контролю [4].

Дослідження пропонують аналізатор відповідності та доказів на базі модуля ШІ. Він використовує штучний інтелект, обробку природної мови

(NLP) та машинне навчання (ML) для автоматичного виконання перевірок відповідності та підготовки до аудиту. Система спирається на семантичні вбудовування, технологію RAG на базі LangChain та векторний пошук FAISS, щоб пов’язати політику компанії та докази з відповідними заходами контролю СУІБ.

Тепер штучний інтелект може фактично читати політики, досліджувати конфігурації системи, переглядати докази та автоматично пов'язувати все з відповідними елементами контролю ISMS [4].

Даний підхід формує передумови для переходу від періодичного до безперервного аудиту, в межах якого перевірка відповідності виконується постійно на основі актуальних даних із SOC. Таке рішення дозволяє своєчасно виявити відхилення, зменшити ризики невідповідності та підвищити ефективність функціонування ISMS.

Система, що розробляється – «AI-Driven Control Mapping and Evidence Analyzer», значно спрощує перевірку відповідності вимогам СУІБ. Вона використовує штучний інтелект та обробку природної мови для виконання трьох основних завдань:

зіставлення політик із заходами контролю;

аналіз доказів;

формування звітів про відповідність вимогам.

Цей підхід поєднує машинне навчання, векторний пошук за схожістю та міркування штучного інтелекту, тому результати не тільки точні, але й масштабовані, і можливо реально зрозуміти, як вони були отримані. Коли завантажується файл політики або доказів, двигун штучного інтелекту створює вбудовування для вхідного даних, а потім шукає в індексі FAISS найближчі заходи контролю ISMS [4].

Найбільш надійна архітектура зазвичай починається з систем управління і закінчується доказами під час виконання. В основі лежить ISO 27001, оскільки без функціонуючої ISMS решта, як правило, стає фрагментованою та залежить від особистості.

З операційної сторони лежить AI SOC або еквівалентна функція, оскільки середовище контролю не має великого значення, якщо ніхто не може розслідувати, що насправді відбувається [3].

Ефективне управління штучним інтелектом вимагає, щоб безпека не була лише додатковим елементом, а стала фундаментальною складовою, інтегрованою на кожному етапі життєвого циклу систем. Підхід «безпека за замовчуванням» є необхідним для проактивного управління ризиками, забезпечення стійкості та створення надійного штучного інтелекту [5].

Впровадження ШІ-рішень потребує забезпечення прозорості та пояснюваності рішень, оскільки існують ризики помилкових висновків, а також актуальним залишається питання довіри до автоматизованих систем. З цієї причини ключовим принципом залишається підхід, за якого остаточні рішення приймаються фахівцями з інформаційної безпеки. Керівник служби інформаційної безпеки (CISO) забезпечує інформаційну безпеку організації,

включаючи всі інформаційні системи, і в контексті штучного інтелекту (ШІ) його роль стає ще більш важливою.

CISO повинен впроваджувати заходи безпеки, забезпечуючи захист моделей від зловмисних атак, витоку інформації або маніпуляцій під час навчання. Він також бере активну участь в оцінці ризиків, пов'язаних із використанням ШІ, розробляючи превентивні заходи та плани реагування на інциденти [5].

Таким чином, штучний інтелект виступає не окремим інструментом, а інтегруючим аналітичним шаром, що поєднує операційний рівень кібербезпеки з процесами управління ISMS, формуючи єдине інформаційне середовище для прийняття рішень.

Отже, традиційні ручні підходи до управління інформаційною безпекою та реагування на інциденти є занадто повільними для сучасних кіберзагроз і вимог стандартів, таких як ISO/IEC 27001.

Впровадження модуля ШІ вирішує цю проблему, перетворюючись на інтегруючий аналітичний блок, що поєднує стратегічне управління з операційним рівнем кібербезпеки.

З одного боку, моделі AI SOC оптимізують витрати та беруть на себе базові завдання аналітиків з розслідування та кореляції інцидентів. З іншого боку, технології обробки природної мови та машинного навчання дозволяють перейти до безперервного аудиту, автоматично зіставляючи докази та політики з вимогами ISMS.

Таким чином формується комплексна архітектура, де ISMS забезпечує впорядковане середовище управління, а AI SOC – можливість швидкого розслідування та реагування.

Проте, оскільки сам ШІ піддається специфічним ризикам, зокрема маніпуляціям під час навчання, тому критичною залишається роль CISO у захисті цих моделей за принципом «безпека за замовчуванням», де остаточні рішення все одно мають прийматися фахівцями для збереження довіри та прозорості.

Список літератури

1. Licitra S. Leveraging AI Techniques for Automated Security Incident Response: Master Degree Thesis. Politecnico di Torino, 2024. URL: https://webthesis.biblio.polito.it/33833/1/tesi.pdf

2. Sievierinov, O., Ovcharenko, M., & Vlasov, A. (2021). Enterprise Security Operations Center. 2021: Fifth International Scientific and Technical Conference "*Computer and information systems and technologies*".

3. AI SOC, ISO 27001, SOC 2, and the Security Stack Real AI Teams Need in 2026 / Penligent. 2026. URL: https://www.penligent.ai/hackinglabs/ai-soc-iso-27001-soc-2-and-the-security-stack-real-ai-teams-need-in-2026/

4. AI-Driven Control Mapping and Evidence Analyzer / Y. S. Zope, V. N. Sukale, Y. S. Kakade et al. // International Journal of Innovative Research in Technology (IJIRT). 2025. Vol. 12, Iss. 6. URL: https://ijirt.org/publishedpaper/IJIRT186166_PAPER.pdf

5. Study on AI Governance / ISMS Forum. 2025. URL: https://www.ismsforum.es/ficheros/descargas/en---gobierno-de-la-ia1765878738.pdf