ВИКОРИСТАННЯ ШТУЧНОГО ІНТЕЛЕКТУ ЯК ІНСТРУМЕНТУ АУДИТУ ISMS

Нехороших Д.М.
Харківський національний університет радіоелектроніки, Харків, Україна

На сьогоднішній день автоматизація аудиту системи управління інформаційною безпекою (ISMS) – один із найважливіших напрямів розвитку штучного інтелекту (ШІ, AI) в галузі кіберзахисту [1-3]. Раніше ШІ переважно використовувався як допоміжний інструмент для використання окремих завдань. Водночас автоматизація аудиту ISMS тривалий час залишалася складною та фактично неможливою задачею. Однак вектор почав змінюватися із появою великих мовних моделей (LLM) та моделей AI Scient.

Розвиток технологій штучного інтелекту у сфері інформаційної безпеки підтримується міжнародними ініціативами, такими як ISO 42001 AI Management framework, NIST AI Risk Management Framework (2023) та ISO/IEC 38507:2022, які регламентують етичні, правові та управлінські аспекти використання AI. На цьому тлі актуальним є створення AI-аудитора ISMS, який може забезпечити постійний аудит без необхідності людського втручання у рутинні процеси, що особливо важливо для підприємств із обмеженими ресурсами. Одночасно з цим сучасний ландшафт кіберзагроз дедалі більше формується під впливом технологій штучного інтелекту. Як захисники, так і зловмисники використовують AI-технології для автоматизації аналізу, пошуку вразливостей, проведення атак і реагування на інциденти. У цих умовах особливого значення набуває проблема побудови нового інструменту внутрішнього аудиту, здатного забезпечити безперервний моніторинг, динамічну оцінку ризиків, перевірку відповідності стандартам та підтримку прийняття управлінських рішень. На відміну від існуючих рішень, цей інструмент має поєднувати операційний рівень кібербезпеки з процесами управління ризиками та вдосконаленням ISMS у межах циклу PDCA.

Метою доповіді є дослідження підходу AI як інструменту повної автоматизації постійного контролю, оцінки ризиків та аудиту системи управління інформаційною безпекою.

Одним із найважливіших завдань у сфері загального штучного інтелекту є розробка агентів, здатних проводити збір та оцінювати кореляції подій безпеки, виконувати виявлення та реагування на загрози, оцінювати ризики та управління ними, готувати звітність та документування. Хоча наукова спільнота з кіберзахисту досягла значного прогресу в автоматизації окремих компонентів аудиту, система, яка б самостійно керувала всім циклом аудиту системи управління інформаційною безпекою– від створення, впровадження до постійного контролю стану захисту – досі залишається недосяжною [1].

Для вирішення цієї проблеми було представлено в перше модель AI-Аудитора ISMS. Архітектура AI-Аудитора ISMS складається з восьми взаємопов’язаних модулів:

- модуль загального аналізу;
- модуль аналізу контексту;
- модуль інвентаризації активів;
- модуль управління ризиками;
- модуль SOC-моніторингу;
- модуль управління відповідністю;
- модуль зворотного зв'язку (Feedback Loop);
- агенти аудиту.

Кожен із модулів виконує окремі функції і вони інтегровані в процес безперервного внутрішнього аудиту.

З огляду на сучасні тенденції розвитку кіберзагроз і зростання складності інформаційних систем, забезпечення ефективного функціонування систем управління інформаційною безпекою стає дедалі складнішим завданням. Традиційні підходи до внутрішнього аудиту ISMS, що базуються на періодичних перевірках і ручному аналізі, не завжди дозволяють оперативно реагувати на зміни в середовищі загроз. Виклики сучасності, з повязані з використанням AI, вимагають підвищення вимог до постійного внутрішнього аудита, яки має бути динамічним, постійно діючим, що постійно вдосканалює систему, постійно орієнтований на завнішній та внутрішній контекст.

Сучасна проблематика безпеки AI полягає в створені підконтрольної моделі, яка має відповідати не тільки технічним вимогам. Це виклики, пов'язані з стратегічними основами системи управління інформаційною безпекою AI: зрілістю системи управління; прозорістю рішень, організаційною культурою, усвідомленням лідерства. Це відкрита тема, що до якої тільки формуються думки експертів.

Перспективи подальших досліджень пов'язані з практичною реалізацією агентних моделей аудиту, розвитком методів автоматизованого аналізу політик безпеки та використанням компактних AI-моделей, здатних працювати у захищених внутрішніх середовищах організацій. Такі підходи можуть стати основою для створення нових поколінь систем управління інформаційною та кібербезпекою, у яких ШІ виступатиме інтелектуальним інструментом підтримки рішень для фахівців з інформаційної безпеки.

Список літератури

1. Integrating Artificial Intelligence in Audit Workflow: Opportunities, Architecture, and Challenges: A Systematic Review. https://www.preprints.org/manuscript/202601.2060/v1/download?utm_source=chatgpt.com
2. Microsoft Security, "Microsoft raises the bar: a smarter way to measure AI for cybersecurity (ExCyTIn-Bench)," Microsoft Security Blog, 2025.
3. Building Trustworthy AI with ISO/IEC 42001 and the NIST AI Framework https://pecb.com/en/past-webinars/building-trustworthy-ai-with-iso-iec-42001-and-the-nist-ai-framework