

СЕКЦІЯ «КІБЕРБЕЗПЕКА ТА ЗАХИСТ ВЕЛИКИХ ДАНИХ»

Терещенко Катерина Володимирівна, студентка, Державний університет “Київський авіаційний інститут”, м. Київ

Терещенко Тетяна Павлівна, старша наукова співробітниця, Військовий інститут телекомунікацій та інформатизації імені Героїв Крут, м. Київ

**ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ СИСТЕМ ІНФОРМАЦІЙНОЇ
БЕЗПЕКИ НА ОСНОВІ ІНТЕГРАЦІЇ ШТУЧНОГО ІНТЕЛЕКТУ У
ПРОЦЕСИ РЕАГУВАННЯ НА КІБЕРЗАГРОЗИ**

Вступ. Актуальність теми полягає у стрімкому зростанні кількості та складності кіберзагроз в умовах цифровізації суспільства та розвитку інформаційних технологій [3]. Сучасні інформаційні системи обробляють значні обсяги даних, що ускладнює своєчасне виявлення інцидентів традиційними методами моніторингу. Водночас кіберзлочинці активно використовують новітні технології, що вимагає впровадження більш інтелектуальних та адаптивних підходів до захисту інформації.

У цьому контексті застосування штучного інтелекту у процесах моніторингу та реагування на кіберінциденти набуває особливої значущості, оскільки дозволяє підвищити ефективність виявлення загроз, оптимізувати процеси аналізу даних та забезпечити оперативне реагування [4]. Це є критично важливим для забезпечення належного рівня інформаційної безпеки в умовах сучасних кіберризиків.

Метою дослідження є можливе використання штучного інтелекту та розробки рекомендацій щодо його інтеграції у процеси моніторингу та реагування на кіберінциденти.

Інтеграція технологій штучного інтелекту у процеси моніторингу та реагування є перспективним напрямом розвитку систем інформаційної безпеки [4]. Використання ШІ забезпечує можливість виявлення аномалій у поведінці користувачів та систем, що дозволяє своєчасно ідентифікувати потенційні загрози.

Одним із ключових підходів є застосування систем поведінкового аналізу, які дозволяють виявляти відхилення від нормальної активності. Це значно підвищує ефективність виявлення як зовнішніх, так і внутрішніх загроз.

Важливу роль відіграє інтеграція ШІ з сучасними системами управління подіями безпеки (SIEM) та платформами оркестрації і автоматизації реагування (SOAR), що відповідає сучасним підходам до управління інцидентами [5]. Це забезпечує автоматизацію процесів обробки інцидентів, їх класифікації та реагування.

Крім того, застосування методів машинного навчання дозволяє здійснювати прогнозування кіберзагроз на основі аналізу історичних даних, що сприяє переходу від реактивного до проактивного захисту.

Водночас ефективність використання ШІ залежить від якості вхідних даних, необхідності регулярного оновлення моделей та залучення фахівців для контролю результатів їх роботи.

Особливу увагу слід приділяти дотриманню вимог інформаційної безпеки та захисту персональних даних [2], що є важливою умовою ефективного застосування ШІ.

У процесі дослідження було визначено ключові аспекти інтеграції штучного інтелекту у системи моніторингу та реагування на кіберінциденти.

Встановлено, що використання технологій штучного інтелекту сприяє підвищенню ефективності виявлення загроз, автоматизації процесів обробки інцидентів та скороченню часу реагування.

Було визначено, що впровадження поведінкового аналізу, інтеграція з SIEM- та SOAR-системами, а також застосування методів машинного навчання забезпечують підвищення точності аналізу та зменшення кількості хибних спрацювань.

Таким чином, інтеграція штучного інтелекту є ефективним напрямом розвитку систем інформаційної безпеки, що дозволяє підвищити рівень захищеності інформаційних ресурсів та забезпечити стійкість до сучасних кіберзагроз.

Список використаних джерел

1. Закон України «Про інформацію» від 02 жовтня 1992 р. № 2657-ХІІ. URL: <https://zakon.rada.gov.ua/laws/show/2657-12> (дата звернення: 28.03.2026).
2. Закон України «Про захист інформації в інформаційно-комунікаційних системах» від 05 липня 1994 р. № 80/94-ВР. URL: <https://zakon.rada.gov.ua/laws/show/80/94-вр> (дата звернення: 28.03.2026).
3. Закон України «Про основні засади забезпечення кібербезпеки України» від 05 жовтня 2017 р. № 2163-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2163-19> (дата звернення: 28.03.2026).
4. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection – Information security management systems – Requirements. Geneva: International Organization for Standardization, 2022.
5. NIST Special Publication 800-61 Revision 2. Computer Security Incident Handling Guide. Gaithersburg: National Institute of Standards and Technology, 2012. 80 p.

Vydavatel:

Publishing house Education and Science s.r.o. IČO : 271 56 877.
Frýdlanská 15/1314 , Praha 8. MS v Praze , oddíl C, vložka 100614

Global Interdisciplinary Summit: Frontier of Science and Future Technologies

**Proceedings of International Scientific and
Practical Conference**

**April 3, 2026 in Khalifa University Campus,
Dubai, UAE**

Signed for printing on April 6, 2026.
Format 60x90/8. Headset Times New Roman.
Mental printing. arc. 5,65. Edition online.