

Список використаних джерел

1. Гальчинський, А. С. (2019). Цифрова трансформація економіки: теоретичні та практичні аспекти. Київ: Науковий центр досліджень цифрових технологій.
2. Бойко, В. І., Костюк, А. В., & Червінська, І. П. (2020). Застосування технологій штучного інтелекту для прийняття управлінських рішень в умовах цифрової економіки. *Економіка та держава*, (6), 43-48.
3. Гусєв Ю. (2025) Галузеві тренди. Штучний інтелект в Україні: як розвивається галузь. URL: <https://hub.kyivstar.ua/articles/galuzevi-trendi-shtuchnij-intelekt-v-ukrayini-yak-rozvivayetsya-galuz>
4. Скляренко О. В., Федік О. І., Колодінська Я. О. (2021). Digital рішення для управління проектами та бізнес-процесами в умовах сучасних викликів. // *Економіка і управління*. (2). 85–90. URL: <https://e-u.edu.ua/journal/1088.pdf>
5. Онікієнко, В. В., & Ярова, О. М. (2021). Використання штучного інтелекту у менеджменті: можливості та виклики для українського бізнесу. *Вісник економічної науки України*, (2), 78-83.
6. Порожня, О. О., & Федоренко, В. Г. (2020). Штучний інтелект у управлінні персоналом: досвід українських компаній. *Економічний часопис*, (5), 95-101.

Старенький Ю.В.,
здобувач першого (бакалаврського) рівня вищої освіти,
Кудельський В. Е.,
к.е.н., доцент,
Хмельницький університет управління і права імені Леоніда Юзькова

ЗАСТОСУВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В КІБЕРБЕЗПЕЦІ

У сучасному цифровому середовищі, де кіберзагрози стають дедалі складнішими, традиційні методи кібербезпеки часто виявляються недостатніми для ефективного захисту від зловмисних атак. Саме в цьому контексті штучний інтелект (ШІ) постає як потужний союзник, здатний революціонізувати підходи

до виявлення, запобігання та реагування на кіберінциденти. Завдяки своїй здатності аналізувати величезні обсяги даних, виявляти закономірності та приймати швидкі рішення, ШІ відкриває нові горизонти в боротьбі з кіберзлочинністю, пропонуючи більш проактивний та адаптивний рівень захисту.

Штучний інтелект, як імітація людського інтелекту в машинах для логічного мислення та розв'язання проблем, знаходить своє застосування і в кібербезпеці. Тут його швидкість та обчислювальна потужність використовуються для створення протоколів, здатних прогнозувати, виявляти та мінімізувати загрози.

Оскільки понад 80% кіберінцидентів спричинені людським фактором, ШІ може стати ключовим рішенням, автоматизуючи рутинні завдання та виявляючи приховані закономірності [1]. Штучний інтелект відкриває широкі можливості для підсилення кібербезпеки, про що свідчить і різноманіття методів його застосування. Методи та особливості їх застосування представлено у табл. 1.

Використання штучного інтелекту (ШІ) відкриває значні перспективи для підвищення ефективності кібербезпеки на різних рівнях. Згадані вище методи, демонструють, як ШІ може автоматизувати рутинні завдання моніторингу та захисту, значно зменшуючи залежність від людського фактора та підвищуючи оперативність реагування на інциденти.

Однією з важливих переваг ШІ в кібербезпеці є його здатність самостійно навчатися на великих обсягах даних, зокрема на інформації про попередні кіберінциденти. Ключовою перевагою ШІ є його здатність до виявлення складних патернів і аномалій у великих обсягах даних, що дозволяє прогнозувати загрози та виявляти вторгнення на ранніх стадіях. Важливим аспектом є можливість автоматичного реагування на підозрілу активність, що дозволяє миттєво локалізувати та нейтралізувати потенційні загрози без втручання людини. Алгоритми класифікації та кластеризації можуть виявляти нетипову поведінку, наприклад, аномальні запити до серверів або спроби несанкціонованого доступу, що забезпечує швидке реагування на можливі загрози.

Методи застосування ШІ в кібербезпеці

Метод	Особливості застосування
Автоматизований моніторинг і захист	ШІ автоматизує моніторинг та захист інформаційних систем, знижуючи залежність від людського фактора та підвищуючи ефективність кіберзахисту.
Виявлення вторгнень і передбачення загроз	Алгоритми машинного навчання та нейронні мережі виявляють вторгнення та прогнозують потенційні загрози на основі аналізу великих обсягів даних і виявлення патернів поведінки в реальному часі.
Виявлення підозрілої активності в мережі та автоматичне реагування	Методи машинного навчання створюють моделі, які ідентифікують підозрілу активність у мережі та автоматично реагують на потенційні загрози, навчаючись на великих наборах даних для виявлення нових загроз.
Аналіз поведінки в мережі та виявлення шкідливих програм	Нейронні мережі швидко ідентифікують аномальні дії в мережевому трафіку, що можуть вказувати на спроби вторгнення або зараження вірусами, забезпечуючи реагування в реальному часі у великих інформаційних системах.
Самонавчання та адаптація до нових загроз	ШІ дозволяє системам вчитися на основі попередніх атак, покращуючи їхню здатність до адаптації до нових загроз. Прогностичні моделі, створені на основі даних про попередні атаки, визначають, коли система може стати мішенню.
Аналіз загроз у реальному часі	Використання аналітичних інструментів у реальному часі для своєчасного виявлення зловмисної діяльності до завдання шкоди. Інтеграція IDS та засобів збору інформації про загрози для проактивного захисту. Аналіз історичних даних для прогнозування потенційних загроз.
Розробка систем самонавчання	Алгоритми ШІ забезпечують постійне оновлення методів виявлення загроз, адаптуючись до нових викликів через аналіз змін у патернах атак та внесення коректив у захисні механізми (наприклад, за допомогою нейронних мереж).
Виявлення аномалій та захист від маніпуляцій даними	Розробка алгоритмів, що виявляють аномалії та забезпечують захист внутрішніх систем ШІ від атак, коли зловмисники навмисно модифікують вхідні дані.
Прогнозування потенційних загроз	Використання прогностичних моделей для ідентифікації потенційних загроз ще до їх виникнення шляхом аналізу поточних тенденцій у поведінці мережі або користувачів. Забезпечення проактивних стратегій кіберзахисту для мінімізації ризиків.

Джерело: складено автором на основі [2]

Окрім цього, машинне навчання дає змогу створювати системи для прогнозування кібератак на основі історичних даних. Прогностичні алгоритми здатні аналізувати тенденції кіберзлочинності, враховуючи особливості атак, види шкідливого програмного забезпечення та зміни в стратегіях кіберзахисту, що сприяє підвищенню готовності та рівня захисту [3].

Отже, штучний інтелект відіграє важливу роль у кібербезпеці, забезпечуючи проактивний та адаптивний захист від складних кіберзагроз. Його можливості включають автоматизований аналіз даних, виявлення закономірностей, прогнозування загроз та швидке реагування. Інтеграція ШІ підвищує ефективність кібербезпеки завдяки автоматизації, оперативному реагуванню, виявленню складних патернів та постійному вдосконаленню систем захисту, а значить подальший розвиток ШІ є ключовим для боротьби з кіберзлочинністю.

Список використаних джерел

1. BDO Україна В. (2024). *Переваги використання Штучного інтелекту в кібербезпеці*. Міжнародна аудиторська компанія BDO. <https://www.bdo.ua/uk-ua/insights-2/information-materials/2024/corporate-cybersecurity-ai-role-in-data-protection>
2. Різченко, М., & Блавацька, Н. (2024). *Роль штучного інтелекту у забезпеченні кібербезпеки*. **Матеріали II науково-практичної конференції** (с. 69–73). <https://molodyivchenyi.ua/omp/index.php/conference/catalog/download/118/1683/3503-1?inline=1>
3. Лучик, В., & Антошук, С. (2024). *Роль штучного інтелекту в кібербезпеці*. **Protecția drepturilor și libertăților fundamentale ale omului în procesul asigurării ordinii și securității publice** (с. 154–157). https://ibn.idsi.md/sites/default/files/imag_file/154-157_54.pdf