

Наведені приклади свідчать, що можливості штучного інтелекту не обмежуються окремими галузями, а охоплюють широкий спектр економічних, соціальних та екологічних завдань. Використання інтелектуальних технологій сприяє підвищенню ефективності управління ресурсами, покращенню якості життя населення та збереженню навколишнього середовища.

Таким чином, штучний інтелект стає одним із ключових інструментів забезпечення сталого розвитку в умовах сучасних глобальних викликів. Його використання сприяє підвищенню ефективності управління ресурсами, оптимізації економічних процесів, покращенню якості соціальних послуг та зменшенню негативного впливу господарської діяльності на навколишнє середовище. Завдяки здатності аналізувати великі обсяги даних, прогнозувати можливі ризики та підтримувати прийняття управлінських рішень, технології штучного інтелекту відкривають нові можливості для досягнення Цілей сталого розвитку.

Список використаних джерел

1. Evans, R., & Gao, J. (2016). *DeepMind AI reduces Google data centre cooling bill by 40%*. Google DeepMind. Retrieved May 21, 2026, <https://deepmind.google/discover/blog/deepmind-ai-reduces-google-data-centre-cooling-bill-by-40/>
2. Microsoft. (2024). *AI for Earth*. Microsoft. Retrieved May 21, 2026, <https://www.microsoft.com/en-us/ai/ai-for-earth>
3. Google Health. (2026). *Google Health*. Retrieved May 21, 2026, from <https://health.google/>
4. McKinney, S.M., Sieniek, M., Godbole, V. *et al.* International evaluation of an AI system for breast cancer screening. *Nature* 577, 89–94 (2020). <https://doi.org/10.1038/s41586-019-1799-6>
5. UNESCO. (2021). *AI and education: Guidance for policy-makers*. UNESCO. Retrieved May 21, 2026, from <https://unesdoc.unesco.org/ark:/48223/pf0000376709>

Петренко Л.М.,
к.е.н., доцент,

Дем'янчук К.Ю.,
здобувачка першого (бакалаврського) рівня вищої освіти,
Київський національний економічний
університет імені Вадима Гетьмана

АІ ТА КІБЕРБЕЗПЕКА: НОВІ ЗАГРОЗИ І РІШЕННЯ

У сучасному цифровому світі кібербезпека стала ключовим елементом функціонування держав, бізнесу та суспільства. Стрімкий розвиток штучного інтелекту (АІ) суттєво змінив цю сферу, зробивши її більш складною, динамічною та вразливою до нових типів атак. Сьогодні АІ одночасно виступає як потужний інструмент захисту і як нова зброя кіберзлочинців, що формує принципово нові виклики та підходи до безпеки.

Штучний інтелект значно підвищив ефективність кіберзахисту. Він аналізує великі обсяги даних у реальному часі, виявляє аномалії у поведінці користувачів і систем та дозволяє знаходити навіть невідомі типи атак, які складно виявити традиційними методами. Завдяки цьому кібербезпека переходить від реактивної моделі до проактивної, коли загрози не лише фіксуються, а й прогнозуються ще до моменту атаки. Це дозволяє суттєво зменшити час реагування та мінімізувати наслідки інцидентів. Додатково АІ використовується для автоматизації реагування, що дає змогу блокувати підозрілу активність, ізолювати заражені системи та запускати механізми відновлення без участі людини, що особливо важливо для великих інфраструктур [1].

Водночас розвиток АІ суттєво вплинув і на кіберзлочинність, зробивши атаки більш доступними та складними. Тепер навіть користувачі без глибоких технічних знань можуть

використовувати AI-інструменти для створення атак. Однією з найпоширеніших загроз став гіперперсоналізований фішинг, коли повідомлення формуються на основі аналізу соціальних мереж, поведінки та цифрового сліду жертви. Такі атаки виглядають максимально реалістично і часто не викликають підозри [2].

Окрему небезпеку становить використання AI для автоматичного створення шкідливого програмного забезпечення та масового сканування систем на вразливості. Це значно підвищує швидкість атак і дозволяє масштабувати їх на тисячі цілей одночасно. Додатково технології *deepfake* відкривають новий рівень шахрайства, дозволяючи підробляти голос, відео та зображення. У результаті зловмисники можуть видавати себе за керівників компаній або офіційних осіб, що створює серйозні ризики для бізнесу, державних структур [1].

Наступним важливим етапом розвитку став *agentic AI* — автономні системи штучного інтелекту, які можуть не лише аналізувати інформацію, а й самостійно виконувати дії, взаємодіяти з цифровими сервісами та приймати рішення. Такі системи можуть працювати з API, файлами, базами даних і зовнішніми платформами, що значно розширює їхні можливості, але одночасно створює принципово новий рівень загроз. Головною проблемою *agentic AI* є його автономність та складність контролю. Такі системи можуть діяти непередбачувано, особливо у складних або нестандартних сценаріях. Однією з ключових загроз є *prompt-injection*, коли зловмисники через спеціально сформовані запити змушують систему виконувати небажані або небезпечні дії. Це особливо критично, оскільки агентні системи взаємодіють із зовнішніми джерелами інформації і можуть обробляти потенційно шкідливі інструкції [3].

Ще однією серйозною проблемою є «отруєння пам'яті», коли в систему вводяться неправдиві або шкідливі дані, які впливають на її майбутні рішення. Оскільки *agentic AI* може зберігати контекст і використовувати його в подальшій роботі, такі атаки можуть мати довготривалий і накопичувальний ефект. Також важливою загрозою є розширення поверхні атаки, адже агентні системи взаємодіють із великою кількістю сервісів, що створює додаткові точки входу для зловмисників і ускладнює контроль безпеки [3].

Окремо слід зазначити, що AI-системи самі стають об'єктами атак. Це включає підміну навчальних даних (*data poisoning*), обман моделей через спеціально сформовані вхідні дані (*adversarial attacks*), а також спроби крадіжки або копіювання моделей. У результаті система може неправильно класифікувати загрози, ігнорувати реальні атаки або створювати хибні спрацювання. На глобальному рівні розвиток AI суттєво змінює баланс сил у кіберпросторі. Він не лише підвищує ефективність атак, але й робить їх більш автономними та масштабованими. Це збільшує ризик кіберконфліктів між державами та ускладнює визначення джерела атак. Водночас економічні втрати від кіберзлочинності постійно зростають і можуть досягати трильйонів доларів у найближчі роки, що робить цю проблему не лише технічною, а й економічною та політичною.

У відповідь на ці виклики формується новий підхід до кібербезпеки. Одним із ключових принципів є концепція *Zero Trust* (нульова довіра), яка передбачає, що жодна система, користувач або процес не вважаються безпечними за замовчуванням. Кожна дія повинна перевірятися, а доступи мають бути строго обмежені відповідно до мінімально необхідних прав. Також важливими є моніторинг поведінки AI-систем, обмеження їхніх повноважень і впровадження багаторівневих механізмів захисту. Окреме значення має людський фактор. Попри високий рівень автоматизації, саме людина залишається ключовою ланкою у прийнятті рішень. Найбільш ефективною моделлю стає поєднання штучного інтелекту та людського контролю, де AI забезпечує швидкість і аналітику, а людина — контекст, відповідальність і стратегічне мислення.

Отже, штучний інтелект кардинально змінює сферу кібербезпеки. Він робить захист швидшим, точнішим і більш проактивним, але водночас створює нові складні загрози, які раніше не існували. Особливо *agentic AI* відкриває новий рівень ризиків через свою автономність, здатність взаємодіяти з системами та приймати рішення. Майбутнє

кібербезпеки на пряму залежить від здатності поєднати технологічні можливості AI з жорстким контролем, безпековими принципами та відповідальністю людини.

Список використаних джерел

1. Eska. (n.d.). *AI у кібербезпеці: нові можливості чи загроза*. Retrieved May 21, 2026, from <https://eska.global/blog/ai-u-kiberbezpeci-novi-mozhливosti-chi-zagroza>
2. GoIT Global. (n.d.). *AI та кібербезпека: нові виклики для світу*. Retrieved May 21, 2026, from <https://goit.global/ua/articles/ai-ta-kiberbezpeka-novi-vyklyky-dlia-svitu/>
3. Stellar Cyber. (n.d.). *Agentic AI security threats*. Retrieved May 21, 2026, from <https://stellarcyber.ai/uk/learn/agentic-ai-security-threats/>

Петренко Л.М.,
к.е.н., доцент,

Дзьобан В.Б.,
здобувачка першого (бакалаврського) рівня вищої освіти,
Київський національний економічний
університет імені Вадима Гетьмана

ЕМОЦІЙНИЙ ІНТЕЛЕКТ У ВЗАЄМОДІЇ З ЧАТ-БОТАМИ ТА AI-СИСТЕМАМИ

В останні роки емоційний інтелект здобув значну популярність як на інституційному, так і на індивідуальному рівні, демонструючи свій потужний вплив на задоволення життям, розвиток кар'єри, соціальні взаємини, а також на дружбу і залученість до професійної діяльності [1].

Емоційний інтелект виступає важливим фактором підвищення рівня життєстійкості, стресостійкості та здатності до адаптації. Дані аспекти є основою для здорового розвитку особистості на кожному етапі її становлення. Водночас для гармонійної взаємодії з іншими людьми важливий контроль власних імпульсів поривання згідно із наявними соціальними нормами, уміння стабілізувати власний стан за мінливих зовнішніх обставин і на будь-якому рівні на необхідний для виконання поставленого завдання настрій в академічному, робочому чи повсякденному житті. Дані фактори, у свою чергу, значною мірою визначають ефективність роботи та цілеспрямованість працівників [4].

З іншого боку, штучний інтелект демонструє значно вищу ефективність як у цифровому, так і в фізичному бізнес-середовищі. Штучний інтелект не тільки сприяє автоматизації рутинних завдань, що приносить економічну вигоду, але й значно покращує досвід роботи співробітників, де окрім цього, використання чат-ботів у сфері послуг демонструє суттєве підвищення їх якості. У дослідженні К. Оладімеджі та ін. розглянуто вплив штучного інтелекту на укріплення психічного здоров'я. Науковці констатували позитивний вплив нейронної мережі на етапах виявлення, діагностика та лікування психічного розладу. Однак, є гіпотеза, що використання штучного інтелекту у психологічних дослідженнях можна зв'язати з технологіями нейронної мережі та перетворення взаємозалежності із «людина – людина» до «людина – машина» [2].

Необхідно відзначити, що в галузі дослідження інтелекту відбувається зсув з вивчення раціональних до емоційних аспектів. Якщо в XX столітті основним предметом вивчення був переважно абстрактний інтелект, то в XXI столітті дослідники все більше відзначають множинність його вияву. У науковий обіг вводяться такі поняття, як-от: «емоційний інтелект» та «соціальний інтелект». У галузі штучного інтелекту відбуваються подібні зміни: якщо раніше вчені зосереджували свою увагу на його раціональному вияві, то сьогодні дослідники все більше прагнуть до «олюднення» штучного інтелекту, його максимального наближення до інтелекту людини, що й сприяло введенню в науковий обіг поняття «емоційний штучний інтелект» [3].

Учені передбачають новий сплеск інтересу в галузі штучного інтелекту та розмірковують над проблемою нової емоційно-інтелектуальної епохи штучного інтелекту. Наукова фантастика також досить часто презентує майбутні технології штучного інтелекту як систему з наявними