Перспективи подальших досліджень полягають у вивченні ефективності чинних компенсаційних процедур, удосконаленні правового регулювання примусового відчуження майна та розробленні дієвих механізмів відновлення майнових прав осіб, які постраждали внаслідок збройної агресії. Реалізація цих напрямів сприятиме посиленню гарантій права власності та формуванню послідовної й ефективної правової політики України.

**СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:**

1. Комарницька І. І. Право власності та його захист в умовах воєнного стану. *Юридичний науковий електронний журнал*. 2024. № 11. С. 119–121. DOI: https://doi.org/10.32782/

2. Кучер В. О. Право власності в умовах воєнного стану. *Науковий вісник Ужгородського національного університету. Серія: Право*. 2025. Вип. 90, ч. 2. С. 112–117. DOI: https://doi.org/10.24144/2307-3322.2025.90.2.15.

3. Конституція України : Закон України від 28 червня 1996 р. № 254к/96-ВР. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text (дата звернення: 13.10.2026).

4. Цивільний кодекс України : Закон України від 16 січня 2003 р. № 435-IV. URL: https://zakon.rada.gov.ua/laws/show/435-15#Text (дата звернення: 13.10.2026).

**5.** Про компенсацію за пошкодження та знищення окремих категорій об’єктів нерухомого майна внаслідок бойових дій, терористичних актів, диверсій, спричинених збройною агресією Російської Федерації проти України, та Державний реєстр майна, пошкодженого та знищеного внаслідок бойових дій, терористичних актів, диверсій, спричинених збройною агресією Російської Федерації проти України : Закон України від 23 лютого 2023 р. № 2923-IX. URL: https://zakon.rada.gov.ua/laws/show/2923-20#Text (дата звернення: 13.10.2026).

**Настаси В.., здобувач**
**Науковий керівник: Ситніченко О.М.,**
**к.ю.н., доцент, доцент кафедри правового забезпечення безпеки бізнесу,**
**Державний торговельно-економічний університет**
**ORCID:** https://orcid.org/0000-0002-9740-0216

## ШТУЧНИЙ ІНТЕЛЕКТ У КІБЕРБЕЗПЕЦІ: ПРАВОВІ РАМКИ АВТОНОМНИХ СИСТЕМ ПРИЙНЯТТЯ РІШЕНЬ

Сучасні кібератаки відбуваються практично миттєво завдяки автоматизації дій зловмисників. Через це люди вже не встигають ефективно захищати цифрову інфраструктуру традиційними методами, що вимагає впровадження ШІ-систем для швидкого виявлення та зупинки загроз. Однак надати ШІ повну автономію у прийнятті рішень означає зіткнутися з низкою невирішених правових питань [2].

Завдання ШІ в кіберзахисті варіюються від моніторингу даних до реального придушення загроз. Водночас постає гостре питання: як кваліфікувати відповідальність, якщо автономна система хибно заблокує безпечні запити чи завдасть шкоди інфраструктурі? Сучасне законодавство України та світу розраховане лише на людську суб’єктність, тому будь-які рішення, прийняті алгоритмом без втручання людини, наразі залишаються поза чітким правовим полюсом[3].

Згідно з принципами судочинства, будь-яке рішення, що обмежує права чи завдає збитків, має бути обґрунтованим і підлягати оскарженню. Однак більшість складних моделей глибокого навчання працюють за принципом «чорної скриньки», коли їхня внутрішня логіка є закритою навіть для розробників.Через це виникає складнощі з процесуальним використанням системних логів та рішень ШІ як цифрових доказів у суді - як під час розслідування кіберінцидентів, так і при оскарженні помилкових дій системи.

Сьогодні ні в науці, ні на практиці немає єдиної думки щодо того, хто повинен відшкодовувати шкоду, якщо ШІ спрацює помилково (наприклад, через хибне реагування випадково зупинить роботу важливого підприємства)[4]. Досліджуючи проблеми цивільно-правової відповідальності у сфері ІТ, український правознавець Роман Майданик зазначає, що

при експлуатації автоматизованих систем необхідно чітко розмежовувати відповідальність розробника -– за дефекти програмного продукту та алгоритмічні помилки, і володільця чи оператора системи - за неналежне використання, порушення правил експлуатації або відсутність необхідного контролю [1]. Загалом у цьому ланцюжку можна виділити трьох потенційних відповідальних:

- розробників алгоритму - якщо помилку закладено в самому коді чи моделі навчання;
- постачальників даних - якщо для тренування ШІ використали неякісні чи викривлені вибірки;
- власників або операторів системи - якщо вони недостатньо контролювали роботу ШІ або порушили правила його експлуатації [5]. Саме тому зараз вкрай важливо на законодавчому рівні чітко розмежувати ризики та відповідальність між тими, хто створює такі програми, і тими, хто використовує їх на практиці [3].

За кордоном нормативна база для штучного інтелекту вже активно формується. Яскравим прикладом є Європейський Союз, який ухвалив Регламент про ШІ (EU AI Act), заснувавши його на ризико-орієнтованому підході [6].За європейськими стандартами, системи ШІ, що керують критичною інфраструктурою (енергетикою, транспортом чи цифровими мережами), вважаються технологіями високого ризику [6,7]. До них висувають суворі вимоги:

- розробка систем оцінки та мінімізації ризиків разом із високою кіберстійкістю;
- детальне й обов'язкове ведення технічної документації;
- постійна присутність людини в процесі прийняття рішень.

Україна наразі перебуває на етапі імплементації нормативних вимог. Гармонізація українських норм із європейськими має відбуватися з урахуванням умов воєнного стану, де ключовим критерієм для систем захисту є поєднання надійності та критичної швидкості прийняття рішень [7].

Виходячи з вище викладеного можна сказати, що впровадження штучного інтелекту в систему кіберзахисту є необхідним кроком для забезпечення національної безпеки, однак правове поле відстає від темпів технологічного розвитку. Для розв'язання окреслених проблем пропонується: Закріпити на законодавчому рівні поняття «автономної системи прийняття рішень» у сфері кібербезпеки.

Отже, необхідно встановити обов'язкові вимоги до прозорості та роз'яснення алгоритмів, що захищають критичну інфраструктуру. Нормативно визначити модель розподілу юридичної відповідальності між розробником, інтегратором та власником системи кіберзахисту.

**СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:**

1. Майданик Р. А. Цивільно-правова відповідальність за шкоду, завдану функціонуванням систем штучного інтелекту. Право України. 2021. № 4. С. 45–62.

2.Баранов О. А. Інтернет речей, штучний інтелект та робототехніка: правові виклики сьогодення. Правова інформатика. 2021. № 1 (69). С. 15–28.

3.Коваленко В. М. Юридична відповідальність за шкоду, завдану автономними системами штучного інтелекту. Часопис Київського університету права. 2023. № 2. С. 44–50.

4.Taddeo M., Floridi L. Regulating digital technologies is essential to protect public trust. Nature Machine Intelligence. 2022. Vol. 4. P. 821–823.

5.Петрів О. Р. Проблема «чорної скриньки» штучного інтелекту в контексті захисту прав людини. Інформація і право. 2022. № 3 (42). С. 108–115.

6.Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Official Journal of the European Union. L 2024/1689, 12.7.2024.

7.Концепція розвитку штучного інтелекту в Україні: розпорядження Кабінету Міністрів України від 02.12.2020 р. № 1556-р. Урядовий кур'єр. 2020. № 241.