НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
«ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»

Кафедра цивільного права

ІТ-ПРАВО ТА КІБЕРБЕЗПЕКА В УМОВАХ ГІБРИДНОЇ ВІЙНИ

МАТЕРІАЛИ
Всеукраїнського круглого столу

Одеса,
12 квітня 2025 року

Одеса
Фенікс
2025

УДК 342.95 : 343.32 (477): 351.863
І-52

За загальною редакцією
доктора юридичних наук, професора **Є. Харитонова**,
кандидатки юридичних наук, доцентки **Ю. Кривенко**.

Упорядники-укладачі:
Кривенко Юлія – к.ю.н., доцентка кафедри цивільного права Національного університету «Одеська юридична академія», доцентка;
Лешкова Єлизавета – лаборантка кафедри цивільного права Національного університету «Одеська юридична академія».

ІТ-право та кібербезпека в умовах гібридної війни : матеріали Всеукр. круглого столу (м. Одеса, 12 квіт. 2025 р.) / за заг. ред.: Є. О. Харитонова, Ю. Кривенко ; кафедра цив. права НУ «Одес. юрид. академія». – Одеса : Фенікс, 2025. – 138 с. – Режим доступу: ….

І-52

ISBN 978-617-8430-57-3

Збірник містить матеріали доповідей з теоретичних, історичних і методологічних проблем ІТ-права та кібербезпеки, які були оприлюднені на Всеукраїнському круглому столі «ІТ-право та кібербезпека в умовах гібридної війни» 12 квітня 2025 у Національному університеті «Одеська юридична академія».

Збірник спрямований на ознайомлення громадськості з дослідженнями науковців у сфері ІТ-права та кібербезпеки і може бути корисний як у навчальному процесі, так і в практичній діяльності.

УДК 342.95 : 343.32 (477): 351.863

ISBN 978-617-8430-57-3

8. Брижко В.М. Сучасні основи захисту персональних даних в правових актах. Інформація і право. 2016. № 3 (18). С. 45–57.

9. Зеркаль О.В. Деякі питання захисту персональних даних. Бюлетень Міністерства юстиції України. 2012. № 1 (123). С. 5–14.

10. Кондратенко Н.М. Щодо правового регулювання захисту персональних даних. Держава та регіони. Право. 2012. № 3 (37). С. 62–66.

11. Похиленко І. Правове регулювання захисту персональних даних. Scientific works of National Aviation University. Series: Law Journal «Air and Space Law». 2023. Т. 4, № 69. С. 94–99. URL: https://doi.org/10.18372/2307–9061.69.18322

Рогожа Валерія Василівна,
студентка 2-го курсу факультету прокуратури та слідства (кримінальна юстиція) Національного університету «Одеська юридична академія».
Науковий керівник: к.ю.н., доц., проф. кафедри цивільного права
Калітенко О.М.

РОЛЬ ШТУЧНОГО ІНТЕЛЕКТУ В КІБЕРБЕЗПЕЦІ: ЗАХИСТ ЧИ ЗАГРОЗА?

Інтеграція штучного інтелекту в системи кібербезпеки відкриває нові можливості для ефективного захисту даних та інформаційних інфраструктур у сучасному цифровому світі, де кіберзагрози стають дедалі складнішими та більш витонченими. З огляду на зростаючу складність і динамічність кіберзагроз, традиційні методи захисту виявляються недостатньо ефективними, що зумовлює необхідність пошуку нових підходів.

Штучний інтелект (ШІ) має потенціал значно підвищити ефективність систем кібербезпеки, забезпечуючи автоматизацію процесів виявлення загроз, аналіз аномалій, прогнозування можливих атак та адаптацію захисних механізмів у режимі реального часу. Це стає можливим завдяки здатності ШІ обробляти великі масиви даних, виявляти складні закономірності та взаємозв'язки, які можуть залишитися непомітними для людини. Проте, інтеграція ШІ в кібербезпеку супроводжується низкою викликів. Основними проблемами є забезпечення точності та надійності роботи ШІ, оскільки помилкові спрацьовування можуть призвести до збоїв у системі захисту або навіть спричинити помилкове блокування ле-

гітимної активності. Крім того, алгоритми ШІ можуть стати об'єктом атак, що вимагає розробки заходів захисту самих алгоритмів від маніпуляцій та втручання. Існує також питання етичності та прозорості прийняття рішень штучним інтелектом у контексті конфіденційності даних та потенційних обмежень доступу до критично важливої інформації.

У наукових працях зазначається, що методи і стратегії кібербезпеки на основі ШІ можуть забезпечити надійніший захист від сучасних загроз. Дослідження, що фокусуються на огляді цих методів, зокрема аналізують, як ШІ допомагає виявляти нові види атак і адаптуватися до швидко змінюваного кіберсередовища [1, 2]. Наприклад, розглядаються системи, що використовують штучний інтелект для аналізу поведінкових аномалій, що дозволяє виявляти кіберзлочини на ранніх етапах.

Інший напрямок досліджень фокусується на питаннях забезпечення кібербезпеки в самих системах штучного інтелекту, зокрема на аналізі їхніх вразливостей і контрзаходів, необхідних для протидії цим уразливостям. У цих публікаціях підкреслюється, що кібербезпека систем, які використовують ШІ, потребує унікального підходу, оскільки вони схильні до атак типу «отруєння даних» та інших маніпуляцій, що можуть змінити результати моделі [3]. Зокрема, аналізуються типи атак і заходи для їхнього попередження, що мають критичне значення у безпеці автоматизованих систем [4].

Інноваційні рішення для бізнесу, особливо в електронному комерційному середовищі, також активно обговорюються в публікаціях. Дослідники підкреслюють, що використання ШІ у бізнесових структурах є одночасно перспективним і ризикованим, оскільки тут необхідно не лише враховувати технічні аспекти, але й забезпечувати постійний моніторинг та оперативне реагування на нові види загроз [5]. Етичні аспекти застосування штучного інтелекту в кібербезпеці стають дедалі важливішими, оскільки використання автоматизованих систем для захисту інформації та даних впливає на базові права користувачів і піднімає складні питання відповідальності та прозорості. Одним із ключових етичних викликів є

забезпечення конфіденційності даних. Алгоритми ШІ обробляють великі обсяги інформації, включаючи персональні та конфіденційні дані, що створює ризики несанкціонованого доступу або неналежного використання цих даних. Водночас організації повинні гарантувати, що інформація зберігається та обробляється відповідно до принципів захисту персональних даних і забезпечення конфіденційності, щоб уникнути порушення прав користувачів.

Прозорість рішень, що приймаються алгоритмами штучного інтелекту, також є важливим аспектом у сфері кібербезпеки. У більшості випадків алгоритми, зокрема алгоритми глибинного навчання, функціонують як «чорні ящики», що ускладнює розуміння процесу прийняття рішень та причини конкретних дій системи. Це може викликати сумніви щодо об'єктивності та справедливості рішень, особливо коли йдеться про автоматичне блокування доступу до даних або виявлення підозрілої поведінки. Прозорість рішень важлива не тільки для довіри користувачів, але й для забезпечення підзвітності.

Організації повинні мати можливість пояснити, чому алгоритм прийняв певне рішення, особливо якщо це стосується дій, що мають серйозні наслідки для безпеки чи приватності.

Адаптивні можливості систем кібербезпеки на базі штучного інтелекту вже демонструють високу ефективність у різних галузях, таких як банківський сектор, корпоративні мережі та хмарні платформи. Наприклад, у банківському секторі використовується автоматичне налаштування ШІ для виявлення підозрілих транзакцій у реальному часі. Якщо система виявляє аномалії у поведінці користувача, такі як спроба входу з незвичних геолокацій або нетипові суми переказів, вона автоматично блокує операцію та сповіщає клієнта. Це значно підвищує рівень безпеки та запобігає потенційному шахрайству.

Ще одним практичним прикладом є застосування ШІ в електронній пошті для захисту від фішингових атак. Система аналізує нові вхідні повідомлення, порівнюючи їхній стиль та вміст із відомими фішинговими шаблонами, і адаптується до нових методів

обману, які зловмисники використовують для обходу традиційних захисних фільтрів. Коли з'являються нові методи фішингу, система самостійно оновлює свої алгоритми для точнішого розпізнавання загроз, що мінімізує ризик несанкціонованого доступу через електронну пошту.

Крім того, для підтримання гнучкості кіберсистем доцільно запровадити комплексний план навчання персоналу, що включає не тільки технічні знання, але й етичні принципи роботи з ШІ та кібербезпекою. Це дозволяє співробітникам діяти відповідно до стандартів та знижує ймовірність помилок при експлуатації ШІ-систем. Подібні навчальні програми мають бути постійно актуалізованими з урахуванням нових загроз і тенденцій у сфері кібербезпеки.

Ці практичні рекомендації, що включають управління доступом до даних, розвиток міждисциплінарної співпраці, регулярні аудити алгоритмів та навчання персоналу, формують основу для ефективного і відповідального використання штучного інтелекту в кібербезпеці.

На основі проведеного дослідження встановлено, що інтеграція тучного інтелекту в системи кібербезпеки має значний потенціал для підвищення рівня захисту інформаційних інфраструктур завдяки здатності ШІ-алгоритмів виявляти нові загрози, аналізувати аномалії та прогнозувати потенційні атаки. Основними проблемами при впровадженні ШІ в кібербезпеку є забезпечення точності алгоритмів та їхньої стійкості до зовнішніх втручань, а також етичні виклики, пов'язані з конфіденційністю даних і прозорістю рішень.

Суттєвою перешкодою залишається потреба у висококваліфікованих кадрах і значні фінансові витрати на впровадження та підтримку ШІ-систем.

ЛІТЕРАТУРА:

1. Лунгол О. Огляд методів та стратегій кібербезпеки засобами штучного інтелекту. «Кібербезпека: освіта, наука, техніка». 2024. № 1.25. С. 379–389. DOI: https://doi.org/10.28925/2663–4023.2024.25.379389

2. Онищенко Ю., Каланча А., Гельдт С. Застосування штучного інтелекту у сфері кібербезпеки. Trends, theories and ways of improving science:

The 8th International scientific and practical conference Madrid, Spain: International Science Group. 2023. С. 544. URL: http://surl.li/urooxa

3. Неретін О., Харченко В. Забезпечення кібербезпеки систем штучного інтелекту: аналіз вразливостей, атак і контрзаходів. *Information Systems And Networks.* 2022. № 12. С. 7–20.

4. Черевко К. О. Штучний інтелект як інструмент протидії злочинності. *Вісник Кримінологічної асоціації України*. 2023. № 28.1. С. 124–133.

5. Шкоденко Т. Роль штучного інтелекту в сучасних стратегіях кібербезпеки: аналіз потенційних загроз для електронного бізнесу. Grail of Science. 2024. № 37. С. 239–240. URL: https://archive.journal-grail.science/index.php/2710–3056/article/view/2158

Фасій Анастасія Володимирівна,
студентка 2-го курсу факультету цивільної та господарської юстиції
Національного університету «Одеська юридична академія».
Науковий керівник: к.ю.н., доц., доц. кафедри цивільного права
Завальнюк С. В.

ДО ПИТАННЯ ПРО ПРАВОВЕ РЕГУЛЮВАННЯ РЕКЛАМИ В СОЦІАЛЬНИХ МЕРЕЖАХ

Розвиток цифрових технологій став ключовим фактором інформаційної революції, що призвела до формування глобального інформаційного середовища. Онлайн-простір став універсальним засобом обміну даними, що відкриває нові можливості для реклами.

Новий рівень громадянського суспільства в інформаційну епоху пов'язаний із появою соцмереж. Соціальні мережі стали платформою для комунікації, обговорення та інтеграції суспільства.[1, с. 20]

На сьогодні популярність інтернет-реклами в соцмережах зростає разом із кількістю користувачів. Серед них більшість – це молодь, яка має найвищу споживчу спроможність. Популярними платформами для розміщення реклами в Україні є Instagram, Facebook, Telegram та інше.

Реклама на платформах соціальних мереж є одним із найбільш результативних методів донесення інформації до споживачів. Од-