УДК 342.951

ФЕДОРЧЕНКО О.С., молодший науковий співробітник Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України
ORCID: https://orcid.org/0009-0007-7358-7753

РОЛЬ ШТУЧНОГО ІНТЕЛЕКТУ У ЗАБЕЗПЕЧЕННІ КІБЕРБЕЗПЕКИ УКРАЇНИ: СУЧАСНИЙ СТАН ТА ПЕРСПЕКТИВИ РОЗВИТКУ

DOI: https://doi.org/10.37750/2616-6798.2025.3(54).340521

Анотація. *Стаття присвячена аналізу ролі штучного інтелекту у сфері забезпечення кібербезпеки. Досліджено основні напрями застосування технологій ШІ для виявлення та запобігання кіберзагроз. Проаналізовано переваги та обмеження цих технологій, а також визначено правові та етичні аспекти їхнього застосування в контексті вітчизняного законодавства. Висвітлено актуальність впровадження ШІ-технологій в умовах посилення кіберзагроз, особливо в умовах воєнного стану на території України. Зроблено висновок щодо необхідності удосконалення нормативно-правової бази з питань використання ШІ у сфері кібербезпеки. Визначено шляхи врегулювання суспільних відносин у сфері розвитку штучного інтелекту на законодавчому рівні.*

Ключові слова: *штучний інтелект, кібербезпека, кіберзагрози, машинне навчання, шпигунське програмне забезпечення, права людини.*

Summary. *The article analyzes the role of artificial intelligence in the field of cybersecurity. The main areas of application of AI technologies for detecting and preventing cyber threats are investigated. The advantages and limitations of these technologies are analyzed, and the legal and ethical aspects of their application in the context of Ukrainian legislation are determined. The author highlights the relevance of introducing AI technologies in the context of increasing cyber threats, especially in the context of martial law in Ukraine. The author concludes that it is necessary to form a legal framework for regulating the use of AI in the field of cybersecurity. Ways to regulate public relations in the field of artificial intelligence development at the legislative level are identified.*

Keywords: *artificial intelligence, cybersecurity, cyber threats, machine learning, spyware, human rights.*

Постановка проблеми.

Сьогодні бурхливий розвиток цифрових технологій супроводжується як новими можливостями для суспільства, так і новими загрозами. Особливе місце серед них займають кіберзагрози, які створюють ризики не тільки для окремих користувачів, а й стратегічних галузей економіки, державного управління та оборони. Сьогодні питома вага кіберзагроз зростає і ця тенденція в міру розвитку інформаційних технологій та їх конвергенції з технологіями штучного інтелекту в найближче десятиліття посилюватиметься. Зростання такого впливу на функціонування структур управління як національних, так і транснаціональних формує нову безпекову ситуацію[1]. В контексті протидії таким загрозам посилюється роль штучного інтелекту (ШІ), який дозволяє: автоматизувати процеси аналізу даних, виявлення аномалій, прогнозування та реагування на кібератаки. При цьому поширюється інструментарій, що передбачає накопичення великих масивів інформації щодо поведінки людини, соціальних груп та використання сучасних досягнень у сфері ШІ [1]. Фахівці з кібербезпеки відзначають,

що у майбутньому роль штучного інтелекту у кібербезпеці стане більш помітною. Очікується, що у 2027 році ринкова вартість ШІ в кібербезпеці досягне 46,3 мільярда доларів США[2]. Сьогодні компанії, що займаються кібербезпекою ШІ, пропонують значні переваги, надаючи організаціям безцінні інструменти для навігації в кібербезпеці [2].

Результати аналізу наукових публікацій. Аналіз сучасних наукових досліджень свідчить про зростання інтересу до використання ШІ у сфері кібербезпеки. Роль ШІ у забезпеченні кібербезпеки досліджували С. Гуржій [3], І. Зоря[4], А. Марущак [4], О. Неретін [5], М. Різченко [6], В. Савченко [7], О. Шаповаленко [7], В. Харченко та ін [5].

Правові аспекти регулювання ШІ в контексті зарубіжного та міжнародного досвіду вивчали О. Жидкова, С. Цяпа [8], М. Леонович [9], І. Смірнов [10], Л. Товкун [9], О. Турута та ін.

У 2025 році надруковано монографію О. Баранова "Штучний інтелект та система права", де викладено загальну концепцію визначення правового статусу робота із штучним інтелектом в контексті визнання його правоздатності, дієздатності та деліктоздатності [11]. Водночас, недосконаліть правового регулювання ШІ, відсутність концептуальних засад державної політики в галузі ШІ в контексті забезпечення кібербезпеки зумовлює актуальність дослідження ролі ШІ у цій сфері.

Метою статті є дослідження ролі штучного інтелекту у забезпеченні кібербезпеки в контексті удосконалення його правового регулювання та оцінки ризиків, пов'язаних з його використанням.

Виклад основного матеріалу.

У Концепції розвитку штучного інтелекту в Україні під штучним інтелектом розуміється організована сукупність інформаційних технологій, із застосуванням якої можливо виконувати складні комплексні завдання шляхом використання системи наукових методів досліджень і алгоритмів обробки інформації, отриманої або самостійно створеної під час роботи, а також створювати та використовувати власні бази знань, моделі прийняття рішень, алгоритми роботи з інформацією та визначати способи досягнення поставлених завдань [12].

Не дивлячись на законодавче визначення поняття "штучний інтелект", у юридичній літературі тривають дискусії навколо цього визначення. Незважаючи на зусилля великої кількості дослідників досі не напрацьовано загально прийнятого визначення поняття або терміну "штучний інтелект". Узагальнивши існуючі визначення ШІ, український вчений О. Баранов пропонує їх поділити на дві основні групи: перша група визначень зводиться до наділення "машин", "машинних систем", "комп'ютерів", "програмних систем", "технологій", "агентів" тощо певними безвідносними властивостями такими як: здатними адаптуватися, досягати мети, робити прогнози, рекомендації чи рішення, що впливають на реальне чи віртуальне середовище, сприймати навколишнє середовище, інтерпретувати зібрані структуровані або неструктурованих дані, приймати найкращі рішення тощо; друга група визначень зводиться до наділення "машин", "машинних систем", "комп'ютерів", "програмних систем", "технологій" [11]. Для подальших термінологічних міркувань цей автор пропонує базовий термін "штучний інтелект" – це система, яка складається із сукупності технологій, методів, способів, засобів та пристроїв, насамперед, комп'ютерних, що імітує (моделює) певну сукупність когнітивних функцій еквівалентних відповідним когнітивним функціям людини [11]. Слід уточнити, що у частині забезпечення кібербезпеки – це програмні засоби, швидкі обчислювальні алгоритми, математичні методи опису складних динамічних систем та

обробки великих даних, обчислювальні ресурси комп'ютерів та суперкомп'ютерів, хмарні технології тощо.

Впровадження інформаційних технологій, частиною яких є технології штучного інтелекту, є невід'ємною складовою забезпечення кібербезпеки. Концепція розвитку штучного інтелекту в Україні проголошує: "Основним завданням у сфері кібербезпеки під час реалізації державної політики розвитку галузі штучного інтелекту є захист комунікаційних, інформаційних та технологічних систем, інформаційних технологій, передусім тих, що використовуються операторами (постачальниками) ключових послуг (включаючи об'єкти критичної інфраструктури) і є важливими для безперервності функціонування держави, суспільства та безпеки громадян" [12].

Штучний інтелект у сфері кібербезпеки використовується для:

виявлення аномалій у мережевому трафіку;

автоматичного аналізу подій у кібепросторі;

захисту від несанкціонованого доступу до інформаційних ресурсів;

аналізу і структуризація інформації про кіберзагрози;

реагування на кіберінциденти в режимі реального часу;

прогнозування кібератак на основі аналізу великих масивів даних;

розробки передових алгоритмів, які допомагають виявляти кібератаки та запобігання їх негативним проявам;

машинного навчання на підставі набутого досвіду;

Розглянемо більш детально окреслені напрямки використання ШІ у сфері кібербезпеки.

Для виявлення аномалій у мережевому трафіку ШІ використовує нейронні мережі для аналізу поведінки в мережі та виявлення шкідливих програм[6]. Ці системи здатні швидко ідентифікувати аномальні дії в мережевому трафіку, які можуть вказувати на спроби вторгнення або зараження системи вірусами. Нейронні мережі допомагають ідентифікувати загрози у великих інформаційних системах і забезпечують реагування в реальному часі [13, с. 3].

Виявлення аномальної поведінки полягає у встановленні ознак, за якими дії користувачів вважаються зловмисними для звичайних систем захисту. У разі коли деякі з цих ознак збігаються, система реєструє вторгнення. У той же момент, штучний інтелект може ідентифікувати параметри, які навіть не враховувалися раніше. Це дозволяє створити більш ефективну предикативну модель[4]. Зокрема, системи ШІ використовуються для створення моделей, які здатні ідентифікувати підозрілу активність у мережі. ШІ може безперервно у режимі 24/7 моніторити мережу та виявляти аномальну поведінку, яка у свою чергу, може свідчити про кіберзагрозу [3, с. 210]. Такий тип моніторингу допомагає виявити аномальну поведінку до того, як вона трансформується у майбутню шкідливу діяльність [3, с.212].

Так, за даними А. Каплінського, ШІ-системи забезпечують високий рівень точності виявлення аномалій у мережевому трафіку, що дозволяє оперативно реагувати на потенційні загрози [14].

ШІ володіє здатністю аналізувати та обробляти великі обсяги даних, а також виявляти та уникати ризики, що пов'язані з кіберзагрозами, завдяки своїм можливостям самонавчання. Алгоритми машинного навчання аналізують величезні обсяги даних, сприяючи виявленню аномалій у мережевому трафіку та ідентифікації потенційно небезпечних вразливостей [6]. Експерти з кібербезпеки стверджують, що чим більше даних ви надаєте, тим більше він навчається, тому штучний інтелект з часом поліпшує

свої можливості прогнозування. Методи машинного навчання відіграють ключову роль у процесах забезпечення кібербезпеки [15, с. 2].

З цього приводу М. Бондаренко зазначає, що машинне навчання дозволяє значно скоротити час на виявлення та усунення вразливостей в інформаційних системах [16]. Використовуючи методи машинного навчання, системи ШІ можуть оперативно аналізувати великі обсяги даних з різноманітних джерел, таких як: месенджери, соціальні мережі, е-публікації, телеграмканали, дарк веб-форуми з метою виявлення загрозливих тенденцій та уразливостей [3, с.209]. ШІ може використовувати дані про попередні кібератаки з метою покращення своїх алгоритмів та забезпечення більш точного виявлення ризиків та загроз у майбутньому. ШІ дозволяє гарантувати ефективний захист від автоматичних або скерованих кібератак[4]. Використання алгоритмів машинного навчання для виявлення атак показує значні досягнення у порівнянні з традиційними підходами, що базуються на правилах [17, с. 11]. Завдяки алгоритмам машинного навчання та нейронним мережам, системи на базі ШІ можуть не лише виявляти вторгнення, але й передбачати потенційні загрози [4].

Однією з основних сфер застосування штучного інтелекту є виявлення несанкціонованого дослідження інформаційного ресурсу. Системи ШІ на базі алгоритмів машинного навчання та лінгвістичних нейромереж широко використовуються для захисту даних у сучасних інструментах [18]. Системи автоматично виявляють зловмисний код або незвичайний інтернет-трафік і реагують на незвичайну поведінку користувачів. Для цього активно використовується шкідливе програмне забезпечення (ШПЗ) [4]. Постійно змінюючись, сигнатури шкідливих програм можуть допомогти зловмисникам обійти статичні засоби захисту, такі як брандмауери та системи виявлення за периметром. Аналогічним способом, шкідливе програмне забезпечення зі ШІ може перебувати усередині системи, збираючи дані та спостерігаючи за поведінкою користувача, доки не буде готове розпочати нову фазу атаки [3, с.212]. Крім того, ШІ може автоматично реагувати на загрози, блокуючи доступ хакерів до систем та запобігати витоку конфіденційних даних. Іншою його перевагою є значне скорочення людського фактору – тобто ШІ не схильний до різних психологічних впливів або втоми. Реагування безпеки на кіберзагрози, автоматизоване за допомогою ШІ вимагає менше часу та знижує ризик людської помилки [3, с.210].

Ідентифікація ризиків має вирішальне значення для прогнозування ШІ в кібербезпеці. ШІ може аналізувати зміни мережі та використовувати ці шаблони для прогнозування на основі історичних даних потенційних векторів кібератак, особливо методів і шляхів, які кіберзловмисники можуть використовувати для доступу до системи або мережі [2].

Як ми бачимо, застосування ШІ має низку переваг, серед яких виділяється: висока швидкість обробки даних; можливість одночасного аналізу великої кількості факторів; автономне реагування на загрози без участі людини; наявність механізмів самонавчання; прогнозування кіберризиків.

Поряд з вражаючими перспективами, які відкриваються з використанням ШІ, багато хто звертає увагу громадськості й на не менш важливі, на їх думку, ризики, пов’язані з розвитком та масштабами використання ШІ. Так, О. Баранов одночасно із перевагами звертає увагу на деякі проблеми та певні загрози ШІ: обмеженість в можливостях адаптації та трансформації технологіями штучного інтелекту своїх можливостей у випадку зміни умов функціонування; труднощі у передбачувані та пояснення поведінки ШІ в умовах недостатності знань про алгоритми їх функціонування; вірогідну дискримінацію та упередженість методів та способів

машинного навчання; чутливість до навмисних чи ненавмисних дій щодо порушення штатного режиму функціонування технологій штучного інтелекту [11].

Найбільш поширеним є підхід, згідно з яким зміст ризиків застосування ШІ зумовлює: високу залежність від якості тренувальних даних; маніпуляції, інші злочинні дії з боку хакерів (adversarial attacks); проблеми з поясненням рішень ШІ (black box problem); порушення права на конфіденційність та захист персональних даних; етичні питання, пов'язані з автономними системами.

Таку позицію відстоює І. Лукіна (2024), яка справедливо вважає, що використання ШІ в кібербезпеці має певні обмеження, які стосуються, зокрема, проблем з прозорістю алгоритмів, етичних питань та порушень прав на конфіденційність [19].

Одним із головних викликів є те, що системи ШІ самі можуть стати мішенню кібератак. Наприклад, змагальні атаки на алгоритми машинного навчання, спрямовані на модифікацію вхідних даних, щоб викликати помилки в їх роботі [20, с. 23]. Зловмисники можуть навмисно маніпулювати або підміняти ці дані, що призводить до небажаних результатів. Такі атаки становлять серйозну проблему для впровадження машинного навчання в критично важливі системи [17, с. 13].

Ще одним із викликів у сфері кібербезпеки є змагальний характер розвитку засобів кібербезпеки в умовах швидких прогресуючих змін інформаційно-комунікаційних технологій, зокрема хмарних та квантових обчислень, 5G-мереж, великих даних, Інтернету речей, штучного інтелекту тощо [1].

Серед першочергових проблем розвитку ШІ в Україні обґрунтовано відносять: низький рівень цифрової грамотності, поінформованості населення щодо загальних аспектів, можливостей, ризиків та безпеки використання штучного інтелекту; відсутність або недосконаліть правового регулювання штучного інтелекту (в тому числі у сферах освіти, економіки, публічного управління, кібербезпеки, оборони), а також недосконаліть законодавства про захист персональних даних; низький рівень інвестицій у розроблення технологій штучного інтелекту; низький рівень впровадження та реалізації суб'єктами господарювання інноваційних проектів з використанням технологій штучного інтелекту порівняно із провідними країнами світу, що призводить до зниження продуктивності праці і появи великого відсотка робочих місць, які необхідно автоматизувати; недостатній рівень якості вищої освіти та освітніх програм, спрямованих на підготовку спеціалістів у галузі штучного інтелекту в закладах вищої освіти; відсутність сучасних програм підвищення кваліфікації для викладачів закладів вищої освіти у галузі штучного інтелекту; низький рівень інвестицій у проведення досліджень із штучного інтелекту у закладах вищої освіти; відсутність грантового фінансування наукової діяльності у галузі штучного інтелекту; недостатній рівень інформаційної безпеки та захисту даних в інформаційно-телекомунікаційних системах державних органів внаслідок застарілості автоматичних систем виявлення та оцінки інформаційних загроз, невикористання потенціалу прогнозування та передбачення загроз з метою своєчасної підготовки системи до можливої атаки; зростання кількості спроб несанкціонованого втручання в роботу автоматизованих системи, комп'ютерних мереж; недосконаліть механізмів прийняття управлінських рішень у публічній сфері, забюрократизованість системи надання адміністративних послуг; обмеженість доступу до інформації та її низька якість; недостатній рівень впровадження електронного документообігу між державними органами, а також низький ступінь оцифрованості даних, що перебувають у власності державних органів; складність перевірки відповідності роботи систем штучного інтелекту законодавству та існуючим етичним принципам; відсутність єдиних підходів, що застосовуються при визначенні критеріїв

етичності під час розроблення та використання технологій штучного інтелекту для різних галузей, видів діяльності та сфер національної економіки; наявність ризиків зростання рівня безробіття у зв'язку з використанням технологій штучного інтелекту; відсутність застосування технологій штучного інтелекту в судовій практиці[12].

Наведене свідчить про необхідність розроблення єдиної скоординованої державної політики, невід'ємною складовою якої є нормативно-права база регулювання ШІ. Сьогодні ця база перебуває на стадії формування. Серед ключових нормативних актів, які формують правове поле використання ШІ, виділяються, зокрема, закони України "Про захист персональних даних", "Про авторське право і суміжні права" та Рамкова конвенція РЄ зі штучного інтелекту, прав людини, демократії та верховенства права.

Ще 2 грудня 2020 р. Кабінетом Міністрів України схвалено Концепцію розвитку штучного інтелекту в Україні, метою якої є визначення пріоритетних напрямів і основних завдань розвитку технологій штучного інтелекту для задоволення прав та законних інтересів фізичних та юридичних осіб, побудови конкурентоспроможної національної економіки, вдосконалення системи публічного управління [12].

Ця Концепція проголошує, що: "комплексне розв'язання проблем кібербезпеки вимагає виконання таких завдань: удосконалення законодавства і створення сучасної нормативно-правової бази для впровадження кращих світових практик штучного інтелекту у сфері кібербезпеки і кіберзахисту; розроблення інноваційних систем кібербезпеки, які широко застосовують технології штучного інтелекту для автоматичного аналізу та класифікації загроз і автоматичного вибору стратегії їх стримування і запобігання; вивчення питання ліцензування іноземних розробок штучного інтелекту у сфері кібербезпеки, особливо у державному секторі; створення національних інформаційних систем, платформ і продуктів з метою зменшення частки іноземного програмного забезпечення у сфері кібербезпеки, що використовується органами державного управління; оновлення державних стандартів щодо інформаційної безпеки, зокрема державних інформаційних ресурсів, а також розроблення нових національних стандартів у сфері кібербезпеки і кіберзахисту, зокрема організаційних і технічних вимог, що стосуються безпеки додатків, мобільних пристроїв, робочих станцій, серверів і мереж, моделей хмарних обчислень" [12].

9 травня 2025 р. Кабінет Міністрів України затвердив план заходів з реалізації Концепції розвитку штучного інтелекту в Україні на 2025-2026 роки [21]. Більшість положень цього плану присвячено питанням забезпечення кібербезпеки. Зокрема, цим Планом передбачено: розроблення та подання Кабінетові Міністрів України законопроекту щодо правового врегулювання у сфері розвитку штучного інтелекту (п. 1 - IV квартал 2026 року); проведення оцінки стану захищеності інформаційно-комунікаційних систем, які використовують штучний інтелект для виявлення та протидії кіберзагрозам (п. 3 щорічно); розроблення рекомендацій з кібербезпеки, які передбачатимуть пропозиції з використання технологій штучного інтелекту, зокрема щодо захисту моделей машинного навчання від несанкціонованого втручання в роботу (п 2. IV квартал 2025 року) [21].

Україна, яка є членом Спеціального комітету із штучного інтелекту при Раді Європи, у жовтні 2019 року приєдналася до Рекомендацій Організації економічного співробітництва і розвитку з питань штучного інтелекту (Organisation for Economic Co-operation and Development, Recommendation of the Council on Artificial Intelligence, OECD).

З 1 серпня 2024 році в Європейському Союзі почав діяти закон, який регулює правила у сфері штучного інтелекту. Цей Закон спрямований на створення

гармонізованого ринку штучного інтелекту в ЄС, стимулювання впровадження цієї технології та створення сприятливих умов для інновацій та інвестицій. Згідно з цим законом, системи на базі штучного інтелекту, такі як чат-боти, повинні чітко інформувати користувачів про взаємодію з машиною. Системи ШІ, які будуть визначені як такі, що мають високий ризик, повинні відповідати суворим вимогам, вести реєстрацію активності, надавати чітку інформацію для користувачів та дотримуватися кібербезпеки [22].

За цим законом країни-члени ЄС зобов'язані до 2 серпня 2025 року визначити національні компетентні органи, які здійснюватимуть нагляд за дотриманням правил для систем на основі штучного інтелекту та наглядатимуть за ринком[22].

Очікується, що для формування високоякісних наборів даних в ЄС буде створено Європейські спільні простори даних для обміну даними між підприємствами та урядом. Наприклад, Європейський простір даних про охорону здоров'я сприятиме недискримінаційному доступу до даних про охорону здоров'я та навчанню алгоритмів штучного інтелекту на цих наборах даних у безпечний, своєчасний, прозорий та надійний спосіб, із збереженням конфіденційності та з відповідним інституційним управлінням [23, с.50].

Висновки. Правові та організаційні аспекти ШІ набувають особливого значення в контексті забезпечення кібербезпеки. Використання технологій ШІ з дотриманням етичних стандартів повинне сприяти захисту комунікаційних, інформаційних та технологічних систем, інформаційних технологій, а також зменшенню обсягу витрат, підвищенню ефективності кіберебезпеки.

Вважаємо за доцільне прискорити розроблення законопроекту щодо правового врегулювання у сфері розвитку штучного інтелекту. В рамках цього законопроекту важливим є визначення компетентних органів, відповідальних за дотримання правил для систем на основі штучного інтелекту, а також відповідальності за порушення таких правил.

В контексті правового регулювання ШІ слід забезпечити: захист прав та свобод учасників відносин у галузі штучного інтелекту; розроблення Етичного кодексу штучного інтелекту за участю широкого кола заінтересованих сторін; опрацювання питання відповідності законодавства України керівним принципам, установленим Радою Європи, щодо розроблення та використання технологій штучного інтелекту та гармонізація його з європейським; залучення наукових установ та громадськості до опрацювання питання щодо необхідності врегулювання суспільних відносин у сфері розвитку штучного інтелекту на законодавчому рівні[12].

Використана література

1. Стратегія кібербезпеки України: затвердж. Указом Президента України від 26 серпня 2021 р. № 447. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text.

2. Роль штучного інтелекту в кібербезпеці: передбачення та запобігання атакам. URL: https://www.bdo.ua/uk-ua/insights-2/information-materials/2024/the-role-of-ai-in-cybersecurity-anticipating-and-preventing-attacks.

3. Гуржій С.В. Особливості використання штучного інтелекту у питаннях забезпечення кібербезпеки. *Інформація і право.* 2023. № 4(47). С. 207-216.

4. Зоря І.С., Марущак А.В. Застосування штучного інтелекту для виявлення та реагування на кіберзагрози. URL:https://mail-attachment.googleusercontent.com/attachment/u/0/?ui=2&ik=1ecb16ab28&attid=0.1&permmsgid=msg-a:

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

6. Різченко М.Д. Роль штучного інтелекту в забезпеченні кібербезпеки URL:https://molodyivchenyi.ua/omp/index.php/conference/catalog/download/118/1683/3503-1?inline=1.

7. Савченко В.А., Шаповаленко О.Д. Основні напрями застосування технологій штучного інтелекту у кібербезпеці. *Сучасний захист інформації.* 2020. № 4 (44). С. 6-11.

8. Цяпа С.М. Огляд зарубіжних законодавчих ініціатив стратегічного використання технологій штучного інтелекту в сучасних умовах. *Інформація і право.* 2021. № 2(37). С. 51-59.

9. Товкун Л.В., Леонович М.Ю. Правове регулювання штучного інтелекту: міжнародний досвід та перспективи впровадження для України. *Юридичний науковий електронний журнал* 2024. № 12. С. 278-281.

10. Смірнов І. Правове регулювання штучного інтелекту: міжнародний досвід та українські перспективи. URL:https://biz.ligazakon.net/ analitycs/223351

11. Баранов О. Штучний інтелект та система права: монографія. Державна наукова установа «Інститут інформації, безпеки і права Національної академії правових наук України». 2025. Київ-Одеса, «Фенікс», 255 с.

12. Концепція розвитку штучного інтелекту в України : схвалено розпорядженням Кабінету Міністрів України від 2 грудня 2020 р. № 1556-р. URL:https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text.

13. Das R., Sandhane R. Artificial Intelligence in Cyber Security. Journal of Physics: Conference Series. 2021. Vol. 1964, no. 4. P. 042072. DOI: https://doi.org/ 10.1088/1742-6596/1964/4/042072.

14. Каплінський А.В. Штучний інтелект у кібербезпеці: сучасні підходи. *Вісник кібербезпеки.* 2022. № 3. С. 45–57.

15. Wafa A. W. A., Muzammil Hussain M. H. A Literature Review of Artificial Intelligence. *UMT Artificial Intelligence Review*. 2021. Vol. 1, no. 1. P. 1. DOI: https://doi.org/10.32350/air.11.01.

16. Бондаренко М.Ю. Використання машинного навчання для аналізу кіберзагроз. *Науковий вісник права.* 2023. № 2. С. 112–124.

17. Класифікації моделей застосування машинного навчання у кібербезпеці. А. В. Антоненко та ін. *Таврійський науковий вісник. Серія: Технічні науки.* 2023. № 4. С. 11–22. DOI: https://doi.org/10.32782/tnv-tech.2023.4.2.

18. Валентина Шимкович. «Штучний інтелект не захистить, якщо не використовувати інтелект природний»: як розвиток ШІ впливає на кібербезпеку. robot_dreams - онлайн-курси для фахівців у сфері big data, machine learning, data science | Робот Дрімс. URL: https://robotdreams.cc/uk/blog/352-shtuchniy-intelekt-ne-zahistit-yakshcho-nevikoristovuvati-intelekt-prirodniy-yak-rozvitok-shi-vplivaye-na-kiberbezpeku.

19. Лукіна І. В. Етичні та правові аспекти застосування ШІ в інформаційній сфері. *Право і суспільство.* 2024. № 1. С. 78–90.

20. Dilek S., Cakır H., Aydın M. Applications of Artificial Intelligence Techniques to Combating Cyber Crimes: A Review. International Journal of Artificial Intelligence & Applications. 2015. Vol. 6, no. 1. P. 21–39. DOI: https://doi.org/10.5121/ ijaia.2015.6102.

21. План заходів з реалізації Концепції розвитку штучного інтелекту в Україні на 2025-2026 роки : схвалено розпорядженням Кабінету Міністрів України від 9 травня 2025 р. №457-р URL:https://zakon.rada.gov.ua/laws/show/457-2025-%D1%80#Text

22. У ЄС набув чинності перший у світі закон, який регулюватиме правила у сфері штучного інтелекту. URL:https://zmina.info/news/u-yes-nabuv-chynnosti-pershyj-u-sviti-zakon-yakyj-regulyuvatyme-pravyla-u-sferi-shtuchnogo-intelektu/.

23. Дубняк М.В. Правові підходи в законі ЄС про штучний інтелект: досвід для України. *Інформація і право.* 2024. № 3(50). С. 40-53.

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~