УДК 004.89
DOI https://doi.org/10.32782/tnv-tech.2024.2.8

СТРАТЕГІЇ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ДАНИХ У СИСТЕМАХ ШТУЧНОГО ІНТЕЛЕКТУ

Примиська С. О. *– кандидат технічних наук, старший викладач кафедри технічних та програмних засобів автоматизації інженерно-хімічного факультету Національного технічного університету України «Київський політехнічний інститут імені Ігоря Сікорського» ORCID ID: 0000-0002-5832-0686*

Кримська А. О. *– кандидат технічних наук, старший викладач кафедри менеджменту, маркетингу і міжнародної логістики Чернівецького торговельно-економічного інституту Державного торговельно-економічного університету ORCID ID: 0000-0001-6410-9476*

Супрун О. М. *– кандидат фізико-математичних наук, доцент кафедри комп'ютеризованих систем управління Національного авіаційного університету ORCID ID: 0000-0002-1196-5655*

У статті розглядаються комплексні підходи до захисту інформації в умовах швидкого розвитку технологій штучного інтелекту (ШІ). Аналізуються потенційні загрози, що виникають при використанні ШІ в різних сферах – від кібербезпеки до етичних дилем. Важливість безпеки даних у системах ШІ постійно зростає відповідно до популярності використання інтелектуальних технологій при розробці різного роду інформаційних систем. Основна увага приділяється не лише технічним аспектам безпеки, а й соціальним та правовим вимірам, що передбачають регулювання й контроль за діяльністю систем ШІ. Окремо в статті підкреслюється важливість міжнародної співпраці й обміну знаннями для створення глобальної системи безпеки в галузі ШІ.

Мета даного дослідження полягає в розробці стратегій забезпечення безпеки даних у контексті ШІ та їхнього впливу на загальну безпеку інформаційних систем.

У межах дослідження було розглянуто методи аналізу наявних моделей захисту даних, синтезу нових рішень та оцінки їх ефективності в тестових умовах. Запропоновано низку стратегій, які містять розробку надійних алгоритмів, створення стандартів безпеки даних та впровадження систем моніторингу для запобігання зловмисному використанню ШІ.

Основні результати дозоляють зробити висновки, згідно з якими створення єдиних стандартів безпеки даних не лише допоможе підвищити рівень захисту конфіденційної інформації в системах ШІ, але й сприятиме зростанню довіри громадськості до їх використання. Це може мати значний вплив на розвиток нових технологій, економічний розвиток та захист прав і свобод людини в цифровому світі. Результати дослідження мають практичну значущість, оскільки пропонують рекомендації щодо впровадження розроблених стратегій у реальних системах ШІ, а це може слугувати основою для подальшого законодавчого регулювання в цій сфері.

Ключові слова: *штучний інтелект, інтелектуальні інформаційні технології, захист інформації, кібербезпека.*

Prymyska S. O., Krymska A. O., Suprun O. M. Strategies for ensuring data security in artificial intelligence systems

This article explores comprehensive approaches to information protection in the context of rapid advancements in artificial intelligence (AI) technologies. It analyzes potential threats that appear when people use AI across different areas from cybersecurity to ethical dilemmas.

The relevance of data security in AI constantly increases according to the popularity of smart technologies using in the development of different types of information systems. The main focus is not only on the technical aspects of security, but also on the social and legal dimensions, including regulation and control over the activities of AI systems. The article also touches upon the importance of international cooperation and knowledge exchange to establish a global security framework in the field of AI.

The purpose of this research is developing of strategies for ensuring data security in the context of AI and their influence on the general safety of information systems.

As a part of research, there are considered analysis methods of existing data protection models, synthesis of new solutions and evaluation of their efficiency in the test conditions. Also, there are proposed a number of strategies that include the development of the reliable algorithms, the establishment of data security standards and the implementation of monitoring systems to prevent malicious use of AI.

The main results allow us to conclude that the creation of unified data security standards will help not only the level of protection of confidential information in AI systems, but also will contribute to increasing public trust in the use of these systems. This can have a significant impact on the development of new technologies, economic evolution and the protection of human rights and freedoms in the digital world. The research results have practical significance as they offer recommendations for the developed strategies implementation in the real AI systems, which, in turn, can serve as a basis for further legislative regulation in this area.

Key words: *artificial intelligence, intelligent information technologies, information security, cybersecurity.*

Вступ. В умовах стрімкого розвитку технологій ШІ забезпечення безпеки даних набуває особливої актуальності. У сучасному світі, де кількість цифрових даних зростає експоненційно, захист інформації стає надзвичайно важливим завданням. За останні роки значний прогрес у сфері ШІ зумовив впровадження інтелектуальних технологій в різні галузі людської діяльності. Популярність систем ШІ призвела до того, що вони стали необхідним елементом бізнес-процесів та повсякденного життя. Інтелектуальні системи використовуються у фінансах, медицині, виробництві, транспорті та багатьох інших сферах. ШІ дозволяє автоматизувати процеси й аналізувати великі обсяги даних, що робить його необхідним інструментом в сучасному світі.

Проте активне використання інтелектуальних технологій супроводжується ризиками з погляду захисту даних. Інформація, яка зберігається й обробляється різними інформаційними системами, може містити особисті дані, комерційну таємницю чи іншу конфіденційну інформацію. Недостатній захист цих даних може призвести до серйозних наслідків. Саме розвиток ШІ відкриває нові можливості для захисту даних, зокрема йдеться про автоматизоване виявлення загроз та реагування на них. Разом із тим ШІ також може бути використаний для створення більш складних кібератак, що підвищує ризики для безпеки даних. Впровадження інтелектуальних технологій вимагає розробки нових методів захисту даних, але враховувати при цьому треба не тільки технічні, а й правові, етичні та соціальні аспекти.

З огляду на це розробка ефективних стратегій захисту даних у системах ШІ стає надзвичайно важливим завданням. Крім того, розвиток законодавства щодо захисту даних стає невід'ємною частиною цього процесу. Забезпечення ефективного захисту даних у системах ШІ має важливе значення для довіри громадськості до цих технологій. Особливу увагу слід приділяти спільним зусиллям науковців, виробників програмного забезпечення та регулювальних органів для забезпечення безпеки даних у нову епоху цифрового розвитку.

Отже, стрімкий розвиток ШІ має значний вплив на сучасні стратегії захисту даних. Традиційні методи кібербезпеки можуть виявитися неефективними в контексті інтелектуальних систем, які можуть використовувати складні алгоритми й методи аналізу, що ускладнює виявлення потенційних загроз та реагування на

них. Розвиток ШІ вимагає від компаній та організацій перегляду своїх політик конфіденційності та захисту даних.

Метою роботи є аналіз і розробка ефективних стратегій захисту даних у системах ШІ, зокрема створення нових технологій та підходів до забезпечення безпеки, враховуючи специфіку роботи інтелектуальних систем та їх вплив на сучасні підходи до кібербезпеки.

Аналіз останніх досліджень і публікацій. Тема ШІ за останні декілька років набула неабиякої популярності, що підтверджується значною кількістю наукових робіт із цієї галузі. Дослідженню впровадження систем ШІ в різні сфери людської діяльності присвятили свої наукові роботи такі вітчизняні вчені, як Н. І. Черненко [1], К. О. Черевко [2], О. В. Цеслів [3], С. О. Лебеденко [4], І. С. Гунько [5] та інші.

Окрім напрямів впровадження систем ШІ, предметом наукового інтересу таких дослідників, як В. І. Богом'я, А. С. Гудзь [6], Д. П. Пчелянський, С. А. Воінова [7], є питання перспектив майбутнього їх розвитку. О. В. Добровольська, В. І. Штанько [8] розглядають філософські аспекти розвитку інтелектуальних комп'ютерних технологій.

У сфері захисту даних в інформаційних системах останні дослідження й публікації відображають широкий спектр стратегій та методологій, спрямованих на зміцнення безпеки в умовах активізації кіберзагроз.

У роботі П. В. Діхтієвського [9] аналізуються напрями захисту персональних даних в умовах воєнного стану, де особлива увага приділяється гібридним війнам та «викраденню» персональних даних.

М. А. Мірошник [10], В. Б. Дудикевич, Б. П. Томашевський, Р. В. Сергієнко [11] вивчають методи інформаційної безпеки й захисту даних у комп'ютерних системах та мережах. Дослідження в цій галузі дають уявлення про моделі загроз інформації та описують основні механізми й протоколи захисту, включаючи криптографічне перетворення даних.

Одним із ключових напрямів досліджень є вивчення правового регулювання ШІ, зокрема співвідношення права й моралі в контексті захисту даних. І. І. Онищук [12] робить акцент на необхідності формування міждисциплінарного підходу, який би враховував економічні, правові, етичні, політичні й соціальні аспекти використання ШІ. Дослідник наголошує на необхідності розробки відповідного законодавства та нормативно-правових рамок, які б забезпечували ефективний захист даних, збереження приватності й етичну обробку інформації.

Ю. І. Тюря [13] зазначає, що Європейський Союз виступає з «європейським підходом» до регулювання ШІ, який базується на принципах «орієнтованого на людину» підходу. Цей підхід містить «екосистему досконалості» та «екосистему довіри», що передбачає контроль, технічну надійність, конфіденційність даних, прозорість, недискримінацію та підзвітність.

Такі науковці, як О. О. Посикалюк [14], К. С. Токарєва та Н. О. Савліва [15] підкреслюють необхідність заохочення розробок нових форм регулювання, які б сприяли прозорості й дотриманню етичних принципів у сфері захисту даних. Вони закликають до створення державно-правових гарантій, які б забезпечували захист прав, свобод і безпеки людини в контексті використання ШІ.

Загалом, аналіз останніх досліджень і публікацій демонструє, що питання захисту даних у системах ШІ є предметом активного наукового діалогу. Ці дослідження й публікації відіграють важливу роль у формуванні стратегій захисту даних, надаючи фахівцям та організаціям необхідні знання для розробки ефективних заходів безпеки в інформаційних системах.

Виклад основного матеріалу дослідження. У сфері ШІ стратегії захисту даних відіграють ключову роль у забезпеченні конфіденційності й безпеки інформації. Розробка ефективних стратегій вимагає глибокого розуміння потенційних загроз та вразливостей, які можуть виникнути в результаті використання ШІ.

Насамперед важливо здійснити глибокий аналіз практик використання ШІ провідними компаніями в галузі інформаційних технологій з особливим акцентом на методи захисту даних в їхніх інформаційних системах [16–18]. Такий аналіз дозволяє виявити ключові тенденції й найкращі практики, які можуть бути застосовані для підвищення рівня безпеки. Результати такого аналітичного дослідження були узагальнені та представлені у формі порівняльної таблиці, що включає опис напрямів використання ШІ кожною компанією, а також методи, за допомогою яких вони забезпечують захист інформації у своїх системах. Ця таблиця має на меті допомогти зрозуміти поточний стан захисту даних та основні тенденції у сфері ШІ, виокремити провідні стратегії забезпечення захисту даних в системах ШІ.

Таблиця 1

Результати аналітичного дослідження використання технологій ШІ провідними компаніями в галузі інформаційних технологій

Компанія	Напрями використання ШІ	Захист інформації
Google	Пошук, реклама, аналітика даних, мовний переклад, розробка програмного забезпечення, автономні транспортні засоби, кібербезпека	Захист конфіденційної інформації користувачів, шифрування даних, аудит безпеки
Microsoft	Хмарні сервіси, операційні системи, офісні програми, машинне навчання, комп'ютерний зір, обробка природної мови	Захист корпоративних даних, мережева безпека, захист від кіберзагроз
Amazon	Електронна комерція, хмарні сервіси, голосові помічники, роботизована доставка товарів, прогнозування попиту, персоналізація	Шифрування даних, безпека від кібератак, захист особистих даних користувачів
Facebook	Соціальні мережі, реклама, аналітика даних, віртуальна реальність, розпізнавання облич, генерація тексту	Захист конфіденційної інформації користувачів, контроль доступу, криптографія
Apple	Мобільні пристрої, операційні системи, голосові помічники, комп'ютерний зір, персоналізація, розробка програмного забезпечення	Захист особистих даних, шифрування даних, безпека від кіберзагроз

Отже, як бачимо, ШІ стає все більш важливою технологією в ІТ-галузі. Провідні ІТ-компанії постійно інвестують у дослідження й розробку інтелектуальних технологій, а також використовують ШІ для покращення своїх продуктів і послуг.

До ключових тенденцій у використанні ШІ в ІТ-галузі належать[18]:

− автоматизація: ШІ використовується для автоматизації завдань, які раніше виконувалися людьми. Це може призвести до підвищення продуктивності та зниження витрат;

− персоналізація: ШІ використовується для персоналізації продуктів і послуг для користувачів. Це може покращити досвід користувачів і підвищити їх лояльність;

– нові продукти та послуги: ШІ використовується для розробки нових продуктів і послуг, які раніше неможливо було уявити. Це може зумовити появу нових ринків і можливостей для бізнесу.

Очікується, що використання ШІ в ІТ-галузі буде активізуватися найближчими роками. При цьому захист інформації стає все більш важливою проблемою, оскільки компанії все більше покладаються на ШІ, системи якого можуть бути вразливими до кібератак та використовуватися для крадіжки даних або зловживання ними.

Основними ризиками, пов'язаними з використанням ШІ та захистом інформації, є [19]:

– кібератаки: ШІ-системи можуть бути вразливими до кібератак, таких як DDoS-атаки, атаки на ланцюжок постачання та атаки на ШІ;

– витік даних: ШІ-системи можуть використовуватися для крадіжки даних або зловживання ними, йдеться про особисту чи фінансову інформацію, а також комерційну таємницю;

– упередженість: ШІ-системи можуть бути упередженими, що може призвести до дискримінації або несправедливого ставлення до певних груп людей.

Для захисту своїх даних та систем від зазначених вище ризиків ІТ-компанії, які використовують ШІ, вживають таких заходів [20]:

– шифрування даних: може допомогти захистити їх від крадіжки або несанкціонованого доступу;

– контроль доступу: може допомогти гарантувати, що доступ до ШІ-систем мають лише авторизовані користувачі;

– моніторинг безпеки: може допомогти виявити кібератаки або інші інциденти безпеки;

– аналіз даних про кібербезпеку: може допомогти компаніям краще зрозуміти ризики й розробити більш ефективні заходи захисту.

Після здійснення аналізу напрямів забезпечення безпеки даних у системах ШІ, які використовують провідні ІТ-компанії, вбачається доцільним чітко визначити перелік стратегій захисту даних в інформаційних системах [10, 11].

Аналіз ризиків є першим кроком у формуванні стратегій захисту даних. Це передбачає ідентифікацію та оцінку потенційно слабких місць у системах, які можуть бути використані для несанкціонованого доступу або витоку даних. Проте для успішного аналізу необхідно враховувати широкий спектр загроз, зокрема зовнішні й внутрішні загрози, загрози з боку сторонніх агентів та вразливості в програмному забезпеченні.

Розробка політик безпеки та їх постійне оновлення є важливими для адаптації до змінюваних умов та нових загроз. Політики повинні передбачити процедури відповіді на інциденти, що дозволяє швидко реагувати на будь-які порушення безпеки. Забезпечення наявності механізмів негайного реагування й відновлення в разі інцидентів є критично важливим для запобігання серйозним наслідкам у разі виникнення проблем.

Освітні програми для співробітників можуть значно знизити ризик внутрішніх загроз. Навчання персоналу основам кібербезпеки й формування навичок розпізнавання фішингових атак є критично важливим. Проведення систематичних тренінгів та організація внутрішніх навчальних заходів сприяє формуванню культури безпеки серед персоналу, що підвищує загальний рівень захищеності компанії від кіберзагроз.

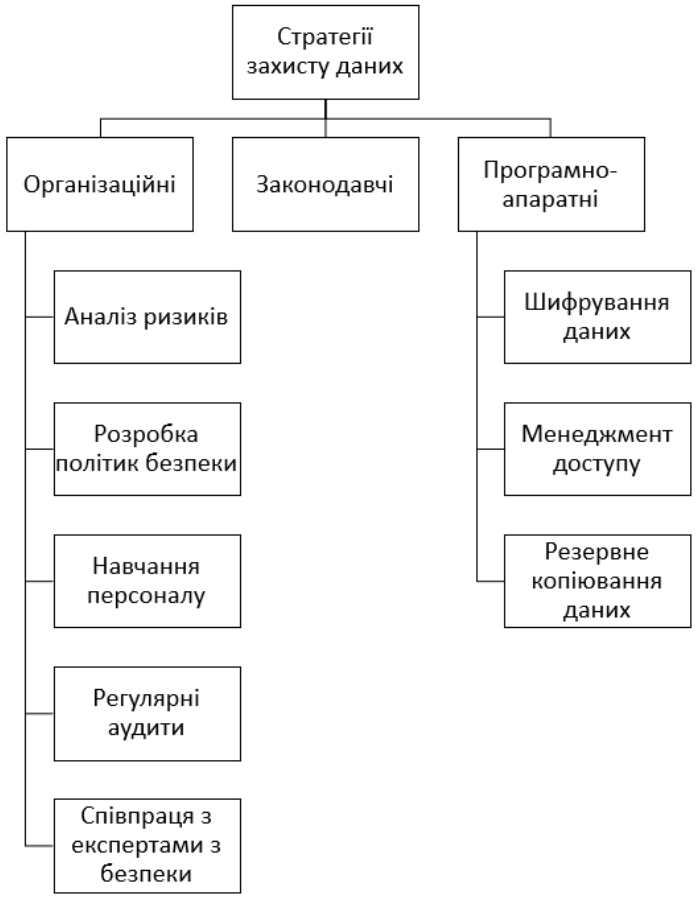

Рис. 1. Стратегії захисту даних

Джерело: власна розробка авторів

Регулярні аудити безпеки допомагають виявляти й усувати потенційні вразливості. Йдеться про перевірку систем на предмет останніх оновлень безпеки та виправлення будь-яких виявлених проблем. Додатково аудит може включати аналіз ризиків та виявлення слабких місць, що дозволяє компанії ефективно вдосконалювати свої заходи захисту.

Співпраця з експертами з безпеки дозволяє використовувати зовнішній досвід для підвищення рівня захисту систем. Експерти можуть допомогти в ідентифікації слабких місць та розробці спеціалізованих рішень. Встановлення довгострокових партнерських відносин із провідними компаніями з кібербезпеки дозволяє вирішувати складні завдання щодо захисту даних та ефективно реагувати на зміни в загрозах.

Шифрування даних є однією з найважливіших стратегій захисту. Використання сучасних алгоритмів шифрування дозволяє забезпечити недоступність даних для неавторизованих осіб навіть у випадку їх витоку. Крім того, шифрування може передбачати застосування складних алгоритмів обміну ключами й регулярне оновлення шифрувальних методів для забезпечення максимального рівня безпеки.

Менеджмент доступу встановлює суворі правила для контролю тих, хто має доступ до важливих даних. Це означає впровадження багаторівневої системи автентифікації для забезпечення додаткового рівня захисту, застосування правильного рівня доступу для кожного користувача та постійний моніторинг ідентифікаційних даних, що дозволяє запобігати несанкціонованому доступу й зловживанню.

Резервне копіювання даних надзвичайно допомагає в їх захисті. Забезпечення резервних копій даних для відновлення в разі втрати є важливою стратегією. Планування регулярного резервного копіювання, а також забезпечення географічного розподілу копій даних для запобігання одночасній втраті важливої інформації є критичними аспектами безпеки даних.

Законодавча підтримка є необхідною для створення правової основи, яка регулює збір, обробку й захист даних. Це також передбачає міжнародну співпрацю для боротьби з кіберзлочинністю на глобальному рівні. Закони, що стосуються захисту даних, повинні бути гнучкими й адаптивними, щоб враховувати швидкий розвиток технологій та зміну характеру кіберзагроз. До того ж важливо забезпечити взаємодію між країнами для обміну найкращими практиками та спільного реагування на кібератаки й інші загрози.

Крім визначення загальних стратегій захисту даних в інформаційних системах, необхідно окреслити стратегії використання ШІ для захисту даних, які повинні включати розробку систем, здатних автоматично виявляти та блокувати підозрілу активність, що є важливим кроком у протидії кібератакам. ШІ може стати потужним інструментом для протидії цим атакам. Завдяки своїй швидкості, точності й масштабованості системи ШІ можуть допомогти організаціям краще захищати свої дані та системи.

Рис. 2. Стратегії захисту даних з використанням систем ШІ

Джерело: власна розробка авторів

Отже, використання ШІ передбачає насамперед аналіз наявних даних для подальшого виявлення аномалій. Проаналізувавши записи в системних журналах, можна виявити нетипові шаблони, які можуть свідчити про кібератаку. Наприклад, раптове збільшення кількості невдалих входів або несанкціонований доступ до файлів. Також можна за допомогою ШІ аналізувати мережевий трафік для виявлення підозрілої активності. Наприклад, сканування портів або DDoS-атаки. Крім того, сучасні системи ШІ дозволяють здійснювати аналіз поведінки користувачів і виявляти підозрілу активність.

Проаналізувавши наявні дані, можна створювати різноманітні інтелектуальні моделі:

- моделі прогнозування ймовірних атак;
- моделі поведінки для розпізнавання нормальної та аномальної активності;
- моделі прогнозування інцидентів та порядку дій реагування на них;
- моделі для класифікації кібератак, що дозволяють автоматично реагувати на них. Наприклад, блокувати IP-адресу або ізолювати заражений пристрій.

Також системи ШІ можуть допомогти покращити кібергігієну інформаційної системи загалом. Для цього можна делегувати ШІ автоматизацію завдань із кібербезпеки. Наприклад, оновлення програмного забезпечення та патчів.

Крім того, ШІ можна використати для навчання користувачів основам кібербезпеки та кращого захисту своїх даних. ШІ чудово працює в системах підтримки прийняття рішень, відповідно інтелектуальні технології можуть бути використані для надання рекомендацій щодо кібербезпеки та допомоги в прийнятті ефективних рішень.

До переваг використання ШІ для протидії кібератакам належать:

- швидкість: ШІ може аналізувати великі обсяги даних значно швидше, ніж люди, тому може виявляти кібератаки на ранній стадії;
- точність: ШІ може бути навчений на великих наборах даних для точного виявлення кібератак, зменшуючи кількість помилкових спрацьовувань;
- масштабованість: ШІ може бути масштабований для захисту великих мереж і систем із мінімальними людськими ресурсами.

Необхідно зазначити, що на особливу увагу заслуговують також аспекти законодавчих стратегій захисту даних в інформаційних системах, що використовують інтелектуальні технології. У сучасному світі, де ШІ застосовується в усіх сферах нашого життя, проблема законодавчого регулювання його використання є надзвичайно важливою.

Закони, що регулюють ШІ, мають важливе значення для захисту прав людини, забезпечення соціальної справедливості й дотримання етичних норм. Правове регулювання ШІ вимагає глибокого розуміння технологій та їх потенційного впливу на суспільство. Воно повинно враховувати не тільки технічні аспекти, але й соціальні наслідки використання ШІ, такі як втручання в приватне життя, дискримінація та зловживання владою.

У всьому світі спостерігається посилення уваги до правових, соціальних та етичних аспектів використання ШІ. Європейський Союз, наприклад, розробляє регуляції, що мають на меті забезпечити безпечне й етичне використання ШІ, у той час, як інші країни запроваджують національні стратегії. Законодавче регулювання ШІ має балансувати між заохоченням інновацій та захистом суспільства від потенційних ризиків. Це передбачає розробку стандартів для транспарентності алгоритмів, відповідальності за прийняті ШІ рішення та захисту від упередженості й дискримінації.

Таким чином, розробка законодавчих безпекових стратегій у системах ШІ на сьогодні є актуальним завданням, розв'язання якого вимагає постійного діалогу між законодавцями, технічними експертами, етичними комісіями та громадськістю.

Висновки. Таким чином, розвиток ШІ зумовлює значні ризики для безпеки даних, адже системи ШІ можуть використовуватися для збору, зберігання та обробки великих обсягів персональних та конфіденційних даних. Зловмисне використання цих даних може призвести до їх крадіжки, шахрайства, шантажу, дискримінації та інших злочинів. Забезпечення безпеки даних в умовах розвитку ШІ стає все більш нагальною проблемою, що потребує комплексного підходу.

Захист даних в контексті ШІ вимагає застосування заходів технічного, соціального та правового характеру. З цією метою необхідно розробити етичні норми використання ШІ, вдосконалити законодавство про захист даних, створити міжнародні норми й стандарти безпеки ШІ. Жодна країна не може самостійно розв'язати проблему захисту даних в умовах розвитку ШІ. Необхідно об'єднати зусилля на міжнародному рівні для створення глобальної системи безпеки ШІ й розробки спільних стандартів та протоколів захисту даних.

Розроблені стратегії безпеки даних у системах ШІ пропонують створення надійних алгоритмів ШІ, які мінімізують ризики витоків даних та зловживань, забезпечать прозорість і підзвітність систем ШІ. Крім того, впровадження даних стратегій передбачає розробку єдиних стандартів безпеки даних для систем ШІ, що може значно підвищити довіру користувачів до них. У підсумку це зумовить більш широке використання ШІ в різних сферах життя.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ:

1. Черненко Н. І. Штучний інтелект в управлінні персоналом. *Таврійський науковий вісник. Серія: Економіка*. 2022. № 12. С. 76–83. URL: https://doi.org/10.32851/2708-0366/2022.12.11 (дата звернення 08.04.2024).

2. Черевко К. О. Штучний інтелект як інструмент протидії злочинності. *Вісник Кримінологічної асоціації України*. 2023. Т. 28. № 1. С. 124–133. URL: https://doi.org/10.32631/vca.2023.1.10 (дата звернення 08.04.2024).

3. Цеслів О. Штучний інтелект в економіці. *Наука і техніка сьогодні*. 2022. № 6(6). С. 70–78. URL: https://doi.org/10.52058/2786-6025-2022-6(6)-70-78 (дата звернення 08.04.2024).

4. Лебеденко С. О. Штучний інтелект в маркетингу. *Ефективна економіка*. 2023. № 4. URL: https://doi.org/10.32702/2307-2105.2023.4.38 (дата звернення 08.04.2024).

5. Гунько І. Тестування програмного забезпечення у 2023 році: нові тенденції та проблеми. *Herald of Kiev Institute of Business and Technology*. 2023. Вип. 49. № 1–2. С. 25–36. URL: https://doi.org/10.37203/kibit.2023.49.03 (дата звернення 08.04.2024).

6. Богом'я В., Гудзь А. Штучний інтелект: сучасний стан і перспективи застосування. *Сучасні інформаційні технології у сфері безпеки та оборони*. 2023. Т. 46. № 1. С. 13–17. URL: https://doi.org/10.33099/2311-7249/2023-46-1-13-17 (дата звернення 10.04.2024).

7. Пчелянський Д. П., Воінова С. А. Штучний інтелект: перспективи та тенденції розвитку. *Automation of technological and business processes*. 2019. Т. 11. № 3. С. 59–64. URL: https://doi.org/10.15673/atbp.v11i3.1500 (дата звернення 08.04.2024).

8. Добровольська О. В., Штанько В. І. Філософський аналіз еволюції штучного інтелекту. *Studies in history and philosophy of science and technology*. 2019. Т. 28. № 1. С. 10–19. URL: https://doi.org/10.15421/271902 (дата звернення 12.04.2024).

9. Діхтієвський П. В. Адміністративно-правове забезпечення захисту персональних даних громадян в умовах воєнного стану. *Проблеми сучасних трансформацій. Серія: право, публічне управління та адміністрування*. 2023. № 10. URL: https://doi.org/10.54929/2786-5746-2023-10-01-15 (дата звернення 08.04.2024).

10. Мірошник М. А. Розробка засобів захисту інформації в розподілених комп'ютерних системах та мережах. *Інформаційно-керуючі системи на залізничному транспорті*. 2015. № 1. С. 18–25. URL: https://doi.org/10.18664/ikszt.v0i1.51555 (дата звернення 08.04.2024).

11. Дудикевич В. Б., Томашевський Б. П., Сергієнко Р. В. Протоколи і механізми безпеки інформації в комп'ютерних системах і мережах. *Ukrainian information security research journal*. 2009. Т. 11. № 2(43). URL: https://doi.org/10.18372/2410-7840.11.4043 (дата звернення 15.04.2024).

12. Онищук І. І. Правове регулювання технологій штучного інтелекту: теоретико-прикладні та етичні засади. *Scientific Papers of the Legislation Institute of the Verkhovna Rada of Ukraine*. 2020. № 3. С. 50–57. URL: https://doi.org/10.32886/instzak.2020.03.06 (дата звернення 08.04.2024).

13. Тюря Ю. І. Правове регулювання використання штучного інтелекту на основі європейського підходу. *Знання європейського права*. 2022. № 2. С. 141–145. URL: https://doi.org/10.32837/chern.v0i2.362 (дата звернення 08.04.2024).

14. Посикалюк О. Правове регулювання відносин щодо використання штучного інтелекту: перспективи з точки зору порівняльного права. *Право України*. 2021. № 10. С. 202–210. URL: https://doi.org/10.33498/louu-2021-10-202 (дата звернення 15.04.2024).

15. Токарєва К., Савліва Н. Особливості правового регулювання штучного інтелекту в Україні. *Scientific works of National Aviation University. Series: Law Journal «Air and Space Law»*. 2021. № 60 (3), С. 148–153. URL: https://doi.org/10.18372/2307-9061.60.15967 (дата звернення 08.04.2024).

16. Даниленко Ю. Від Ш до І: що таке штучний інтелект та як він трансформує світ. *SPEKA*. 2022. URL: https:/speka.media/ai/vid-s-do-i-shho-take-stucnii-intelekt-ta-yak-vin-transformuje-svit-xv7039 (дата звернення 08.04.2024).

17. Тартачний О. Чому Google зосереджується на штучному інтелекті? Офіційне пояснення компанії. *SPEKA*. 2023. URL: https://speka.media/comu-google-zoseredzujetsya-na-stucnomu-intelekti-oficiine-poyasnennya-kompaniyi-9x5mwp. (дата звернення 08.04.2024).

18. 50 найперспективніших компаній, які будують бізнес на основі штучного інтелекту. Список Forbes. *Forbes.* 2023. URL: https://forbes.ua/innovations/spisok-nayperspektivnishikh-privatnikh-kompaniy-yaki-buduyut-biznes-na-osnovi-shtuchnogo-intelektu-20042023-13200 (дата звернення 08.04.2024).

19. Голубенко О. І., Лемешко А. В., Поліщук А. Р., Кузьменко М. В., Дегтярьов Є. О. Дослідження застосування штучного інтелекту у кібербезпеці. *ITSynergy.* 2023. № 2. С. 71–78. URL: https://doi.org/10.53920/its-2023-2-5 (дата звернення 08.04.2024).

20. Савченко В.А., Шаповаленко О.Д. Основні напрями застосування технологій штучного інтелекту у кібербезпеці. *Сучасний захист інформації.* 2020. № 4. С. 6–11. URL: https://doi.org/10.31673/2409-7292.2020.040611 (дата звернення 08.04.2024).

REFERENCES:

1. Chernenko, N. I. (2022). Shtuchnyi intelekt v upravlinni personalom [Artificial intelligence in personnel management]. *Tavriiskyi naukovyi visnyk. Seriia: Ekonomika – Tavria Scientific Herald. Series: Economics*, 12, 76–83. Retrieved from https://doi.org/10.32851/2708-0366/2022.12.11 [in Ukrainian].

2. Cherevko, K. O. (2023). Shtuchnyi intelekt yak instrument protydii zlochynnosti [Artificial intelligence as a tool to combat crime]. *Visnyk Kryminolohichnoi asotsiatsii Ukrainy – Bulletin of the Criminological Association of Ukraine*, 28 (1), 124–133. Retrieved from https://doi.org/10.32631/vca.2023.1.10 [in Ukrainian].

3. Tsesliv, O. (2022). Shtuchnyi intelekt v ekonomitsi [Artificial intelligence in economics]. *Nauka i tekhnika sohodni – Science and Technology Today*, 6(6), 70–78. Retrieved from https://doi.org/10.52058/2786-6025-2022-6(6)-70-78 [in Ukrainian].

4. Lebedenko, S. O. (2023). Shtuchnyi intelekt v marketynhu [Artificial intelligence in marketing]. *Efektyvna ekonomika – Effective Economics*, 4. Retrieved from https://doi.org/10.32702/2307-2105.2023.4.38 [in Ukrainian].

5. Hunko, I. (2023). Testuvannia prohramnoho zabezpechennia u 2023 rotsi [Software testing in 2023: new trends and challenges]. *Visnyk: Kyivskyi instytut biznesu ta tekhnolohii – Herald of Kyiv Institute of Business and Technology*, 49(1–2), 25–36. Retrieved from https://doi.org/10.37203/kibit.2023.49.03 [in Ukrainian].

6. Bohomia, V., & Hudz, A. (2023). Shtuchnyi intelekt: suchasnyi stan i perspektyvy zastosuvannia [Artificial intelligence: Current state and prospects of application]. *Suchasni informatsiini tekhnolohii u sferi bezpeky ta oborony – Modern Information Technologies in Security and Defense Sphere*, 46(1), 13–17. Retrieved from https://doi.org/10.33099/2311-7249/2023-46-1-13-17 [in Ukrainian].

7. Pchelianskyi, D. P., & Voinova, S. A. (2019). Shtuchnyi intelekt: perspektyvy ta tendentsii rozvytku [Artificial intelligence: Prospects and development trends]. *Avtomatyzatsiia tekhnolohichnykh i biznes-protsesiv – Automation of Technological and Business Processes*, 11(3), 59–64. Retrieved from https://doi.org/10.15673/atbp.v11i3.1500 [in Ukrainian].

8. Dobrovolska, O. V., & Shtanko, V. I. (2019). Filosofskyi analiz evoliutsii shtuchnoho intelektu [Philosophical analysis of the evolution of artificial intelligence]. *Doslidzhennia z istorii i filosofii nauky i tekhniky – Studies in History and Philosophy of Science and Technology*, 28(1), 10–19. Retrieved from https://doi.org/10.15421/271902 [in Ukrainian].

9. Dikhtiyevsky, P. V. (2023). Administratyvno-pravove zabezpechennia zakhystu personalnykh danykh hromadian v umovakh voiennoho stanu [Administrative-legal support for the protection of citizens' personal data in conditions of martial law]. *Problemy suchasnykh transformatsii. Seriia: pravo, publichne upravlinnia ta administruvannia – Problems of Modern Transformations. Series: Law, Public Administration, and Administration*, 10. Retrieved from https://doi.org/10.54929/2786-5746-2023-10-01-15 [in Ukrainian].

10. Myroshnyk, M. A. (2015). Rozrobka zasobiv zakhystu informatsii v rozpodilenykh kompiuternykh systemakh ta merezhakh [Development of information protection tools in distributed computer systems and networks]. *Informatsiino-keruiuchi systemy na zaliznychnomu transporti – Information and Control Systems in Railway Transport*, 1, 18–25. Retrieved from https://doi.org/10.18664/ikszt.v0i1.51555 [in Ukrainian].

11. Dudikevich, V. B., Tomashovsky, B. P., & Serhiienko, R. V. (2009). Protokoly i mekhanizmy bezpeky informatsii v kompiuternykh systemakh i merezhakh [Information security protocols and mechanisms in computer systems and networks]. *Ukrainian Information Security Research Journal*, 11(2(43)). Retrieved from https://doi.org/10.18372/2410-7840.11.4043 [in Ukrainian].

12. Onyshchuk, I. I. (2020). Pravove rehuliuvannia tekhnolohii shtuchnoho intelektu: teoretyko-prykladni ta etychni zasady [Legal regulation of artificial intelligence technologies: Theoretical, applied, and ethical foundations]. *Naukovi zapysky Instytutu zakonodavstva Verkhovnoi Rady Ukrainy – Scientific Papers of the Legislation Institute of the Verkhovna Rada of Ukraine*, 3, 50–57. Retrieved from https://doi.org/10.32886/instzak.2020.03.06 [in Ukrainian].

13. Tyuria, Y. I. (2022). Pravove rehuliuvannia vykorystannia shtuchnoho intelektu na osnovi yevropeiskoho pidkhodu [Legal regulation of the use of artificial intelligence based on the European approach]. *Znannia yevropeiskoho prava – Knowledge of European Law*, 2, 141–145. Retrieved from https://doi.org/10.32837/chern.v0i2.362 [in Ukrainian].

14. Posikalyuk, O. (2021). Pravove rehuliuvannia vidnosyn shchodo vykorystannia shtuchnoho intelektu: perspektyvy z tochky zoru porivnialnoho prava [Legal regulation of relations regarding the use of artificial intelligence: Prospects from the perspective of comparative law]. *Pravo Ukrainy – Law of Ukraine,* 10, 202–210. Retrieved from https://doi.org/10.33498/louu-2021-10-202 [in Ukrainian].

15. Tokareva, K., & Savlyva, N. (2021). Osoblyvosti pravovoho rehuliuvannia shtuchnoho intelektu v Ukraini [Features of legal regulation of artificial intelligence in Ukraine]. *Scientific Works of National Aviation University. Series: Law Journal «Air and Space Law»*, 3(60), 148–153. Retrieved from https://doi.org/10.18372/2307-9061.60.15967 [in Ukrainian].

16. Danilenko, Yu. (2022). Vid Sh do I: shcho take shtuchnyi intelekt ta yak vin transformuie svit [From Z to I: what is artificial intelligence and how it transforms the world]. *SPEKA*. Retrieved from https://speka.media/ai/vid-s-do-i-shho-take-stucnii-intelekt-ta-yak-vin-transformuje-svit-xv7039 [in Ukrainian].

17. Tartachny, O. (2023). Chomu Google zoseredzhuietsia na shtuchnomu intelekti? Ofitsiine poiasnennia kompanii [Why is Google focusing on artificial intelligence? Official explanation of the company]. *SPEKA*. Retrieved from https://speka.media/comu-google-zoseredzujetsya-na-stucnomu-intelekti-oficiine-poyasnennya-kompaniyi-9x5mwp. [in Ukrainian].

18. 50 naiperspektyvnishykh kompanii, yaki buduiut biznes na osnovi shtuchnoho intelektu. Spysok Forbes [Forbes magazine website. 50 most promising companies that build business on the basis of artificial intelligence. Forbes list]. *Forbes*. Retrieved from https://forbes.ua/innovations/spisok-nayperspektivnishikh-privatnikh-kompaniy-yaki-buduyut-biznes-na-osnovi-shtuchnogo-intelektu-20042023-13200. [in Ukrainian].

19. Golubenko, O. I., Lemeshko, A. V., Polishchuk, A. R., Kuzmenko, M. V., Degtyarev, E. O. (2023) Doslidzhennia zastosuvannia shtuchnoho intelektu u kiberbezpetsi [Research on the use of artificial intelligence in cyber security]. *ITSynergy*, 2, 71–78. Retrieved from https://doi.org/10.53920/its-2023-2-5 [in Ukrainian].

20. Savchenko, V.A., & Shapovalenko, O.D. (2020) Osnovni napriamy zastosuvannia tekhnolohii shtuchnoho intelektu u kiberbezpetsi [The main areas of application of artificial intelligence technologies in cyber security]. *Suchasnyi zakhyst informatsii – Modern information protection,* 4, 6–11. Retrieved from https://doi.org/10.31673/2409-7292.2020.040611 [in Ukrainian].