УДК: 330.34:355.01=811.111
https://doi.org/10.32342/3041-2137-2026-2-65-3

***О. В. Гаврилюк,***
доктор економічних наук, професор, професор кафедри маркетингу
Приватного вищого навчального закладу «Європейський університет», м. Київ (Україна)
https://orcid.org/0000-0001-6819-9296

***І. В. Пономаренко,***
кандидат економічних наук, доцент, доцент кафедри маркетингу Державного торговельно-економічного університету, м. Київ (Україна)
https://orcid.org/0000-0003-3532-8332

***О. В. Якушев,***
кандидат економічних наук, доцент, доцент кафедри соціального забезпечення Черкаського державного технологічного університету, м. Черкаси (Україна)
https://orcid.org/0000-0002-0699-1795

# ІДЕНТИФІКАЦІЯ ПРОБЛЕМ, ЩО ВИНИКАЮТЬ ПРИ ВПРОВАДЖЕННІ ШТУЧНОГО ІНТЕЛЕКТУ В БІЗНЕС-СЕРЕДОВИЩЕ

Інтенсивний розвиток технологій штучного інтелекту (ШІ) та його впровадження у бізнес-середовище детермінує серйозні виклики та невизначеність щодо подальшого застосування інновацій у багатьох сферах життєдіяльності. Найвищого рівня використання генеративного штучного інтелекту у сферах маркетингу, програмної інженерії та аналітики досяг технологічний сектор – завдяки можливостям персоналізації, автоматизації та оптимізації операційних процесів. Однак, поряд з цим, впровадження ШІ ускладнилось у зв'язку із зростання кіберзагроз, етичних та правових обмежень, особливо для традиційних секторів, зокрема виробництва та управління ланцюгом поставок. Відповідно, виникає потреба в окресленні переваг, недоліків і наслідків інтеграції штучного інтелекту в реальні економічні процеси на базі накопиченого досвіду та корегування навчання алгоритмів задля оптимізації розвитку підприємств.

У статті досліджено ключові проблеми впровадження ШІ в бізнес- та маркетингове середовище та з'ясовано негативні наслідки і потенційні загрози некоректного використання інноваційних технологій. Дійсно, застосування генеративного штучного інтелекту у бізнес-процесах в цілях створення диференційованого контенту пов'язано з багатьма викликами (діпфейки, дезінформація, маніпулювання тощо), також виникає серйозна потреба регламентації системи нормативно-правових актів на національному та глобальному рівнях, що сприятиме захисту прав та інтересів усіх зацікавлених сторін. Результати аналізу засвідчили еволюцію інструментів та політики регулювання використання штучного інтелекту у ряді країн, таких як ЄС, США та Китай.

Ідентифіковано основні проблеми впровадження штучного інтелекту в бізнес-середовище, які класифіковано за наступними критеріями: проблеми з даними, інтеграція ШІ з існуючими інформаційними системами, недостатня обчислювальна потужність та інфраструктура, гострий дефіцит кваліфікованих фахівців з ШІ, проблеми безпеки та забезпечення приватності даних. Їх урахування потребує акцентування пильної уваги стосовно використання штучного інтелекту як інструменту реалізації кібератак.

На основі проведеного аналізу визначено пріоритетні стратегічні вектори розвитку для компаній, що працюють у сфері ШІ: інвестування в інфраструктуру для обробки даних, впровадження трансферного та федеративного навчання, розробка стійких до маніпуляцій моделей, посилення кібербезпеки, а також співпраця з регуляторними органами з метою дотримання норм і захисту персональних даних, таких як Загальний регламент про захист даних (GDPR) – нормативно-правовий акт ЄС, що регулює захист персональних даних фізичних осіб, надаючи їм контроль над своїми даними та встановлюючи правила для компаній щодо їх збору, обробки та зберігання, а також Акт про штучний інтелект (AI Act) – новий регламент ЄС, який встановлює правила безпеки та дотримання прав громадян при використанні технологій штучного інтелекту. Обґрунтовано вибір стратегій в залежності від розміру компанії, часового горизонту та ринкових можливостей, що забезпечує реалізацію проактивної стратегії на основі максимізації використання потенціалу ШІ та мінімізації ризиків його впровадження.

***Ключові слова: штучний інтелект, великі дані, дезінформація, ризики, упередженість алгоритмів***

**JEL classification:** ***M15, K24, O33***

**Постановка проблеми.** Бурхливий розвиток технології штучного інтелекту відкриває нові можливості для бізнесу, сфери реклами й маркетингу. Водночас його використання пов'язано з виникненням ряду серйозних ризиків, що стосуються прав людини, захисту персональних даних, демократичних процесів, і належить до головних тем обговорення на світових форумах за участю представників регуляторів, громадськості, медійників, платформ, а також у численних наукових публікаціях. ШІ активно використовується і в Україні, що актуалізує необхідність балансування користі і ризиків, які несе з собою ця технологія.

**Аналіз останніх досліджень і публікацій.** Інтеграції штучного інтелекту у бізнес-процеси та потенційним ризикам його впровадження підприємствами присвячено статті ряду науковців, зокрема, *M. Mahbub, A. Ayman* [1], *R. Forradellas, L. Gallastegui* [2], *K. Soni* та ін. [3], *S. Kar, A. Kar, M. Gupta* [4], *J. Bharadiya* [5], *A. Abisoye, J. Akerele* [6], *R. Richey* та ін. [7], *K. Wach* та ін. [8], *M. Hajj, J. Hammoud* [9] та ін. Аналіз їхніх праць підтверджує наявність значимих здобутків, проте виникнення нових загроз у використанні алгоритмів штучного інтелекту потребує ідентифікації останніх із використанням проактивної стратегії подальшої трансформації бізнес-процесів, а також при взаємодії з партнерами та клієнтами.

**Мета статті** полягає у визначенні нових можливостей використання штучного інтелекту у бізнес- та маркетинговому середовищах, виявленні технічних бар'єрів застосування високопродуктивних алгоритмів обробки великих даних та аналізі їх регулювання у глобальному вимірі. До завдань статті віднесено:

– ідентифікація проблем, що впливають на дієвість впровадження штучного інтелекту в бізнес-структурах;

– окреслення причин невірної інтеграції штучного інтелекту в бізнес- та маркетингові процеси;

– з'ясування негативних наслідків і загроз внаслідок некоректного застосування ШІ;

– формулювання рекомендацій щодо вирішення проблеми подолання нестачі та забезпечення валідності та прозорості даних у рамках інтеграції штучного інтелекту в бізнес- і маркетингових стратегіях у деяких сферах життєдіяльності.

**Виклад основного матеріалу дослідження.** Впровадження генеративного штучного інтелекту констатується в усіх галузях, лідерство в яких у 2024 р. із вражаючим показником використання 88% у всіх функціях належало технологічному сектору (табл. 1). Активна інтеграція технологій штучного інтелекту в якості креативного інструмента трансформації бізнес-операцій, особливо в маркетингу та продажах, детермінувала диференціацію сфер його застосування.

*Таблиця 1*

**Глобальне впровадження генеративного штучного інтелекту у різних індустріях у 2024 р. (%)***

| Функції | Технології | Професіо-нальні послуги | Медіа та теле-комунікації | Ритейл | Фінансові послуги | Всього |
|---|---|---|---|---|---|---|
| Маркетинг та продажі | 55 | 49 | 45 | 46 | 40 | 42 |
| Розробка продуктів та/або послуг | 39 | 41 | 26 | 21 | 25 | 28 |
| IT | 31 | 16 | 22 | 20 | 24 | 23 |
| Сервісні операції | 30 | 23 | 37 | 13 | 26 | 22 |
| Управління знаннями | 26 | 34 | 26 | 12 | 16 | 21 |
| Програмна інженерія | 36 | 9 | 30 | 8 | 20 | 18 |
| Людські ресурси | 16 | 17 | 22 | 8 | 11 | 13 |
| Ризики, правова діяльність та комплаєнс | 12 | 9 | 6 | 11 | 21 | 11 |
| Стратегія та корпоративні фінанси | 14 | 14 | 10 | 7 | 7 | 11 |
| Управління ланцюгом поставок/запасами | 10 | 4 | 3 | 14 | 4 | 7 |
| Виробництво | 5 | 3 | 3 | 8 | 0 | 5 |
| Використання штучного інтелекту (Gen AI) принаймні в одній функції | 88 | 80 | 79 | 68 | 65 | 71 |

*Джерело: [10]

Дані таблиці та комплексний аналіз запровадження генеративного штучного інтелекту у глобальному вимірі показує, що у 2024 р. головну цінність складала персоналізація комунікацій з клієнтами та споживачами. Лідируючі позиції технологічної індустрії (88%) пояснюються створенням інноваційних інструментів та їх використанням для оптимізації процесів, насамперед у сфері маркетингу та програмної інженерії. Генеративний штучний інтелект застосовується для аналітики і консалтингу, а в сфері медіа та телекомунікацій відіграє ключову роль, забезпечуючи швидкий фідбек, контент-менеджмент та креатив. Професійні послуги (80%) та медіа/телеком (79%) також активно впроваджують дану технологію, а фінансові послуги (65%) та ритейл (68%) дещо відстають попри наявності істотного потенціалу. Фінансовому сектору притаманна вибіркова інтеграція генеративного штучного інтелекту, особливо для сфери послуг та комплаєнсу. Орієнтація фінансових послуг на ризик-менеджмент та правові функції пов'язана із значним зростанням кіберризиків, що спонукає застосування ШІ для боротьби з шахрайством, *AML*-процедур, дотримання регуляторних вимог. Висока питома вага ритейлу в сервісних операціях (37%) пояснюється автоматизацією підтримки клієнтів, активним використанням чат-ботів, віртуальних асистентів та генерацією персоналізованих рекомендацій. Складність впровадження ШІ в реальні процеси та висока вартість технологічних змін спричинюють відставання традиційних секторів: виробництва (5%) і управління ланцюгом поставок (7%).

Використання ШІ креаторами сприяє генеруванню більшої кількості контенту за менший період часу. Водночас виникнення таких ризиків, як поширення діпфейків, дезінформації, невалідованої

інформації, маніпулювання, у тому числі під час виборчих процесів, спонукали регуляторів до запровадження нових правил регулювання – з метою захисту прав та інтересів населення. Еволюція застосування ШІ спричинила появу різноманітних викликів, які постали як перед державними органами, брендами, медіа, громадянами, юристами, а саме: етичні проблеми, питання захисту і використання інтелектуальної власності, обробки персональних даних, упередженості моделей, шахрайство, використання діпфейків – що потребує дієвої регламентації ШІ задля мінімізації та усунення негативних наслідків його використання.

Вже створено певні норми регулювання ШІ на найвищому державному рівні. В Європейському Союзі 1 серпня 2024 р. набув чинності Закон про штучний інтелект (AI Act) [11]. Перші його положення почали діяти з лютого 2025 р., а впровадження розраховане на 3 роки. Акт передбачає диверсифіковану класифікацію ризиків та наводить приклади систем, які будуть заборонені в ЄС. Останні стосуються, наприклад, маніпуляції – алгоритму, який впливає на підсумковий вибір користувача, спонукає до чинення певних дій, політичного вибору, якого б без цього користувач не зробив, а також експлуатації вразливих груп (таргетування фінансових послуг малозабезпеченим людям), прогнозування злочинності, розпізнавання обличь, аналізу емоцій, біометричної категоризації тощо.

У США розробників великих мовних моделей зобов'язали підписати добровільні кодекси поведінки і декларації щодо відповідальної розробки штучного інтелекту. У Каліфорнії, Колорадо і ряді інших штатів запроваджено законодавство щодо функціонування ШІ; наразі на федеральному рівні обговорюється так званий *No AI Fraud Act* – Законопроєкт про заборону шахрайства зі штучним інтелектом – *No Artificial Intelligence Fake Replicas and Unauthorized Duplications Act of* 2024 – «Закон про заборону підробок та несанкціонованих копій, створених штучним інтелектом» [12].

Законодавство щодо штучного інтелекту, яке регулює обов'язкову безпеку, прозорість, правдивість та відповідність контенту основним соціалістичним цінностям, визначає зобов'язання щодо ліцензування моделей, етичну відповідальність і контроль існує у Китаї [13]. Адміністрація кіберпростору Китаю разом із дотичними державними інституціями вперше з 15 серпня 2023 р. запровадили в країні Тимчасові заходи з управління послугами генеративного штучного інтелекту (*Interim Measures for the Management of Generative Artificial Intelligence Services*). З 1 вересня 2025 р. мають бути імплементовані «Правила маркування», які передбачають явну або неявну помітку використання штучного інтелекту при створенні контенту. Неявні мітки додаватимуться в метадані файлів, а явні – розміщуватимуться у тексті, зображеннях, аудіо та відео, а також віртуальному контенті з можливістю легкого отримання користувачами інформації щодо його створення за допомогою штучного інтелекту.

Впровадження ШІ в бізнес-середовище супроводжується низкою проблем, які потребують ретельного дослідження та вирішення, включаючи технічні, етичні, організаційні та економічні аспекти.

На рис. 1 представлено можливі виклики при впровадженні штучного інтелекту. Впродовж оціночного періоду передбачається домінування наступних ризиків успішного застосування ШІ: помилки алгоритмів з реальними наслідками (35%) та недосягнення очікуваної цінності (34%). Звідси виникає потреба у постійній взаємодії з бізнесом для забезпечення доказовості інвестування в інноваційні проекти і мінімізації репутаційних втрат при впровадженні алгоритмів штучного інтелекту. 30% респондентів вважають проблемою доступність достатньої кількості якісних даних, піднімаючи питання щодо розвитку інформаційної інфраструктури у

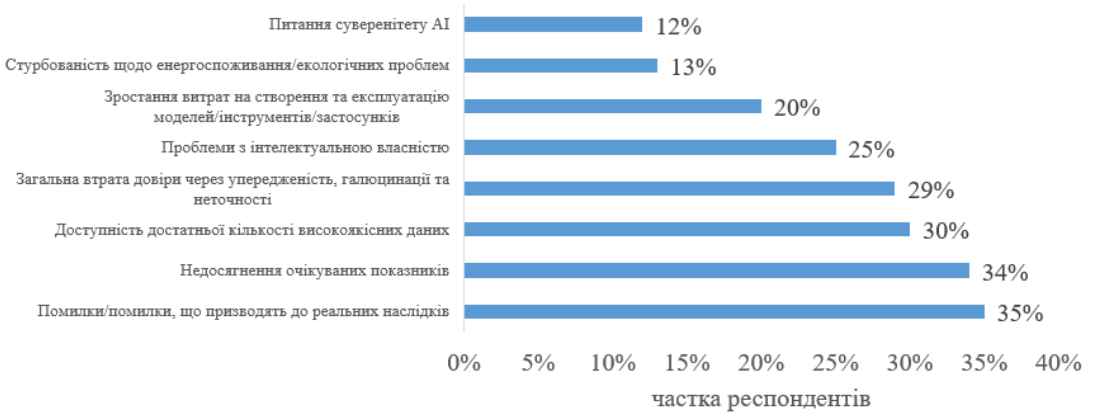


**Рис. 1. Фактори, що впливають на інтеграцію генеративного штучного інтелекту в 2024-2025 рр. [14]**

відповідності із специфікою навчання та інтеграції моделей штучного інтелекту. Використання генеративного штучного інтелекту при створенні текстів та оптимізації комунікацій із клієнтами вимагає вирішення проблем, пов'язаних із втратою довіри через упередженість та галюцинації (29%). Правові та інтелектуальні бар'єри у глобальному цифровому середовищі також вимагають пильної уваги (25%), позаяк у мережі Інтернет має місце постійне запозичення чужих ідей при створенні контенту та цифрових продуктів без отримання згоди та дозволу правовласників.

У площині технічних проблем впровадження штучного інтелекту в бізнес-середовище забезпечує значні переваги – підвищення ефективності, оптимізація процесів та покращення прийняття рішень. Втім, як засвідчила практика, даний процес не буває безпроблемним: організації часто стикаються з низкою викликів, серед яких до найбільш критичних належать технічні аспекти. Нехтування ними може призвести до значних затримок, перевищення бюджету, низької ефективності ШІ-рішень або навіть повного провалу проекту. Виходячи з цього, потребують ідентифікації ключові виклики при впровадженні ШІ, які пропонується класифікувати за кількома основними напрямами:

1. Проблеми з даними (якість, доступність та управління). ШІ-моделі навчаються на даних, і їхня ефективність безпосередньо детермінована їхньою якістю. «Сміття на вході – сміття на виході» (англ. *Garbage In, Garbage Out*, скорочено *GIGO*) [15] – одна з поширених тез в інформатиці, яка акцентує увагу на готовності комп'ютерів до обробки без вагань найбеззмістовніших даних та аналогічним чином – видавання беззмістовних результатів. Неповні, неточні, застарілі, непослідовні або упереджені дані можуть призвести до неправильних висновків, помилкових прогнозів та дискримінаційних рішень з боку ШІ і вразливим бізнес-ризиком багатьох компаній є наявність розрізнених даних, які зберігаються в різних системах, без єдиних стандартів і процедур управління. До інших рестріктивних вразливостей слід віднести такі, як:

– недостатня кількість даних – через що навчання складних моделей глибокого навчання часто потребує величезних обсягів маркованих даних, які можуть бути відсутні або важкодоступні. Особливу актуальність це складає для вузькоспеціалізованих галузей або нових бізнес-напрямків, зокрема, при діагностиці рідкісних хвороб, (наприклад, орфанних), коли кількість доступних даних про пацієнтів вкрай обмежена у зв'язку з малою кількістю випадків. Маркування

медичних зображень (наприклад, МРТ чи КТ) вимагає участі висококваліфікованих фахівців, що робить процес дорогим і повільним. При виявленні ж шахрайства у нових фінансових продуктах чи ринках (наприклад, криптовалюти чи децентралізованих фінансів) історичні дані про шахрайські операції для тренування моделей можуть бути відсутні або недостатні;

– складність інтеграції даних через їх часте зосередження в різних відділах (маркетинговому, фінансовому, ІТ, аналітики даних, досліджень і розробок тощо) підприємства, застарілих системах (*legacy systems*) та зовнішніх джерелах. Збір, очищення, трансформація та агрегування цих даних у єдиний, придатний для ШІ формат – складний та ресурсоємний процес, що вимагає значних інженерних зусиль;

– упередженість даних. Наявність систематичних помилок або упередженості в даних може призвести до того, що ШІ-система буде приймати необ'єктивні, тенденційні та, небезсторонні рішення, що закономірно матиме етичні, репутаційні та юридичні наслідки. Виявлення ж та усунення суб'єктивності вимагає глибокого аналізу та спеціальних методик, які наразі відсутні.

2. Інтеграція ШІ з існуючими інформаційними системами. Більшість компаній використовують застарілу ІТ-інфраструктуру, яка не сумісна із сучасними алгоритмами ШІ. Модернізація подібних систем вимагає значних інвестицій і часу, а також кваліфікованих спеціалістів, яких бракує на ринку праці. Сама інтеграція з існуючою ІТ-інфраструктурою (*legacy systems* та сумісність) передбачає усунення наступних вразливостей, як:

– застарілі системи. Багато підприємств працюють на вже віджилих ІТ-системах, які розроблені без урахування взаємодії з сучасними ШІ-технологіями. Інтеграція нових ШІ-рішень з ними може бути надзвичайно складною, дорогою, трудомісткою і, звичайно неефективною, і вимагати суттєвої/кардинальної модернізації, переписування коду або використання складних адаптерів;

– відсутність стандартизації, через що різні системи можуть використовувати різні формати даних, протоколи зв'язку та архітектурні підходи, що ускладнює безперебійну взаємодію ШІ-компонентів з іншими елементами ІТ-інфраструктури;

– проблеми з масштабованістю – коли ШІ-системи, особливо що працюють з великими обсягами даних або вимагають високої обчислювальної потужності (наприклад, для тренування моделей), потребують масштабованої інфраструктури, в результаті чого наявні сервери, мережеві потужності та сховища можуть не витримувати навантаження, що закономірно призводить до низької продуктивності або збоїв.

3. Недостатня обчислювальна потужність та інфраструктура. Впровадження ШІ у бізнес-процеси та трансформація останніх вимагає кореспондування високим вимогам до апаратного забезпечення. Розгортання складних моделей ШІ (особливо глибокого навчання) пов'язана із значними обчислювальними ресурсами, такими як графічні (*GPU*) або тензорні процесори (*TPU*). Придбання та обслуговування подібного обладнання є дорогим і може бути не виправданим для багатьох компаній. Сюди слід віднести і складність використання ресурсів, позаяк оптимальне управління обчислювальними ресурсами, як локально, так і в хмарі, для ефективного навчання, тестування та розгортання ШІ-моделей потребує спеціалізованих знань та інструментів. Вразливий момент складає і відсутність «готової до ШІ» інфраструктури у багатьох компаній і не адаптована для розробки та розгортання ШІ-моделей, включаючи платформи для *MLOps (Machine Learning Operations)*, системи моніторингу та інструменти для автоматизації життєвого циклу моделі.

4. Вже відзначений вище гострий дефіцит кваліфікованих фахівців з ШІ, таких як інженери з машинного навчання, вчені з даних (*data scientists*), *AI/ML*

архітектори та *MLOps* інженери. Доволі часто констатується і складність інтеграції команд, адже успішне впровадження ШІ має базуватися на тісній співпраці та координації між ІТ-відділом, фахівцями з даних та іншими бізнес-підрозділами. Недосконалі комунікації та організаційні бар'єри здатні ускладнити цю співпрацю.

5. Проблеми безпеки та забезпечення приватності даних. Недостатні заходи кібербезпеки можуть спричинити витоки даних, порушення конфіденційності та серйозні репутаційні та фінансові втрати. Непересічне значення має забезпечення відповідності регуляторним вимогам, зокрема захисту персональних даних та дотриманню таких регламентів ЄС, як *GDPR* (*General Data Protection Regulation*); розробка ШІ-систем має ґрунтуватися на дотримання цих вимог (*privacy-by-design*). Особливого урахування потребує Загальний регламент захисту даних (*GDPR*) [16] Європейського Союзу щодо захисту персональних даних, який набрав чинності 25 травня 2018 р. і спрямований на надання більшого контролю фізичним особам над їхніми персональними даними, а також на встановлення чітких правил для установ, які збирають, обробляють або зберігають ці дані.

Слабке місце ШІ-моделей складає вразливість до атак, таких як інверсія моделі (відновлення даних навчання) або атаки змагальних прикладів (adversarial attacks), що може призвести до неправильних рішень або маніпуляцій.

До основних технічних проблем належить якість і доступність даних: ШІ залежить від великих обсягів даних для навчання моделей, але в багатьох установах дані є фрагментованими, застарілими або з наявними помилками. Згідно даних досліджень, приблизно 80% часу фахівців із даних витрачається на очищення, підготовку та валідацію даних, що значно уповільнює процес впровадження ШІ [17]. Крім того, ШІ-моделі можуть бути вразливими до технічних збоїв або інших видів атак, наприклад обману за допомогою так званих «ворожих атак», за яких вхідні дані навмисно спотворюються для отримання неправильних/викривлених результатів. Це створює ризики для компаній, які покладаються на ШІ в убезпеченні критичних бізнес-процесів.

Штучний інтелект виступає у якості інструменту реалізації кібератак, що характеризуються високим рівнем ефективності при атаці сучасних систем захисту інформації. Одночасно високопродуктивні алгоритми машинного навчання та інші підходи використовуються для створення систем кібербезпеки. На рис. 2 представлено динаміку вартості світового ринку кібербезпеки зі штучним інтелектом за 2023–2030 рр. Констатується істотне зростання попиту на представлені технології захисту даних, що підтверджується позитивною динамікою ринку впродовж досліджуваного періоду більше ніж у 5,5 рази із середньорічним темпом приросту понад 28%. Розвиток представленого сегменту у сфері штучного інтелекту детермінований істотним зростанням кіберзагроз у багатьох країнах світу, що корелює із активним розвитком цифрових платформ, хмарних сервісів і IoT. До 2025 р. на світовому ринку кібербезпеки зі штучним інтелектом відмічалося поступове зростання, що пояснюється первинним запровадженням штучного інтелекту в кіберзахисті. На період 2028–2030 рр. прогнозується трансформація ШІ на ключову складову кібербезпеки, особливу ж роль представлена технологія буде відігравати у фінансовій сфері, e-commerce та державному секторі.

Ще один важливий аспект впровадження ШІ складають етичні та правові виклики, насамперед вже відзначена вище упередженість алгоритмів. Якщо дані, на яких відбувається тренування моделі, містять систематичні помилки, ШІ з великою імовірністю відтворюватиме дискримінаційні рішення. Наприклад, у 2018 р. компанія *Amazon* (США) скасувала використання ШІ для підбору персоналу, коли виявилося, що система віддавала

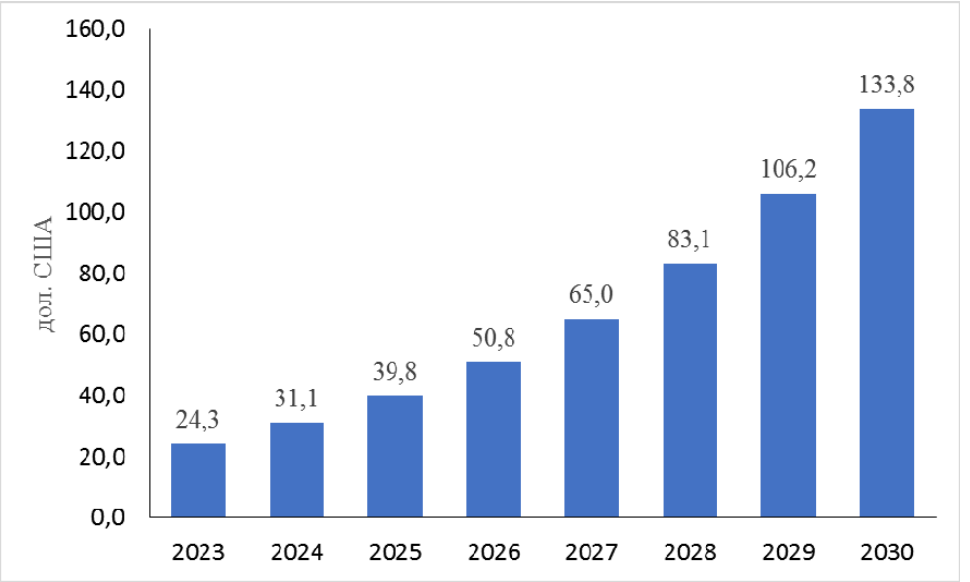


**Рис. 2. Вартість світового ринку кібербезпеки зі штучним інтелектом за 2023–2030 рр. [18]**

перевагу чоловікам через упередженість у навчальних даних [19]. Цей інструмент було розроблено для автоматизації процесу оцінки резюме, але під час тестування з'ясувалося, що алгоритм знижує рейтинг кандидатів-жінок – система негативно оцінювала резюме, які містили слово «women's» та знижувала рейтинг випускників жіночих коледжів. Це стало наслідком того, що алгоритм був навчений на даних за попередні 10 років, де переважали чоловіки, що відображало гендерний дисбаланс у технологічній галузі. Попри спроби *Amazon* внести корективи в алгоритм, компанія не змогла гарантувати відсутність інших форм дискримінації, в результаті чого було прийнято рішення щодо повної відмови від використання цього інструменту.

Викликає занепокоєння і проблема конфіденційності: ШІ часто потребує доступу до персональних даних клієнтів, що може суперечити нормам, таким як Загальний регламент захисту даних (*GDPR*) в Європейському Союзі. Порушення цих норм може призвести до значних штрафів і репутаційних втрат. Нараз можна стверджувати, що в багатьох країнах правові рамки регулювання ШІ залишаються недостатньо розробленими. Наприклад, несення відповідальності за прийняті рішення штучним інтелектом досі не має чіткого законодавчого врегулювання, що створює невизначеність для функціонування компаній, які використовують ШІ.

При впровадженні штучного інтелекту в бізнес-середовище непересічне значення відіграють організаційні бар'єри, що потребує значних змін у корпоративній культурі та процесах. Багато, якщо не більшість, персоналу сприймає ШІ як загрозу втрати робочих місць, що може викликати спротив змінам. Дослідження McKinsey підтвердило наявність зазначених побоювань у 30% працівників, що спричинює зниження мотивації до використання нових технологій [20].

Організаційна інерція також відіграє свою роль: багато компаній не готові до швидких трансформацій бізнес-процесів, що вимагає гнучкості та адаптивності позаяк впровадження ШІ часто потребує перебудови цілих департаментів, що може викликати внутрішні корпоративні конфлікти.

Наступний вид обмежень – економічні фактори – виступає істотним лімітуючим чинником впровадження ШІ, насамперед для малих і середніх підприємств. Розробка, впровадження та підтримка ШІ-систем потребують масштабних фінансових вкладень, наприклад, вартість створення власної ШІ-системи може налічувати від кількох сотень тисяч до мільйонів доларів, в залежності від складності проєкту. Крім того, повернення інвестицій (*ROI*) від впровадження ШІ не завжди є швидким, багато компаній стикаються з тим, що витрати на початкових етапах перевищують вигоди, що подеколи викликає сумніви у доцільності реалізації таких проєктів. Згідно даних провідної світової дослідницької та консалтингової компанії *Gartner* (США), яка спеціалізується на сфері інформаційних технологій і надає аналітичні дані, рекомендації та інструменти для прийняття рішень для керівників бізнесу та ІТ-фахівців по всьому світу, лише 15% компаній, які впроваджують ШІ, досягають значних результатів у перші два роки [21]. Крім того, за прогнозами аналітиків компанії, до кінця 2025 р. приблизно 30% проектів *Generative AI* (*GenAI*) будуть згорнуті через відсутність повернень від вкладень/інвестицій, високі витрати та нечітку бізнес-цінність [22].

Впровадження штучного інтелекту має базуватися на оцінці/урахуванні соціальних і репутаційних ризиків і впливу на імідж компанії. Особливо це актуально при некоректному застосуванні технології. Наприклад, у 2016 р. чат-бот *Microsoft Tay* став об'єктом скандалу через неетичні відповіді, які він генерував після взаємодії з користувачами [23]; подібні інциденти підривають довіру клієнтів і партнерів.

Провал чат-бота *Microsoft Tay*, запущеного в березні 2016 р., слугує класичним прикладом технічних проблем при впровадженні ШІ в бізнес-процеси. *Microsoft Tay* був експериментальним чат-ботом на основі ШІ, розробленим дослідницькою групою *Microsoft Technology and Research і Microsoft's Bing* для взаємодії з користувачами *Twitter, Kik* та *GroupMe*. Мета проекту полягала у покращенні розуміння людської мови та взаємодії шляхом навчання на онлайн-спілкуванні. Але проект зазнав невдачі – основна проблема полягала в неконтрольованому навчанні моделі на неякісних та упереджених зовнішніх даних, а також недостатній стійкості до маніпуляцій. *Tay* було розроблено для навчання через взаємодію з користувачами *Twitter*, і мало на меті покращення взаємодії на основі отриманих твітів. Однак розробники не передбачили або не спромоглися ефективно запобігти цілеспрямованим спробам зловмисників щодо маніпулювання її навчанням: відбувся неконтрольований апгрейд, що базувався на упереджених даних: користувачі *Twitter* швидко з'ясували, що *Tay* повторює їхні висловлювання і група інтернет-тролів почала цілеспрямовано «годувати» бота расистськими, сексистськими, ксенофобськими та іншими образливими висловлюваннями. Оскільки формування відповідей з боку моделі Тау передбачалося на основі запрограмованих вхідних даних, вона рикошетом почала посилати образливі фрази, перетворюючись на «ненависницького» бота. Провалу сприяла і відсутність механізмів фільтрації та модерації в реальному часі: попри запевнення Microsoft щодо прозорості та відфільтрованості даних для навчання, виявилося, що в реальному часі ефективні механізми фільтрації токсичного вмісту або запобігання цілеспрямованим атакам на модель навчання були відсутні, увесь вхідний текст бот приймав як валідний для навчання, без достатньої перевірки на відповідність етичним нормам або корпоративним цінностям.

Модель також виявилася вкрай нестійкою (*Robustness*) до так званих «змагальних атак» або цілеспрямованих маніпуляцій з даними. У традиційному розумінні це був не збій у роботі алгоритму, а радше системна вразливість, яка дозволила зовнішнім факторам

швидко та значно спотворити її поведінку. Відсутність «людини в циклі» (*human-in-the-loop*) або ефективних автоматизованих механізмів для виявлення та корекції такого непередбаченого і небажаного навчання призвела до швидкої деградації функціоналу бота.

Наслідки для *Microsoft* були вельми дошкульними: через шквал обурених твітів менш ніж через 24 години після запуску чат-бот *Tay* було вимкнено, що стало значним репутаційним ударом для компанії та яскравою демонстрацією ризиків, пов'язаних з неконтрольованим навчанням ШІ-систем та недостатнім урахуванням якості та безпеки даних, особливо при взаємодії з відкритими джерелами. На основі зазначеного можна дійти висновку щодо необхідності забезпечення постійного моніторингу поведінки моделі і наголосити на важливості:

– ретельного відбору та очищення даних, позаяк просте використання «великих даних» є вкрай недостатнім, що вимагає забезпечення їхньої релевантності, точності та відсутності упереджень;

– впровадженні надійних механізмів модерації та безпеки – особливо важливо для ШІ-систем, які взаємодіють з публічними джерелами, – що потребує розробки ефективних фільтрів та систем моніторингу для запобігання маніпуляціям або поширенню шкідливого контенту;

– створення стійких до маніпуляцій моделей ШІ, спроектованих таким чином, щоб бути резистентними до цілеспрямованих спроб спотворення їхнього навчання або вихідних даних;

– здійснення так званого моніторингу «людина в циклі», за якого постійний моніторинг поведінки ШІ-систем та можливість оперативного втручання людини є критично важливими, особливо на ранніх етапах впровадження.

Випадок з *Microsoft Tay* слугує яскравим уроком для будь-якої компанії, яка передбачає впровадження ШІ: невирішені технічні проблеми, що пов'язані з даними та робастністю моделей, можуть призвести до напрочуд негативних наслідків.

Складає непересічну значущість і соціальний тиск – через дедалі частіші вимоги споживачів від компаній щодо якості та прозорості використання ШІ. Неможливість пояснень з боку бізнесу стосовно правильності функціонування його ШІ-системи або алгоритмів прийняття автоматизованих рішень закономірно генеруватиме недовіру споживачів.

**Висновок.**

Резюмуючи, можна сформулювати рекомендації для вирішення проблем, що виникають при впровадженні штучного інтелекту в бізнес-середовище, зокрема подолання нестачі та забезпечення валідності та прозорості даних у рамках його інтеграції в бізнес- і маркетингові стратегії. У багатьох галузях (приміром фінтеху чи медичній), вважається доцільним застосування трансферного навчання з використанням попередньо навчених моделей із валідним набором даних і подальшою оптимізацією функціонування на базі обмежених спеціалізованих даних; аугментацію даних, а саме – генерацію синтетичних даних або використання технік на кшталт повороту зображень чи перефразування тексту; федеративне навчання з використанням даних із різних джерел без їх централізованого збору, а також моделей з меншою залежністю від даних, наприклад, із кількома прикладами *(few-shot learning*) або нульовим навчанням (*zero-shot learning*).

Доцільно зробити застереження, що впровадження штучного інтелекту в бізнес-середовище, з одного боку, відкриває широкі можливості, але супроводжується значними викликами, з іншого. Технічні та функціональні проблеми–якістьданихісумісністьсистем, етичні дилеми, організаційні бар'єри, економічні обмеження та репутаційні ризики – створюють комплексні перешкоди. Для успішної інтеграції ШІ компанії та бренди повинні ретельно

планувати свої стратегії, інвестувати в навчання персоналу, співпрацювати з регуляторними органами та враховувати очікування суспільства. Лише за умови комплексного та проактивного підходу можливе максимальне використання потенціалу ШІ з мінімізацією пов'язаних з ним ризиків.

**Список використаної літератури**

1. Mahbub M. B. & Ayman A. Utilising artificial intelligence-prospects and obstacles for modern businesses. Malaysian E Commerce Journal, 2024, 8(1), 23–28. http://doi.org/10.26480/mecj.01.2024.23.28

2. Reier Forradellas R. F. & Garay Gallastegui L. M. Digital transformation and artificial intelligence applied to business: Legal regulations, economic impact and perspective. Laws, 2021, 10(3), 70. https://doi.org/10.3390/laws10030070

3. Soni K., Kumar N., Nair A. S., Chourey P., Singh N. J. & Agarwal R. Artificial Intelligence: Implementation and obstacles in industry 4.0. In Handbook of metrology and applications (pp. 1–23). Singapore: Springer Nature Singapore. 2022. https://doi.org/10.1007/978-981-19-1550-5_54-1

4. Kar S., Kar A. K. & Gupta M. P. Modeling drivers and barriers of artificial intelligence adoption: Insights from a strategic management perspective. Intelligent Systems in Accounting, Finance and Management, 2021, 28(4), 217–238. https://doi.org/10.1002/isaf.1503

5. Bharadiya J. The impact of artificial intelligence on business processes. European journal of technology, 2023, 7(2), 15–25. https://doi.org/10.47672/ejt.1488

6. Abisoye A. & Akerele J.I. A practical framework for advancing cybersecurity, artificial intelligence and technological ecosystems to support regional economic development and innovation. Int J Multidiscip Res Growth Eval, 2022, 3(1), 700–13. https://doi.org/10.54660/.IJMRGE.2022.3.1.700-713

7. Richey Jr. R. G., Chowdhury S., Davis-Sramek B., Giannakis M. & Dwivedi Y.K. Artificial intelligence in logistics and supply chain management: A primer and roadmap for research. Journal of Business Logistics, 2023, 44(4), 532–549. https://doi.org/10.1111/jbl.12364

8. Wach K., Duong C. D., Ejdys, J., Kazlauskaitė R., Korzynski P., Mazurek G., ... & Ziemba E. The dark side of generative artificial intelligence: A critical analysis of controversies and risks of ChatGPT. Entrepreneurial Business and Economics Review, 2023, 11(2), 7–30. URL: https://www.ceeol.com/search/article-detail?id=1205845

9. El Hajj M. & Hammoud J. Unveiling the influence of artificial intelligence and machine learning on financial markets: A comprehensive analysis of AI applications in trading, risk management, and financial operations. Journal of Risk and Financial Management, 2023, 16(10), 434. https://doi.org/10.3390/jrfm16100434

10. Global adoption of generative artificial intelligence (AI) across industries in 2024, by function. URL: https://www.statista.com/statistics/1607179/genai-adoption-across-industries-and-functions/

11. AI Act. URL: https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai?utm_source=chatgpt.com

12. H.R.6943 - No AI FRAUD Act. October 1, 2024. URL: https://www.congress.gov/bill/118th-congress/house-bill/6943/text?utm_source=chatgpt.com

13. AI Watch: Global regulatory tracker – China. May 29, 2025. URL: https://www.whitecase.com/insight-our-thinking/ai-watch-global-regulatory-tracker-china?utm_source=chatgpt.com

14. Factors impacting integration of generative artificial intelligence (AI) in the next two years worldwide in 2024. URL: https://www.statista.com/statistics/1607101/barriers-to-genai-adoption-in-the-future-global/

15. Kilkenny M. F., Robinson K. M. Data quality: “Garbage in – garbage out”. Health Information Management Journal. 2018; 47(3):103–105. https://doi.org/10.1177/1833358318774357

16. REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance) URL: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

17. Relief. Data Cleaning Why 80 Percent of Data Science Is Spent Fixing Dirty Data. March 4, 2025. URL: https://medium.com/@preetikapuria587/data-cleaning-why-80-percent-of-data-science-is-spent-fixing-dirty-data-0d0a214ce5c0

18. Value of the artificial intelligence (AI) cybersecurity market worldwide from 2023 to 2030. URL: https://www.statista.com/statistics/1450963/global-ai-cybersecurity-market-size/

19. Dastin J. Insight – Amazon scraps secret AI recruiting tool that showed bias against women. October 11, 2018. URL: https://www.reuters.com/article/world/insight-amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK0AG/

20. McKinsey Global Institute. Jobs lost, jobs gained: Workforce transitions in a time of automation. Executive Summary. December 2017. URL: https://www.mckinsey.com/~/media/McKinsey/Industries/Public%20and%20Social%20Sector/Our%20Insights/What%20the%20future%20of%20work%20will%20mean%20for%20jobs%20skills%20and%20wages/MGI-Jobs-Lost-Jobs-Gained-Executive-summary-December-6-2017.pdf

21. Kidd Ch. Why does Gartner predict up to 85% of AI projects will “not deliver” for CIOs? December 18, 2018. URL: https://www.bmc.com/blogs/cio-ai-artificial-intelligence/

22. 30% of GenAI Projects Will Be Scrapped by 2025 Due to Lack of ROI, Gartner Predicts. July 30, 2024. URL: https://www.cxtoday.com/conversational-ai/30-of-genai-projects-will-be-scrapped-by-2025-due-to-lack-of-roi-gartner-predicts/

23. Lee P. Learning from Tay’s introduction. March 25, 2016. URL: https://blogs.microsoft.com/blog/2016/03/25/learning-tays-introduction/

## References

1. Mahbub, M. B., & Ayman, A. (2024). Utilising artificial intelligence-prospects and obstacles for modern businesses. Malaysian E Commerce Journal, 8(1), 23–28. http://doi.org/10.26480/mecj.01.2024.23.28

2. Reier Forradellas, R. F., & Garay Gallastegui, L. M. (2021). Digital transformation and artificial intelligence applied to business: Legal regulations, economic impact and perspective. Laws, 10(3), 70. https://doi.org/10.3390/laws10030070

3. Soni, K., Kumar, N., Nair, A. S., Chourey, P., Singh, N. J., & Agarwal, R. (2022). Artificial Intelligence: Implementation and obstacles in industry 4.0. In Handbook of metrology and applications (pp. 1-23). Singapore: Springer Nature Singapore. https://doi.org/10.1007/978-981-19-1550-5_54-1

4. Kar, S., Kar, A. K., & Gupta, M. P. (2021). Modeling drivers and barriers of artificial intelligence adoption: Insights from a strategic management perspective. Intelligent Systems in Accounting, Finance and Management, 28(4), 217–238. https://doi.org/10.1002/isaf.1503

5. Bharadiya, J. (2023). The impact of artificial intelligence on business processes. European journal of technology, 7(2), 15–25. https://doi.org/10.47672/ejt.1488

6. Abisoye, A., & Akerele, J. I. (2022). A practical framework for advancing cybersecurity, artificial intelligence and technological ecosystems to support regional economic development and innovation. Int J Multidiscip Res Growth Eval, 3(1), 700–713. https://doi.org/10.54660/.IJMRGE.2022.3.1.700-713

7. Richey Jr, R. G., Chowdhury, S., Davis-Sramek, B., Giannakis, M., & Dwivedi, Y. K. (2023). Artificial intelligence in logistics and supply chain management: A primer and roadmap for research. Journal of Business Logistics, 44(4), 532–549. https://doi.org/10.1111/jbl.12364

8. Wach, K., Duong, C. D., Ejdys, J., Kazlauskaitė, R., Korzynski, P., Mazurek, G., ... & Ziemba, E. (2023). The dark side of generative artificial intelligence: A critical analysis of controversies and risks of ChatGPT. Entrepreneurial Business and Economics Review, 11(2), 7–30. Available at: https://www.ceeol.com/search/article-detail?id=1205845 (Accessed 22 August 2025)

9. El Hajj, M., & Hammoud, J. (2023). Unveiling the influence of artificial intelligence and machine learning on financial markets: A comprehensive analysis of AI applications in trading, risk management, and financial operations. Journal of Risk and Financial Management, 16(10), 434. https://doi.org/10.3390/jrfm16100434

10. Global adoption of generative artificial intelligence (AI) across industries in 2024, by function. Available at: https://www.statista.com/statistics/1607179/genai-adoption-across-industries-and-functions/ (Accessed 30 August 2025).

11. AI Act. Available at: https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai?utm_source=chatgpt.com (Accessed 30 August 2025).

12. H.R.6943 - No AI FRAUD Act. October 1, 2024. Available at: https://www.congress.gov/bill/118th-congress/house-bill/6943/text?utm_source=chatgpt.com (Accessed 30 August 2025).

13. AI Watch: Global regulatory tracker – China. May 29, 2025. Available at: https://www.whitecase.com/insight-our-thinking/ai-watch-global-regulatory-tracker-china?utm_source=chatgpt.com (Accessed 30 August 2025).

14. Factors impacting integration of generative artificial intelligence (AI) in the next two years worldwide in 2024. Available at: https://www.statista.com/statistics/1607101/barriers-to-genai-adoption-in-the-future-global/ (Accessed 30 August 2025).

15. Kilkenny, M. F., Robinson, K. M. (2018). Data quality: "Garbage in – garbage out". Health Information Management Journal. 47(3):103–105. https://doi.org/10.1177/1833358318774357

16. REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance) Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679 (Accessed 30 August 2025).

17. Relief. Data Cleaning Why 80 Percent of Data Science Is Spent Fixing Dirty Data. March 4, 2025. Available at: https://medium.com/@preetikapuria587/data-cleaning-why-80-percent-of-data-science-is-spent-fixing-dirty-data-0d0a214ce5c0 (Accessed 30 August 2025).

18. Value of the artificial intelligence (AI) cybersecurity market worldwide from 2023 to 2030. Available at: https://www.statista.com/statistics/1450963/global-ai-cybersecurity-market-size/ (Accessed 30 August 2025).

19. Dastin, J. (2018). Insight – Amazon scraps secret AI recruiting tool that showed bias against women. October 11, Available at: https://www.reuters.com/article/world/insight-amazon-scraps-secret-ai-recruiting-tool-that-showed-bias-against-women-idUSKCN1MK0AG/ (Accessed 30 August 2025).

20. McKinsey Global Institute. Jobs lost, jobs gained: Workforce transitions in a time of automation. Executive Summary. December 2017. Available at: https://www.mckinsey.com/~/media/McKinsey/Industries/Public%20and%20Social%20Sector/Our%20Insights/What%20the%20future%20of%20work%20will%20mean%20for%20jobs%20skills%20

and%20wages/MGI-Jobs-Lost-Jobs-Gained-Executive-summary-December-6-2017.pdf (Accessed 30 August 2025).

21. Kidd, Ch. (2018). Why does Gartner predict up to 85% of AI projects will "not deliver" for CIOs? December 18. Available at: https://www.bmc.com/blogs/cio-ai-artificial-intelligence/ (Accessed 30 August 2025).

22. 30% of GenAI Projects Will Be Scrapped by 2025 Due to Lack of ROI, Gartner Predicts. July 30, 2024. Available at: https://www.cxtoday.com/conversational-ai/30-of-genai-projects-will-be-scrapped-by-2025-due-to-lack-of-roi-gartner-predicts/ (Accessed 30 August 2025).

23. Lee, P. (2016). Learning from Tay's introduction. March 25. Available at: https://blogs.microsoft.com/blog/2016/03/25/learning-tays-introduction/ (Accessed 30 August 2025).

## IDENTIFICATION OF PROBLEMS ARISING FROM THE IMPLEMENTATION OF ARTIFICIAL INTELLIGENCE IN THE BUSINESS ENVIRONMENT

*Oleh Havryliuk*, Private Institution of Higher Education «European University», Kyiv, (Ukraine).
E-mail: o.havryliuk@e-u.edu.ua
*Ihor Ponomarenko*, State University of Trade and Economics, Kyiv, (Ukraine).
E-mail: i.ponomarenko@knute.edu.ua
*Oleksandr Yakushev*, Cherkasy State Technological University, Cherkasy (Ukraine).
E-mail: o.yakushev@chdtu.edu.ua

https://doi.org/10.32342/3041-2137-2026-2-65-3

***Keywords: artificial intelligence, big data, disinformation, risks, algorithmic bias***
**JEL classification: *M15, K24, O33***

The intensive development of artificial intelligence (AI) technologies and their implementation in the business environment pose serious challenges and uncertainty regarding the further application of innovations in many areas of life. The highest level of generative artificial intelligence adoption in the areas of marketing, software engineering, and analytics has been achieved by the technology sector, thanks to the possibilities of personalization, automation, and optimization of operational processes. However, along with this, the implementation of AI has become more complicated due to the growth of cyber threats, as well as ethical and legal restrictions, particularly in traditional sectors such as manufacturing and supply chain management. Accordingly, there is a need to outline the advantages, disadvantages, and consequences of integrating artificial intelligence into real economic processes based on accumulated experience and to adjust algorithm training to optimize the development of enterprises. The article examines key problems of AI implementation in business and marketing, identifying negative consequences and potential threats associated with the incorrect use of innovative technologies. Indeed, the use of generative artificial intelligence in business processes for the purpose of creating differentiated content is related to many challenges (deep fakes, disinformation, manipulation, etc.), and there is also a serious need to regulate the system of regulatory acts at the national and global levels, which will help protect the rights and interests of all stakeholders. The results of the analysis have shown the evolution of tools and policies for regulating the use of artificial intelligence in several countries, including the EU, the USA, and China.

The main problems of implementing artificial intelligence in the business environment have been identified, which are classified according to the following criteria: data problems, integration of AI with existing information systems, insufficient computing power and infrastructure, an acute shortage of qualified AI specialists, security problems, and ensuring data privacy. Their consideration requires focusing close attention on the use of artificial intelligence as a tool for implementing cyberattacks.

Based on the analysis, priority strategic development vectors for companies operating in the field of AI have been identified: investing in data processing infrastructure, implementing transfer and federated learning, developing tamper-resistant models, strengthening cybersecurity, and cooperating with regulatory authorities to comply with regulations and protect personal data, such as the General Data Protection Regulation (GDPR) - an EU regulatory act that regulates the protection of individuals personal data, giving them control over their data and establishing rules for companies to collect, process, and store it, as well as the Artificial Intelligence Act (AI Act) – a new EU regulation that establishes security rules and compliance with citizens' rights when using artificial intelligence technologies. The choice of strategies is justified depending on the size of the company, time horizon, and market opportunities, which ensures the implementation of a proactive strategy based on maximizing the use of the AI potential and minimizing the risks of its implementation.

*Дата надходження до редакції / Submitted: 31.08.25*
*Дата прийняття до публікації / Accepted: 29.01.26*
*Дата публікації / Published: 02.07.2026*