Електронний журнал «Ефективна економіка» включено до переліку наукових фахових видань України з питань економіки (Категорія «Б», Наказ Міністерства освіти і науки України № 975 від 11.07.2019). Спеціальності – 051, 071, 072, 073, 075, 076, 292.

Ефективна економіка. 2025. № 3.

DOI: http://doi.org/10.32702/2307-2105.2025.3.7
УДК [34:005.5]:004.8](061.1ЄС+477)

І. Г. Яненкова,
д. е .н., доцент, провідний науковий співробітник сектору цифрової економіки, ДУ «Інститут економіки та прогнозування НАН України»
ORCID ID: https://orcid.org/0000-0002-7007-4481

РЕГУЛЮВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ В ЄС: УРОКИ ДЛЯ УКРАЇНИ

I. Yanenkova,
Doctor of Economic Science, Associate professor, Leading researcher of the Digital economy Sector, State Organization «Institute for Economics and Forecasting of National academy of Science of Ukraine»

REGULATION OF ARTIFICIAL INTELLIGENCE IN THE EU: LESSONS FOR UKRAINE

У статті проведено аналіз основних законодавчих і нормативних актів Європейського союзу в галузі використання штучного інтелекту. Основну увагу зосереджено на Законі про штучний інтелект (Регламент (ЄС) 2024/1689), його проблемних місцях, узгодженості з іншими законодавчими актами та особливостях впровадження. Висвітлено зміст поетапного впровадження положень Закону про штучний інтелект у контексті впливу на перспективи діяльності бізнесу, що підпадає під вимоги

даного закону. Розроблено рекомендації для бізнесових структур щодо підготовки до відповідності вимогам Закону про штучний інтелект. Визначено ключові акценти, які можуть бути використані урядовими структурами України для адаптації законодавчих ініціатив ЄС щодо штучного інтелекту до умов національної економіки. Зокрема, створення репозиторію для підтримки грамотності штучного інтелекту, увага моделям штучного інтелекту загального призначення, відповідальність у ланцюжку створення вартості для систем високого ризику, забезпечення авторського права тощо. Зроблено наголос на необхідності інвестування у технології штучного інтелекту, зокрема для забезпечення безпечного їх впровадження та використання.

The article analyzes the main legislative and regulatory acts of the European Union in the field of artificial intelligence. The main attention is focused on the Law on Artificial Intelligence (Regulation (EU) 2024/1689), its problematic areas, consistency with other legislative acts and implementation features. The content of the phased implementation of the provisions of the Law on Artificial Intelligence is highlighted in the context of the impact on the prospects of business activities falling under the requirements of this law. Recommendations are developed for business structures on preparing to comply with the requirements of the EU AI Act. Key accents are identified that can be used by government structures of Ukraine to adapt EU legislative initiatives on AI to the conditions of the national economy. In particular, the creation of a repository to support artificial intelligence literacy, attention to general-purpose AI models, responsibility in the value chain for high-risk systems, ensuring copyright, etc. The need for investment in artificial intelligence technologies is emphasized, in particular to ensure their safe implementation and use. Key recommendations include: adopting a security-first approach (based on an assessment of the risks of implementing AI); conducting a multidisciplinary AI risk assessment involving legal, cyber, compliance, technology, risk, HR, and ethics professionals from

business units; and ensuring sufficient investment in cybersecurity controls to protect AI systems. It is emphasized that preparing for the EU AI Act requires a systematic approach to understanding the obligations and implementing appropriate measures. While the requirements may seem complex, they facilitate the responsible development and deployment of AI. By investing in vigilance now, companies can build user trust and enhance their competitive advantage. By prioritizing cybersecurity and mitigating risks, organizations can protect their AI investments and support responsible innovation. A secure approach to AI adoption not only enhances resilience, but also enhances the value and reliability of these powerful technologies.

Ключові слова: *штучний інтелект; законодавство; регулювання; бізнес; Європейський Союз; кібербезпека.*

Keywords: *artificial intelligence; legislation; regulation; business; European Union; cybersecurity.*

Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями. Протягом останніх 5-7 років у світі спостерігається беспрецедентне зростання використання технологій штучного інтелекту (ШІ) практично в усіх сферах економіки та суспільства. Це означає, що інвестиції у розвиток ШІ також стрімко зростають. Так, США планують інвестувати 500 млрд.дол.США у проєкт з розвитку ШІ під назвою «Stargate»[1]. Уряд Китаю планує вкласти трильйон юанів (близько 140 млрд.дол.США) протягом пяти років на розробку алгоритмів, створення обчислювальних центрів і навчання фахівців, а також інтеграцію ШІ в економіку та оборону[2]. ЄС ухвалив рішення про початок у 2026 р. будівництва центрів навчання ШІ ("гігафабрик") з планами інвестувати 1,96 млрд. Євро[3]. Крім того, Президент Франції Еммануель Макрон зробив заяву, що інвестиції Франції в технологію ШІ у розмірі понад €100 млрд

протягом наступних кількох років «еквівалентні тому, що оголосили США в рамках проекту «Stargate»[4].

Разом з тим, внаслідок появи нового китайського штучного інтелекту DeepSeek американські компанії втратили за один день 1 трлн.дол.США. Зокрема, акції компанії NVIDIA, яка активно заробляла на зростанні ШІ через продаж великої кількості відеокарт, впали на 15% за добу, а її ринкова капіталізація значно скоротилася - на понад 400 млрд.дол.США[5]. Розробка DeepSeek коштувала Китаю лише $6 млн., що у сотні разів дешевше за ChatGPT і це відкриває можливості для аналогічних розробок у небагатих країнах, які мають необхідний інтелектуальний ресурс.

Водночас до 2030 року Україна планує виготовляти 1% світового обсягу чіпів[6]. (Для порівняння: ЄС ухвалив Європейський акт про чіпи, спрямований на інвестицію 43 млрд. євро у виробництво мікрочипів, з амбітною метою зайняти 20% світового ринку до 2030 року). За даними Світової організації статистики торгівлі напівпровідниками (WSTS), у 2025 році ринок може зрости на 11,2%, що призведе до оцінки в приблизно $697 млрд. Наразі серед найбільших гравців галузі Nvidia (США), Broadcom (США), TSMC (Тайвань), ASML (Нідерланди) та Samsung (Південна Корея).

Таким чином, боротьба за світове лідерство у сфері використання цифрових технологій (зокрема штучного інтелекту) виходить на новий рівень за обсягом капіталовкладень. США та Китай при цьому залишаються лідерами серед усіх країн світу. Хоча Україна обрала наздоганяючу стратегію, ключовим є факт, що розробити значно потужніший та розумніший аналог ШІ можна значно меншим коштом, що відкриває нові можливості для бідних країн, які мають необхідний інтелектуальний потенціал, але стикаються з браком інвестицій.

Аналіз останніх досліджень і публікацій. Сьогодні людство перебуває на етапі розвитку інформаційно-мережевих систем, найбільш розвинутою формою яких є нейромережеві системи, що виникають на основі математичного моделювання роботи нервової діяльності й людського мозку і

відкривають перспективу штучного інтелекту з усіма наслідками, що випливають звідти [7, с.36].

На саміті зі штучного інтелекту, який пройшов у Франції 10-11 лютого 2025 року 60 країн (серед яких Франція, Китай, Індія) підписали Міжнародну декларацію щодо ШІ, яка передбачає необхідність забезпечення прозорості, безпеки, надійності та достовірності ШІ, а також необхідність "зробити ШІ стійким для людей і планети. Деякі країни відмовилися підписати Декларацію, зокрема Великобританія та США. Представник США зазначив, що занадто жорстке регулювання штучного інтелекту "може вбити галузь, що трансформується, у той момент, коли вона тільки починає розвиватися"[8]. Політика розвитку ШІ має бути пріоритетнішою за безпеку. Для цього потрібне регулювання, яке сприятиме розвитку ШІ, а не перешкоджатиме йому. Отже, попри широкого визнання необхідності міжнародної співпраці та вироблення загальноприйнятих правил у сфері ШІ, існують певні суперечності щодо бачення яким має бути регулювання і це потребує узгодження.

Триває обговорення European Commission’s AI Act (Закон про штучний інтелект (Регламент (ЄС) 2024/1689) [9], який поступово вступає в дію. Закон про штучний інтелект (надалі Закон про ШІ) є першою правовою рамкою, що встановлює узгоджені правила щодо штучного інтелекту в ЄС.

Формулювання цілей статті (постановка завдання).

Мета статті - з’ясувати особливості впливу законодавчого регулювання штучного інтелекту в ЄС на перспективи його розвитку та розробити рекомендації для бізнесових структур щодо підготовки до відповідності вимогам Закону про штучний інтелект.

Виклад основного матеріалу дослідження. Станом на 2 лютого 2025 року набули чинності перші положення Закону про ШІ, включаючи визначення системи штучного інтелекту, вимоги до грамотності штучного інтелекту та заборони на таке використання штучного інтелекту, яке вважається неприйнятним ризиком у межах ЄС. Закон забороняє конкретні

додатки штучного інтелекту, зокрема системи соціального рейтингу, прогностичний поліцейський ШІ для індивідуального профілювання та розпізнавання емоцій на робочому місці чи в школі. Також заборонені: використання вразливостей людей, маніпуляції або підсвідомі методи, розпізнавання обличчя в режимі реального часу в громадських місцях і біометрична категоризація для ідентифікації особистих характеристик за деякими винятками з боку правоохоронних органів. Загалом зі 150 сторінок Закону майже 140 сторінок - про те, що забороняється.

Створення репозиторію для підтримки грамотності ШІ

Європейська Комісія створила діючий репозиторій для підтримки грамотності ШІ, як того вимагає стаття 4 Закону про ШІ. Ця стаття набула чинності 2 лютого 2025 року і зобов'язує постачальників і розгортальників штучного інтелекту забезпечувати достатню грамотність ШІ серед своїх співробітників і користувачів. У відповідь на це Бюро ЄС зі штучного інтелекту зібрало поточні практики грамотності зі ШІ від організацій, які беруть участь у Пакті про ШІ (Pact AI)[10]. Репозиторій, доступний у форматі PDF, який можна завантажити, демонструє різні практики, класифіковані за статусом їх реалізації: повністю впроваджені, частково розгорнуті або заплановані. Репозиторій не є вичерпним і регулярно оновлюється, і тиражування цих практик не гарантує дотримання статті 4. Натомість воно слугує ресурсом для сприяння навчанню та обміну між постачальниками та розгортальниками ШІ. Комісія не схвалює та не оцінює перелічені практики, але підтримує впровадження.

Особлива увага моделям штучного інтелекту загального призначення

З серпня цього року моделі штучного інтелекту загального призначення повинні забезпечувати прозорість щодо технічної документації та навчальних даних, а основні моделі вимагають аудиту безпеки. Після цього правила поширюватимуться на високоризикові програми штучного інтелекту в інфраструктурі, освіті, працевлаштуванні, банківській справі, правосудді та інших секторах. Порушення можуть призвести до штрафів: до

7% від загального обсягу продажів за заборонені дії та 3% за інші порушення. Франція наполягає на перегляді критеріїв, які визначають, коли модель штучного інтелекту загального призначення становить «системний ризик» відповідно до Закону про ШІ, до того, як відповідний пункт Закону набуде чинності 2 серпня 2025 р. Уряд Франції просить Європейську комісію оновити порогове значення, контрольні критерії та показники, що використовуються для цієї класифікації. Закон про ШІ накладає вимоги на постачальників моделей штучного інтелекту загального призначення, включаючи такі великі технологічні компанії, як OpenAI, Google і Meta. Моделі, навчені з обчислювальною потужністю вище певного порогу, вважаються такими, що становлять системні ризики для суспільства, і тому підпадають під особливо суворі правила.

Відповідальність у ланцюжку створення вартості для систем високого ризику

Закон про ШІ регулює системи штучного інтелекту з високим ризиком шляхом розподілу обов'язків по всьому ланцюжку створення вартості, включаючи постачальників, уповноважених представників, імпортерів, дистриб'юторів і розгортачів. Хоча цей лінійний підхід сприяє підзвітності та відповідності, він має значні обмеження. Закон визначає чіткі обов'язки на основі рівня контролю кожного учасника, причому постачальники несуть основну відповідальність за забезпечення відповідності до виходу на ринок. Для постачальників за межами ЄС необхідно призначити уповноваженого представника ЄС. Однак лінійна основа закону може не врегулювати належним чином складні відносини між багатьма сторонами в різних контекстах, потенційно створюючи прогалини у підзвітності. Є занепокоєння щодо перекладання відповідальності, особливо від постачальників до розгортачів, особливо коли великі технологічні компанії обмежують свою відповідальність контрактами. Розв'язання серйозних інцидентів, передбачене Законом, є проблематичним, тому розгортачі повинні інформувати провайдерів раніше за органи влади. Враховуючи непрозорість

систем штучного інтелекту, встановлення причинно-наслідкових зв'язків між задумом і шкодою може бути складним, а положення Закону про ШІ не пов'язують належним чином осіб, які постраждали, з відповідальними сторонами.

Статус і проблеми стандартизації "високоризикових вимог" Закону про ШІ

Повільний прогрес у стандартизації створює правову невизначеність, збільшує витрати на відповідність і потенційно перешкоджає інноваціям ШІ та запуску продуктів. Хоча участь Європейської комісії в цьому процесі необхідна, вона має бути збалансованою, щоб підтримувати ефективність і незалежність у технічних дискусіях. Документ виступає за надання пріоритету загальним стандартам, які є достатньо гнучкими, щоб відповідати потребам галузі та існуючим стандартам, що також може прискорити процес стандартизації. Європейські стандарти повинні узгоджуватися з міжнародними стандартами ISO/IEC, щоб полегшити доступ до ринку та запобігти перешкодам у торгівлі. Узгодженість усіх стандартів Закону про ШІ та їх взаємодія з іншими горизонтальними правовими актами має важливе значення, а вимоги та визначення, де це можливо, мають доповнювати одне одного.

Кодекс практики штучного інтелекту загального призначення (GPAI)

Кодекс практики Закону про ШІ (представлений у статті 56) [11] є набором вказівок щодо дотримання Закону про ШІ. Вони стануть ключовим інструментом для забезпечення відповідності зобов'язанням Закону про ШІ в ЄС, особливо в проміжний період між набуттям чинності зобов'язань постачальника моделі штучного інтелекту загального призначення (GPAI) (серпень 2025 року) та прийняттям стандартів (серпень 2027 року або пізніше). Хоча вони не є юридично обов'язковими, дотримання цих вказівок слугуватиме «презумпцією відповідності» зобов'язанням постачальника моделі GPAI, доки не набудуть чинності більш надійні стандарти. Кодекс практики розробляється у співпраці з багатьма зацікавленими сторонами, за

участю робочих груп, академічних і незалежних експертів, постачальників моделей ШІ, членів громадянського суспільства тощо. Очікується, що документ буде готовий у квітні 2025 року.

Кодекс практики поширюється на компанії, які працюють з моделями штучного інтелекту загального призначення, включаючи OpenAI, Anthropic, Google, Meta та Microsoft. На цей час тривають гострі дискусії з питань, які містяться у Кодексі. Так, Google і Meta стверджують, що Кодекс практики слід послабити, тому що його вимоги є «непрацездатними та технічно нездійсненними». Зокрема, документ вводить вимоги, що виходять за межі сфери розкриття даних навчання та управління системними ризиками, а саме щодо авторського права та тестування моделей третьої сторони. Громадянське суспільство також занепокоєне Кодексом: деякі групи громадянського суспільства погрожують вийти з процесу розробки Кодексу практики штучного інтелекту загального призначення через невдоволення щодо його інклюзивності та прозорості. Ці занепокоєння посилилися після саміту AI Action Summit у Франції 10-11 лютого 2025 року, де питання безпеки та прав людини були затьмарені інтересами бізнесу. Коаліція з питань безпеки, до складу якої входять професор Стюарт Рассел і вісімнадцять науковців і аналітичних центрів, подала рекомендації, в яких наголошується на необхідності проведення обов'язкових зовнішніх оцінок і більш чітких порогових значень ризику. Водночас правозахисні організації критикують віднесення пов'язаних з правами ризиків до «додаткових міркувань», а не до основних проблем.

Європейська Комісія відкликала заплановану директиву про відповідальність проти ШІ та обмежить вимоги до звітності в Кодексі практики щодо штучного інтелекту. Дотримуючись існуючих правил платформи, положення опрацюють щодо забезпечення рівних умов гри.

Питання авторського права в Законі про ШІ

Аксель Восс, ключовий архітектор законодавства ЄС про авторське право, попередив, що «безвідповідальна» правова прогалина в Законі про ШІ

робить творчих професіоналів уразливими. Його занепокоєння підтримали 15 культурних організацій, які написали до Європейської комісії, попереджаючи, що проекти правил імплементації послаблюють захист авторських прав. Восс, німецький депутат Європарламенту, який відіграв центральну роль у розробці директиви ЄС щодо авторського права 2019 року, пояснив, що це законодавство не було розроблено для генеративних моделей ШІ, які можуть створювати текст, зображення чи музику за допомогою простих підказок. Він висловив розчарування тим, що законодавці ЄС не змогли забезпечити надійний захист авторських прав під час переговорів щодо Закону про ШІ. Ситуація ускладнюється виключенням із аналізу тексту та даних, яке, як стверджує Восс, було неправильно витлумачено. Спочатку призначений для обмеженого приватного використання, тепер він потенційно дозволяє великим компаніям збирати величезну кількість інтелектуальної власності.

Алгоритмічна дискримінація відповідно до Закону про ШІ та Загального регламенту захисту даних (GDPR)

Прийняття Закону про штучний інтелект у серпні 2024 року викликає важливі питання щодо його зв'язку з Загальним регламентом захисту даних (GDPR). Хоча Закон про ШІ спрямований на сприяння орієнтованому на людину, надійному та стійкому штучному інтелекті, який поважає основні права, включаючи захист персональних даних, між цими двома нормативними актами існує напруженість. Основною метою Закону про ШІ є пом'якшення дискримінації та упередженості в системах ШІ з високим рівнем ризику. Таким чином, Закон дозволяє обробку «спеціальних категорій персональних даних» за певних умов із заходами щодо збереження конфіденційності. Однак GDPR використовує більш обмежувальний підхід до обробки таких конфіденційних даних. Це створює правову невизначеність щодо того, як слід тлумачити положення Закону про ШІ щодо обробки спеціальних категорій персональних даних для уникнення дискримінації. Рамки GDPR можуть виявитися обмежувальними в середовищі, де домінує

ШІ, що характеризується масовою обробкою даних у різних секторах економіки. Для вирішення цих проблем може знадобитися законодавча реформа GDPR або додаткові вказівки, що пояснюють взаємодію між двома нормативними актами.

Нормативна база ЄС далека від досконалості. Наприклад, GDPR може бути переглянуто, щоб усунути непропорційний тягар, який він накладає на суб'єктів господарювання, порівняно з їхнім потенціалом порушувати конфіденційність (можливо, менші компанії не повинні мати порівнянних обов'язків з великими технологічними гравцями). Він має посилити антимонопольне правозастосування та контроль за злиттям, щоб посилити конкуренцію, суворо застосовувати DMA та DSA, посилити Закон про ШІ та створити надійну етичну основу для нових технологій. У довгостроковій перспективі добре закріплена нормативна база принесе конкурентні переваги, дозволить зменшити невизначеність.

Вплив Закону про ШІ на малий і середній бізнес

Закон про ШІ демонструє значну увагу до малих і середніх підприємств (МСП) - містить численні положення, спеціально розроблені для підтримки та спрощення відповідності МСП. Основні заходи, орієнтовані на МСП, включають регуляторні пісочниці, які забезпечують пріоритетний безкоштовний доступ і спрощення тестування. Закон вирішує фінансові проблеми, забезпечуючи пропорційні збори за оцінку та зобов'язуючи проводити регулярні перевірки для зменшення витрат на відповідність.

Основними викликами для малого бізнесу від впровадження цього Закону є такі:

- відповідність нормативним вимогам;
- витрати на відповідність;
- сповільнення інноваційної діяльності;
- вхідні бар'єри на ринок;
- штрафи та ризики.

Крім викликів, Закон відкриває і можливості для зростання та конкурентних переваг:

- диференціація ринку та довіра;
- доступ до єдиного ринку;
- використання нових бізнес-моделей та сервісів;
- підтримка та фінансові можливості (гранти тощо) від ЄС [12];
- глобальне лідерство та довгострокова стійкість.

Європейська Комісія опублікувала роз'яснення до Закону про ШІ [13], де викладено тлумачення «що таке системи ШІ», у чому сутність концепції ШІ тощо і розробляє спрощені форми технічної документації, які національні органи влади прийматимуть для оцінки відповідності, поряд із навчальними заходами, адаптованими до МСП, для підтримки відповідності. Законодавство також встановлює спеціальні канали зв'язку для вказівок і відповідей на запити. Зобов'язання для постачальників моделей штучного інтелекту загального призначення будуть пропорційними до типу постачальника, з окремими ключовими показниками ефективності для МСП відповідно до Кодексу практики. Також Європейська Комісія опублікувала рекомендації щодо заборонених практик штучного інтелекту відповідно до Закону про ШІ, зосередивши увагу на практиках, які загрожують європейським цінностям і основним правам. Рекомендації стосуються конкретних проблем, таких як шкідливі маніпуляції, соціальна оцінка та дистанційна біометрична ідентифікація в реальному часі. Хоча вони спрямовані на забезпечення послідовного застосування Закону про ШІ в ЄС, ці вказівки залишаються необов'язковими, а остаточні тлумачення зарезервовано за Судом Європейського Союзу. Щоб допомогти зацікавленим сторонам у розумінні та дотриманні Закону, вказівки містять юридичні пояснення та практичні приклади.

"Сірі зони", які виникають під час тлумачення Закону про ШІ

Закон про ШІ є частиною продуктового законодавства і є рамковим (framework), тобто відрізняється від Загального регламенту захисту даних

(GDPR), який не є продуктовим законом (product law). Є певні наслідки у застосуванні за територіальною ознакою. Зазвичай у продуктовому законі розглядається, де цей продукт знаходиться на ринку. Відносно Закону про ШІ відповідно потрібно дивитись, де ШІ знаходиться на ринку або де використовуються результати ШІ - в ЄС чи за його межами. Якщо в ЄС, то Закон застосовується. Якщо поза межами ЄС, то Закон не застосовується. Логіка Закону не враховує, де знаходиться виробник, важливо саме де знаходяться результати його діяльності. Важливо, як буде взаємодіяти Закон про ШІ з іншими інструментами, наприклад такими законами у сфері кібербезпеки як Закон про Кібербезпеку (The Cybersecurity Act (Regulation (EU) 2019/881) [14], Директива (ЄС) 2022/2555 Європейського Парламенту та Ради від 14 грудня 2022 року про заходи щодо високого загального рівня кібербезпеки в ЄС (Directive 2022/2555 (NIS2) [15]. Поки що це не ясно.

Рекомендації для підтримки конкурентоспроможності у сфері ШІ

Документ Європейського технічного альянсу «Забезпечення конкурентоспроможності Європи» [16] описує кроки для європейських компаній, щоб залишатися глобальними конкурентоспроможними у сфері штучного інтелекту у світлі Кодексу практики (GPAI). У документі стверджується, що ефективний Кодекс практики повинен підтримувати розвиток штучного інтелекту, сприяти чесній конкуренції та уникати непотрібного регуляторного тягаря. Він пропонує п’ять ключових принципів для розробників політики: 1) уникати бар’єрів для входу на ринок, 2) зробити використання штучного інтелекту практичним, 3) підтримувати чесну конкуренцію як компас, 4) зробити так, щоб правила штучного інтелекту працювали для всіх компаній, і 5) підтримувати подвійний перехід. Крім того, документ рекомендує чотири конкретні дії для забезпечення чіткості, пропорційності та узгодженості Кодексу GPAI із Законом про ШІ: 1) обмежити сферу застосування постачальниками GPAI, 2) забезпечити відповідну документацію, 3) уникнути обов’язкової участі у встановленні стандартів і 4) запровадити спеціальні зовнішні оцінки.

Оскільки компрометація системи штучного інтелекту може мати серйозні наслідки для бізнесу, організаціям слід скорегувати свій підхід до використання ШІ, якщо вони хочуть отримати безпечну вигоду від його впровадження. Набір основоположних заходів безпекового підходу включає найкращі методи захисту та забезпечення стійкості систем ШІ:

1. Організаціям необхідно застосовувати підхід, що ґрунтується на оцінці ризику до впровадження ШІ.
2. Широке коло зацікавлених сторін має бути залучено до управління ризиками наскрізно всередині організації. Потрібна міждисциплінарна оцінка ризиків штучного інтелекту із залученням таких команд, як юридичні, кібернетичні, комплаєнс, технології, ризики, людські ресурси (HR), етика та бізнес-підрозділи відповідно до конкретних потреб і контексту.
3. Перелік додатків ШІ може допомогти організаціям оцінити, як і де використовується штучний інтелект в організації, включно з тим, чи є він частиною критично важливого ланцюжка поставок, допомагаючи зменшити «тіньовий штучний інтелект» і ризики, пов’язані з ланцюгом поставок.
4. Організації мають забезпечити адекватну дисципліну під час переходу від експериментів до оперативного використання, особливо в критично важливих програмах.
5. Організації мають забезпечити достатні інвестиції в основні засоби контролю кібербезпеки, необхідні для захисту систем ШІ, і гарантувати, що вони готові реагувати на збої та відновлюватися після них.
6. Необхідно поєднати як безпеку перед розгортанням (тобто принцип «позапроектної безпеки»), так і заходи після розгортання для моніторингу та забезпечення стійкості та відновлення систем, що використовуються. Оскільки технологія розвивається, цей підхід необхідно повторювати протягом усього життєвого циклу.
7. Технічні засоби контролю навколо самих систем ШІ мають бути доповнені елементами управління на основі людей і процесів на інтерфейсі між технологією та бізнес-операціями.

8. Потрібно приділяти увагу управлінню інформацією – зокрема, які дані будуть надаватися ШІ та які засоби контролю потрібні, щоб забезпечити дотримання організаційної політики даних.

Висновки та рекомендації

Розвинуті ліберальні демократії загалом погоджуються з необхідністю певної міри регулювання штучного інтелекту на основі ризиків. Україні слід взяти уроки з Закону ЄС про ШІ, зокрема щодо заборони певних програм штучного інтелекту, наприклад тих, що використовують методи ідентифікації особистих характеристик людини. Ключовою перевагою Закону є його чіткість і передбачуваність. Розробники знають, чого очікувати, створюючи системи для 500-мільйонного ринку ЄС. Для регулювання штучного інтелекту в Україні важливого значення має взаємодія та співпраця. Враховуючи невеликий розмір українського ринку як для розробки, так і для розгортання, країні потрібно буде імпортувати системи штучного інтелекту та забезпечити сумісність місцевих систем з міжнародними правилами.

Ключові рекомендації для українського бізнесу у світлі підготовки до вимог Закону про ШІ зводяться до наступного:

1) Потрібно з’ясувати, чи знаходиться продукт компанії в категорії “неприйнятний ризик” та прийняти рішення про видалення цього продукту з ринку ЄС або забезпечити основні елементи відповідності:

-Встановити комплексні системи управління ризиками;

- Впровадити ефективні методи управління даними;

- Вести детальну технічну документацію щодо відповідності;

- Увімкнути автоматичне ведення записів;

- Забезпечити можливості людського нагляду;

- Розглянути можливості використання платформи спостереження ШІ.

2) Потрібно з’ясувати, чи знаходиться продукт компанії в категорії “високий ризик”. Якщо так, то треба вжити заходів до 26 серпня 2025 року, тобто до

того, як Закон в цій частині вступить в дію. Якщо компанія потрапляє в цю категорію, то потрібно впровадити чіткі сповіщення про розголошення ШІ. Іншими словами, користувачам має бути зрозуміло, що вони взаємодіють зі ШІ. Крім того, доцільно:

- планувати розробку надійних систем маркування вмісту;
- створити зручну прозору документацію;
- налаштувати базовий моніторинг;
- розглянути автоматичне маркування контенту, створеного ШІ.

3) Взяти до уваги статтю 25, параграф 4: йдеться про те, що компанія повинна мати всі документи провайдера ШІ щодо відповідності Закону, навіть якщо ця компанія не є стороною контракту із постачання продукту з ШІ, але цей продукт містить хоч одну вироблену нею деталь.

4) Найняти юриста для підстраховки та впевненості у правильності своїх дій.

Підготовка до Закону ЄС про ШІ вимагає систематичного підходу до розуміння зобов'язань і впровадження відповідних заходів. Незважаючи на те, що вимоги можуть здатися складними, вони, зрештою, сприяють відповідальній розробці та розгортанню ШІ. Інвестуючи в спостережливість зараз, компанії зможуть зміцнити довіру користувачів і підвищити власні конкурентні переваги.

Для керівництва компанії вкрай важливо визначити ключові параметри для прийняття рішень щодо впровадження ШІ та пов'язаних з цим проблем кібербезпеки. Надаючи пріоритет кібербезпеці та зменшуючи ризики, організації можуть захистити свої інвестиції в ШІ та підтримувати відповідальні інновації. Безпековий підхід до впровадження ШІ не тільки посилює стійкість, але також підсилює цінність і надійність цих потужних технологій.

Література

1. Jacobs J. Trump announces up to $500 billion in private sector AI infrastructure investment. January 22, 2025. URL:

https://www.cbsnews.com/news/trump-announces-private-sector-ai-infrastructure-investment/

2. Aleksandra K. The Empire Strikes Back: China Prepares One Trillion Yuan AI Plan to Rival $500 Billion US Stargate Project. January 26, 2025. URL: https://www.techpowerup.com/331636/the-empire-strikes-back-china-prepares-one-trillion-yuan-ai-plan-to-rival-usd-500-billion-us-stargate-project

3. Jacob WulffWold. Comission introduces “AI Gigafactories” in final Competitiveness Compass URL: https://www.euractiv.com/section/tech/news/commission-introduces-ai-gigafactories-in-final-competitiveness-compass/

4. Macron unveils plans for €109bn of AI investment in France. Financial Times. February 9, 2025. URL: https://www.ft.com/content/fc6a2d7a-5ed6-436e-84a5-dda86fc258d3

5. David Goldman, Matt Egan. A shocking Chinese AI advancement called DeepSeek is sending US stocks plunging January 27, 2025. URL: https://edition.cnn.com/2025/01/27/tech/deepseek-stocks-ai-china/index.html

6. Українська влада прагне забезпечити 1% світового виробництва чипів до 2030 року. URL: https://ain.ua/2025/01/27/ukraine-semiconductors-plan/

7. Гриценко А.А. Інформаційно-цифровий етап розвитку соціально-економічних систем. *Економіка України.* 2022. № 1. С. 29—46. https://doi.org/10.15407/economyukr.2022.01.029

8. Zoe Kleinman & Liv McMahon. (February 11, 2025) UK and US refuse to sign international AI declaration. URL: https://www.bbc.com/news/articles/c8edn0n58gwo)

9. The EU AI Act (June, 13, 2024). URL: https://artificialintelligenceact.eu/ai-act-explorer/

10. AI Pact. URL: https://digital-strategy.ec.europa.eu/en/policies/ai-pact

11. European Comission. General-Purpose AI Code of Practice (2025). URL: https://digital-strategy.ec.europa.eu/en/policies/ai-code-practice

12. Growth Opportunities for AI Startups. URL: https://innovation.f6s.com/ai-startups-and-public-funding-growth-opportunities/

13. Guidelines on the definition of an artificial intelligence system established by AI Act (February 2025) URL: https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-ai-system-definition-facilitate-first-ai-acts-rules-application

14. The Cybersecurity Act (Regulation (EU) 2019/881) URL: https://eur-lex.europa.eu/eli/reg/2019/881/oj/eng

15. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union. URL: https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng

16. Ensuring Europe's Competitiveness: Key Principles and Actions for the GPAI Code of Practice (2025) URL: https://eutechalliance.eu/ensuring-europes-competitiveness-in-ai-key-principles-and-actions-for-the-gpai-code-of-practice/

References

1. Jacobs, J. (2025), "Trump announces up to $500 billion in private sector AI infrastructure investment ", available at: https://www.cbsnews.com/news/trump-announces-private-sector-ai-infrastructure-investment/ (Accessed 05 March 2025).

2. Aleksandra, K. (2025), "The Empire Strikes Back: China Prepares One Trillion Yuan AI Plan to Rival $500 Billion US Stargate Project", available at: https://www.techpowerup.com/331636/the-empire-strikes-back-china-prepares-one-trillion-yuan-ai-plan-to-rival-usd-500-billion-us-stargate-project (Accessed 05 March 2025).

3. WulffWold, J. (2025), "Comission introduces "AI Gigafactories" in final Competitiveness Compass", available at: https://www.euractiv.com/section/tech/news/commission-introduces-ai-gigafactories-in-final-competitiveness-compass/ (Accessed 05 March 2025).

4. Financial Times (2025), “Macron unveils plans for €109bn of AI investment in France”, available at: https://www.ft.com/content/fc6a2d7a-5ed6-436e-84a5-dda86fc258d3 (Accessed 05 March 2025).

5. Goldman, D. and Egan, M. (2025), “A shocking Chinese AI advancement called DeepSeek is sending US stocks plunging”, available at: https://edition.cnn.com/2025/01/27/tech/deepseek-stocks-ai-china/index.html (Accessed 05 March 2025).

6. Molodkovets', M. (2025), “Ukrainian authorities aim to provide 1% of global chip production by 2030”, available at: https://ain.ua/2025/01/27/ukraine-semiconductors-plan/ (Accessed 05 March 2025).

7. Grytsenko, A. (2022), “Information-digital stage of development of socio-economic systems”, *Economy of Ukraine*, vol. 1, pp. 29—46. https://doi.org/10.15407/economyukr.2022.01.029

8. Kleinman, Z. & McMahon, L. (2025), “UK and US refuse to sign international AI declaration”, available at: (Accessed 05 March 2025).https://www.bbc.com/news/articles/c8edn0n58gwo)

9. The EU AI Act (2024), available at: https://artificialintelligenceact.eu/ai-act-explorer/ (Accessed 05 March 2025).

10. European Comission (2024), “AI Pact”, available at: 2024https://digital-strategy.ec.europa.eu/en/policies/ai-pact (Accessed 05 March 2025).

11. European Comission (2025), “ General-Purpose AI Code of Practice ”, available at: https://digital-strategy.ec.europa.eu/en/policies/ai-code-practice (Accessed 05 March 2025).

12. F6S Innovation (2025), “Growth Opportunities for AI Startups”, available at: https://innovation.f6s.com/ai-startups-and-public-funding-growth-opportunities/ (Accessed 05 March 2025).

13. European Comission (2025), “Guidelines on the definition of an artificial intelligence system established by AI Act”, available at: https://digital-strategy.ec.europa.eu/en/library/commission-publishes-guidelines-ai-system-definition-facilitate-first-ai-acts-rules-application (Accessed 05 March 2025).

14. European Union (2019), “The Cybersecurity Act (Regulation (EU) 2019/881)”, available at: https://eur-lex.europa.eu/eli/reg/2019/881/oj/eng (Accessed 05 March 2025).

15. European Union (2022), “Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union”, available at: https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng (Accessed 05 March 2025).

16. European Tech Alliance (2025), “Ensuring Europe’s Competitiveness: Key Principles and Actions for the GPAI Code of Practice”, available at: https://eutechalliance.eu/ensuring-europes-competitiveness-in-ai-key-principles-and-actions-for-the-gpai-code-of-practice/ (Accessed 05 March 2025).

Стаття надійшла до редакції 15.03.2025 р.