Застосування штучного інтелекту в розвідці: порівняння практик США та правові обмеження в ЄС

The Application of Artificial Intelligence in Intelligence: A Comparison of U.S. Practices and Legal Constraints in the EU

Сергій Стефанцев [A]

Corresponding author: кандидат технічних наук, старший викладач кафедри, e-mail: stefancevss@gmail.com, ORCID ID: https://orcid.org/0000-0002-7629-7563

Вадим Сокур [A]

кандидат технічних наук, старший викладач кафедри, e-mail: vad.sokur@gmail.com, ORCID ID: https://orcid.org/0009-0005-8728-8995

Андрій Булавін [B]

здобувач, e-mail: gustav3713gustav@proton.me, ORCID ID: https://orcid.org/0009-0008-0220-1064

Serhii Stefantsev [A]

Corresponding author: Ph.D. (Tech.), Senior Lecturer of the Department, e-mail: stefancevss@gmail.com, ORCID ID: https://orcid.org/0000-0002-7629-7563

Vadym Sokur [A]

Ph.D. (Tech.), Senior Lecturer of the Department, e-mail: vad.sokur@gmail.com, ORCID ID: https://orcid.org/0009-0005-8728-89955

Andrii Bulavin [B]

Recipient, e-mail: gustav3713gustav@proton.me, ORCID ID: https://orcid.org/0009-0008-0220-1064

[A] Воєнна академія імені Євгенія Березняка, м. Київ, Україна
[B] Міністерство оборони України, м. Київ, Україна

[A] Yevgeny Bereznyak Military Academy, Kyiv, Ukraine
[B] Ministry of Defense of Ukraine, Kyiv, Ukraine

Received: January 14, 2026 | Revised: February 17, 2026 | Accepted: February 28, 2026

DOI: https://doi.org/10.33445/sds.2026.16.1.21

Мета роботи. Здійснити виявлення структурних відмінностей між практикою інтеграції штучного інтелекту в розвідувальну діяльність США та нормативно-правовою моделлю Європейського Союзу, а також оцінити їх вплив на ефективність розвідувального циклу.

Метод дослідження. Системний аналіз, порівняльний аналіз.

Результати дослідження. Проаналізовано еволюцію інтеграції штучного інтелекту в розвідувальну діяльність США та відповідні правові й етичні норми ЄС. Визначено основні напрями його впливу на розвідувальний цикл, систематизовано правові, етичні та технічні обмеження використання штучного інтелекту. Доведено, що твердження про повномасштабну революцію ШІ в розвідці є передчасними.

Теоретична цінність дослідження. Результати можуть бути використані для подальших досліджень у сфері когнітивних та інформаційних технологій безпеки, а також для розвитку теорії прийняття рішень у розвідувальній діяльності.

Цінність дослідження. Матеріали статті можуть бути корисними для фахівців сектору безпеки і оборони під час оцінювання можливостей та ризиків впровадження технологій штучного інтелекту.

Майбутні дослідження. Доцільно зосередитися на розробці конкретних правових норм для регулювання ШІ в розвідці та методів мінімізації когнітивних упереджень у системах людина-машина.

Тип статті. Аналітична.

Purpose. Identify structural differences between the practice of integrating artificial intelligence into U.S. intelligence activities and the regulatory-legal model of the European Union and assess their impact on the effectiveness of the intelligence cycle.

Method. System analysis, comparative analysis.

Findings. The evolution of artificial intelligence integration into U.S. intelligence activities, as well as the corresponding legal and ethical norms of the EU, has been analyzed. The main areas of its impact on the intelligence cycle have been identified, and the legal, ethical, and technical limitations of AI use have been systematized. It has been demonstrated that claims of a full-scale AI revolution in intelligence are premature.

Theoretical implications. The results can be used for further research in the field of cognitive and information security technologies, as well as for the development of decision-making theory in intelligence activities.

Value. The materials of the article may be useful for security and defense sector professionals when assessing the opportunities and risks of implementing artificial intelligence technologies.

Future research. It is advisable to focus on the development of legal norms regulating the use of artificial intelligence in intelligence agencies and methods for reducing cognitive biases in human-machine systems.

Papertype. Analytical.

Ключові слова: штучний інтелект, розвідка, цифрові інновації, аналіз даних, технічні, етичні та правові виклики.

Key words: Artificial Intelligence, Intelligence, Digital Innovations, Data Analysis, Technical, Ethical, and Legal Challenges.

Вступ

Стрімкий розвиток технологій штучного інтелекту (ШІ) суттєво трансформує сучасне безпекове середовище, впливаючи на способи збирання, обробки та інтерпретації інформації у сфері національної безпеки. Особливо це відчутно у розвідувальній діяльності, де обсяги даних,

зібраних технічними засобами, особливо в кіберпросторі, зростають експоненційно [1, 4, 8, 9]. У таких умовах традиційні аналітичні підходи дедалі частіше стикаються з “феноменом “смогу даних” (data smog), коли кількість зібраної інформації перевищує можливості людини щодо її оперативної обробки та осмислення [2, 3].

Штучний інтелект розглядається як технологічна відповідь на цю проблему, оскільки дозволяє автоматизувати рутинні аналітичні операції, виявляти приховані закономірності у великих масивах даних та підтримувати прийняття рішень у режимі реального часу. Водночас питання інтеграції ШІ в розвідувальний цикл виходить за межі суто технологічної площини та охоплює організаційні, правові, етичні й стратегічні аспекти.

Повномасштабна війна російської федерації проти України продемонструвала масове використання алгоритмічних систем для аналізу розвідувальної інформації та управління безпілотними апаратами, що прискорило інтеграцію ШІ у воєнну сферу [4, 8, 9]. Конфлікт став своєрідним каталізатором прискореного впровадження технологій ШІ у воєнній сфері, актуалізувавши питання технологічної переваги, швидкості обробки даних та адаптивності управлінських рішень [4].

На глобальному рівні формуються різні моделі інтеграції ШІ у воєнну сферу. США демонструють практично-інноваційний підхід, що ґрунтується на тісній співпраці розвідувального співтовариства з приватним технологічним сектором, активному експериментуванні та швидкому впровадженні рішень [2]. Натомість у ЄС розвиток ШІ відбувається в умовах жорсткішого нормативного регулювання, зокрема в межах Загального регламенту про захист даних (GDPR) та Акта про штучний інтелект (EU AI Act), які встановлюють високі стандарти захисту прав людини, підзвітності та управління ризиками [14, 15].

Хоча існує багато досліджень застосування ШІ у воєнній сфері, його використання в розвідці недостатньо систематизоване. Більшість наукових публікацій зосереджені або на технологічних аспектах алгоритмів, або на загальних питаннях оборонної політики, тоді як порівняльний аналіз інституційних і правових моделей інтеграції ШІ у розвідці здійснюється фрагментарно [2, 4, 6–11]. Зокрема, відсутня формалізація критеріїв порівняння між американською практикою та європейською нормативною моделлю, що ускладнює об’єктивну оцінку їх стратегічних наслідків.

Таким чином, постає наукова проблема визначення структурних відмінностей між моделями застосування ШІ у розвідувальній діяльності США та ЄС, а також оцінки впливу правових і організаційних чинників на ефективність інтеграції цих технологій.

У межах цього наукового дослідження сформовано такі завдання:

1. Проаналізувати інституційні та організаційні особливості інтеграції ШІ у розвідувальну діяльність США.

2. Проаналізувати правові та етичні механізми, що регулюють застосування ШІ у країнах ЄС.

3. Дослідити, чи створюють нормативні обмеження ЄС структурні бар’єри для розвитку ШІ в розвідці порівняно з американською моделлю.

Дослідження ґрунтується на припущенні, що регуляторне середовище безпосередньо впливає на темпи та глибину інтеграції ШІ у розвідувальну діяльність, формуючи відмінні інституційні моделі його застосування.

Метою статті є виявлення та систематизація структурних відмінностей між практикою впровадження штучного інтелекту в розвідувальну діяльність США та нормативно-правовою моделлю ЄС, а також оцінка їх впливу на трансформацію розвідувального циклу.

Наукова новизна дослідження полягає у:

формалізації критеріїв порівняння моделей застосування ШІ у розвідувальній сфері;

систематизації правових, організаційних і технологічних факторів, що визначають темпи інтеграції ШІ;

обґрунтуванні взаємозв'язку між нормативними обмеженнями та рівнем інноваційної адаптивності розвідувальних структур.

Теоретична значущість роботи полягає у розвитку підходів до аналізу цифрової трансформації розвідувальної діяльності в умовах зростання ролі алгоритмічних систем. Практичне значення результатів дослідження полягає у можливості використання отриманих висновків при формуванні політики впровадження ШІ в секторі безпеки та оборони, з урахуванням необхідності балансу між технологічною ефективністю та дотриманням правових і етичних стандартів.

Теоретичні основи дослідження

Застосування технологій ШІ у розвідувальній діяльності активно досліджується, проте більшість публікацій фокусуються на військових аспектах цієї технології, зокрема на стратегічній важливості застосування технологій ШІ у обороні держав-членів НАТО [1, 2]. Водночас специфіка використання ШІ у розвідувальній діяльності залишається менш вивченою, що можна частково пояснити високим ступенем секретності. Ця сфера, на відміну від воєнних технологій, має значно більше обмежень у відкритому обговоренні та публікаціях, що впливає на глибину доступних досліджень.

Попри це, останніми роками спостерігається значне зростання інтересу до використання ШІ в розвідувальних процесах. Зокрема, Національна комісія зі штучного інтелекту США у звіті за 2021 рік заявила, що ШІ вже "революціонізує практику розвідки". Цей висновок підтверджується аналізом експертів з Центру Белфера (Гарвардський університет, США) які стверджують, що впровадження ШІ в розвідувальну діяльність може змінити її так само, як авіація та ядерна зброя трансформували військову стратегію в попередні епохи [2].

Сьогодні вітчизняні та зарубіжні дослідження акцентують увагу на різноманітних аспектах використання ШІ в розвідувальній діяльності. Серед ключових напрямів виокремлюються:

використання інструментарію ШІ для аналізу розвідувальної інформації для подолання когнітивних обмежень людини-аналітика та підвищення ефективності обробки великих масивів даних [4];

використання можливостей ШІ у кіберрозвідці з метою генерації переконливих фішингових повідомлень [5];

застосування технологій ШІ у кіберрозвідці для симуляції кібератак і тестування на проникнення [6];

використання можливостей ШІ у кіберрозвідці для аналізу шкідливого програмного забезпечення [7];

військові технологічні інновації в контексті впровадження ШІ [8];

управління цілерозподілом рою різнотипних ударних безпілотних літальних апаратів для ураження нестаціонарних групових цілей на основі адаптивного алгоритму з використанням методів оптимізації та елементів ШІ [9];

упровадження ШІ в орієнтованих на дані підприємствах на основі десятифазової моделі, розробленої за результатами кількох кейс-досліджень у поєднанні з підходом Design Science Research [10];

розробка автономних систем для моніторингу та безпеки, а також удосконалення алгоритмів для обробки великих обсягів інформації (big data) [11].

При цьому важливою проблемою залишається забезпечення високої точності аналізу розвідувальних даних, особливо в умовах "смогу даних", коли людські можливості для обробки та інтерпретації великих масивів даних значно обмежені.

Одним із важливих аспектів у даній тематиці є роль людської інтуїції в процесах аналізу та прийняття рішень. Крістофер Р. Моран, Дж. Бертон та Дж. Крістоу розглядають способи,

якими розвідувальне співтовариство США використовує можливості ШІ для цілей національної безпеки. Спираючись на розсекречені розвідувальні записи, автори стверджують, що це співтовариство захоплюється ШІ вже десятиліттями. Історичний контекст застосування ШІ у розвідувальній спільноті США забезпечив країні перевагу першопрохідця та сформував прецеденти, які визначають сучасні практики та підходи [2].

У контексті практичного використання, посібники та інструкції, розроблені компаніями та науковими установами, що займаються розвідкою, активно описують конкретні етапи застосування ШІ в розвідувальному циклі. Наприклад, компанія Scale детально розкриває потенціал ШІ на кожному етапі – від збору розвідувальної інформації до її аналізу та інтерпретації [3]. Це дає змогу практикам зрозуміти, як саме технології можуть бути інтегровані в існуючі розвідувальні процеси та які виклики можуть виникнути при їх впровадженні.

Під “революцією ШІ у розвідці” розуміється якісна трансформація розвідувального циклу, що змінює співвідношення між автоматизованими та людськими компонентами прийняття рішень.

Постановка проблеми

Попри технологічний прогрес, інтеграція ШІ в розвідку ще не спричинила радикальної трансформації процесів прийняття рішень. Основними проблемами залишаються залежність від приватного сектора технологій, обмеження доступу до даних, ризики упередженості алгоритмів та збереження вирішальної ролі чинника когнітивності.

Таким чином, теоретичні основи дослідження застосування ШІ у розвідці вказують на значні перспективи цієї технології для майбутнього розвитку галузі. Водночас потребує глибшого вивчення інтеграція ШІ в розвідку на прикладі досвіду США та правових і етичних норм ЄС. Для систематичного дослідження цих аспектів застосовано комплекс методологічних підходів.

Методологія дослідження

У дослідженні застосовано методи системного та порівняльного аналізу. Порівняння США та ЄС здійснювалося за такими критеріями:

інституційна модель інтеграції ШІ;
рівень співпраці з приватним сектором;
нормативно-правові обмеження;
етичні стандарти та підзвітність;
ризики та механізми їх мінімізації.

Джерельну базу становлять нормативно-правові акти ЄС, стратегічні документи розвідувального співтовариства США, рецензовані наукові публікації 2021–2025 років, а також аналітичні матеріали провідних дослідницьких центрів. Відбір джерел здійснювався за критеріями актуальності, наукової рецензованості, інституційної значущості та релевантності тематиці застосування штучного інтелекту у воєнній сфері.

Результати

1. Аналіз розвитку застосування ШІ розвідкою США

Інтерес розвідувальної спільноти США до ШІ не є новим феноменом та має глибокі історичні корені, що сягають часів Холодної війни, коли комп’ютерні науки тільки починали розвиватися [2, 12]. Перші експерименти з ШІ в розвідці США датуються 1983 роком, коли Центральне розвідувальне управління (ЦРУ) описало гіпотетичну програму “Analiza” – примітивний ШІ для допиту ворожих шпигунів. Ця програма, позбавлена емоцій та втоми, мала ідеальну пам’ять і здатність виявляти слабкості, що робило її ідеальним інструментом для допиту [2].

Однією з ключових фігур, що сприяли просуванню ШІ в ЦРУ в 1980-х роках, був Джон Мак-Магон – заступник директора ЦРУ. Він усвідомлював необхідність технологічних інновацій для обробки зростаючих обсягів даних і трансформації розвідувальної діяльності. Для цього Мак-Магон організував перші симпозіуми з питань ШІ, залучаючи представників уряду, бізнесу та академічних кіл, а також започаткував програми навчання для менеджерів розвідки. Мак-Магон підкреслював важливість співпраці з приватним сектором і університетами для розвитку інновацій у цій сфері, що стало основою для сучасної моделі партнерства між державою та приватним сектором у розвитку ШІ.

Цей історичний імпульс отримав новий розвиток у XXI столітті, а саме у 2015 році ЦРУ створило Директорат цифрових інновацій. Цей директорат створено з метою інтеграції кіберспроможностей у діяльність агентства. До 2018 року ЦРУ вже реалізувало 137 проєктів у сфері ШІ, багато з яких розроблялися у співпраці з компаніями “Силіконової долини” [2]. У 2019 році Офіс директора національної розвідки (ODNI) опублікував Ініціативу AIM, стратегію, спрямовану на розширення можливостей розвідки за допомогою машин [12]. Це свідчить про системний підхід до інтеграції ШІ та його критичну важливість для національної безпеки США.

З самого початку розвідувальна спільнота усвідомлювала, що для розвитку передових технологій ШІ необхідна співпраця з приватним сектором. Як зазначав Мак-Магон, технологічні інновації приходять з приватного сектору та університетів, а не від уряду [2]. Сьогодні ця залежність лише посилилася, адже великі технологічні компанії, наприклад Google, Amazon, Microsoft, Palantir, володіють ресурсами, даними та талантами, що перевищують можливості урядових структур [1, 13]. Партнерство з ними є критично важливим для розвідки США. Так, програмне забезпечення компанії Palantir зіграло важливу роль у пошуку Осами бін Ладена, аналізуючи великі масиви неструктурованих даних [2].

Однак співпраця з приватними компаніями не позбавлена викликів. Технологічний сектор США є надзвичайно різноманітним за своїми ідеологіями та інтересами, що ускладнює узгодження цілей. Зокрема, у 2018 році понад 3000 співробітників Google підписали лист із протестом проти контракту з Пентагоном (штаб-квартира Міністерства оборони США) щодо аналізу відео з дронів, побоюючись, що технологія буде використана для автономних ударів. У результаті Google відмовилася продовжувати контракт [1]. Це створило дилему: чи продовжувати співпрацю з талановитими, але ідеологічно неузгодженими фахівцями, чи слід йти на ризик витоків інформації та саботажу?

Технологічний розвиток ШІ в розвідці США також стикається з серйозними ризиками. Ідеологічна несумісність між технологічними компаніями та урядовими структурами може призвести до загроз. Наприклад, Пері Блейз та Джошуа Шульт працювали з ЦРУ. Блейз, розчарувавшись у роботі на уряд, став публічно критикувати діяльність ЦРУ, а Шульт, у 2017 році став винуватцем найбільшого витоку секретної інформації в історії агентства – витоку інструментів для кібершпигунства ”Vault 7” [2].

ШІ впливає на всі етапи традиційного розвідувального циклу*Engineering and Technology*, збір, обробку, аналіз, поширення та оцінку [3]. Застосування ШІ на кожному з цих етапів дозволяє значно підвищити ефективність розвідки, зокрема автоматизуючи рутинні завдання, підвищуючи точність аналізу та допомагаючи оперативно розпізнавати аномалії у великих масивах даних [2]. Прикладом цього є проєкт “SABLE SPEAR” Агентства оборонної розвідки США, де модель ШІ допомогла виявити глобальну мережу обігу фентанілу, виявивши на 400 % більше причетних осіб, ніж традиційні методи [3].

Незважаючи на всі досягнення, використання ШІ в розвідці все ж не позбавлене ризиків. Ворожі держави та недержавні актори активно застосовують ШІ для досягнення своїх цілей, зокрема у кібератаках, маніпулюванні інформацією та поширенні дезінформації.

Зростає потреба в постійному вдосконаленні технологій кіберзахисту та виявлення маніпуляцій з інформацією, зокрема через технології "діпфейк" [9, 14].

Хоча розвідка США досягла значного прогресу в інтеграції ШІ у свою діяльність, цей процес стикається з правовими, етичними та технологічними викликами, що вимагають уважного управління та адаптації до нових умов.

Таким чином, історична еволюція інтеграції ШІ у розвідці США свідчить про послідовну інституціоналізацію технологічного експериментування, що стало структурною особливістю американської моделі.

2. Правові та етичні норми Європейського Союзу щодо застосування ШІ в розвідці

У Європейському Союзі (ЄС) питання застосування ШІ в розвідці є значно ускладненим через суворі правові обмеження, зокрема через "Загальний регламент про захист даних (GDPR)" та "Акт про штучний інтелект (EU AI Act)", які встановлюють одні з найжорсткіших у світі стандартів обробки персональних даних [14, 15]. Хоча "Акт про штучний інтелект" прямо виключає військові та оборонні застосування з його сфери дії, його людиноцентричний підхід і класифікація ризиків мають неминучий вплив на дискусії щодо оборонного ШІ, зокрема у випадках технологій подвійного призначення [1, 15]. Важливим аспектом є те, що суд ЄС (CJEU) має право накладати значні штрафи на компанії, що порушують вимоги щодо передачі даних громадян ЄС до США. Це створює додаткові труднощі для трансатлантичної співпраці в воєнній сфері [2]. Ці правові обмеження означають, що розвідувальні агенції демократичних країн не мають необмеженого доступу до великих масивів даних, необхідних для навчання потужних моделей ШІ. Це ставить їх у менш вигідне становище порівняно з країнами, такими, як Китай, де держава контролює дані на національному рівні [1].

Застосування ШІ в розвідці породжує етичні проблеми, зокрема упередженість. Алгоритми, навчання яких ґрунтується на історичних даних, можуть відтворювати та посилювати соціальні упередження. Наприклад, програми для розпізнавання обличчя часто мають гірші результати при ідентифікації жінок та людей з темною шкірою, оскільки вони були навчені на даних, здебільшого зібраних від білих чоловіків [12]. У контексті боротьби з тероризмом це може призвести до дискримінаційного профілювання та стигматизації окремих етнічних чи релігійних груп, що має серйозні соціальні та правові наслідки [14].

Іншою важливою проблемою є підзвітність. Коли автономна система приймає рішення, яке призводить до трагедії, постає питання встановлення відповідальності. Встановити, хто несе відповідальність – розробник, оператор чи сама система – стає надзвичайно складно. Це питання є особливо актуальним для летальних автономних систем озброєння (LAWS), щодо яких у Європейському парламенті та Організації Об'єднаних Націй тривають активні дискусії про необхідність заборони або жорсткого регулювання [1]. Питання підзвітності створює серйозні юридичні виклики, оскільки встановлення винних у разі помилок таких систем є надзвичайно важким.

Зрештою, недовіра суспільства до методів роботи розвідувальних агенцій залишається серйозною проблемою. Таємність їх діяльності сприяє виникненню численних конспірологічних теорій, а застосування непрозорих алгоритмів ШІ може посилювати ці суспільні побоювання [2].

Попри значний прогрес у розвитку ШІ, на сьогодні більшість моделей є "вузьким ШІ", який ефективно виконує чітко визначені завдання, але не володіє загальним інтелектом, інтуїцією чи здоровим глуздом, що притаманні людині. Науковці вказують на суттєві технічні обмеження ШІ, зокрема у прогнозуванні рідкісних подій, таких як терористичні атаки, через брак достатньої кількості даних для навчання ШІ [8]. Крім того, терористичні групи постійно змінюють свої методи, що швидко робить моделі ШІ, побудовані на старих даних, застарілими. У таких нестабільних умовах людська інтуїція, що ґрунтується на довгострокових трендах і глибокому розумінні контексту, залишається незамінною.

Також існує ряд обмежень у застосуванні ШІ в розвідці. Наприклад, ШІ не може замінити співробітника розвідувального органу, який проводить операцію з проникнення в організацію, оскільки це вимагає фізичної присутності особи та складних соціальних взаємодій. Крім того, навіть у тих сферах, де ШІ може бути корисним, виникають проблеми з прийняттям технології користувачами. Наприклад, під час війни в Афганістані військові часто надавали перевагу роботі з перекладачами-людьми замість автоматичних систем через більшу довіру до людей та кращого розуміння ними певних нюансів [14].

Таким чином, на цьому етапі дослідження ШІ слід розглядати не як заміну людського інтелекту, а як потужний допоміжний інструмент. Він може автоматизувати рутинні завдання, значно прискорити обробку розвідувальних даних та розширити аналітичні можливості людини, але не здатен замінити критичне мислення та інтуїцію, які є ключовими для ефективної роботи співробітників розвідувальних органів. Його впровадження вимагає збалансованого підходу, що враховує правові, етичні та технічні аспекти, а також специфіку національних систем безпеки.

Проведемо порівняння підходів США та ЄС до застосування ШІ в розвідці, яке здійснимо на рівні нормативно-інституційних моделей. Це порівняння не претендує на повне відображення закритих операційних аспектів діяльності розвідувальних структур.

Таблиця 1: Порівняння підходів Сполучених Штатів Америки та Європейського Союзу до застосування ШІ в розвідці

Критерій	США	ЄС
Модель інтеграції	Практично-інноваційна, орієнтована на швидке впровадження	Нормативно-регуляторна
Роль приватного сектору	Ключова (наприклад компанії Google, Palantir, Amazon)	Обмежена жорстким регулюванням
Доступ до даних	Ширший, залежить від партнерств	Суттєво обмежений “Загальним регламентом про захист даних”
Правове регулювання	Секторальне, фрагментарне	Комплексне (“Загальний регламент про захист даних”, “Акт про штучний інтелект”)
Етичні обмеження	Внутрішні директиви та політики	Формалізовані наднаціональні норми
Стратегічний ефект	Прискорення інновацій	Пріоритет прав людини над швидкістю впровадження

Джерело: підготовлено авторами за матеріалами проведеного аналізу

Наведене порівняння засвідчує, що відмінності між США та ЄС полягають не стільки у рівні технологічної готовності до впровадження ШІ, скільки у характері інституційно-нормативного середовища, в межах якого відбувається його інтеграція. Американська модель демонструє пріоритет операційної ефективності та технологічної адаптивності, що забезпечується гнучкістю регулювання і тісною взаємодією з приватним сектором. Натомість європейська модель вибудовується навколо принципу превентивного управління ризиками, де захист прав людини та підзвітність алгоритмічних систем виступають визначальними умовами впровадження інновацій. У результаті формується асиметрія: США отримують перевагу в темпах експериментального впровадження та масштабування рішень, тоді як ЄС забезпечує вищий рівень нормативної легітимності та суспільного контролю. Таким чином, різниця між підходами відображає більш глибоку стратегічну дилему сучасної цифрової трансформації розвідки – співвідношення швидкості технологічного розвитку та рівня його правової інституціоналізації.

Обговорення

Отримані результати свідчать про наявність двох різних моделей інтеграції ШІ у розвідувальну діяльність, які відображають відмінності в інституційній архітектурі, правовій культурі та стратегічних пріоритетах США та ЄС.

1. Щодо поняття “революція” ШІ у розвідці.

У наукових дослідженнях стверджується, що впровадження ШІ здатне здійснити революційну трансформацію розвідувального процесу, змінюючи саму природу збору та аналізу інформації. Зокрема, вказується на потенціал алгоритмічних систем кардинально підвищити швидкість обробки даних та мінімізувати когнітивні обмеження аналітиків.

Однак результати проведеного аналізу дозволяють уточнити ці оцінки. Хоча технологічні можливості ШІ справді суттєво розширюють інструментарій розвідки, вони не призвели до структурного витіснення людського фактора з процесу прийняття рішень. Навпаки, існує тенденція до формування гібридної моделі, у межах якої алгоритмічні системи виконують функції підсилення, тоді як стратегічна інтерпретація та відповідальність залишаються за людиною.

Таким чином, доцільніше говорити не про революцію, а про еволюційну трансформацію розвідувального циклу, що характеризується поступовою алгоритмізацією окремих його етапів – насамперед збору, фільтрації та первинної обробки розвідувальних матеріалів.

2. Структурні відмінності моделей США та ЄС.

Порівняльний аналіз засвідчує, що ключова відмінність між США та ЄС полягає не у рівні технологічного розвитку, а у характері регуляторного середовища та інституційній логіці впровадження інновацій.

Американська модель характеризується:

високим рівнем інституційної автономії розвідувальних структур;

активною співпрацею з приватним технологічним сектором;

орієнтацією на експериментування та швидке масштабування рішень;

гнучким, секторальним підходом до нормативного регулювання.

Модель ЄС ґрунтується на:

пріоритеті прав людини та захисту персональних даних;

формалізованій системі управління ризиками;

наднаціональному правовому контролі;

підвищених вимогах до прозорості та підзвітності алгоритмічних систем.

Ці відмінності формують різні траєкторії розвитку розвідувального ШІ. У США швидкість інтеграції визначається насамперед технологічними можливостями та партнерствами з приватними компаніями. У ЄС темпи впровадження значною мірою залежать від відповідності правовим нормам і процедурним вимогам.

3. Роль приватного сектору та інноваційні ризики.

Варто окремо розглянути зростаючу залежність розвідувальних структур від приватних технологічних компаній. З одного боку, саме приватний сектор є джерелом інновацій, обчислювальних потужностей і кадрового потенціалу. З іншого – така залежність створює ризики ідеологічних конфліктів, витоків інформації та нестабільності партнерств.

Аналіз доводить, що співпраця з приватними компаніями стає не додатковим, а системоутворювальним елементом сучасної розвідки. Це трансформує традиційну модель державної монополії на стратегічні технології та формує нову конфігурацію “державно-приватної безпекової екосистеми”.

Результати дослідження дають підстави запропонувати концептуальне уточнення природи цифрової трансформації розвідки. Інтеграцію ШІ доцільно розглядати не як заміну

людського інтелекту алгоритмічними системами, а як перехід до моделі когнітивного симбіозу, у межах якої ШІ забезпечує масштабування аналітичних можливостей, людина зберігає функції стратегічної інтерпретації та нормативної відповідальності, правове середовище виступає регулятором глибини алгоритмізації.

У цьому контексті ефективність ШІ в розвідці визначається не лише технічними характеристиками алгоритмів, а й інституційною здатністю держави інтегрувати їх без порушення легітимності та суспільної довіри.

4. Обмеження дослідження.

Дослідження має певні обмеження, зумовлені закритістю розвідувальної діяльності та обмеженим доступом до емпіричних даних щодо реальних алгоритмічних систем. Аналіз базується переважно на відкритих джерелах, стратегічних документах та наукових публікаціях, що може не повністю відображати реальні масштаби впровадження ШІ в розвідку.

Подальші дослідження можуть бути спрямовані на емпіричну оцінку ефективності конкретних систем, а також на кількісне вимірювання впливу регуляторних обмежень на темпи інновацій у воєнній сфері.

Висновки

У статті здійснено порівняльний аналіз моделей інтеграції штучного інтелекту в розвідувальну діяльність США та ЄС з урахуванням інституційних, правових і технологічних чинників.

Встановлено, що впровадження штучного інтелекту у розвідувальній сфері має переважно еволюційний характер і не призвело до радикальної трансформації розвідувального циклу. Алгоритмічні системи істотно підвищують швидкість обробки даних, розширюють можливості виявлення аномалій та автоматизують рутинні аналітичні процедури, однак не заміщують стратегічну інтерпретацію, відповідальність і прийняття рішень людиною. Таким чином, сучасний етап розвитку характеризується формуванням гібридної моделі “людина – алгоритм”.

Виявлено структурні відмінності між американською та європейською моделями інтеграції штучного інтелекту. Американський підхід орієнтований на технологічну адаптивність, активну співпрацю з приватним сектором та швидке масштабування інноваційних рішень. Європейська модель, навпаки, базується на пріоритеті прав людини, формалізованому управлінні ризиками та жорсткому нормативному регулюванні, що безпосередньо впливає на темпи та масштаби впровадження штучного інтелекту у воєнній сфері.

Доведено, що ключовим фактором, який визначає траєкторію розвитку штучного інтелекту в розвідці, є не лише технологічний потенціал, а й регуляторне середовище. Нормативні обмеження можуть одночасно виступати як гарантією легітимності та підзвітності, так і чинником, що уповільнює інноваційну динаміку. У цьому контексті дилема “ефективність — підзвітність” набуває системного характеру.

Показано, що зростаюча роль приватного технологічного сектору трансформує традиційну модель функціонування розвідувальних структур, формуючи нову державно-приватну безпекову екосистему. Така модель розширює доступ до інновацій, але водночас створює ризики залежності, конфліктів інтересів та витоків інформації.

Наукова новизна отриманих результатів полягає у формалізації критеріїв порівняння моделей застосування штучного інтелекту у розвідувальній діяльності, систематизації інституційних і правових факторів, що визначають темпи алгоритмізації розвідки, а також у концептуальному обґрунтуванні моделі когнітивного симбіозу як домінуючої форми взаємодії людини та штучного інтелекту в сучасному розвідувальному циклі.

Практичне значення результатів полягає у можливості використання запропонованих підходів при формуванні державної політики впровадження штучного інтелекту в секторі безпеки та оборони з урахуванням необхідності забезпечення балансу між технологічною

ефективністю, правовою підзвітністю та суспільною довірою.

Перспективи подальших досліджень пов'язані з емпіричним вимірюванням ефективності конкретних алгоритмічних систем у розвідувальній діяльності, а також із розробленням кількісних індикаторів впливу регуляторних режимів на інноваційну спроможність держав у воєнній сфері.

Фінансування

Це дослідження не отримало конкретної фінансової підтримки.

Конкуруючі інтереси

Автори заявляють, що у них немає конкуруючих інтересів.

Список використаних джерел

1. Clapp, S. (2025). *Defence and artificial intelligence* (Members' Research Service PE 569.580 – April 2025). European Parliamentary Research Service. URL: https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/769580/EPRS_BRI(2025)769580_EN.pdf
2. Moran, C. R., Burton, J., & Christou, G. (2023). The US Intelligence Community, Global Security, and AI: From Secret Intelligence to Smart Spying. *Journal of Global Security Studies*, 8(2). https://doi.org/10.1093/jogss/ogad005.
3. Guide to AI for the Intelligence Community. (б. д.). URL: https://scale.com/guides/guide-to-ai-for-the-intelligence-community.
4. Пилипчук, В. В., & Попов, М. О. (2025). Напрями використання інструментарію штучного інтелекту для аналізу розвідувальної інформації. *Сучасні інформаційні технології у сфері безпеки та оборони*, 53(2), 150–155. https://doi.org/10.33099/2311-7249/2025-53-2-150-155.
5. Koroniotis, N., Moustafa, N., Turnbull, B., Schiliro, F., Gauravaram, P., & Janicke, H. (2021). A Deep Learning-based Penetration Testing Framework for Vulnerability Identification in Internet of Things Environments. У 2021 *IEEE 20th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*. IEEE. https://doi.org/10.1109/trustcom53373.2021.00125.
6. Schmitt, M., & Flechais, I. (2024). Digital Deception: Generative Artificial Intelligence in Social Engineering and Phishing. *Artificial Intelligence Review*, 57(12). https://doi.org/10.1007/s10462-024-10973-2.
7. Mehta, R., Jureˇckov´a, O., & Stamp, M. (2023). A Natural Language Processing Approach to Malware Classification. *Journal of Computer Virology and Hacking Techniques*, 20, 1–20. URL: https://arxiv.org/pdf/2307.11032.
8. Баланда, А., & Мокляк, С. (2025). Військові технологічні інновації в контексті впровадження штучного інтелекту. *Social Development and Security*, 15(3), 302-307. https://doi.org/10.33445/sds.2025.15.3.26.
9. Шовкошитний, І. І., & Василенко, О. А. (2025). Управління цілерозподілом рою різнотипних ударних безпілотних літальних апаратів для ураження нестаціонарних групових цілей на основі адаптивного алгоритму з використанням методів оптимізації та елементів штучного інтелекту. *Сучасні інформаційні технології у сфері безпеки та оборони*, 54(3), 15–24. https://doi.org/10.33099/2311-7249/2025-54-3-15-24.
10. Ендрасьяк, К., & Гавлічек, П. (2025). Упровадження штучного інтелекту в орієнтованих на дані підприємствах на основі десятифазової моделі, розробленої за результатами кількох кейс-досліджень. *Social Development and Security*, *15*(5), 17-34. https://doi.org/10.33445/sds.2025.15.5.2 https://doi.org/10.33445/sds.2025.15.5.2.

11. Яковенко, Я., Білик, М., & Олійник, Є. (2024). Штучний інтелект, Big Data і відповідальне споживання як імператив інноваційного розвитку бізнес-структур в умовах формування цифрової економіки. *Економіка та суспільство*, (60). https://doi.org/10.32782/2524-0072/2024-60-151.
12. Townley, D. (2023, 3 травня). Intelligence agencies have used AI since the cold war – but now face new security challenges. *The conversation*. URL: https://doi.org/10.64628/AB.7wa6ftgvp.
13. Savage, C. (2024, 14 листопада). Spy Agency Memo Sets Rules for Artificial Intelligence and Americans' Private Data. *The New York Times*, *Section A*, с. 31. URL: https://www.nytimes.com/2024/11/14/us/ai-privacy-guidelines-intelligence.html.
14. Artificial intelligence at the service of intelligence? (2021, 2 грудня). *Numalis*. URL: https://numalis.com/artificial-intelligence-at-the-service-of-intelligence/.
15. The EU Artificial Intelligence Act, The EU AI Act № Regulation (EU) 2024/1689 (2024, 12 липня). *Official Journal of the European Union*. URL: https://artificialintelligenceact.eu/the-act/.

References

1. Clapp, S. (2025). *Defence and artificial intelligence* (Members' Research Service PE 569.580 – April 2025). European Parliamentary Research Service. URL: https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/769580/EPRS_BRI(2025)769580_EN.pdf
2. Moran, C. R., Burton, J., & Christou, G. (2023). The US Intelligence Community, Global Security, and AI: From Secret Intelligence to Smart Spying. *Journal of Global Security Studies*, 8(2). https://doi.org/10.1093/jogss/ogad005.
3. Guide to AI for the Intelligence Community. URL: https://scale.com/guides/guide-to-ai-for-the-intelligence-community.
4. Pylypchuk, V., & Popov, M. (2025). Trends of Using Artificial Intelligence Tools for Intelligence Analysis. *Modern Information Technologies in the Sphere of Security and Defence*, 53(2), 150–155. https://doi.org/10.33099/2311-7249/2025-53-2-150-155.
5. Koroniotis, N., Moustafa, N., Turnbull, B., Schiliro, F., Gauravaram, P., & Janicke, H. (2021). A Deep Learning-based Penetration Testing Framework for Vulnerability Identification in Internet of Things Environments. У 2021 *IEEE 20th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*. IEEE. https://doi.org/10.1109/trustcom53373.2021.00125.
6. Schmitt, M., & Flechais, I. (2024). Digital Deception: Generative Artificial Intelligence in Social Engineering and Phishing. *Artificial Intelligence Review*, 57(12). https://doi.org/10.1007/s10462-024-10973-2.
7. Mehta, R., Jureˇckov´a, O., & Stamp, M. (2023). A Natural Language Processing Approach to Malware Classification. *Journal of Computer Virology and Hacking Techniques*, 20, 1–20. URL: https://arxiv.org/pdf/2307.11032.
8. Balanda, A., & Mokliak, S. (2025). Military Technological Innovations in the Context of Artificial Intelligence Implementation. *Social Development and Security*, 15(3), 302-307. https://doi.org/10.33445/sds.2025.15.3.26.
9. Shovkoshytnyi, I., & Vasylenko, O. (2025). Management of the Target Distribution of a Swarm of Different Types of Strike Unmanned Aerial Vehicles for Striking Non-Stationary Group Targets Based on an Adaptive Algorithm Using Optimisation Methods and Elements of Artificial Intelligence. *Modern Information Technologies in the Sphere of Security and Defence*, 54(3), 15–24. https://doi.org/10.33099/2311-7249/2025-54-3-15-24.
10. Jędrasiak, K., & Gawliczek, P. (2025). Implementing Artificial Intelligence in Data-Driven

Enterprises through a Ten-Phase Framework Based on Multiple Case Studies. *Social Development and Security*, 15(5), 17-34. https://doi.org/10.33445/sds.2025.15.5.2.

11. Yakhovenko, Y., Bilyk, M., & Oliynyk, Y. (2024). Artificial Intelligence, Big Data, and Responsible Consumption as an Imperative of Innovative Development of Business Structures in the Context of Digital Economy Formation. *Economics and Society*, (60). https://doi.org/10.32782/2524-0072/2024-60-151.
12. Townley, D. (2023, May 3). Intelligence Agencies Have Used AI Since the Cold War – But Now Face New Security Challenges. *The Conversation*. URL: https://doi.org/10.64628/AB.7wa6ftgvp.
13. Savage, C. (2024, November 14). Spy Agency Memo Sets Rules for Artificial Intelligence and Americans' Private Data. *The New York Times*, *Section A*, P. 31. URL: https://www.nytimes.com/2024/11/14/us/ai-privacy-guidelines-intelligence.html.
14. Artificial Intelligence at the Service of Intelligence? (2021, December 2). *Numalis*. URL: https://numalis.com/artificial-intelligence-at-the-service-of-intelligence/.
15. The EU Artificial Intelligence Act, The EU AI Act № Regulation (EU) 2024/1689 (2024, July 12). *Official Journal of the European Union*. URL: https://artificialintelligenceact.eu/the-act/.