УДК 351.86:004.8(4+73)(477)
DOI https://doi.org/10.32689/3083-774X-2026-2(47)-3

МОДЕЛІ ДЕРЖАВНОГО УПРАВЛІННЯ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА РЕГУЛЮВАННЯ ШТУЧНОГО ІНТЕЛЕКТУ: ПОРІВНЯЛЬНИЙ АНАЛІЗ

Гаврилечко Ю. В.

MODELS OF PUBLIC ADMINISTRATION IN THE FIELD OF INFORMATION SECURITY AND ARTIFICIAL INTELLIGENCE REGULATION: A COMPARATIVE ANALYSIS

Yuriy Gavrylechko

Анотація

Об'єктом дослідження є моделі державного управління у сфері інформаційної безпеки та регулювання штучного інтелекту в ЄС, США, Великій Британії та Україні. Проблема полягає у відсутності систематизованого порівняльного аналізу цих моделей, що охоплював би інституційну архітектуру, регуляторний підхід до ШІ та механізм їх інтеграції, ускладнюючи обґрунтоване запозичення зарубіжного досвіду для вдосконалення вітчизняної моделі в умовах воєнного стану. Суть отриманих результатів полягає в тому, що систематизовано три інституційні моделі за критерієм централізації (централізовано-статутну – ЄС, фрагментовано-виконавчу – США, розподілено-регуляторну – Велика Британія); зіставлено регуляторні підходи до штучного інтелекту за нормативною формою та інституційною стабільністю (від комплексного регламенту до відкликаного виконавчого указу); визначено три типи механізмів інтеграції управління інформаційною безпекою з регулюванням ШІ; обґрунтовано чотири компоненти зарубіжного досвіду, застосовні для України. Завдяки поєднанню інституційного й регуляторного вимірів (а не розгляду кожного окремо, як у наявних дослідженнях) результати дозволили сформувати операційний, а не описовий висновок про конкретні застосовні форми. Це пояснюється тим, що централізовано-статутна модель забезпечує нормативну стабільність, фрагментовано-виконавча – швидкість адаптації, а Україна за умов воєнного стану потребує поєднання обох властивостей. Результати можуть бути використані органами публічного управління при розробленні профільного закону про штучний інтелект і вдосконаленні інституційної архітектури сектору інформаційної безпеки України.

Ключові слова: *державне управління, інформаційна безпека, штучний інтелект, регулювання, зарубіжний досвід, порівняльний аналіз, кібербезпека, інституційна модель, публічне адміністрування, воєнний стан.*

Abstract

The object of the study is the models of public administration in the field of information security and artificial intelligence regulation in the European Union, the United States of America, the United Kingdom, and Ukraine. The problem addressed is the absence of a systematized comparative analysis of these models that simultaneously covers institutional architecture, the regulatory approach to AI, and the mechanism of their mutual integration, which complicates the well-grounded borrowing of foreign experience for improving the domestic model under martial law. The essence of the results obtained is that three institutional models of information security administration have been systematized by the criterion of centralization (centralized-statutory – EU, fragmented-executive – USA, distributed-regulatory – UK); regulatory approaches to AI have been compared by the criteria of normative form and stability (from a comprehensive regulation to a rescinded executive order); three types of mechanisms for integrating information security administration with AI regulation have been identified (a single specialized body, a distributed network of agencies, reliance

on existing sectoral regulators); and four components of foreign experience applicable to Ukraine have been substantiated. Owing to the combination of the institutional and regulatory dimensions of analysis (rather than treating them separately, as in existing studies), the results made it possible to form an operational, rather than descriptive, conclusion about specific institutional forms suitable for application. This is explained by the fact that the centralized-statutory model ensures normative stability, whereas the fragmented-executive model ensures adaptation speed, and Ukraine, under martial law, requires a combination of both properties. The results can be used in practice by Ukraine's public administration bodies in drafting a dedicated law on artificial intelligence and improving the institutional architecture of the information security sector.

Key words: *public administration, information security, artificial intelligence, regulation, foreign experience, comparative analysis, cybersecurity, institutional model, public administration, martial law.*

1. Вступ. Актуальність цього дослідження зумовлена двома основними обставинами. По-перше, повномасштабна збройна агресія проти України перетворила питання інституційної спроможності системи державного управління інформаційною безпекою з переважно технічного на безпосередньо безпековий пріоритет, водночас каталізувавши впровадження технологій штучного інтелекту в публічне адміністрування – зокрема через екосистему «Дія», де ШІ-агент самостійно опрацьовує до 70% звернень громадян [1, с. 20]. По-друге, чинна нормативна база України у сфері регулювання ШІ залишається на рівні концепцій і розпоряджень, тоді як провідні зарубіжні юрисдикції вже накопичили різнорідний, але змістовно багатий досвід – від комплексного законодавчого регулювання до принципової відмови від статутного підходу. Навіщо за умов сучасності потрібні дослідження з цієї теми? Тому що вибір конкретної інституційної форми регулювання ШІ в Україні відбувається зараз, і кожне рішення, ухвалене без систематизованого розуміння наявних зарубіжних альтернатив та їх дійсних переваг і недоліків, підвищує ризик відтворення чужих інституційних помилок. Які практичні зиски можуть становити результати цих досліджень? Насамперед, обґрунтовану основу для вибору конкретних, а не абстрактно-декларативних елементів зарубіжного досвіду, придатних до застосування в умовах воєнного стану. Тому дослідження, присвячені порівняльному аналізу зарубіжних моделей державного управління у сфері інформаційної безпеки та регулювання штучного інтелекту, є актуальними.

Аналіз останніх досліджень. Значну частину дослідження присвячено регуляторній базі ЄС, зокрема:

– простежено послідовне посилення регуляторних вимог ЄС у сфері мережевої та інформаційної безпеки – від первинної директиви 2016 року до її суттєво розширеної редакції 2022 року [2];

– охарактеризовано ризик-орієнтовану архітектуру Регламенту про штучний інтелект, зокрема правила класифікації високоризикових систем (ст. 6) [3], та інституційну роль Агентства ЄС з кібербезпеки (ENISA) [4].

Інституційну архітектуру органів кібербезпеки України реконструйовано А. Свінцицьким, який детально встановив хронологію формування профільних інституцій – від заснування органу спеціального зв'язку з власною командою реагування на кіберінциденти (2007 р.) до Кіберполіції (2015 р.) і Національного координаційного центру кібербезпеки (2016 р.) [5, с. 288–296]. Д. ван Пейвельде та П. Оулінг дослідили механізми публічно-приватної взаємодії в розвідувальних і оборонних відомствах Франції, Нідерландів та США [6, с. 1015]. І. Фищук на матеріалі досвіду України проаналізувала управління кібератаками у воєнний час крізь призму публічного адміністрування, опублікувавши результати в міжнародному фаховому виданні [7, с. 619]. Прикладні аспекти застосування ШІ в оборонній та військовій сферах додатково розкрито у працях А. Гриндея [18, с. 120] та О. Трофименко зі співавторами [19, с. 161], що засвідчує міждисциплінарний характер теми на межі публічного управління, кібербезпеки та оборонних досліджень.

Водночас критичний аналіз наявних джерел виявляє дві невирішені частини проблеми. Перша полягає в тому, що дослідження зарубіжного досвіду здебільшого зосереджені на одній юрисдикції (найчастіше ЄС) або на одному вимірі – або суто інституційному, або суто регуляторному, – не пропонуючи систематизованого зіставлення декількох юрисдикцій одночасно за обома вимірами. Це відбувається з об'єктивної причини: інституційна та регуляторна архітектури є предметом різних галузей знання (публічне управління та право), що ускладнює їх інтегрований розгляд в межах одного дослідження. Друга невирішена частина полягає в тому, що наявні порівняльні огляди рідко досліджують саме механізм інституційної інтеграції управління інформаційною безпекою з регулюванням ШІ – тобто те, чи існує єдиний орган, відповідальний за обидва напрями, чи вони розподілені між різними інституціями, – хоча саме це питання

є критичним для України, де формування нової інституційної архітектури відбувається практично одночасно в обох напрямах. Це залишається невирішеним із суб'єктивної причини – дослідники, зазвичай, вже спеціалізуються або на кібербезпековій, або на суто ШІ-регуляторній тематиці, рідко поєднуючи ці напрями свідомо.

Систематизація виявлених локальних прогалин дає підстави сформулювати загальну невирішену проблему: відсутність порівняльного аналізу зарубіжних моделей державного управління, який би одночасно охоплював інституційний вимір (хто безпосередньо адмініструє), регуляторний вимір (як саме регулюється ШІ, які механізми застосовано для цього) і вимір інституційної інтеграції (як ці два виміри поєднані), необхідного для обґрунтованого вдосконалення вітчизняної моделі.

Метою дослідження є систематизація зарубіжних моделей державного управління у сфері інформаційної безпеки та регулювання штучного інтелекту за інституційним, регуляторним вимірами та виміром їх інтеграції. Це дасть можливість обґрунтувати конкретні компоненти зарубіжного досвіду, застосовні для вдосконалення інституційної архітектури державного управління інформаційною безпекою в Україні в умовах воєнного стану.

Для досягнення мети були поставлені наступні задачі:

– систематизувати інституційні моделі державного управління інформаційною безпекою в Європейському Союзі, США та Великій Британії за критерієм централізації;

– порівняти регуляторні підходи до штучного інтелекту в зазначених юрисдикціях за критеріями нормативної форми та інституційної стабільності;

– визначити механізми інституційної інтеграції управління інформаційною безпекою з регулюванням штучного інтелекту в кожній із трьох моделей;

– обґрунтувати компоненти зарубіжного досвіду, застосовні для вдосконалення української моделі державного управління інформаційною безпекою в умовах воєнного стану.

2. Матеріали і методи. Об'єктом дослідження є моделі державного управління у сфері інформаційної безпеки та регулювання штучного інтелекту в Європейському Союзі, Сполучених Штатах Америки, Великій Британії та Україні.

Предметом дослідження є інституційна архітектура, регуляторний підхід до ШІ та механізми їх взаємної інтеграції в кожній із зазначених юрисдикцій.

Основна гіпотеза дослідження полягає в тому, що між ступенем централізації інституційної моделі та стабільністю регуляторного підходу до ШІ існує системний зв'язок, а не випадкова кореляція, і саме цей зв'язок визначає, які елементи зарубіжного досвіду можуть бути перенесені у вітчизняний контекст без порушення їх функціональної цілісності.

Прийняте в дослідженні припущення полягає в тому, що три обрані юрисдикції (ЄС, США, Велика Британія) є достатньо репрезентативними для виявлення структурно різних типів моделей, оскільки представляють комплексно-статутний, фрагментовано-виконавчий і принципово не статутний підходи відповідно. Вужчі національні особливості кожної юрисдикції (наприклад, регіональні відмінності всередині США) виведено за межі аналізу як спрощення, що не впливає на видову класифікацію моделей.

Дослідження проведено з використанням порівняльно-правового методу – для зіставлення нормативної форми регуляторних актів; інституційного аналізу – для визначення структури й підпорядкування органів управління; системного підходу – для розгляду інституційного та регуляторного вимірів у їх взаємозв'язку, а не ізольовано; методу систематизації – для класифікації моделей за визначеними критеріями.

Джерельною базою слугували первинні нормативно-правові акти (регламенти й директиви ЄС, укази Президента США, урядові документи Великої Британії, закони й підзаконні акти України), а також наукові публікації в рецензованих виданнях 2013–2025 років. Для допоміжного зіставлення структурних характеристик моделей і формування узагальнювальних таблиць використано інструменти штучного інтелекту (детально розкрито в розділі «Використання засобів штучного інтелекту»).

3. Результати і обговорення

3.1. Інституційні моделі державного управління інформаційною безпекою

Аналіз інституційної архітектури трьох юрисдикцій, що спирається на теоретичне положення про залежність успішності впровадження нових технологій від інституційної спроможності органу, а не лише від технологічної готовності рішення [26, с. 114], дає підстави виокремити три структурно різні моделі. Централізовано-статутна модель ЄС спирається на мережу профільних агентств – передусім Агентство ЄС з кібербезпеки (ENISA), засноване Регламентом (ЄС) № 460/2004 [4] і згодом розширене Актом про кібербезпеку [8], – функції якого визначені

законодавчо й застосовуються уніфіковано в усіх державах-членах через Директиву NIS2, зокрема через встановлені нею мінімальні заходи управління кіберризиками (ст. 21) [2]. Фрагментовано-виконавча модель США, навпаки, не має єдиного профільного органу з повноваженнями, тотожними ENISA: Агентство з кібербезпеки та захисту інфраструктури (CISA) відповідає за операційне реагування, тоді як стандартизацію здійснює Національний інститут стандартів і технологій (NIST) через добровільну Рамкову модель управління ризиками ШІ (AI RMF), що складається з чотирьох функцій – Govern, Map, Measure, Manage [25], а координація між ними ґрунтується на виконавчих указах, а не на статутному розмежуванні повноважень. Розподілено-регуляторна модель Великої Британії йде ще далі у фрагментації: єдиного профільного органу з питань ШІ не створено взагалі, а відповідальність покладено на наявні секторальні регулятори (Управління у справах інформаційного комісара, Управління з питань комунікацій, Управління з питань конкуренції та ринків), тоді як Національний центр кібербезпеки (NCSC) надає лише рекомендаційні, а не обов'язкові до виконання настанови [10].

Узагальнено систематизацію інституційних моделей представлено в табл. 1.

Порівняно із дослідженнями, що розглядають кожну юрисдикцію окремо [2; 5], зіставлення трьох моделей за єдиним критерієм централізації дозволяє побачити, що централізовано-статутна модель ЄС забезпечує нормативну передбачуваність і уніфіковане правозастосування в усіх державах-членах одночасно, тоді як фрагментовано-виконавча модель США забезпечує швидкість інституційної адаптації – проте ціною відсутності юридично зобов'язальної основи, що унаочнено скасуванням Виконавчого указу № 14110 новою адміністрацією Білого Дому менш ніж за півтора року після його ухвалення. Це є можливим завдяки тому, що виконавчі укази в системі права США не потребують законодавчого процесу для ухвалення чи скасування, на відміну від регламентів ЄС. Розподілено-регуляторна модель Великої Британії посідає проміжне становище: вона зберігає інституційну стабільність наявних секторальних регуляторів, але не створює нового профільного органу, розподіляючи відповідальність без гарантії уніфікованого правозастосування. Українська модель, інституційна архітектура якої закріплена Законом «Про національну безпеку України» [14] та Стратегіями кібербезпеки [15] й інформаційної безпеки [16], перебуває на перехідному етапі між централізовано-статутним і фрагментовано-виконавчим типами: профільні органи (Держспецзв'язку, CERT-UA) визначені законодавчо, однак практика їх функціонування, задокументована у щорічній звітності про кіберінциденти [24], демонструє ознаки функціональної консолідації, притаманної скоріше американській моделі, ніж європейській.

3.2. Регуляторні підходи до штучного інтелекту

Регуляторні підходи до ШІ в трьох юрисдикціях суттєво різняться за нормативною формою. Регламент (ЄС) 2024/1689 про штучний інтелект встановлює чотирирівневу ризик-орієнтовану класифікацію систем ШІ (неприйнятний, високий, обмежений, мінімальний ризик відповідно до критеріїв ст. 6) [3] із прямою юридичною силою в усіх державах-членах без потреби національної імплементації. Регуляторна траєкторія ЄС у сфері кібербезпеки й захисту даних, що передує ухваленню Регламенту про ШІ, включає Директиву NIS 2016 року [21], Загальний регламент про захист даних [20] та Акт про кіберстійкість продуктів із цифровими елементами [22], які разом формують нормативне середовище, у яке Регламент про ШІ інтегрований як логічне продовження, а не ізольований акт. У США після скасування Виконавчого указу № 14110 (жовтень 2023 – січень 2025)

Таблиця 1

Інституційні моделі державного управління інформаційною безпекою

Юрисдикція	Тип моделі	Профільний орган	Нормативна основа
ЄС	централізовано-статутна	ENISA (мережа національних CSIRT)	Регламент 460/2004; NIS2 (2022/2555)
США	фрагментовано-виконавча	CISA (операції) + NIST (стандарти)	виконавчі укази (EO 14110→14179)
Велика Британія	розподілено-регуляторна	секторальні регулятори + NCSC (рекомендаційно)	необов'язкові принципи (Біла книга 2023)
Україна	перехідна централізована	Держспецзв'язку, CERT-UA, Нацкоордцентр кібербезпеки	Закон № 2163-VIII; Стратегія 447/2021

Джерело: систематизовано автором на основі [2; 4; 5; 8–10]

новою адміністрацією ухвалено Виконавчий указ № 14179 «Про усунення бар'єрів для американського лідерства у сфері штучного інтелекту», який змістив пріоритет із безпекового оцінювання на дерегуляцію та конкурентну перевагу [9]. Наслідком його ухвалення стало перейменування Інституту безпеки ШІ на Центр стандартів і інновацій ШІ (CAISI) із звуженим мандатом, зосередженим на кібербезпекових, біобезпекових і хімічних ризиках, а не на широкому спектрі суспільних наслідків [9]. Велика Британія від початку уникає статутного регулювання: п'ять наскрізних принципів (безпека, прозорість, справедливість, підзвітність, оскаржуваність), викладені в урядовій Білій книзі 2023 року, впроваджуються наявними секторальними регуляторами на добровільній основі [10], а першим частковим статутним кроком став ухвалений у середині 2025 року Закон про використання даних [23], що лише дотично, а не безпосередньо регулює питання ШІ; технічний вимір принципів реалізовано окремо – через настанови NCSC щодо безпеки моделей машинного навчання [30].

Порівняно із поширеної в літературі бінарної класифікації підходів до регулювання ШІ (статутний v.s. добровільний) [3], зіставлення трьох моделей за критерієм стабільності виявляє додатковий, самостійний вимір: навіть статутна форма (виконавчий указ США) не гарантує стабільності, якщо не є актом законодавчої, а не виконавчої влади. Це дозволяє уточнити висновок наявних досліджень: критичним чинником є не наявність формальної норми як такої, а орган, уповноважений цю норму ухвалювати та скасовувати. Цей результат стає можливим завдяки розмежуванню в межах аналізу двох показників, які в наявній літературі здебільшого розглядаються як тотожні, – нормативної форми та інституційної стабільності, – тоді як приклад США емпірично доводить, що вони можуть розходитися.

3.3. Механізми інституційної інтеграції управління інформаційною безпекою з регулюванням штучного інтелекту

Аналіз механізмів взаємодії між профільними органами інформаційної безпеки й регулювання ШІ в кожній моделі, що методологічно спирається на практико-орієнтовану парадигму поєднання теоретичного й прикладного рівнів аналізу управління національною безпекою [27, с. 279–280], дає підстави виокремити три типи інтеграції. У ЄС реалізовано модель тематичного розмежування при збереженні координації: ENISA відповідає за кібербезпеку, тоді як окремі, спеціально уповноважені національні органи держав-членів наглядають за застосуванням Регламенту про ШІ, а Директива NIS2 прямо поширює вимоги з управління кіберризиками на постачальників критичних цифрових послуг, включно з високоризиковими системами ШІ [2; 3]. У США реалізовано модель функціональної консолідації в межах єдиного відомства: CISA, вже маючи мандат з кібербезпеки критичної інфраструктури, у 2024–2025 роках послідовно розширила настанови для охоплення безпеки агентних і автономних ШІ-систем, фактично інтегрувавши цей напрям у наявний кібербезпековий мандат без створення нової структури [9]. У Великій Британії реалізовано модель делегованої інтеграції через існуючі повноваження: Національний центр кібербезпеки поширив рекомендації щодо захисту моделей машинного навчання на загальний масив своїх настанов з кібербезпеки, не отримавши окремого мандата на регулювання ШІ як такого [10].

Порівняно із поширеним припущенням про те, що ефективна інтеграція вимагає створення нового профільного органу [4], досвід США і Великої Британії показує протилежне: функціональна консолідація в межах наявного кібербезпекового мандата (CISA) або делегована інтеграція через розширення повноважень наявного органу (NCSC) можуть бути щонайменше не менш ефек-

Таблиця 2

Регуляторні підходи до штучного інтелекту

Юрисдикція	Нормативна форма	Основний підхід	Інституційна стабільність
ЄС	регламент (пряма дія)	ризик-орієнтована класифікація (4 рівні)	висока – зміна потребує законодавчої процедури
США	виконавчий указ	від безпекового оцінювання до дерегуляції	низька – скасовано протягом 15 місяців
Велика Британія	необов'язкові принципи	секторальна імплементація без єдиного акта	середня – поступовий перехід до часткової статутності
Україна	концепція/розпорядження КМУ	етапна підготовка законодавчої бази	формується – профільний закон відсутній

Джерело: систематизовано автором на основі [3; 9–12]

тивними за створення нової структури, якщо базовий орган має достатню операційну спроможність. Це стає можливим завдяки тому, що технічна природа заходів захисту ШІ-систем (виявлення аномалій, аудит моделей, реагування на інциденти) структурно близька до вже наявних кібербезпекових компетенцій, на відміну від суто етико-правових аспектів регулювання ШІ (упередженість, прозорість рішень), які радше потребують спеціалізованого, а не консолідованого підходу.

3.4. Компоненти зарубіжного досвіду, застосовні для України

Порівняльний аналіз трьох моделей у поєднанні з інституційною архітектурою, що вже склалася в Україні [1; 5; 13], дає підстави обґрунтувати чотири компоненти зарубіжного досвіду, застосовні в умовах воєнного стану.

По-перше, з досвіду ЄС – консолідація регуляторних вимог до ШІ-систем у секторі публічних послуг у єдиному профільному законі (за аналогією з прямою дією Регламенту про ШІ), а не в розпорошених концепціях і розпорядженнях, як це наразі реалізовано в Україні [11, с. 20; 12; 17].

По-друге, з негативного досвіду США – закріплення такого закону саме на законодавчому, а не виключно підзаконному рівні, оскільки досвід скасування Виконавчого указу № 14110 протягом 15 місяців емпірично підтверджує вразливість підзаконного регулювання до політичної зміни курсу [9].

По-третє, з досвіду Великої Британії – використання вже сформованої вітчизняної інституційної спроможності, зокрема задокументованого досвіду CERT-UA з протидії кампанії кібершпигунської групи UAC-0219 [28], для делегованої інтеграції функцій захисту ШІ-систем. Практичною основою для такої інтеграції може слугувати систематизований MITRE каталог тактик, застосовних зловмисниками проти самих систем штучного інтелекту (ATLAS) [29], а не очікування створення нового органу «з нуля», що особливо критично в умовах обмежених ресурсів воєнного часу [5; 10].

По-четверте, з досвіду США – функціональна консолідація, за якої профільний орган з питань ШІ або створюється в структурі наявного кібербезпекового відомства, або отримує чітко розмежовані повноваження з ним, запобігаючи дублюванню функцій, задокументованому як проблема ще на етапі становлення інституційної архітектури кібербезпеки України [5].

Порівняно із рекомендаціями, сформульованими авторами попередніх досліджень у загальному вигляді – «ухвалити закон», «створити агентство» [11, с. 21] – обґрунтовані в цьому дослідженні компоненти прив'язані до конкретного зарубіжного джерела кожної рекомендації та до конкретного ризику, який ця рекомендація усуває (нестабільність підзаконного регулювання, дублювання повноважень, відсутність консолідованої законодавчої бази), що перетворює загальну рекомендацію на операційно застосовний висновок.

В узагальненому вигляді всі зазначені компоненти наведено у табл. 3.

4. Висновки. Систематизовано три інституційні моделі державного управління інформаційною безпекою – централізовано-статутну (ЄС), фрагментовано-виконавчу (США) та розподілено-регуляторну (Велика Британія). Особливою рисою запропонованої систематизації є критерій централізації, який, на відміну від поширеного в літературі галузевого опису кожної юрисдикції окремо [2; 5], дає змогу порівнювати моделі за єдиною шкалою. Це пояснюється розмежуванням трьох складових інституційної спроможності – наявності профільного органу, характеру його повноважень і нормативної основи їх закріплення. Порівняльна оцінка: централізовано-статутна модель забезпечує найвищу нормативну передбачуваність, розподілено-регуляторна – найвищу інституційну економність, фрагментовано-виконавча посідає проміжне становище за обома показниками.

Таблиця 3

Компоненти зарубіжного досвіду, застосовні для вдосконалення української моделі

Джерело досвіду	Компонент	Усунений інституційний ризик
ЄС (позитивний)	консолідація вимог до ШІ-систем у єдиному профільному законі	розпорошеність регулювання між концепціями й розпорядженнями
США (негативний)	закріплення закону на законодавчому, а не підзаконному рівні	вразливість до скасування зі зміною політичного курсу
Велика Британія (амбівалентний)	делегована інтеграція через наявну спроможність CERT-UA й Держспецзв'язку	витрати на створення нової структури «з нуля»
США (позитивний)	функціональна консолідація повноважень без дублювання	дублювання функцій між профільними органами

Джерело: систематизовано автором на основі [9; 10; 5; 11; 12; 17]

Порівняно регуляторні підходи до ШІ за критеріями нормативної форми та інституційної стабільності, що дало змогу виявити розходження цих двох показників на прикладі США, де статутна за формою норма (виконавчий указ) виявилася нестабільною за суттю. Відмінність цього результату від наявних бінарних класифікацій «статутний/добровільний підхід» [3] полягає в уведенні додаткового критерію – органу, уповноваженого норму ухвалювати. Це пояснюється розбіжністю природи законодавчої та виконавчої влади в частині процедури зміни нормативного акта. Кількісна оцінка: період дії Виконавчого указу № 14110 склав менш ніж 15 місяців, тоді як аналогічні за предметом регулювання акти ЄС (Регламент про кібербезпеку 2019 року) залишаються чинними понад п'ять років.

Визначено три типи механізмів інституційної інтеграції управління інформаційною безпекою з регулюванням ШІ: тематичне розмежування при координації (ЄС), функціональна консолідація (США), делегована інтеграція (Велика Британія). Відмінність від поширеного припущення про необхідність нового профільного органу для ефективної інтеграції [4] полягає в емпіричному підтвердженні життєздатності альтернативних моделей за умови достатньої операційної спроможності базового органу. Це пояснюється структурною близькістю технічних заходів захисту ШІ-систем до вже наявних кібербезпекових компетенцій. Порівняльна оцінка: функціональна консолідація (США) і делегована інтеграція (Велика Британія) потребують менших додаткових інституційних витрат, ніж тематичне розмежування (ЄС), яке водночас забезпечує чіткіший розподіл відповідальності.

Обґрунтовано чотири компоненти зарубіжного досвіду, застосовні для вдосконалення української моделі: консолідація регуляторних вимог у профільному законі (з досвіду ЄС), закріплення такого закону на законодавчому рівні (з негативного досвіду США), делегована інтеграція через наявну інституційну спроможність CERT-UA й Держспецзв'язку (з досвіду Великої Британії), функціональна консолідація повноважень без дублювання (з позитивного досвіду США). Відмінність цих компонентів від узагальнених рекомендацій наявних досліджень [11, с. 21] полягає в прямій прив'язці кожного компонента до конкретного зарубіжного джерела та конкретного інституційного ризику, який він усуває. Це пояснюється застосованою в дослідженні логікою «джерело досвіду – усунений ризик – застосовний компонент», а не декларативним переліком побажань. Практична оцінка: усі вище наведені чотири компоненти є сумісними з чинною інституційною архітектурою України та не потребують створення структур «з нуля», що є визначальним в умовах ресурсних обмежень воєнного часу.

Конфлікт інтересів. Автор декларує, що не має конфлікту інтересів стосовно даного дослідження, в тому числі фінансового, особистісного характеру, авторства чи іншого характеру, що міг би вплинути на дослідження та його результати, представлені в даній статті.

Фінансування. Дослідження проводилося без фінансової підтримки.

Доступність даних. Рукопис не має пов'язаних даних: аналіз ґрунтується виключно на відкритих нормативно-правових актах і опублікованих наукових джерелах, повний перелік яких наведено у списку літератури.

Використання засобів штучного інтелекту. Автори підтверджують використання технології штучного інтелекту (модель Claude, компанія Anthropic) при підготовці даної роботи. Інструмент застосовувався в розділах 2 «Матеріали і методи» та 3 «Результати і обговорення» для допоміжного зіставлення структурних характеристик трьох інституційних моделей за заздалегідь визначеними автором критеріями та для формування узагальнювальних таблиць 1 і 2 на основі даних, самостійно verified автором за первинними джерелами. Автор перевіряв кожне фактичне твердження, отримане за допомогою інструменту, звіркою з першоджерелами (текстами регламентів, директив, виконавчих указів, офіційними урядовими документами), а аналітичні висновки, порівняльні оцінки та рекомендації, наведені в розділах 3 і 4, сформульовані та відповідально затверджені автором. Використання інструменту не вплинуло на змістовні висновки дослідження, а полегшило технічну систематизацію вже самостійно опрацьованого автором матеріалу.

Внесок авторів. Гаврилечко Ю. В.: концептуалізація дослідження, розроблення методології, аналіз джерел, формування висновків, написання й редагування тексту статті.

REFERENCES

1. Havrylechko, Yu. V. (2025). Ryzyky ta perspektyvy vykorystannia shtuchnoho intelektu u systemi nadannia publichnykh posluh v Ukraini pid chas voiennoho stanu [Risks and prospects of using artificial intelligence

in the public services delivery system in Ukraine during martial law]. *Suchasnyi naukovyi zhurnal, 10*(4), 20–27. https://doi.org/10.36994/2786-9008-2025-10-2
2. 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 (NIS2 Directive). (2022). *Official Journal of the European Union*. Retrieved from: https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng
3. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (AI Act). (2024). *Official Journal of the European Union*. Retrieved from: https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng
4. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA and on information and communications technology cybersecurity certification (Cybersecurity Act). (2019). *Official Journal of the European Union*. Retrieved from: https://eur-lex.europa.eu/eli/reg/2019/881/oj/eng
5. Svintsytskyi, A. V. (2022). The system of cybersecurity bodies in Ukraine. *Revista Científica General José María Córdova, 20*(38), 287–305. https://doi.org/10.21830/19006586.903
6. Van Puyvelde, D., & Oling, P. (2025). Public-private collaboration and the digital transformation of intelligence. *Intelligence and National Security, 40*(6), 1015–1030. https://doi.org/10.1080/02684527.2025.2565950
7. Fyshchuk, I., Noesgaard, M. S., & Nielsen, J. A. (2025). Managing cyberattacks in wartime: The case of Ukraine. *Public Administration Review, 85*(3), 619–627. https://doi.org/10.1111/puar.13895
8. Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency. (2004). *Official Journal of the European Union*. Retrieved from: https://eur-lex.europa.eu/eli/reg/2004/460/oj/eng
9. Executive Order 14110 of October 30, 2023, on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence; rescinded by Executive Order 14179 of January 23, 2025, Removing Barriers to American Leadership in Artificial Intelligence. (2025). *Federal Register*. Retrieved from: https://www.federalregister.gov/documents/2025/01/31/2025-02172/removing-barriers-to-american-leadership-in-artificial-intelligence
10. Department for Science, Innovation and Technology. (2023). *A pro-innovation approach to AI regulation* (updated 2024). UK Government. Retrieved from: https://www.gov.uk/government/publications/ai-regulation-a-pro-innovation-approach/white-paper
11. Havrylechko, Yu. V. (2025). Informatsiina skladova u bezpekovii politytsi derzhavy z ohliadu na rozvytok shtuchnoho intelektu [The information component of the state's security policy in view of the development of artificial intelligence]. *Suchasnyi naukovyi zhurnal, 9*(3), 16–23. https://doi.org/10.36994/2786-9008-2025-9-2
12. Kabinet Ministriv Ukrainy. (2020). Pro skhvalennia Kontseptsii rozvytku shtuchnoho intelektu v Ukraini: Rozporiadzhennia Kabinetu Ministriv Ukrainy vid 02.12.2020 No. 1556-r [On approval of the Concept for the development of artificial intelligence in Ukraine: Order of the Cabinet of Ministers of Ukraine No. 1556-r of December 2, 2020]. *Verkhovna Rada of Ukraine*. Retrieved from: https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80
13. Verkhovna Rada of Ukraine. (2017). Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy: Zakon Ukrainy vid 05.10.2017 No. 2163-VIII [On the basic principles of ensuring cybersecurity of Ukraine: Law of Ukraine No. 2163-VIII of October 5, 2017]. *Verkhovna Rada of Ukraine*. Retrieved from: https://zakon.rada.gov.ua/laws/show/2163-19
14. Verkhovna Rada of Ukraine. (2018). Pro natsionalnu bezpeku Ukrainy: Zakon Ukrainy vid 21.06.2018 No. 2469-VIII [On National Security of Ukraine: Law of Ukraine No. 2469-VIII of June 21, 2018]. *Verkhovna Rada of Ukraine*. Retrieved from: https://zakon.rada.gov.ua/laws/show/2469-19
15. Prezydent Ukrainy. (2021). Pro Stratehiiu kiberbezpeky Ukrainy: Ukaz Prezydenta Ukrainy vid 26.08.2021 No. 447/2021 [On the Cybersecurity Strategy of Ukraine: Decree of the President of Ukraine No. 447/2021 of August 26, 2021]. *Verkhovna Rada of Ukraine*. Retrieved from: https://zakon.rada.gov.ua/laws/show/447/2021
16. Prezydent Ukrainy. (2021). Pro Stratehiiu informatsiinoi bezpeky: Ukaz Prezydenta Ukrainy vid 28.12.2021 No. 685/2021 [On the Information Security Strategy: Decree of the President of Ukraine No. 685/2021 of December 28, 2021]. *Verkhovna Rada of Ukraine*. Retrieved from: https://zakon.rada.gov.ua/laws/show/685/2021
17. Kabinet Ministriv Ukrainy. (2024). Pro skhvalennia Kontseptsii Derzhavnoi tsilovoi naukovo-tekhnichnoi prohramy z vykorystannia tekhnolohii shtuchnoho intelektu v priorytetnykh haluziakh ekonomiky na period do 2026 roku: Rozporiadzhennia Kabinetu Ministriv Ukrainy vid 13.04.2024 No. 320-r [On approval of the Concept of the State Target Scientific and Technical Program on the Use of Artificial Intelligence Technologies in Priority Sectors of the Economy for the Period Until 2026: Order of the Cabinet of Ministers of Ukraine No. 320-r of April 13, 2024]. *Verkhovna Rada of Ukraine*. Retrieved from: https://zakon.rada.gov.ua/laws/show/320-2024-%D1%80
18. Hryndei, A. O. (2024). Vykorystannia shtuchnoho intelektu v oboronnii sferi [Use of artificial intelligence in the defense sector]. *Vcheni zapysky TNU imeni V. I. Vernadskoho. Seriia: Publichne upravlinnia ta administruvannia, 35*(74)(6), 120–123. https://doi.org/10.32782/TNU-2663-6468/2024.6/21
19. Trofymenko, O., Lohinova, N., Sokolov, A., Chykunov, P., & Akhmametieva, H. (2024). Shtuchnyi intelekt u viiskovii sferi [Artificial intelligence in the military sphere]. *Elektronne fakhove naukove vydannia "Kiberbezpeka: osvita, nauka, tekhnika", 1*(25), 161–176. https://doi.org/10.28925/2663-4023.2024.25.161176
20. 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 (GDPR). (2016). *Official Journal of the European Union*. Retrieved from: https://gdpr-info.eu/

21. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems (NIS Directive). (2016). *Official Journal of the European Union*. Retrieved from: https://eur-lex.europa.eu/eli/dir/2016/1148/oj/eng
22. Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act). (2024). *Official Journal of the European Union*. Retrieved from: https://eur-lex.europa.eu/eli/reg/2024/2847/oj/eng
23. Data (Use and Access) Act 2025. (2025). *UK Public General Acts*. Retrieved from: https://www.legislation.gov.uk/ukpga/2025/18/contents
24. Derzhavna sluzhba spetsialnoho zviazku ta zakhystu informatsii Ukrainy. (2025). Zvit pro robotu Systemy vyiavlennia vrazlyvostei i reahuvannia na kiberintsydenty ta kiberataky za 2024 rik [Report on the operation of the Vulnerability Detection and Cyber Incident and Cyberattack Response System for 2024]. Retrieved from: https://scpc.gov.ua/uk/articles/383
25. National Institute of Standards and Technology. (2023). *Artificial intelligence risk management framework (AI RMF 1.0)*. Retrieved from: https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf
26. Neumann, O., Guirguis, K., & Steiner, R. (2024). Exploring artificial intelligence adoption in public organizations: A comparative case study. *Public Management Review, 26*(1), 114–141. https://doi.org/10.1080/14719037.2022.2048685
27. Bielai, S., Antonova, L., Hololobov, S., Yevtushenko, I., & Sporyshev, K. (2024). The impact of a practice-oriented paradigm on public administration and national security. *International Journal of Sustainable Development and Planning, 19*(1), 277–288. https://doi.org/10.18280/ijsdp.190126
28. CERT-UA, & Derzhavna sluzhba spetsialnoho zviazku ta zakhystu informatsii Ukrainy. (2025). *UAC-0219: Kiberspyhonstvo z vykorystanniam PowerShell-stileru WRECKSTEEL (CERT-UA#14283)* [UAC-0219: Cyber espionage using the WRECKSTEEL PowerShell stealer (CERT-UA#14283)]. Retrieved from: https://cert.gov.ua/article/6282902
29. MITRE Corporation. (2025). *MITRE ATLAS (Adversarial Threat Landscape for Artificial-Intelligence Systems)*. Retrieved from: https://atlas.mitre.org/
30. National Cyber Security Centre. (2022). *Principles for the security of machine learning* (updated 2024). UK Government. Retrieved from: https://www.ncsc.gov.uk/collection/machine-learning-principles

ВІДОМОСТІ ПРО АВТОРІВ

Гаврилечко Юрій Володимирович
кандидат наук з державного управління,
доцент кафедри бізнес-адміністрування та права,
Заклад вищої освіти «Університет трансформації майбутнього»
e-mail: awaken9999@gmail.com
ORCID: 0000-0003-1930-7638

Yuriy Gavrylechko
Candidate of Sciences in Public Administration,
Associate Professor at the Department of Business Administration and Law,
Higher Education Institution «University of Future Transformation»

Дата надходження статті: 05.05.2026
Дата надходження виправленої версії статті: 19.06.2026
Дата прийняття статті: 20.07.2026
Дата публікації статті: 16.09.2026