УДК: 351:004.056:316.77(100:477)
JEL Classification: H83, D83, F52, O33

МІЖНАРОДНИЙ ДОСВІД ДЕРЖАВНОГО УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ ПОЛІТИКОЮ В УМОВАХ СУЧАСНИХ БЕЗПЕКОВИХ ВИКЛИКІВ: МОЖЛИВОСТІ АДАПТАЦІЇ ДЛЯ УКРАЇНИ

ДАБІЖА Віра
ЗВО «Відкритий міжнародний університет розвитку людини «Україна»
https://orcid.org/0000-0002-7000-4635
e-mail: verynchik@ukr.net

У статті досліджено міжнародний досвід державного управління інформаційною політикою в умовах сучасних безпекових викликів і цифрової трансформації. Обґрунтовано трансформацію державної інформаційної політики від регулювання інформаційних відносин до комплексного напряму публічного управління, що охоплює інформаційну та кібербезпеку, стратегічні комунікації, захист інформаційних прав і забезпечення цифрової стійкості. Здійснено порівняльний аналіз моделей державного управління інформаційною політикою США, Канади, Німеччини та Франції. Визначено особливості національних підходів: безпеково-стратегічну спрямованість американської моделі, державно-координаційний характер канадської, нормативно-правові та правозахисні засади німецької, міжвідомчий і багаторівневий характер французької. Встановлено спільні тенденції посилення стратегічного управління, міжвідомчої координації, державно-приватної взаємодії та технологічної протидії інформаційним загрозам. Обґрунтовано доцільність селективно-комбінованого підходу до адаптації міжнародного досвіду в Україні з урахуванням безпекових потреб та євроінтеграційних пріоритетів. Визначено напрями вдосконалення державної інформаційної політики, зокрема стратегічне планування, розвиток міжвідомчої взаємодії, нормативно-правового забезпечення, державно-приватного партнерства та оцінювання ефективності управлінських рішень. Окреслено перспективи формування адаптивної моделі управління для підвищення інформаційної стійкості держави та суспільства.

Ключові слова: державна інформаційна політика, державне управління, публічне управління, міжнародний досвід, інформаційна безпека, національна безпека, цифровізація, кібербезпека, інформаційна стійкість, міжнародне співробітництво.

https://doi.org/10.31891/mdes/2026-22-8

This is an Open Access article distributed under the terms of the Creative Commons CC-BY 4.0

Стаття надійшла до редакції / Received 03.09.2026
Прийнята до друку / Accepted 02.11.2026
Опубліковано / Published 12.11.2026

© ДАБІЖА Віра

ПОСТАНОВКА ПРОБЛЕМИ У ЗАГАЛЬНОМУ ВИГЛЯДІ ТА ЇЇ ЗВ'ЯЗОК ІЗ ВАЖЛИВИМИ НАУКОВИМИ ЧИ ПРАКТИЧНИМИ ЗАВДАННЯМИ

Стрімка цифровізація суспільних процесів, глобалізація інформаційного простору та зростання кількості гібридних загроз суттєво трансформують підходи до формування та реалізації державної інформаційної політики. В умовах сучасних безпекових викликів інформаційний простір став одним із ключових середовищ забезпечення національної безпеки, функціонування системи державного управління та захисту демократичних інститутів. Інформаційні впливи, кібератаки, дезінформаційні кампанії, інформаційно-психологічні операції та втручання у цифрову інфраструктуру дедалі частіше використовуються як інструменти політичного, економічного і військового протистояння.

Особливої актуальності зазначена проблематика набула для України в умовах повномасштабної збройної агресії Російської Федерації, коли інформаційна політика стала невід'ємною складовою державної політики у сфері національної безпеки та оборони. Ефективність державного управління інформаційною сферою сьогодні визначається не лише якістю нормативно-правового забезпечення, а й здатністю державних інституцій оперативно реагувати на інформаційні загрози, координувати діяльність органів влади, взаємодіяти з громадянським суспільством і міжнародними партнерами, а також забезпечувати стійкість інформаційного середовища.

Світова практика свідчить, що провідні держави виробили різні моделі державного управління інформаційною політикою, які поєднують нормативно-правові, інституційні, організаційні та технологічні механізми забезпечення інформаційної безпеки. Водночас міжнародний досвід потребує не механічного запозичення, а науково обґрунтованої адаптації до українських реалій з урахуванням особливостей функціонування системи публічного управління, воєнного стану, євроінтеграційного курсу та сучасних цивілізаційних викликів. Саме тому дослідження міжнародного досвіду державного управління інформаційною політикою та визначення можливостей його імплементації в Україні є актуальним науковим і практичним завданням.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Проблематика формування та реалізації державної інформаційної політики, забезпечення інформаційної безпеки й удосконалення механізмів державного управління інформаційною

сферою перебуває в центрі уваги вітчизняних і зарубіжних науковців. Вагомий внесок у дослідження теоретико-правових засад регулювання інформаційних відносин здійснила Г. Виноградова, яка розглянула особливості правового забезпечення інформаційних процесів в Україні. Сучасні тенденції розвитку державної інформаційної політики в умовах глобальних викликів і загроз досліджували С. Головко та Н. Головко, акцентуючи увагу на міжнародному досвіді та можливостях його використання в Україні. І. Килимник зосередив увагу на проблемах інформаційного суспільства, інформаційної безпеки та новітніх загрозах інформаційному середовищу. Науковий інтерес становлять також дослідження Н. Ржевської, присвячені сучасній інформаційній політиці США та можливостям використання американського досвіду в українських умовах.

Важливе значення для дослідження міжнародних підходів до забезпечення інформаційної та кібернетичної безпеки мають аналітичні й стратегічні документи зарубіжних держав. Зокрема, у звіті Канадського центру кібербезпеки National Cyber Threat Assessment 2025–2026 висвітлено актуальні кібернетичні загрози та тенденції їх розвитку, а в Національній стратегії кібербезпеки Канади 2025 року визначено стратегічні пріоритети забезпечення безпеки цифрового середовища. Водночас важливим нормативно-правовим орієнтиром для європейських держав залишається Регламент Європейського Союзу 2016/679 (GDPR), який встановлює правові засади захисту персональних даних та впливає на формування національних підходів до регулювання інформаційних відносин.

Узагальнення зазначених наукових праць і документів свідчить про багатогранність досліджуваної проблематики та поступове розширення предметного поля державної інформаційної політики. Водночас потребують подальшого опрацювання питання системного порівняння зарубіжних моделей державного управління інформаційною політикою за єдиними критеріями, визначення особливостей їх нормативно-правового, інституційного, організаційно-координаційного та безпеково-технологічного забезпечення, а також обґрунтування пріоритетних напрямів удосконалення відповідних механізмів в Україні з урахуванням сучасних безпекових викликів, цифровізації та євроінтеграційних процесів.

ВИДІЛЕННЯ НЕВИРІШЕНИХ РАНІШЕ ЧАСТИН ЗАГАЛЬНОЇ ПРОБЛЕМИ, КОТРИМ ПРИСВЯЧУЄТЬСЯ СТАТТЯ

Незважаючи на значну увагу науковців до проблем державної інформаційної політики, інформаційної безпеки та зарубіжного досвіду їх нормативно-правового й інституційного забезпечення, недостатньо дослідженими залишаються питання комплексного порівняння моделей державного управління інформаційною політикою та визначення можливостей адаптації їх окремих елементів до сучасних умов України. Зокрема, потребують подальшого наукового обґрунтування критерії порівняння національних моделей, особливості поєднання стратегічних, нормативно-правових, інституційних та безпеково-технологічних механізмів, а також напрями їх інтеграції в систему публічного управління України.

Особливої актуальності набуває проблема формування адаптивної моделі державного управління інформаційною політикою, здатної враховувати одночасний вплив воєнних загроз, цифрової трансформації та євроінтеграційних процесів. У цьому контексті невирішеним залишається питання визначення найбільш ефективних елементів міжнародного досвіду та обґрунтування підходів до їх вибіркового поєднання з урахуванням національних безпекових потреб, інституційних можливостей і необхідності забезпечення інформаційних прав людини. Саме на вирішення зазначених питань спрямоване це дослідження.

ФОРМУЛЮВАННЯ МЕТИ СТАТТІ

Метою статті є здійснення комплексного порівняльного аналізу міжнародного досвіду державного управління інформаційною політикою в умовах сучасних безпекових викликів, визначення особливостей функціонування зарубіжних моделей управління інформаційною сферою та обґрунтування пріоритетних напрямів адаптації найбільш ефективних міжнародних практик до системи державного управління України.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

Сучасний розвиток інформаційного суспільства супроводжується докорінною трансформацією ролі інформації у функціонуванні держави та суспільства. Якщо раніше інформаційна політика розглядалася переважно як інструмент регулювання діяльності засобів

масової інформації та забезпечення доступу громадян до інформації, то сьогодні вона перетворилася на один із ключових напрямів державного управління, який охоплює питання національної безпеки, кібербезпеки, цифрової трансформації, стратегічних комунікацій, захисту критичної інформаційної інфраструктури та інформаційного суверенітету держави [1].

У сучасних умовах інформаційний простір фактично став окремим середовищем реалізації державної політики, де поряд із традиційними інструментами управління активно використовуються цифрові технології, великі масиви даних, штучний інтелект, автоматизовані системи аналізу інформації та механізми стратегічних комунікацій. Відповідно, державне управління інформаційною політикою набуває комплексного характеру та передбачає узгоджену діяльність органів державної влади, сектору безпеки і оборони, правоохоронних органів, органів місцевого самоврядування, приватного сектору, наукової спільноти та інститутів громадянського суспільства.

Особливого значення інформаційна політика набуває в умовах сучасних безпекових викликів. Поряд із традиційними воєнними загрозами держави дедалі частіше стикаються з масштабними кібератаками, інформаційно-психологічними операціями, кампаніями з дезінформації, втручанням у функціонування критичної цифрової інфраструктури, використанням соціальних мереж як інструменту зовнішнього впливу та іншими проявами гібридного протиборства [3]. За таких умов ефективність державного управління визначається не лише рівнем нормативно-правового забезпечення, а й спроможністю державних інституцій своєчасно виявляти загрози, координувати діяльність суб'єктів інформаційної безпеки та забезпечувати стійкість інформаційного середовища [2].

У міжнародній практиці державне управління інформаційною політикою дедалі більше ґрунтується на інтегрованому підході, який поєднує правові, організаційні, технологічні та інституційні механізми. Порівняльні дослідження у сфері публічного управління свідчать, що ефективність державної політики значною мірою залежить від здатності органів влади адаптувати перевірені міжнародні практики до власних політико-правових і безпекових умов, а не від механічного запозичення окремих інституцій чи норм.

Для України зазначена проблематика має особливе значення в умовах широкомасштабної збройної агресії рф. Воєнні дії підтвердили, що інформаційний простір є одним із ключових театрів сучасного протиборства, а ефективна система державного управління інформаційною політикою безпосередньо впливає на рівень національної стійкості, обороноздатності, довіри громадян до державних інституцій та ефективність міжнародної взаємодії. Саме тому дослідження міжнародного досвіду державного управління інформаційною політикою є важливою передумовою вироблення сучасної моделі розвитку інформаційної сфери України [7].

Порівняльний аналіз зарубіжного досвіду є одним із найбільш ефективних інструментів удосконалення системи публічного управління, оскільки дозволяє виявити закономірності функціонування різних моделей державної політики, оцінити ефективність управлінських механізмів та визначити можливості їх адаптації до національних умов. У сучасній компаративістиці державне управління розглядається не як сукупність універсальних моделей, а як система інституційних рішень, ефективність яких залежить від політичного устрою, правової системи, рівня цифрового розвитку, суспільної довіри та характеру безпекових загроз.

Аналіз міжнародного досвіду у сфері державного управління інформаційною політикою засвідчує, що, незважаючи на відмінності між країнами, можна виокремити спільні тенденції. До них належать централізація стратегічного управління інформаційною безпекою, створення спеціалізованих інституцій з питань кібербезпеки, розвиток механізмів міжвідомчої координації, активне залучення приватного сектору до захисту критичної інформаційної інфраструктури, інтеграція цифрових технологій у процеси державного управління, а також формування комплексної нормативно-правової бази, що забезпечує баланс між національною безпекою, правами людини та свободою інформації.

Матеріали, що характеризують досвід США, Канади, Німеччини та Франції, свідчать про різні організаційні підходи до державного управління інформаційною політикою, проте всі вони ґрунтуються на системності, інституційній координації та безперервному вдосконаленні механізмів реагування на нові інформаційні загрози [7]. Саме тому подальший аналіз доцільно здійснювати за єдиними критеріями: нормативно-правове забезпечення, інституційна модель управління, механізми міжвідомчої взаємодії, технологічне забезпечення та можливості адаптації відповідного досвіду до української системи публічного управління. Отже, переходимо від окремих

національних моделей до їх порівняльного аналізу та вироблення практичних рекомендацій для України.

Дослідження міжнародного досвіду державного управління інформаційною політикою потребує застосування єдиних критеріїв порівняння, оскільки просте зіставлення нормативно-правових актів або повноважень окремих державних інституцій не дозволяє повною мірою визначити системні особливості відповідних моделей. З позицій публічного управління доцільно оцінювати не лише наявність спеціалізованих органів чи нормативних документів, а й характер розподілу управлінських повноважень, механізми координації суб'єктів, способи реагування на інформаційні та кібернетичні загрози, участь недержавного сектору та здатність системи адаптуватися до зміни безпекового середовища [4]. З огляду на це досвід США, Канади, Німеччини та Франції доцільно порівнювати за нормативно-правовим, інституційним, організаційно-координаційним, безпеково-технологічним критеріями та з позиції можливостей адаптації відповідних практик для України.

За нормативно-правовим критерієм найбільш характерною рисою американської моделі є послідовне формування розгалуженої системи правового регулювання інформаційної сфери, яка розвивалася відповідно до трансформації характеру загроз. Правове забезпечення охоплює питання захисту приватності, доступу до інформації, безпеки комп'ютерних систем, протидії комп'ютерним злочинам, захисту державних інформаційних ресурсів та кібербезпеки. Важливою особливістю цієї моделі є поєднання законодавчого регулювання зі стратегічними документами та актами глави держави, завдяки чому інформаційна безпека поступово інтегрувалася у систему національної безпеки та оборони.

Канадська модель характеризується поєднанням безпекового регулювання з розвитком інформаційного суспільства, електронного урядування та захистом конфіденційності. У вихідному матеріалі особливе значення надається формуванню критеріїв безпеки комп'ютерних систем, розвитку «інформаційної магістралі», захисту персональної інформації та поступовому формуванню комплексного стратегічного підходу до кібербезпеки [10]. Така модель демонструє прагнення держави забезпечити не лише захищеність власних інформаційних систем, а й безпечне функціонування цифрового середовища для громадян та приватного сектору.

Для Німеччини характерним є виражений правозахисний компонент державної інформаційної політики. Значна увага приділяється конфіденційності інформації, захисту персональних даних, визначенню правових підстав їх збору, обробки та використання. Водночас розвиток кібернетичних загроз зумовив поступове посилення безпекового компонента та формування спеціальних механізмів державного реагування. Таким чином, німецька модель демонструє поєднання двох принципово важливих завдань державного управління: забезпечення інформаційної та кібернетичної безпеки і дотримання прав людини в інформаційній сфері.

Французький підхід характеризується комплексним використанням норм різних галузей права. Захист державної таємниці, персональних даних, комерційної інформації та протидія правопорушенням в інформаційній сфері забезпечуються через взаємодію кримінально-правових, цивільно-правових, трудових та адміністративних механізмів. Це свідчить про інтеграцію інформаційної безпеки у ширшу систему державного регулювання суспільних відносин, а не її відокремлення в межах одного вузького напряму політики.

За інституційним критерієм найбільш розгалуженою є модель США. Забезпечення інформаційної та кібернетичної безпеки здійснюється значною кількістю державних інституцій, серед яких у вихідному матеріалі виокремлено Агентство національної безпеки, Федеральне бюро розслідувань, Центральне розвідувальне управління та структури, відповідальні за кібербезпеку. Характерною особливістю американського підходу є розподіл функцій між цивільними, правоохоронними, розвідувальними та військовими структурами при одночасному збереженні стратегічного рівня координації державної політики. Це дозволяє розглядати інформаційну безпеку не як компетенцію одного відомства, а як міжсекторальний напрям державного управління.

Канадська модель також базується на спеціалізації державних інституцій, однак характеризується більш вираженою орієнтацією на координацію діяльності державних органів, захист електронного уряду та критичної інфраструктури. Формування спеціальних структур для інформаційних операцій та реагування на кіберінциденти свідчить про поступове інституційне розмежування стратегічних, військових і технічних функцій у сфері інформаційної безпеки [9].

У Німеччині важливе місце посідають спеціалізовані державні інституції, відповідальні за інформаційну та кібернетичну безпеку, а також механізми координації діяльності різних федеральних структур. Особливістю німецького підходу є інституціоналізація взаємодії між

органами державної влади та приватним ІТ-сектором. Відповідно, можна поєднувати державний контроль, експертне забезпечення та технологічні можливості недержавних суб'єктів.

Французька модель вирізняється поєднанням центрального та регіонального рівнів реагування. Важливу роль відіграють не лише центральні державні структури, а й спеціалізовані підрозділи на регіональному рівні, зокрема у сфері протидії злочинам, пов'язаним з інформаційними технологіями. Такий підхід забезпечує наближення механізмів реагування до конкретних загроз і водночас дозволяє залучати до вирішення проблем фахівців різного профілю.

За організаційно-координаційним критерієм американська модель характеризується розвиненою міжвідомчою взаємодією та активним залученням приватного сектору. Особливого значення це набуває з огляду на те, що значна частина інформаційної та критичної інфраструктури функціонує поза безпосереднім державним управлінням. Співробітництво держави з телекомунікаційними, фінансовими, енергетичними, технологічними та науковими структурами стає необхідною умовою забезпечення національної інформаційної стійкості.

Для Канади характерною є значна роль держави у координації інформаційних процесів і забезпеченні інформаційної безпеки. У вихідному матеріалі ця особливість пов'язується, зокрема, з високим рівнем суспільної довіри до державних інституцій. Водночас розвиток кібербезпеки сприяв розширенню механізмів обміну інформацією між федеральними органами, взаємодії з приватним сектором та міжнародного співробітництва.

Німецький підхід характеризується інституціоналізованою координацією та прагненням об'єднати діяльність органів державної влади, спеціалізованих безпекових структур і приватних ІТ-компаній. У цьому випадку держава виконує не лише контрольну, а й координаційну та консультативну функції, створюючи умови для вироблення спільних стандартів і механізмів реагування.

У Франції організаційний механізм має більш децентралізовані елементи. Залучення регіональних поліцейських структур та фахівців у галузях права, фінансів, аудиту й інформаційних технологій свідчить про застосування міждисциплінарного підходу до протидії інформаційним загрозам. Таким чином, координація забезпечується не лише вертикальними зв'язками в системі державного управління, а й горизонтальною взаємодією між різними професійними та інституційними середовищами.

За безпеково-технологічним критерієм найбільш виражений оборонний характер має американська модель. Інформаційна безпека в США тісно пов'язана з питаннями національної оборони, розвідувальної діяльності, інформаційних операцій, кіберзахисту та захисту критичних мереж. Розвиток систем попередження і реагування на кібератаки, захищених державних комунікацій, кіберконтррозвідки та спеціальних програм виявлення втручань свідчить про перехід від переважно реактивної до превентивної моделі управління інформаційними ризиками [7].

Канадський підхід характеризується орієнтацією на захист урядових інформаційних систем, критичної інфраструктури та громадян у цифровому середовищі. Технологічний компонент поєднується з інформаційною грамотністю та консультаційною підтримкою, що дозволяє розглядати інформаційну безпеку не лише як технічну функцію держави, а і як елемент суспільної стійкості.

Для Німеччини характерним є ризик-орієнтований підхід, у межах якого технологічні механізми кіберзахисту поєднуються з нормативними вимогами щодо обробки інформації та захисту персональних даних. Відповідно, технологічна модернізація не протиставляється правовим обмеженням, а здійснюється в межах визначених державою правових гарантій.

Французький досвід демонструє поєднання цивільного і військового вимірів інформаційної безпеки. Інформаційні загрози розглядаються як такі, що можуть виникати у військовій, адміністративній, економічній та правоохоронній сферах [8]. Відбувається процес використання різних механізмів реагування залежно від характеру та рівня загрози.

Проведений аналіз дозволяє зробити висновок, що міжнародна практика не сформувала єдиної універсальної моделі державного управління інформаційною політикою. Натомість можна говорити про декілька домінуючих підходів. Американська модель має переважно безпеково-стратегічний характер і ґрунтується на потужній інституційній системі, міжвідомчій координації та державно-приватній взаємодії. Канадську модель доцільно визначити як державно-координаційну та суспільно орієнтовану, оскільки в ній захист державних інформаційних ресурсів поєднується з розвитком електронного урядування та безпечного цифрового середовища. Німецька модель має виражений нормативно-інституційний та правозахисний характер, поєднуючи кібербезпеку із захистом персональних даних і прав людини. Французьку модель можна

охарактеризувати як міжвідомчу та функціонально децентралізовану, оскільки протидія інформаційним загрозам інтегрована в діяльність різних державних і регіональних структур.

При цьому відмінності між національними моделями не заперечують наявності спільної тенденції: державне управління інформаційною політикою поступово трансформується від відносно вузького регулювання інформаційної сфери до комплексного управління інформаційною стійкістю держави. Його складовими стають нормативно-правове забезпечення, стратегічне планування, інституційна спроможність, міжвідомча координація, державно-приватна взаємодія, технологічний захист та оперативне реагування на інформаційні й кібернетичні загрози.

Для України принципово важливим є те, що жодна із проаналізованих моделей не може бути перенесена у національну систему державного управління в незмінному вигляді. Українські умови характеризуються одночасною дією декількох факторів: збройною агресією, необхідністю протидії інформаційно-психологічним операціям та кібератакам, цифровою трансформацією публічного управління, європейською інтеграцією та необхідністю збереження демократичних стандартів і прав людини. Тому більш доцільним є селективно-комбінований підхід, який передбачає адаптацію окремих елементів міжнародних моделей відповідно до функціональних потреб української системи державного управління.

З американського досвіду найбільш перспективними для України є механізми стратегічної координації, державно-приватної взаємодії та інтеграції інформаційної і кібернетичної безпеки у систему національної безпеки. Канадський досвід є цінним з позиції поєднання безпеки державних цифрових систем із розвитком електронного урядування та інформаційної стійкості суспільства. Німецька практика має особливе значення у контексті європейської інтеграції України, оскільки демонструє необхідність забезпечення балансу між безпековими потребами держави та гарантіями захисту персональних даних і прав людини [6]. Французький досвід є корисним для розвитку міжвідомчої та багаторівневої системи реагування на інформаційні загрози із залученням правоохоронного, безпекового, технологічного й експертного середовищ.

Зокрема, міжнародний досвід доцільно розглядати не як сукупність готових управлінських рішень для запозичення, а як ресурс для формування власної адаптивної моделі державного управління інформаційною політикою України [5]. Її ключовою характеристикою має стати здатність поєднати централізоване стратегічне управління з міжвідомчою та міжсекторальною взаємодією, технологічну спроможність із належним правовим регулюванням, а безпекові потреби держави – із забезпеченням інформаційних прав і свобод людини.

Узагальнення результатів порівняльного аналізу вказує на те, що ефективність державного управління інформаційною політикою визначається не стільки кількістю спеціалізованих державних інституцій або нормативно-правових актів, скільки характером їх функціональної взаємодії, узгодженістю управлінських рішень та спроможністю системи своєчасно адаптуватися до трансформації інформаційних загроз. Відповідно, особливого значення набуває формування цілісного механізму державного управління, у межах якого стратегічне планування, нормативно-правове регулювання, інституційна координація, технологічне забезпечення та контроль результативності функціонують як взаємопов'язані складові.

Таблиця 1

Порівняльна характеристика моделей державного управління інформаційною політикою

Критерій	США	Канада	Німеччина	Франція	Потенціал для України
Нормативно-правовий	Розгалужене безпекове та кіберрегулювання	Поєднання кібербезпеки, е-урядування і приватності	Сильний захист персональних даних та кібербезпеки	Комплексне міжгалузеве регулювання	Гармонізація безпекового законодавства зі стандартами ЄС і НАТО
Інституційний	Розподілена система спеціалізованих безпекових, розвідувальних і правоохоронних органів	Спеціалізовані органи кіберзахисту та реагування	Спеціалізовані федеральні структури та механізми координації	Поєднання центрального і регіонального рівнів	Чітке розмежування компетенцій і посилення координації
Організаційно-координаційний	Міжвідомча та державно-приватна взаємодія	Сильна державна координація	Держава + приватний IT-сектор	Міжвідомча та міжпрофесійна взаємодія	Єдиний координаційний контур та державно-приватне партнерство
Безпеково-технологічний	Кібероборона, превентивний моніторинг, захист критичних мереж	Захист державних систем і критичної інфраструктури	Ризик-орієнтований кіберзахист	Поєднання цивільного та військового реагування	Розвиток превентивної та ризик-орієнтованої системи
Домінуючий тип моделі	Безпеково-стратегічна	Державно-координаційна, суспільно орієнтована	Нормативно-інституційна, правозахисна	Міжвідомча, функціонально децентралізована	Селективно-комбінована адаптивна модель

Джерело: узагальнено та складено автором

Важливим результатом дослідження є встановлення того, що окремі переваги національних моделей мають взаємодоповнювальний характер. Зокрема, стратегічна спрямованість американського підходу може поєднуватися з канадськими механізмами забезпечення суспільної інформаційної стійкості, німецькими принципами правової визначеності та захисту інформаційних прав людини, а також французькою практикою багаторівневої міжвідомчої взаємодії. Таке поєднання створює концептуальне підґрунтя для формування національної моделі, орієнтованої одночасно на забезпечення інформаційної безпеки, розвиток цифрового середовища та дотримання демократичних принципів державного управління.

Водночас адаптація зарубіжного досвіду потребує врахування особливостей українського безпекового середовища. На відміну від держав, інформаційна політика яких розвивається переважно в умовах мирного часу, Україна змушена одночасно забезпечувати протидію інформаційно-психологічним операціям, кібернетичним загрозам, зовнішньому інформаційному впливу та деструктивним процесам у цифровому середовищі. Виникає необхідність поєднання довгострокових стратегічних пріоритетів із механізмами оперативного реагування, що забезпечують безперервність державного управління в умовах підвищеної безпекової невизначеності [6].

З огляду на зазначене, селективно-комбінований підхід до використання міжнародного досвіду доцільно розглядати як спосіб обґрунтованого добору та інтеграції управлінських практик, які відповідають національним інституційним можливостям, правовим зобов'язанням і актуальним безпековим потребам. Його практична реалізація передбачає визначення пріоритетних напрямів удосконалення державної інформаційної політики, встановлення відповідних управлінських інструментів та очікуваних результатів їх застосування.

Таблиця 2

Пріоритетні напрями адаптації міжнародного досвіду державного управління інформаційною політикою до умов України

Напрям удосконалення	**Зарубіжний досвід**	**Пропоновані управлінські заходи для України**	**Очікуваний результат**
Стратегічне управління	США	Узгодження стратегічних документів, визначення спільних пріоритетів інформаційної політики та безпеки	Послідовність і системність державної політики
Міжвідомча координація	США, Франція	Удосконалення обміну інформацією та процедур спільного реагування між державними інституціями	Зменшення дублювання функцій, оперативність рішень
Інформаційна стійкість суспільства	Канада	Розвиток цифрової грамотності, механізмів інформування населення та протидії дезінформації	Підвищення суспільної стійкості до інформаційних впливів
Нормативно-правове забезпечення	Німеччина	Узгодження інформаційної політики з європейськими стандартами захисту персональних даних і прав людини	Правова визначеність та захист інформаційних прав
Державно-приватна взаємодія	США, Німеччина	Розвиток партнерства з операторами критичної інфраструктури, технологічними компаніями та експертними установами	Посилення спроможностей кіберзахисту
Багаторівневе реагування	Франція	Розвиток взаємодії центральних і місцевих органів влади та спеціалізованих структур	Підвищення ефективності реагування на загрози
Моніторинг і оцінювання	Узагальнений міжнародний досвід	Запровадження показників результативності інформаційної політики, регулярного оцінювання ризиків і коригування рішень	Адаптивність і підзвітність державного управління

Джерело: узагальнено та складено автором

ВИСНОВКИ З ДАНОГО ДОСЛІДЖЕННЯ І ПЕРСПЕКТИВИ ПОДАЛЬШИХ РОЗВІДОК У ДАНОМУ НАПРЯМІ

За результатами проведеного дослідження встановлено, що сучасна державна інформаційна політика поступово трансформується від переважно нормативного регулювання інформаційних відносин до комплексного напряму публічного управління, який охоплює забезпечення інформаційної та кібернетичної безпеки, захист інформаційних прав людини, розвиток цифрового середовища, стратегічні комунікації та формування інформаційної стійкості держави і суспільства. В умовах зростання масштабів і складності інформаційних загроз ефективність державної інформаційної політики дедалі більше залежить від узгодженості управлінських механізмів, інституційної спроможності та здатності державних інституцій своєчасно реагувати на зміни безпекового середовища.

На основі порівняльного аналізу досвіду США, Канади, Німеччини та Франції систематизовано основні підходи до державного управління інформаційною політикою. Визначено, що американська модель характеризується переважно безпеково-стратегічною спрямованістю, канадська – державно-координаційним та суспільно орієнтованим характером, німецька – нормативно-інституційним підходом із вираженим правозахисним компонентом, а французька – міжвідомчою взаємодією та функціональною багаторівневістю. Встановлено, що відмінності між зазначеними моделями зумовлені особливостями політико-правових систем, розподілом управлінських повноважень, характером інформаційних загроз і пріоритетами національної безпекової політики.

Обґрунтовано, що спільною тенденцією розвитку державного управління інформаційною політикою в досліджуваних країнах є посилення міжвідомчої координації, розширення державно-приватної взаємодії, інтеграція технологічних інструментів захисту інформаційного середовища та підвищення значення стратегічного планування. Водночас встановлено, що універсальної моделі державного управління інформаційною політикою не існує, оскільки результативність окремих управлінських механізмів залежить від їх відповідності національним інституційним умовам і характеру безпекових викликів.

На основі узагальнення міжнародного досвіду обґрунтовано доцільність застосування селективно-комбінованого підходу до вдосконалення державного управління інформаційною політикою України, який передбачає цілеспрямований добір, поєднання та адаптацію окремих елементів зарубіжних моделей відповідно до національних потреб. Визначено пріоритетні напрями його реалізації, серед яких удосконалення стратегічного управління, посилення міжвідомчої координації, розвиток державно-приватного партнерства, гармонізація нормативно-правового забезпечення з європейськими стандартами, формування інформаційної стійкості суспільства та запровадження механізмів оцінювання результативності державної інформаційної політики.

Доведено доцільність формування адаптивної моделі державного управління інформаційною політикою України, заснованої на поєднанні централізованого стратегічного управління, функціонально розподіленої міжвідомчої взаємодії, технологічного забезпечення інформаційної безпеки та дотримання інформаційних прав і свобод людини. Практична реалізація запропонованого може сприяти підвищенню узгодженості управлінських рішень, розвитку інституційної спроможності держави та зміцненню інформаційної стійкості в умовах воєнних і гібридних загроз.

Перспективи подальших наукових досліджень пов’язані з розробленням організаційно-функціональних механізмів реалізації запропонованого підходу, визначенням критеріїв та показників результативності державної інформаційної політики, а також оцінюванням можливостей інтеграції окремих міжнародних управлінських практик у національну систему публічного управління з урахуванням безпекових потреб України та її євроінтеграційних зобов’язань.

ЛІТЕРАТУРА:

1. Виноградова Г. В. Правове регулювання інформаційних відносин в Україні : навч. посіб. Київ : Юстініан, 2006. 176 с.
2. Головко С., Головко Н. Державна інформаційна політика як інструмент протидії глобальним викликам і загрозам: міжнародний досвід та його імплементація в Україні. *Наукові праці Київського авіаційного інституту. Серія: Юридичний вісник «Повітряне і космічне право»*. 2025. № 1 (74). С. 71–78. DOI: https://doi.org/10.18372/2307-9061.74.19888
3. Килимник І. І. Інформаційне суспільство та інформаційна безпека. Нові виклики та шляхи подолання інформаційних загроз. *Науковий вісник Ужгородського національного університету. Серія: Право*. 2023. Вип. 76, ч. 2. DOI: https://doi.org/10.24144/2307-3322.2022.76.2.8
4. Лешик С. В. Особливості інформаційної політики в процесі євроінтеграції України. *Політологічний вісник*. 2024. Вип. 92. С. 198–211. DOI: https://doi.org/10.17721/2415-881x.2024.92.198-211
5. Мотлях О. Сучасна державна інформаційна політика України у сфері масмедіа. *Український інформаційний простір*. 2022. № 2 (10). С. 156–170. DOI: https://doi.org/10.31866/2616-7948.10.2022.269851
6. Федоренко Т. В. Теоретико-правові засади та механізми реалізації державної інформаційної політики України в умовах цифрової трансформації. Журнал східноєвропейського права. № 146. 2026. С. 437-443. DOI: https://doi.org/10.71404/24096415.146.45
7. Ржевська Н. Сучасна інформаційна політика: досвід США для України. *Політичні дослідження*. 2024. № 1 (7). С. 68–85. DOI: https://doi.org/10.53317/2786-4774-2024-1-4
8. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). *Official Journal of the European Union*. 2016. L 119. P. 1–88. URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj

9. Canadian Centre for Cyber Security. *National Cyber Threat Assessment 2025–2026*. Communications Security Establishment Canada, 2024. URL: https://www.cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2025-2026
10. Public Safety Canada. *Canada's National Cyber Security Strategy: Securing Canada's Digital Future*. Government of Canada, 2025. URL: https://www.securitepublique.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg-2025/index-en.aspx

REFERENCES:

1. Vynohradova, H. V. (2006). Pravove rehuliuvannia informatsiinykh vidnosyn v Ukraini [Legal regulation of information relations in Ukraine]. Kyiv: Yustynian. 176 p. [in Ukrainian].
2. Holovko, S., & Holovko, N. (2025). Derzhavna informatsiina polityka yak instrument protydii hlobalnym vyklykam i zahrozam: mizhnarodnyi dosvid ta yoho implementatsiia v Ukraini [State information policy as a tool for countering global challenges and threats: International experience and its implementation in Ukraine]. Yurydychnyi visnyk «Povitriane i kosmichne pravo», 1(74), 71–78. https://doi.org/10.18372/2307-9061.74.19888 [in Ukrainian].
3. Kylymnyk, I. I. (2023). Informatsiine suspilstvo ta informatsiina bezpeka: novi vyklyky ta shliakhy podolannia informatsiinykh zahroz [Information society and information security: New challenges and ways to overcome information threats]. Naukovyi visnyk Uzhhorodskoho natsionalnoho universytetu. Seriia: Pravo, 76(2). https://doi.org/10.24144/2307-3322.2022.76.2.8 [in Ukrainian].
4. Leshyk, S. V. (2024). Osoblyvosti informatsiinoi polityky v protsesi yevrointehratsii Ukrainy [Peculiarities of information policy in the process of Ukraine's European integration]. Politolohichnyi visnyk, (92), 198–211. https://doi.org/10.17721/2415-881x.2024.92.198-211 [in Ukrainian].
5. Motliakh, O. (2022). Suchasna derzhavna informatsiina polityka Ukrainy u sferi masmedia [Modern state information policy of Ukraine in the mass media sphere]. Ukrainskyi informatsiinyi prostir, 10(2), 156–170. https://doi.org/10.31866/2616-7948.10.2022.269851 [in Ukrainian].
6. Orlova, N. S., & Buryk, Z. M. (2021). Derzhavna informatsiina polityka v Ukraini u sferi okhorony zdorovia [State information policy in Ukraine in the field of healthcare]. Ekspert: paradyhmy yurydychnykh nauk i derzhavnoho upravlinnia, 2(14), 233–242. https://doi.org/10.32689/2617-9660-2021-2(14)-233-242 [in Ukrainian].
7. Rzhevska, N. (2024). Suchasna informatsiina polityka: dosvid SShA dlia Ukrainy [Modern information policy: U.S. experience for Ukraine]. Politychni doslidzhennia, 1(7), 68–85. https://doi.org/10.53317/2786-4774-2024-1-4 [in Ukrainian].
8. European Parliament and Council of the European Union. (2016). Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Official Journal of the European Union, L 119, 1–88. https://eur-lex.europa.eu/eli/reg/2016/679/oj [in English].
9. Canadian Centre for Cyber Security. (2024). National Cyber Threat Assessment 2025–2026. Communications Security Establishment Canada. Retrieved from: https://www.cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2025-2026 [in English].
10. Public Safety Canada. (2025). Canada's National Cyber Security Strategy: Securing Canada's Digital Future. Government of Canada. Retrieved from: https://www.securitepublique.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg-2025/index-en.aspx [in English].

DABIZHA Vira
HEI "Open International University of Human Development "Ukraine"

The study substantiates the feasibility of applying a selective and combined approach to adapting international experience within Ukraine's public administration system of information policy. This approach involves the selective integration of effective elements of foreign models, taking into account national security needs, institutional capacities, and European integration priorities. Priority areas for improving Ukraine's state information policy are systematized, including strategic planning, the development of interagency cooperation, improvement of the