УДК 351.86
JEL H11, H12, O38, L86
DOI https://doi.org/10.32782/2786-765X/2026-14-8

Гбур З.В.
доктор наук з державного управління, професор,
професор кафедри публічного управління та адміністрування,
Державний університет інформаційно-комунікаційних технологій
ORCID: https://orcid.org/0000-0003-4536-2438

МІЖНАРОДНИЙ ДОСВІД ДЕРЖАВНОГО РЕГУЛЮВАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УМОВАХ ГЛОБАЛЬНИХ ЦИВІЛІЗАЦІЙНИХ ВИКЛИКІВ: УРОКИ ДЛЯ УКРАЇНИ

У статті досліджено міжнародний досвід державного регулювання інформаційної безпеки в умовах глобальних цивілізаційних викликів та визначено можливості його адаптації з метою вдосконалення державної політики України у цій сфері. Обґрунтовано, що сучасні процеси цифровізації, глобалізації інформаційного простору, поширення технологій штучного інтелекту, великих даних і цифрових платформ, а також зростання масштабів кібернетичних загроз, дезінформації та інформаційних операцій зумовлюють необхідність формування комплексної та адаптивної системи забезпечення інформаційної безпеки держави. Проаналізовано підходи до державного регулювання інформаційної безпеки, сформовані в Європейському Союзі, США, Великій Британії, Естонії, Фінляндії, Сінгапурі та Ізраїлі. Встановлено, що ефективність сучасних моделей державного регулювання забезпечується поєднанням нормативно-правових, інституційних, організаційних і технологічних механізмів, розвитком міжвідомчої та міжсекторальної взаємодії, застосуванням ризик-орієнтованого підходу, безперервним моніторингом інформаційних ризиків, захистом критичної інформаційної інфраструктури та впровадженням інноваційних цифрових технологій. Визначено, що перспективними напрямами використання міжнародного досвіду в Україні є подальше вдосконалення нормативно-правового забезпечення, розвиток інституційних механізмів координації, інтеграція європейських стандартів інформаційної та кібернетичної безпеки, впровадження технологій штучного інтелекту та інтелектуальних систем моніторингу, посилення захисту критичної інформаційної інфраструктури, розвиток стратегічних комунікацій, протидія дезінформації та підвищення цифрової компетентності посадових осіб органів публічної влади. Зроблено висновок, що комплексна адаптація кращих міжнародних практик сприятиме підвищенню ефективності державного регулювання інформаційної безпеки, зміцненню національної безпеки, забезпеченню цифрової стійкості держави та формуванню сучасної системи публічного управління, здатної ефективно функціонувати й оперативно реагувати на інформаційні та кібернетичні загрози в умовах глобальних цивілізаційних трансформацій.

Ключові слова: державне регулювання, інформаційна безпека, глобалізація, цифровізація, правове регулювання, ризики.

Постановка проблеми. Сучасний етап розвитку світового співтовариства характеризується глибокими цивілізаційними трансформаціями, зумовленими цифровізацією суспільних процесів, стрімким розвитком інформаційно-комунікаційних технологій, поширенням технологій штучного інтелекту, зростанням ролі цифрових платформ і глобалізацією інформаційного простору. У цьому контексті особливого значення набуває вивчення міжнародного досвіду державного регулювання інформаційної безпеки. Аналіз таких практик дає змогу визначити найбільш ефективні інструменти державного регулювання та оцінити можливості їх адаптації до українських реалій з урахуванням сучасних безпекових викликів, євроінтеграційного курсу держави та необхідності підвищення ефективності системи публічного управління.

Аналіз останніх досліджень і публікацій. Вагомий внесок у дослідження теоретичних і практичних засад державного регулювання інформаційної безпеки, розвитку інформаційного суспільства, цифрової трансформації публічного управління, забезпечення національної та кібернетичної безпеки здійснили як вітчизняні, так і зарубіжні науковці. Серед українських дослідників вагомими є праці В. Б. Авер'янова [1], В. Д. Бакуменка [2], В. М. Князєва [3], Ю. В. Ковбасюка [4], В. С. Куйбіди [5], О. Ю. Оболенського [6], О. Ф. Андрійко [7], В. Г. Пилипчук [8], а також інших учених, які досліджують проблематику інформаційної політики держави, цифрового врядування, інформаційного права, кібербезпеки та державного управління в умовах сучасних безпекових викликів.

Незважаючи на вагомий науковий доробок, недостатньо дослідженими залишаються питання комплексної адаптації кращих міжнародних практик до української системи публічного управління, гармонізації

національного законодавства з європейськими стандартами у сфері інформаційної та кібернетичної безпеки, розвитку міжсекторальної взаємодії, цифрової стійкості державних інституцій, а також впровадження інноваційних технологій управління інформаційними ризиками в умовах сучасних глобальних цивілізаційних викликів.

Мета статті полягає у дослідженні міжнародного досвіду державного регулювання інформаційної безпеки в умовах глобальних цивілізаційних викликів, узагальненні сучасних підходів до формування ефективних моделей забезпечення інформаційної стійкості держави, визначенні ключових інструментів і механізмів державного регулювання, а також обґрунтуванні напрямів імплементації кращих міжнародних практик у систему публічного управління України з метою підвищення рівня інформаційної та національної безпеки.

Виклад основного матеріалу дослідження. Сучасний розвиток глобального інформаційного суспільства супроводжується масштабними цивілізаційними трансформаціями, що охоплюють усі сфери життєдіяльності держави та суспільства. Стрімке поширення цифрових технологій, розвиток штучного інтелекту, глобалізація інформаційного простору та зростання кількості інформаційних і кібернетичних загроз суттєво змінюють підходи до забезпечення національної безпеки. За цих умов інформаційна безпека перетворюється на один із ключових елементів державної політики, від ефективності якого залежить стійкість функціонування державних інституцій, захист національних інтересів і збереження інформаційного суверенітету. У зв'язку з цим особливої актуальності набуває вивчення міжнародного досвіду державного регулювання інформаційної безпеки та визначення можливостей його адаптації до сучасних умов розвитку України.

Саме тому вивчення міжнародного досвіду набуває особливого значення, оскільки дозволяє проаналізувати ефективні моделі державного регулювання, оцінити сучасні інституційні та нормативно-правові підходи, визначити дієві механізми координації між органами державної влади та адаптувати кращі світові практики до національної системи публічного управління [9]. Особливий інтерес становить досвід країн, які демонструють високий рівень цифрової зрілості, кіберстійкості та інституційної спроможності забезпечувати інформаційну безпеку в умовах сучасних глобальних викликів.

Проведений аналіз свідчить, що міжнародний досвід підтверджує перехід від фрагментарного реагування на інформаційні загрози до комплексних моделей державного регулювання, заснованих на принципах превентивності, цифрової стійкості та безперервного управління ризиками. Незважаючи на відмінності в інституційній побудові та нормативно-правовому забезпеченні, досвід Європейського Союзу, США, Великої Британії, Естонії, Фінляндії, Сінгапуру та Ізраїлю демонструє спільні закономірності розвитку систем інформаційної безпеки. Встановлено, що ефективність реалізації державної політики у цій сфері забезпечується комплексним поєднанням сучасної нормативно-правової бази, високої інституційної спроможності органів державної влади, дієвої міжвідомчої координації, розвитку цифрової інфраструктури, застосування ризик-орієнтованого підходу до управління інформаційними загрозами, захисту критичної інформаційної інфраструктури, формування систем кіберстійкості, а також активної взаємодії державного, приватного й громадського секторів. Для України особливе значення має адаптація цих підходів з урахуванням національних безпекових пріоритетів, процесів європейської інтеграції та необхідності підвищення стійкості системи публічного управління до сучасних цивілізаційних викликів.

Особливу увагу в сучасних умовах доцільно приділити європейським підходам до забезпечення інформаційної безпеки, які формуються в контексті цифрової трансформації, розвитку цифрового єдиного ринку та посилення стійкості держав-членів Європейського Союзу до інформаційних і кібернетичних загроз. На відміну від традиційних моделей, орієнтованих переважно на реагування на інциденти, сучасна європейська модель базується на превентивному управлінні ризиками, міжвідомчій координації, гармонізації нормативно-правового забезпечення та розвитку цифрової стійкості критичної інформаційної інфраструктури [11].

Узагальнення міжнародного досвіду свідчить, що сучасні моделі державного регулювання інформаційної безпеки еволюціонували від переважно реактивного реагування на загрози до комплексних систем стратегічного управління, орієнтованих на запобігання ризикам, підвищення цифрової стійкості та забезпечення безперервності функціонування державних інституцій. Аналіз практик Європейського Союзу, США, Великої Британії, Естонії, Фінляндії, Сінгапуру та Ізраїлю дає підстави стверджувати, що ефективність

Таблиця 1

Порівняльний аналіз міжнародних моделей державного регулювання інформаційної безпеки та можливостей їх адаптації в Україні

Країна	Основні підходи до державного регулювання інформаційної безпеки	Практичне значення для України
ЄС	Формування єдиної політики інформаційної та кібербезпеки, гармонізація законодавства держав-членів, розвиток цифрової стійкості, управління ризиками, посилення захисту критичної інфраструктури, функціонування спільних механізмів реагування на кіберінциденти.	Гармонізація українського законодавства з європейськими стандартами, розвиток цифрової стійкості державних інституцій, впровадження ризик-орієнтованого управління та інтегрованої системи кіберзахисту.
США	Комплексна модель державного регулювання, заснована на стратегічному плануванні, діяльності спеціалізованих федеральних органів, захисті критичної інфраструктури, використанні технологій штучного інтелекту та активному державно-приватному партнерстві.	Посилення міжвідомчої координації, розвиток державно-приватного партнерства, створення єдиної системи управління інформаційними ризиками та прогнозування загроз.
Велика Британія	Інтеграція інформаційної безпеки з національною безпекою, функціонування єдиного центру кібербезпеки, розвиток стратегічних комунікацій, захист інформаційного простору та цифрових державних сервісів.	Удосконалення стратегічних комунікацій, централізація координації реагування на інформаційні загрози, підвищення стійкості державних цифрових сервісів.
Естонія	Побудова цифрової держави на принципах безпечного обміну даними, електронної ідентифікації, децентралізованої цифрової інфраструктури, високого рівня кіберзахисту та цифрової довіри.	Подальший розвиток електронного урядування, інтеграція державних інформаційних ресурсів, удосконалення системи електронної ідентифікації та захисту державних реєстрів.
Фінляндія	Формування загальнодержавної моделі інформаційної стійкості, розвиток медіаграмотності населення, протидія дезінформації, комплексна взаємодія органів влади, бізнесу, науки та громадянського суспільства.	Розвиток інформаційної стійкості суспільства, удосконалення державної політики у сфері медіаграмотності, протидії дезінформації та кризових комунікацій.
Сінгапур	Централізоване управління цифровою безпекою, широке використання інтелектуальних цифрових технологій, цифрове врядування, постійний моніторинг ризиків, високий рівень захисту державної інформаційної інфраструктури.	Запровадження інтелектуальних систем аналізу інформаційних загроз, автоматизація управлінських процесів, розвиток цифрової державної інфраструктури.
Ізраїль	Поєднання інформаційної безпеки, кібероборони та національної безпеки, функціонування спеціалізованої системи кіберзахисту, розвиток інновацій, технологічних стартапів і безперервного моніторингу загроз.	Посилення інноваційної складової державного регулювання, розвиток національної системи кібероборони, впровадження сучасних технологій прогнозування та нейтралізації інформаційних загроз.

Джерело: сформовано автором на основі даних [10]

державної політики у сфері інформаційної безпеки забезпечується реалізацією таких взаємопов'язаних принципів [12]:

1. Адаптивність державного регулювання. Сучасні системи інформаційної безпеки функціонують на основі постійного оновлення нормативно-правової бази, інституційних механізмів та управлінських процедур відповідно до нових цифрових ризиків. Показовим прикладом є прийняття в Європейському Союзі Директиви NIS2, яка значно розширила сферу регулювання порівняно з попередньою редакцією та врахувала сучасні загрози цифрового середовища.

2. Проактивність державної політики. Провідні країни світу дедалі більше орієнтуються не на ліквідацію наслідків інформаційних інцидентів, а на їх своєчасне попередження. Це реалізується через системи раннього виявлення загроз, стратегічне планування, постійне оцінювання ризиків, моделювання кризових ситуацій та регулярне проведення міжвідомчих навчань, що дозволяє мінімізувати потенційні негативні наслідки для держави.

3. Технологічна інноваційність. Ефективність державного регулювання забезпечується активним використанням сучасних цифрових технологій, зокрема штучного інтелекту, аналітики великих даних, машинного навчання, хмарних технологій, автоматизованих систем моніторингу та прогнозування кіберзагроз. Такі підходи широко застосовуються у США,

Сінгапурі та Ізраїлі для оперативного аналізу інформаційних ризиків і підтримки управлінських рішень.

4. Міжсекторальне партнерство. Практика провідних держав демонструє, що забезпечення інформаційної безпеки не може бути виключною функцією державних органів. Висока ефективність досягається завдяки налагодженню системної взаємодії між органами влади, приватним сектором, науковими установами, громадянським суспільством та операторами критичної інфраструктури. Саме така модель співпраці є одним із базових принципів політики Європейського Союзу та США.

5. Безперервний моніторинг інформаційних ризиків. У більшості розвинених країн функціонують інтегровані системи моніторингу цифрового середовища, які забезпечують постійний аналіз кіберінцидентів, оцінювання вразливостей інформаційних систем, обмін інформацією між компетентними органами та оперативне реагування на нові виклики. Такий підхід дозволяє своєчасно виявляти потенційні загрози та підвищувати рівень кіберстійкості держави.

Таким чином, результати проведеного аналізу підтверджують, що сучасні моделі державного регулювання інформаційної безпеки ґрунтуються на інтеграції адаптивних механізмів управління, проактивної державної політики, інноваційних цифрових технологій, міжсекторальної взаємодії, системного моніторингу ризиків і стратегічного прогнозування. Саме комплексне поєднання зазначених принципів забезпечує високий рівень готовності держав до своєчасного виявлення, попередження та нейтралізації сучасних інформаційних і кібернетичних загроз, а також створює передумови для формування стійкої, гнучкої та ефективної системи державного регулювання інформаційної безпеки. Для України врахування цих принципів є необхідною умовою модернізації національної системи публічного управління та її адаптації до сучасних безпекових і євроінтеграційних викликів.

З урахуванням результатів проведеного аналізу можна стверджувати, що для України особливого значення набуває не механічне запозичення зарубіжних практик, а їх адаптація до національних безпекових пріоритетів, інституційних особливостей та євроінтеграційного курсу держави. У цьому контексті перспективними напрямами використання міжнародного досвіду є:

1. Удосконалення нормативно-правового забезпечення інформаційної безпеки. Пріоритетним завданням є подальша гармонізація національного законодавства з європейськими стандартами шляхом імплементації положень Директиви NIS2, Регламенту DORA, GDPR, Cybersecurity Act та інших міжнародних документів. Це сприятиме формуванню цілісної нормативної основи державного регулювання, заснованої на ризик-орієнтованому підході, цифровій стійкості та належному захисті інформаційних ресурсів.

2. Розвиток інституційних механізмів координації. Враховуючи досвід країн Європейського Союзу, США та Великої Британії, доцільним є посилення координації діяльності органів державної влади, сектору безпеки і оборони, операторів критичної інфраструктури, приватного сектору та наукової спільноти. Це дозволить забезпечити своєчасний обмін інформацією, узгоджене реагування на інформаційні загрози та ефективне управління кризовими ситуаціями.

3. Інтеграція європейських стандартів інформаційної та кібернетичної безпеки. Важливим напрямом є впровадження сучасних стандартів управління інформаційною безпекою, систем оцінювання ризиків, сертифікації цифрових продуктів і механізмів захисту критичної інформаційної інфраструктури відповідно до європейських практик. Це сприятиме зміцненню цифрової стійкості державних інституцій та підвищенню рівня довіри до цифрових сервісів.

4. Впровадження інтелектуальних цифрових технологій у систему державного управління. Міжнародний досвід свідчить про доцільність використання технологій штучного інтелекту, аналітики великих даних, машинного навчання, автоматизованих систем моніторингу та прогнозування для виявлення інформаційних загроз, аналізу ризиків, підтримки прийняття управлінських рішень і підвищення оперативності реагування на кризові ситуації.

5. Посилення захисту критичної інформаційної інфраструктури. Особливої актуальності набуває впровадження комплексної системи управління безпекою критичних інформаційних ресурсів, що передбачає регулярне оцінювання вразливостей, аудит інформаційної безпеки, резервування цифрових ресурсів, розвиток центрів реагування на кіберінциденти та забезпечення безперервності функціонування державних інформаційних систем.

Отже, адаптація кращих міжнародних практик має здійснюватися комплексно, поєднуючи нормативно-правові, організаційні, інституційні, технологічні та кадрові складові

державного регулювання. Такий підхід сприятиме підвищенню ефективності державної політики у сфері інформаційної безпеки, зміцненню національної безпеки, забезпеченню цифрової стійкості держави та формуванню сучасної системи публічного управління, здатної своєчасно реагувати на сучасні інформаційні й кібернетичні загрози. Водночас імплементація міжнародного досвіду створить передумови для поглиблення інтеграції України до європейського безпекового та цифрового простору, підвищення інституційної спроможності органів публічної влади та забезпечення ефективного функціонування державних інститутів в умовах сучасних глобальних цивілізаційних викликів.

Висновки. Проведене дослідження підтвердило, що в умовах сучасних глобальних цивілізаційних викликів інформаційна безпека перетворюється на один із визначальних пріоритетів державної політики, від рівня забезпечення якого залежить стійкість системи публічного управління, захист національних інтересів, безперервність функціонування критичної інформаційної інфраструктури та ефективність цифрової трансформації держави. Аналіз міжнародного досвіду засвідчив, що провідні країни світу реалізують комплексні моделі державного регулювання інформаційної безпеки, які поєднують сучасне нормативно-правове забезпечення, високий рівень інституційної спроможності органів державної влади, ризик-орієнтоване управління, міжвідомчу координацію, розвиток цифрової інфраструктури, систем кіберстійкості, стратегічних комунікацій та активне державно-приватне партнерство. Реалізація зазначених напрямів сприятиме формуванню сучасної, стійкої та ефективної системи державного регулювання інформаційної безпеки, здатної забезпечити належний рівень захисту національного інформаційного простору, зміцнення національної безпеки та підвищення ефективності публічного управління в умовах сучасних глобальних цивілізаційних викликів.

Бібліографічний список

1. Авер'янов В. Б. (ред.). Державне управління: європейські стандарти, досвід та адміністративне право. Київ : Юстиніан, 2007. 288 с. URL: https://nvd-nanu.org.ua/7c52a469-d636-cb46-a13a-086f454cd14f/
2. Бакуменко В. Д., Руденко О. М., Туча В. В. Механізми імплементації політичних рішень в державному управлінні : монографія. Київ : АМУ, 2015. 184 с.
3. Князєв В. М. Філософія державного управління, її сутність, особливості та проблемне поле дослідження. *Вісник Національної академії державного управління при Президентові України.* 2014. № 1. С. 5–10. URL: http://nbuv.gov.ua/UJRN/Vnadu_2014_1_3
4. Ковбасюк Ю. В. Енциклопедія державного управління. Том 8. URL: https://irbis-nbuv.gov.ua/ulib/item/ukr0000022817
5. Куйбіда В. С., Петроє О. М., Федулова Л. І.,. Андрощук Г. О. Цифрові компетенції як умова формування якості людського капіталу. *Збірник наукових праць Національної академії державного управління при Президентові України.* 2019. Вип. 1. С. 118-133. URL: http://nbuv.gov.ua/UJRN/znpnadu_2019_1_16
6. Державна служба : підручник : у 2 т. / Нац. акад. держ. упр. при Президентові України ; редкол. : Ю. В. Ковбасюк (голова), О. Ю. Оболенський (заст. голови), С. М. Серьогін (заст. голови) [та ін.]. Київ ; Одеса : НАДУ, 2012. Т. 1. 372 с. URL: https://ktpu.kpi.ua/wp-content/uploads/2014/02/DERZHAVNA-SLUZHBA-tom1-2012.pdf
7. Андрійко О. Ф. Організаційно-правові проблеми державного контролю у сфері виконавчої влади : дис... д-ра юрид. наук: 12.00.07; НАН України, Інститут держави і права ім. В.М. Корецького. Київ, 1999. 378 с.
8. Пилипчук В. Г. Теоретико-правові проблеми розвитку законодавства у сфері національної та інформаційної безпеки України. *Інформація і право.* 2025. №2 (53). С. 9–22. DOI: https://doi.org/10.37750/2616-6798.2025.2(53).334015
9. Бондаренко Р. В., Михальчук В. М. Інформаційна безпека держави. *Інвестиції: практика та досвід.* 2021. № 5. С. 95–101. DOI: https://doi.org/10.32702/2306-6814.2021.5.95
10. Баранов О. А. Правове забезпечення інформаційної сфери: теорія, методологія і практика : монографія. Київ : Видавничий дім «АртЕк», 2014. URL: https://ippi.org.ua/pravove-zabezpechennya-informatsiinoi-sferi-teoriya-metodologiya-i-praktika
11. Антонова С. Є., Мартинюк Г. Ф. Інформаційна безпека. *Державне управління: удосконалення та розвиток.* 2019. № 11. URL: http://www.dy.nayka.com.ua/pdf/11_2019/38.pdf
12. Шатун В. Т., Гладун О. В. Інформаційна безпека – невід'ємна складова національної безпеки України. *Наукові праці Чорноморського державного університету імені Петра Могили комплексу «Києво-Могилянська академія». Серія : Державне управління.* 2016. Т. 267, Вип. 255. С. 174–180. URL: http://nbuv.gov.ua/UJRN/Npchdu_2016_267_255_29

References

1. Averianov V. B. (Ed.) (2007). Derzhavne upravlinnia: yevropeiski standarty, dosvid ta administratyvne pravo [Public Administration: European Standards, Experience and Administrative Law]. Kyiv: Yustinian, 288 p. Available at: https://nvd-nanu.org.ua/7c52a469-d636-cb46-a13a-086f454cd14f/
2. Bakumenko V. D., Rudenko O. M., Tucha V. V. (2015). Mekhanizmy implementatsii politychnykh rishen v derzhavnomu upravlinni [Mechanisms for the Implementation of Political Decisions in Public Administration]. Kyiv: Academy of Municipal Administration, 184 p.
3. Kniaziev V. M. (2014). Filosofiia derzhavnoho upravlinnia, yii sutnist, osoblyvosti ta problemne pole doslidzhennia [The Philosophy of Public Administration: Essence, Features and Research Problems]. *Visnyk Natsionalnoi akademii derzhavnoho upravlinnia pry Prezydentovi Ukrainy – Bulletin of the National Academy of Public Administration under the President of Ukraine*, no. 1, pp. 5–10. Available at: http://nbuv.gov.ua/UJRN/Vnadu_2014_1_3
4. Kovbasiuk Yu. V. (Ed.) (2011). Entsyklopediia derzhavnoho upravlinnia [Encyclopedia of Public Administration]. Vol. 8. Available at: https://irbis-nbuv.gov.ua/ulib/item/ukr0000022817
5. Kuibida V. S., Petroie O. M., Fedulova L. I., Androshchuk H. O. (2019). Tsyfrovi kompetentsii yak umova formuvannia yakosti liudskoho kapitalu [Digital Competencies as a Condition for Human Capital Quality Formation]. *Zbirnyk naukovykh prats Natsionalnoi akademii derzhavnoho upravlinnia pry Prezydentovi Ukrainy – Collection of Scientific Papers of the National Academy of Public Administration under the President of Ukraine*, vol. 1, pp. 118–133. Available at: http://nbuv.gov.ua/UJRN/znpnadu_2019_1_16
6. Kovbasiuk Yu. V., Obolenskyi O. Yu., Serohin S. M. et al. (Eds.) (2012). Derzhavna sluzhba [Civil Service]. Vol. 1. Kyiv; Odesa: NAPA, 372 p. Available at: https://ktpu.kpi.ua/wp-content/uploads/2014/02/DERZHAVNA-SLUZHBA-tom1-2012.pdf
7. Andriiko O. F. (1999). Orhanizatsiino-pravovi problemy derzhavnoho kontroliu u sferi vykonavchoi vlady [Organizational and Legal Problems of State Control in the Executive Branch] (Doctoral dissertation). V. M. Koretsky Institute of State and Law of NAS of Ukraine, Kyiv.
8. Pylypchuk V. H. (2025). Teoretyko-pravovi problemy rozvytku zakonodavstva u sferi natsionalnoi ta informatsiinoi bezpeky Ukrainy [Theoretical and Legal Problems of the Development of Legislation in the Field of National and Information Security of Ukraine]. *Informatsiia i pravo – Information and Law*, no. 2 (53), pp. 9–22. DOI: https://doi.org/10.37750/2616-6798.2025.2(53).334015
9. Bondarenko R. V., Mykhalchuk V. M. (2021). Informatsiina bezpeka derzhavy [Information Security of the State]. *Investytsii: praktyka ta dosvid – Investments: Practice and Experience*, no. 5, pp. 95–101. DOI: https://doi.org/10.32702/2306-6814.2021.5.95
10. Baranov O. A. (2014). Pravove zabezpechennia informatsiinoi sfery: teoriia, metodolohiia i praktyka [Legal Support of the Information Sphere: Theory, Methodology and Practice]. Kyiv: ArtEk. Available at: https://ippi.org.ua/pravove-zabezpechennya-informatsiinoi-sferi-teoriya-metodologiya-i-praktika
11. Antonova S. Ye., Martyniuk H. F. (2019). Informatsiina bezpeka [Information Security]. *Derzhavne upravlinnia: udoskonalennia ta rozvytok – Public Administration: Improvement and Development*, no. 11. Available at: http://www.dy.nayka.com.ua/pdf/11_2019/38.pdf
12. Shatun V. T., Hladun O. V. (2016). Informatsiina bezpeka – nevidiemna skladova natsionalnoi bezpeky Ukrainy [Information Security as an Integral Component of the National Security of Ukraine]. *Naukovi pratsi Chornomorskoho derzhavnoho universytetu imeni Petra Mohyly. Seriia: Derzhavne upravlinnia – Scientific Works of Petro Mohyla Black Sea State University. Series: Public Administration*, vol. 267, no. 255, pp. 174–180. Available at: http://nbuv.gov.ua/UJRN/Npchdu_2016_267_255_29

Zoriana Hbur
Doctor of Science in Public Administration, Professor,
Professor of the Department of Public Administration and Administration,
State University of Information and Communication Technologies
ORCID: https://orcid.org/0000-0003-4536-2438

INTERNATIONAL EXPERIENCE IN GOVERNMENT REGULATION OF INFORMATION SECURITY IN THE CONTEXT OF GLOBAL CIVILIZATIONAL CHALLENGES: LESSONS FOR UKRAINE

This article examines international experience in state regulation of information security in the context of global civilizational challenges and identifies opportunities for its adaptation to improve Ukraine's state policy in this field. It is substantiated that contemporary processes of digitalization, globalization of the information space, the proliferation of artificial intelligence technologies, big data and digital platforms, as well as the increasing scale of cyber threats, disinformation and information operations necessitate the development of a comprehensive and adaptive system for ensuring state information security. The approaches to state regulation of information security implemented in the European Union, the United States, the United Kingdom, Estonia, Finland, Singapore and Israel are analyzed. It is established that the effectiveness of modern regulatory models is ensured through a

combination of legal, institutional, organizational and technological mechanisms, the development of interagency and cross-sectoral cooperation, the application of a risk-based approach, continuous monitoring of information risks, protection of critical information infrastructure and the implementation of innovative digital technologies. The study identifies promising areas for applying international experience in Ukraine, including further improvement of the regulatory framework, development of institutional coordination mechanisms, integration of European information and cybersecurity standards, implementation of artificial intelligence technologies and intelligent monitoring systems, strengthening the protection of critical information infrastructure, development of strategic communications, countering disinformation and enhancing the digital competence of public officials. It is concluded that the comprehensive adaptation of best international practices will contribute to improving the effectiveness of state regulation of information security, strengthening national security, ensuring the digital resilience of the state and developing a modern public administration system capable of functioning effectively and responding promptly to information and cyber threats amid global civilizational transformations.

Keywords: state regulation, information security, globalization, digitalization, legal regulation, risks.

Дата надходження статті: 12.07.2026
Дата прийняття статті до публікації: 11.08.2026
Дата публікації статті: 02.09.2026