УДК 351:004.056
DOI 10.15673/fie.v18i2.3584

**Гбур З.В.**
доктор наук з державного управління, професор
кафедра публічного управління та адміністрування
Заклад вищої освіти Державний університет інформаційно-комунікаційних технологій
вул. Солом'янська, 7, м. Київ, Україна, 03110
E-mail: ernest-natan@ukr.net
ORCID ID: https://orcid.org/0000-0003-4536-2438

# СТРАТЕГІЧНІ НАПРЯМИ РОЗВИТКУ ДЕРЖАВНОГО РЕГУЛЮВАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УМОВАХ СУЧАСНИХ ЦИВІЛІЗАЦІЙНИХ ВИКЛИКІВ

У статті досліджено актуальні питання розвитку державного регулювання інформаційної безпеки в умовах сучасних цивілізаційних викликів, зумовлених процесами глобалізації, цифрової трансформації суспільства, стрімким розвитком інформаційно-комунікаційних технологій, поширенням штучного інтелекту, кіберзагроз, інформаційно-психологічних операцій та гібридних форм ведення війни. Обґрунтовано, що інформаційна безпека набуває статусу одного з ключових елементів забезпечення національної безпеки держави та є важливою передумовою сталого функціонування системи публічного управління, розвитку інформаційного суспільства й захисту національних інтересів. Встановлено, що сучасні цивілізаційні виклики потребують переосмислення традиційних підходів до забезпечення інформаційної безпеки, переходу від переважно реактивної моделі державного управління до стратегічного, ризик-орієнтованого та проактивного управління інформаційними загрозами. Доведено, що стратегічний розвиток державного регулювання інформаційної безпеки повинен ґрунтуватися на принципах системності, адаптивності, комплексності, міжсекторальної взаємодії, відкритості, цифрової трансформації, верховенства права та збалансованого поєднання інтересів держави, суспільства і людини. Аргументовано необхідність формування сучасної моделі державного регулювання, здатної своєчасно реагувати на динамічні зміни безпекового середовища та забезпечувати стійкість інформаційного простору України.

**Ключові слова:** державне регулювання, інформаційна безпека, державна стратегія, національна безпека, цивілізаційні виклики, інформаційна політика, інформаційні загрози, інформаційне суспільство, публічне управління, правове регулювання.



**Постановка проблеми та її зв'язок з важливими науковими та практичними завданнями.** Стрімкий розвиток інформаційно-комунікаційних технологій, цифровізація суспільних процесів, поширення штучного інтелекту, зростання масштабів кіберзлочинності, інформаційно-психологічних операцій, дезінформації та інших проявів гібридного впливу суттєво трансформують сучасне безпекове середовище. За таких умов інформаційна безпека перетворюється на один із ключових чинників забезпечення національної безпеки, державного суверенітету, демократичного розвитку та стійкого функціонування системи публічного управління. Для України проблема забезпечення інформаційної безпеки набуває особливої актуальності в умовах повномасштабної військової агресії Російської Федерації, коли інформаційний простір став одним із головних театрів протиборства. Систематичне використання інформаційно-психологічних операцій, маніпулятивних технологій, кібератак, кампаній із поширення дезінформації та інших інструментів гібридної війни обумовлює необхідність перегляду існуючих підходів до державного регулювання інформаційної безпеки та формування ефективної системи стратегічного управління інформаційними ризиками.

Попри значну кількість наукових досліджень, присвячених проблемам інформаційної безпеки, недостатньо уваги приділено комплексному обґрунтуванню стратегічних напрямів розвитку державного регулювання інформаційної безпеки саме в контексті сучасних цивілізаційних викликів, що зумовлює необхідність подальших наукових пошуків у цьому напрямі.

**Аналіз останніх публікацій по проблемі.** Питання державного регулювання інформаційної безпеки, розвитку системи публічного управління, формування державної інформаційної політики та забезпечення національної безпеки перебувають у

центрі уваги як вітчизняних, так і зарубіжних науковців.

Теоретико-методологічні засади державного управління, розвитку механізмів публічного адміністрування та державної політики висвітлено у працях С. О. Лисенко[1], Ю. О. Саричев [2], А. М. Сиротенко [3], О. І. Пархоменко-Куцевіл [4], В. В. Димитрієв [5], Л. М. Мельник [6], В. Д. Галіпчак [7], М. М. Пендюра [8], В. Ф. Загурська-Антонюк [9] та інших учених. Окремі аспекти забезпечення національної та інформаційної безпеки в умовах цифрової трансформації, розвитку цифрового врядування, кіберпростору та стратегічних комунікацій розглянуто у працях В. М. Грицай [10], В. В. Дабіжа [11], О. В. Карпенко [12] та інших науковців.

Водночас аналіз наукових праць свідчить, що, попри значний доробок учених у сфері державного регулювання інформаційної безпеки, недостатньо дослідженими залишаються питання формування стратегічних напрямів розвитку державного регулювання інформаційної безпеки саме в умовах сучасних цивілізаційних викликів. Подальшого наукового обґрунтування потребують концептуальні засади переходу до стратегічної, ризик-орієнтованої та проактивної моделі державного регулювання, удосконалення міжсекторальної взаємодії, розвитку цифрової стійкості держави та адаптації механізмів публічного управління до сучасних інформаційних загроз, що й обумовлює актуальність цього дослідження.

**Формулювання цілей дослідження**. Обґрунтування стратегічних напрямів розвитку державного регулювання інформаційної безпеки в умовах сучасних цивілізаційних викликів на основі комплексного аналізу сучасних інформаційних загроз, тенденцій цифрової трансформації, розвитку інформаційного суспільства та функціонування системи публічного управління.

**Виклад основних результатів та їх обґрунтування**. Імпорт в умовах сучасних цивілізаційних трансформацій інформаційна безпека стала одним із визначальних чинників забезпечення національної безпеки, стійкого розвитку держави та ефективного функціонування системи публічного управління. Динамічний характер інформаційних загроз, поширення цифрових технологій і зростання масштабів гібридного протиборства зумовлюють необхідність переосмислення стратегічних підходів до державного регулювання у сфері інформаційної безпеки.

Сучасний стан державного регулювання інформаційної безпеки в Україні формується під впливом масштабних трансформацій безпекового середовища, пов'язаних із цифровізацією суспільства, розвитком інформаційно-комунікаційних технологій, поширенням гібридних загроз та необхідністю адаптації національної системи безпеки до міжнародних стандартів, зокрема вимог ЄС у сфері кібербезпеки (Директива NIS2), операційної цифрової стійкості (DORA), захисту персональних даних (GDPR), міжнародних стандартів управління інформаційною безпекою серії ISO/IEC 27000 та рекомендацій НАТО щодо підвищення кіберстійкості. Їх імплементація створює передумови для впровадження ризик-орієнтованого управління, посилення захисту критичної інформаційної інфраструктури, розвитку міжвідомчої взаємодії та підвищення стійкості державної системи інформаційної безпеки [1].

Упродовж останніх років спостерігається послідовне вдосконалення нормативно-правового забезпечення, інституційної структури та механізмів реалізації державної політики у сфері інформаційної безпеки. Водночас ефективність державного регулювання значною мірою залежить від своєчасного врахування комплексу зовнішніх і внутрішніх чинників, які визначають тенденції розвитку інформаційного простору та характер сучасних загроз [2]:

1) Зовнішні фактори – повномасштабна військова агресія проти України, гібридні загрози, геополітична нестабільність, транснаціональна кіберзлочинність, розвиток штучного інтелекту, глобальна цифровізація та інтеграційні процеси у сфері міжнародної безпеки.

2) Внутрішні фактори – рівень розвитку цифрової інфраструктури держави, ефективність функціонування системи публічного управління, стан нормативно-правового забезпечення, якість міжвідомчої взаємодії, кадровий потенціал, рівень цифрової та медіаграмотності населення, а також ресурсне забезпечення реалізації державної політики у сфері інформаційної безпеки.

Отже, сучасний розвиток державного регулювання інформаційної безпеки характеризується переходом до стратегічної моделі управління, орієнтованої на забезпечення стійкості інформаційного простору, підвищення адаптивності державних інституцій та своєчасне реагування на динамічні інформаційні загрози. За таких умов пріоритетного значення набуває формування комплексної державної політики, яка поєднуватиме правові, організаційні, інституційні та технологічні механізми забезпечення інформаційної безпеки відповідно до сучасних цивілізаційних викликів.

Аналіз сучасних тенденцій розвитку інформаційного середовища свідчить, що традиційні підходи до державного регулювання інформаційної безпеки, які переважно ґрунтувалися на реагуванні на вже реалізовані загрози, дедалі менше відповідають сучасним умовам. Динамічність цифрової трансформації, зростання кількості інформаційно-психологічних операцій, активне використання штучного інтелекту, поширення технологій глибокої підробки (deepfake), кіберзлочинності та дезінформації суттєво скорочують часовий проміжок між виникненням загрози та її реалізацією. За таких умов державне регулювання має бути спрямоване не лише на ліквідацію наслідків інформаційних атак, а насамперед на їх своєчасне прогнозування, попередження та мінімізацію потенційних ризиків [3].

Зазначені тенденції підтверджуються не лише теоретичними положеннями, а й сучасною статистикою,

яка демонструє стале зростання інтенсивності інформаційних і кібернетичних загроз, а також ускладнення інструментів їх реалізації. Аналіз офіційних даних свідчить, що інформаційний простір України залишається одним із ключових об'єктів впливу в умовах гібридної війни, що обумовлює необхідність подальшого вдосконалення стратегічних механізмів державного регулювання інформаційної безпеки.

За офіційними даними Національної команди реагування на кіберінциденти CERT-UA, упродовж 2025 року було опрацьовано 5927 кіберінцидентів, що на 37,4 % більше, ніж у 2024 році (4315 кіберінцидентів). Найбільш уразливими залишалися органи державної влади, сектор безпеки і оборони, енергетична галузь, телекомунікації та об'єкти критичної інформаційної інфраструктури. Зростання кількості зафіксованих інцидентів обумовлене як підвищенням інтенсивності ворожих кібератак, так і вдосконаленням механізмів їх виявлення та реагування.

Водночас результати аналізу II півріччя 2025 року, оприлюднені у 2026 році, свідчать про певну зміну характеру сучасних інформаційних загроз. Загальна кількість кіберінцидентів зменшилася приблизно на 4 % порівняно з попереднім півріччям, однак значно зросла складність атак. Основними тенденціями стали активне використання методів соціальної інженерії, стандартизація інструментів хакерських угруповань, застосування технологій штучного інтелекту для створення фішингових кампаній, автоматизація збору розвідувальної інформації та використання deepfake-технологій під час інформаційно-психологічних операцій.

Загальносвітові тенденції також підтверджують посилення ролі цифрових технологій у сучасному інформаційному протиборстві. За оцінками міжнародних експертів, у 2025–2026 роках суттєво зросло використання генеративного штучного інтелекту для проведення цілеспрямованих фішингових атак, створення синтетичних цифрових особистостей, deepfake-контенту та автоматизації інформаційно-психологічного впливу, що свідчить про трансформацію кіберзагроз від поодиноких технічних атак до комплексних інформаційних операцій, що поєднують технологічні, психологічні та когнітивні механізми впливу [4].

Отже, сучасні статистичні дані засвідчують, що розвиток інформаційних загроз характеризується не лише зростанням їх кількісних показників, а й істотним ускладненням змісту, технологій та способів реалізації. За таких умов стратегічний розвиток державного регулювання інформаційної безпеки має бути орієнтований на випереджувальне прогнозування ризиків, широке використання сучасних цифрових технологій моніторингу й аналітики, підвищення стійкості критичної інформаційної інфраструктури та зміцнення інституційної спроможності держави забезпечувати захист національного інформаційного простору в умовах сучасних цивілізаційних викликів.

У зв'язку з цим виникає об'єктивна необхідність переходу від реактивної моделі державного управління до стратегічної, ризик-орієнтованої та проактивної моделі забезпечення інформаційної безпеки, яка передбачає випереджувальне виявлення загроз, системний аналіз ризиків, стратегічне планування, розвиток інституційної спроможності держави та постійне підвищення стійкості інформаційного простору (табл. 1).

Таблиця 1

**Порівняльна характеристика моделей державного регулювання інформаційної безпеки***

| Критерій | Реактивна модель | Стратегічна, ризик-орієнтована та проактивна модель |
|---|---|---|
| Основна мета | Ліквідація наслідків реалізованих загроз | Попередження виникнення загроз та мінімізація ризиків |
| Характер управління | Ситуативний, епізодичний | Системний, безперервний, стратегічний |
| Прийняття управлінських рішень | Після виникнення кризової ситуації | На основі прогнозування, аналізу ризиків та сценарного планування |
| Управління інформаційними ризиками | Обмежене реагування | Комплексна система ідентифікації, оцінювання, моніторингу та управління ризиками |
| Інституційна взаємодія | Фрагментарна координація суб'єктів | Інтегрована міжвідомча взаємодія та партнерство державного і недержавного секторів |
| Використання цифрових технологій | Для реагування на інциденти | Для постійного моніторингу, аналітики, прогнозування та підтримки управлінських рішень |
| Захист критичної інформаційної інфраструктури | Усунення наслідків порушень | Забезпечення стійкості, резервування та безперервності функціонування |
| Очікуваний результат | Зменшення негативних наслідків окремих інформаційних атак | Формування стійкої, адаптивної та безпечної інформаційної екосистеми держави |

**Джерело: сформовано автором на основі даних [4-8]*

Як видно з табл. 1, стратегічна, ризик-орієнтована та проактивна модель державного регулювання значно повніше відповідає сучасним цивілізаційним викликам, ніж традиційна реактивна модель. Її впровадження забезпечує своєчасне виявлення потенційних інформаційних загроз, підвищує

адаптивність системи публічного управління, сприяє розвитку інституційної спроможності органів державної влади та створює передумови для забезпечення довгострокової стійкості інформаційного простору держави. Саме тому стратегічна трансформація державного регулювання інформаційної безпеки повинна розглядатися як один із пріоритетних напрямів державної політики в умовах сучасних цивілізаційних викликів.

Враховуючи трансформацію сучасного безпекового середовища, стратегічний розвиток державного регулювання інформаційної безпеки має здійснюватися комплексно та охоплювати взаємопов'язані напрями, спрямовані на підвищення спроможності держави своєчасно виявляти, прогнозувати та нейтралізовувати інформаційні загрози. На відміну від традиційного підходу, який передбачає вдосконалення окремих елементів системи, сучасна модель державного регулювання повинна ґрунтуватися на інтеграції правових, інституційних, організаційних, технологічних та міжнародних механізмів забезпечення інформаційної безпеки [9].

Ефективність реалізації стратегічної, ризик-орієнтованої та проактивної моделі державного регулювання інформаційної безпеки безпосередньо залежить від рівня інституційної спроможності органів державної влади та ефективності їх взаємодії. Сучасна система державного управління України у сфері інформаційної безпеки сформувала комплекс взаємодоповнюючих інституцій, кожна з яких виконує окремі стратегічні функції щодо прогнозування, попередження та нейтралізації інформаційних загроз. Водночас сучасні цивілізаційні виклики потребують подальшого вдосконалення механізмів міжвідомчої координації, інтеграції цифрових технологій та розвитку ризик-орієнтованого управління (табл. 2).

Таблиця 2

**Оцінка діяльності основних суб'єктів державного регулювання інформаційної безпеки України в умовах сучасних цивілізаційних викликів***

| Суб'єкт державного регулювання | Основні результати діяльності | Стратегічні напрями удосконалення |
|---|---|---|
| Система державного управління України | Сформовано багаторівневу систему забезпечення інформаційної безпеки, посилено нормативно-правове забезпечення та міжвідомчу взаємодію, інтегровано інформаційну безпеку до системи національної безпеки. | Формування єдиної ризик-орієнтованої системи управління інформаційними ризиками, цифрової екосистеми міжвідомчого обміну інформацією та стратегічного прогнозування загроз. |
| РНБО України | Забезпечує стратегічне планування, координацію діяльності суб'єктів сектору безпеки, ухвалення комплексних рішень щодо захисту інформаційного простору. | Розвиток системи стратегічної аналітики, сценарного моделювання та оцінювання інформаційних ризиків на національному рівні. |
| Міністерство цифрової трансформації України | Забезпечує цифровізацію державного управління, розвиток електронних сервісів, цифрової ідентифікації та державних реєстрів. | Інтеграція принципів Security by Design, розвиток безпечної цифрової архітектури державних інформаційних систем та управління цифровими ризиками. |
| Державна служба спеціального зв'язку та захисту інформації України | Реалізує державну політику у сфері кіберзахисту, захисту державних інформаційних ресурсів та критичної інформаційної інфраструктури. | Розширення можливостей кіберрозвідки, автоматизація аналізу кіберзагроз, впровадження сучасних моделей оцінювання кіберризиків. |
| СБУ | Протидіє інформаційно-психологічним операціям, кібертероризму, інформаційній діяльності держави-агресора та загрозам державному суверенітету. | Використання технологій штучного інтелекту для аналізу інформаційного простору, розвиток прогнозної аналітики та міжнародної взаємодії. |
| Центр протидії дезінформації | Здійснює моніторинг інформаційного простору, аналіз дезінформації та координацію стратегічних комунікацій держави. | Запровадження автоматизованого моніторингу інформаційних кампаній, використання технологій машинного навчання для раннього виявлення інформаційних операцій. |
| CERT-UA | Забезпечує моніторинг та реагування на кіберінциденти, здійснює аналіз кіберзагроз і взаємодію з державними органами та міжнародними партнерами. | Розвиток платформ Cyber Threat Intelligence, автоматизований обмін індикаторами компрометації та прогнозування складних кібератак. |

**Джерело: сформовано автором на основі даних [10-14]*

Отже, проведений аналіз свідчить, що в Україні сформовано достатньо розвинену інституційну систему державного регулювання інформаційної безпеки, яка охоплює стратегічний, управлінський, технологічний, оперативний та комунікаційний рівні забезпечення інформаційної

стійкості держави. Разом із тим сучасні цивілізаційні виклики обумовлюють необхідність подальшої трансформації цієї системи шляхом поглиблення міжвідомчої інтеграції, впровадження ризик-орієнтованих механізмів управління, розвитку прогнозної аналітики, використання технологій штучного інтелекту та створення єдиного інформаційно-аналітичного простору підтримки управлінських рішень. Саме такий підхід забезпечить підвищення адаптивності державного регулювання та зміцнення інформаційної стійкості України в умовах сучасних цивілізаційних викликів.

Враховуючи зазначене, пріоритетним напрямом розвитку державного регулювання інформаційної безпеки є впровадження проактивної, ризик-орієнтованої моделі управління, яка забезпечує своєчасне прогнозування загроз, превентивне управління ризиками, підвищення адаптивності державних інституцій та стійкості інформаційного простору [15]. Перевагами такої моделі є скорочення часу реагування на інформаційні інциденти, мінімізація потенційних втрат, підвищення ефективності міжвідомчої взаємодії та обґрунтованості управлінських рішень. Оцінювання результативності її реалізації доцільно здійснювати за критеріями рівня інформаційної стійкості держави, ефективності управління інформаційними ризиками, захищеності критичної інформаційної інфраструктури, інституційної спроможності органів влади та оперативності реагування на сучасні інформаційні загрози.

Адже, запропоновані стратегічні напрями розвитку державного регулювання інформаційної безпеки можуть бути ефективно реалізовані лише за умови їхнього функціонування в межах єдиної концептуальної моделі публічного управління, це зумовлено тим, що сучасні інформаційні загрози характеризуються високою динамічністю, багатовимірністю та міжгалузевим характером, а їх наслідки виходять далеко за межі інформаційної сфери, впливаючи на політичну, економічну, соціальну та оборонну складові національної безпеки. Відтак ефективність державного регулювання визначається не лише наявністю відповідних правових або організаційних механізмів, а й дотриманням системи базових принципів, які забезпечують цілісність, гнучкість та результативність державної політики у сфері інформаційної безпеки.

Проведений аналіз сучасних тенденцій розвитку інформаційного середовища свідчить, що ефективність державного регулювання інформаційної безпеки визначається не окремими механізмами чи інституціями, а узгодженістю базових принципів, на яких функціонує вся система публічного управління. У зв'язку з цим доцільно запропонувати авторську концептуальну модель принципів стратегічного державного регулювання інформаційної безпеки, яка систематизує їх за функціональним призначенням та відображає взаємозв'язок між інституційною основою, управлінськими процесами, цифровими інструментами та кінцевими результатами реалізації державної політики (рис. 1).


**Рис. 1. Концептуальна модель стратегічного державного регулювання інформаційної безпеки***
**Джерело: сформовано автором*

Як видно з рис. 1 особливість концептуальної моделі, полягає у тому, що вона вперше розглядає принципи державного регулювання інформаційної безпеки не як сукупність самостійних положень, а як взаємопов'язану багаторівневу систему, в якій кожен рівень формує передумови для функціонування наступного. На відміну від існуючих підходів, модель інтегрує правові, інституційні, управлінські та цифрові компоненти в єдину ризик-орієнтовану архітектуру державного управління, орієнтовану на прогнозування, попередження та нейтралізацію інформаційних загроз.

Отже, запропонована концептуальна модель демонструє, що стратегічний розвиток державного регулювання інформаційної безпеки має ґрунтуватися на синергетичній взаємодії правових, інституційних, організаційних та цифрових принципів. Такий підхід забезпечує перехід від фрагментарного реагування до проактивного управління інформаційними ризиками, підвищує ефективність міжвідомчої координації, зміцнює стійкість інформаційного простору та формує концептуальне підґрунтя для подальшої модернізації державної політики в умовах сучасних цивілізаційних викликів.

Отже, стратегічний розвиток державного регулювання інформаційної безпеки доцільно розглядати як безперервний процес адаптації системи публічного управління до змін інформаційного середовища, що ґрунтується на поєднанні стратегічного планування, ризик-орієнтованого управління, цифрової трансформації та міжсекторальної взаємодії. Саме така модель створює необхідні передумови для забезпечення стійкості інформаційного простору України, підвищення ефективності функціонування державних інституцій, захисту національних інтересів та дотримання прав і свобод людини в умовах сучасних цивілізаційних викликів.

**Висновки та перспективи подальших досліджень**. Отже, проведене дослідження засвідчило, що сучасні цивілізаційні виклики, цифрова трансформація суспільства, поширення гібридних загроз і стрімкий розвиток інформаційно-комунікаційних технологій обумовлюють необхідність переходу від реактивної до стратегічної, ризик-орієнтованої та проактивної моделі державного регулювання інформаційної безпеки. Встановлено, що стратегічний розвиток цієї сфери має ґрунтуватися на інтеграції правових, інституційних, організаційних, технологічних і міжнародних механізмів, посиленні міжвідомчої взаємодії, впровадженні сучасних цифрових технологій та розвитку системи прогнозування інформаційних ризиків. Запропонована авторська концептуальна модель систематизує ключові принципи державного регулювання за функціональними рівнями та формує цілісний підхід до забезпечення інформаційної стійкості держави. Практична реалізація запропонованих стратегічних напрямів сприятиме підвищенню ефективності публічного управління, зміцненню національної безпеки та формуванню адаптивної системи захисту інформаційного простору України відповідно до сучасних міжнародних стандартів і цивілізаційних викликів.

**Література**

1. Лисенко С. О. Вдосконалення стратегічних принципів державного управління інформаційною безпекою у складі національної безпеки України. *Вчені записки ТНУ імені В.І. Вернадського. Серія: Публічне управління та адміністрування,* 2024. Том 34 (73) № 1. С. 311-316. DOI : https://doi.org/10.32782/TNU-2663-6468/2024.1/54.

2. Саричев Ю. О. Інформаційно-аналітичне забезпечення як вид інформаційного забезпечення в системі державного управління. *Вісник НАДУ при Президентові України (Серія "Державне управління"),* 2017. № 3. С. 120–126.

3. Богданович В. Ю., Свида І. Ю., Сиротенко А. М. Методика формування та управління інтегрованим потенціалом протидії загрозам воєнного характеру для забезпечення визначеного рівня воєнної безпеки держави. *Сучасні інформаційні технології у сфері безпеки та оборони,* 2018. № 2(32). С. 81–86.

4. Пархоменко-Куцевіл О. Сучасні виклики національній безпеці в умовах цифрових викликів: державно-управлінський аспект. Публічне управління: концепції, парадигма, розвиток, удосконалення. 2025. №12. С. 116–123. DOI: https://doi.org/10.31470/2786-6246-2025-12-116-123.

5. Димитрієв В. В. Стратегічні напрями розвитку інформаційної політики України в контексті глобальних викликів. *Держава та регіони. Серія: Публічне управління і адміністрування,* 2022 р. № 2 (76). С. 132-138. DOI : https://doi.org/10.32782/1813-3401.2022.2.22.

6. Галіпчак В., Ротар Н. Інституційні чинники інформаційно-безпекової політики України в умовах воєнного стану: концепт дослідження. Вісник Прикарпатського університету. 2025. Вип. 22. С. 76–82. DOI: https://doi.org/10.32782/2312-1815/2025-22-10

7. Галіпчак В. Д. Сучасні виклики та стратегії забезпечення інформаційної безпеки України в умовах російської агресії: перспективи та завдання. *Регіональні студії,* 2023. №35. С. 65-69. DOI https://doi.org/10.32782/2663-6170/2023.35.10.

8. Пендюра М. М., Тихомиров Д. О., Старицька О. О., Петровський А. В., Кришевич О. В., Мостепанюк Л. О. Державна політика у сфері національної безпеки: правовий аспект : монографія. Київ : 7БЦ, 2025. 208 с. URL : https://elar.navs.edu.ua/server/api/core/bitstreams/70b5dc07-6bd8-495e-9fae-d98f72fde354/content. (дата звернення: 05.04.2026)

9. Загурська-Антонюк В. Ф. Державне управління національною безпекою в умовах геополітичних трансформацій : монографія. Житомир : О.О. Євенок, 2020. 336 с. URL : https://files.znu.edu.ua/files/Bibliobooks/Inshi72/0053295.pdf. (дата звернення: 05.04.2026)

10. Бігняк П. І., Михальчук В. М. Реформування державного управління: цифровізація. Інвестиції: практика та досвід. 2021. № 15. С. 107–113. DOI: https://doi.org/10.32702/2306-6814.2021.15.107

11. Дабіжа В. В. Державне регулювання інформаційної безпеки: проблеми та перспективи розвитку. *Herald of Khmelnytskyi National University. Economic Sciences,* 2026. №352(2). С. 84-91. DOI: https://doi.org/10.31891/2307-5740-2026-352-9.

12. Карпенко О. В., Денисюк Ж. З., Наместнік В. В. Цифрове врядування : монографія / за. ред. О. В. Карпенка. Київ : ІДЕЯ ПРИНТ, 2020. 336 с. URL : https://elib.nakkkim.edu.ua/bitstream/handle/123456789/4638/Monografia_Tsyfrove_vryadyvannya_2020.pdf. (дата звернення: 05.04.2026)

13. Медяник В. А. Суб'єкти формування та реалізації державної соціальної політики: адміністративно-правовий аспек. *Юридичний вісник,* 2021. № 3. С. 128 – 130. DOI: https://doi.org/10.32837/yuv.v0i3.2194. URL : https://dspace.onua.edu.ua/items/8ae674b3-9607-44ee-b7af-3cdbfdabc5c9 (дата звернення: 05.04.2026)

14. Бучковська О. Ю., Веремчук О. В. Електронне урядування як основа взаємодії держави та суспільства в Україні. *Державне управління: удосконалення та розвиток*, 2020. № 3. URL : http://nbuv.gov.ua/UJRN/Duur_2020_3_16. (дата звернення: 05.04.2026)

15. Кириченко Г. В. Трансформація публічного управління у сфері інформаційної безпеки: теоретико-правовий аспект. *Modern Scientific Journal,* 2026. № 11(1). С. 30–38. DOI: https://doi.org/10.36994/2786-9008-2026-11-4

Стаття надійшла 11.04.2026
Стаття прийнята до друку 25.04.2026
Доступно в мережі Internet 15.07.2026

**Hbur Z.**
Doctor of Sciences in Public Administration, Professor
Department of Public Administration and Administration;
State University of Information and Communication Technologies
Solomyanska St. 7, Kyiv, Ukraine, 03110
E-mail: ernest-natan@ukr.net
ORCID ID: https://orcid.org/0000-0003-4536-2438

# STRATEGIC DIRECTIONS FOR THE DEVELOPMENT OF GOVERNMENT REGULATION OF INFORMATION SECURITY IN THE CONTEXT OF CONTEMPORARY CIVILIZATIONAL CHALLENGES

This article examines current issues in the development of state regulation of information security in the context of modern civilizational challenges caused by the processes of globalization, the digital transformation of society, the rapid development of information and communication technologies, the spread of artificial intelligence, cyber threats, information and psychological operations, and hybrid forms of warfare. It has been argued that information security is becoming one of the key elements in ensuring a state's national security and is an important prerequisite for the sustainable functioning of the public administration system, the development of the information society, and the protection of national interests. The current state of state regulation of information security in Ukraine has been analyzed, the main trends in its development have been identified, and a set of external and internal factors influencing the formation of effective state policy in this area has been outlined. It has been established that contemporary civilizational challenges require a rethinking of traditional approaches to ensuring information security, as well as a transition from a predominantly reactive model of public administration to a strategic, risk-oriented, and proactive management of information threats.

Particular attention has been paid to identifying strategic directions for improving state regulation of information security, including: developing the institutional framework for state information policy; improving the regulatory and legal framework for the information sector in accordance with international standards and European practices; strengthening interagency coordination among entities responsible for information security; developing the state's digital resilience and critical information infrastructure; implementing modern mechanisms for monitoring, forecasting, and managing information risks; raising the population's level of media literacy; and developing international cooperation in the field of countering information threats and cybercrime. It has been demonstrated that the strategic development of state regulation of information security must be based on the principles of systematicity, adaptability, comprehensiveness, cross-sectoral cooperation, openness, digital transformation, the rule of law, and a balanced combination of the interests of the state, society, and the individual. The paper argues for the need to develop a modern model of state regulation capable of responding in a timely manner to dynamic changes in the security environment and ensuring the resilience of Ukraine's information space.

**Key words:** state regulation, information security, state strategy, national security, civilizational challenges, information policy, information threats, information society, public administration, legal regulation.

**References**

1. Lysenko, S. O. (2024). Vdoskonalennia stratehichnykh pryntsypiv derzhavnoho upravlinnia informatsiinoiu bezpekoiu u skladi natsionalnoi bezpeky Ukrainy. *Vcheni zapysky TNU imeni V.I. Vernadskoho. Seriia: Publichne upravlinnia ta administruvannia, 34*(73(1), 311–316. DOI: https://doi.org/10.32782/TNU-2663-6468/2024.1/54

2. Sarychev, Yu. O. (2017). Informatsiino-analitychne zabezpechennia yak vyd informatsiinoho zabezpechennia v systemi derzhavnoho upravlinnia. *Visnyk NADU pry Prezydentovi Ukrainy (Seriia "Derzhavne upravlinnia"),* 3, 120–126.

3. Bohdanovych, V. Yu., Svyda, I. Yu., & Syrotenko, A. M. (2018). Metodyka formuvannia ta upravlinnia intehrovanym potentsialom protydii zahrozam voiennoho kharakteru dlia zabezpechennia vyznachenoho rivnia voiennoi bezpeky derzhavy. *Suchasni informatsiini tekhnolohii u sferi bezpeky ta oborony, 2*(32), 81–86.

4. Parkhomenko-Kutsevil, O. (2025). Suchasni vyklyky natsionalnii bezpetsi v umovakh tsyfrovykh vyklykiv: derzhavno-upravlinskyi aspekt. *Publichne upravlinnia: kontseptsii, paradyhma, rozvytok, udoskonalennia,* 12, 116–123. DOI: https://doi.org/10.31470/2786-6246-2025-12-116-123

5. Dymytriiev, V. V. (2022). Stratehichni napriamy rozvytku informatsiinoi polityky Ukrainy v konteksti hlobalnykh vyklykiv. *Derzhava ta rehiony. Seriia: Publichne upravlinnia i administruvannia, 2*(76), 132–138. DOI: https://doi.org/10.32782/1813-3401.2022.2.22

6. Halipchak, V., & Rotar, N. (2025). Instytutsiini chynnyky informatsiino-bezpekovoi polityky Ukrainy v umovakh voiennoho stanu: kontsept doslidzhennia. *Visnyk Prykarpatskoho universytetu,* 22, 76–82. https://doi.org/10.32782/2312-1815/2025-22-10

7. Halipchak, V. D. (2023). Suchasni vyklyky ta stratehii zabezpechennia informatsiinoi bezpeky Ukrainy v umovakh rosiiskoi ahresii: perspektyvy ta zavdannia. *Rehionalni studii,* 35, 65–69. DOI: https://doi.org/10.32782/2663-6170/2023.35.10

8. Pendiura, M. M., Tykhomyrov, D. O., Starytska, O. O., Petrovskyi, A. V., Kryshevych, O. V., & Mostepaniuk, L. O. (2025). *Derzhavna polityka u sferi natsionalnoi bezpeky: pravovyi aspekt.* 7BTs. https://elar.navs.edu.ua/server/api/core/bitstreams/70b5dc07-6bd8-495e-9fae-d98f72fde354/content (Retrieved April 05, 2026)

9. Zahurska-Antoniuk, V. F. (2020). *Derzhavne upravlinnia natsionalnoiu bezpekoiu v umovakh heopolitychnykh transformatsii.* O.O. Yevenok. https://files.znu.edu.ua/files/Bibliobooks/Inshi72/0053295.pdf (Retrieved April 05, 2026)

10. Bihniak, P., & Mykhalchuk, V. (2021). Reformuvannia derzhavnoho upravlinnia: tsyfrovizatsiia. *Investytsii: praktyka ta dosvid,* 15, 107–113. DOI: https://doi.org/10.32702/2306-6814.2021.15.107

11. Dabizha, V. V. (2026). Derzhavne rehuliuvannia informatsiinoi bezpeky: problemy ta perspektyvy rozvytku. *Herald of Khmelnytskyi National University. Economic Sciences, 352*(2), 84–91. DOI: https://doi.org/10.31891/2307-5740-2026-352-9

12. Karpenko, O. V., Denysiuk, Zh. Z., & Namestnik, V. V. (2020). *Tsyfrove vriaduvannia* (O. V. Karpenko, Ed.). IDEIa PRYNT. https://elib.nakkkim.edu.ua/bitstream/handle/123456789/4638/Monografia_Tsyfrove_vryadyvannya_2020.pdf. (Retrieved April 05, 2026)

13. Medianyk, V. A. (2021). Subiekty formuvannia ta realizatsii derzhavnoi sotsialnoi polityky: administratyvno-pravovyi aspekt. *Yurydychnyi visnyk,* 3, 128–130. DOI: https://doi.org/10.32837/yuv.v0i3.2194. https://dspace.onua.edu.ua/items/8ae674b3-9607-44ee-b7af-3cdbfdabc5c9. (Retrieved April 05, 2026)

14. Buchkovska, O. Yu., & Veremchuk, O. V. (2020). Elektronne uriaduvannia yak osnova vzaiemodii derzhavy ta suspilstva v Ukraini. *Derzhavne upravlinnia: udoskonalennia ta rozvytok,* 3. http://nbuv.gov.ua/UJRN/Duur_2020_3_16 (Retrieved April 05, 2026)

15. Kyrychenko, H. V. (2026). Transformatsiia publichnoho upravlinnia u sferi informatsiinoi bezpeky: teoretyko-pravovyi aspekt. *Modern Scientific Journal*, *11*(1), 30–38. DOI: https://doi.org/10.36994/2786-9008-2026-11-4

Received 11 April 2026
Approved 25 April 2026
Available in Internet 15.07.2026

Цитування згідно ДСТУ 8302:20

Гбур З.В. Стратегічні напрями розвитку державного регулювання інформаційної безпеки в умовах сучасних цивілізаційних викликів // Економіка харчової промисловості. 2026. Т.18, вип. 2. С. 121-128. doi 10.15673/fie.v18i2.3584

Cite as APA style citation

Hbur, Z. (2026). Strategic directions for the development of government regulation of information security in the context of contemporary civilizational challenges. *Food Industry Economics, 18*(2), 121-128. doi 10.15673/fie.v18i2.3584