

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ДЕРЖАВНИЙ УНІВЕРСИТЕТ «ЖИТОМИРСЬКА ПОЛІТЕХНІКА»

Кваліфікаційна наукова
праця на правах рукопису

ДУБОВИК Денис Євгенович

УДК 35.078.3:004.738.5

ДИСЕРТАЦІЯ

**МЕХАНІЗМИ РЕАЛІЗАЦІЇ ДЕРЖАВНОЇ ІНФОРМАЦІЙНОЇ
ПОЛІТИКИ**

281 – Публічне управління та адміністрування

28 – Публічне управління та адміністрування

Подається на здобуття наукового ступеня доктора філософії

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____ Д.Є. Дубовик

Науковий керівник: Чиж Віктор Васильович, кандидат наук з державного управління

Житомир – 2026

АНОТАЦІЯ

Дубовик Д. Є. *Механізми реалізації державної інформаційної політики.* – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття ступеня доктора філософії за спеціальністю 281 «Публічне управління та адміністрування».

У дисертаційному дослідженні здійснено теоретичне узагальнення та запропоновано розв’язання важливого науково-прикладного завдання, що полягає в теоретико-методологічному обґрунтуванні й розробленні науково-практичних засад удосконалення механізмів реалізації державної інформаційної політики України в умовах цифрової трансформації, гібридних загроз і європейської інтеграції. Сформовано цілісне бачення переходу від фрагментарного відомчого інформування, ситуативної координації та реактивного спростування окремих повідомлень до інтегрованого, доказового, людиноцентричного й адаптивного управління інформаційною сферою. Одержані результати поєднують категоріальне уточнення предметної сфери, періодизацію еволюції наукової думки, функціонально-цільову систематизацію, методичне забезпечення оцінювання, аналіз сучасного стану інституцій та інструментів взаємодії, класифікацію гібридних ризиків, розроблення інтегрованого організаційно-управлінського механізму, двоконтурної моделі стратегічних комунікацій і системи моніторингу та оцінювання ефективності політики.

Актуальність дослідження зумовлена перетворенням інформації на стратегічний ресурс держави, від якості управління яким залежать реалізація інформаційних прав, легітимність публічної влади, обґрунтованість рішень, стійкість демократичних інститутів і здатність суспільства протидіяти деструктивним впливам. Поширення цифрових платформ, соціальних мереж, алгоритмічних систем, електронних реєстрів і сервісів прискорило обмін інформацією та розширило можливості участі громадян, але водночас посилило залежність від приватної цифрової інфраструктури, ризику непрозорого алгоритмічного поширення контенту, витоків даних, маніпулятивного

мікротаргетування та автоматизованого продукування неправдивих повідомлень. Повномасштабна збройна агресія проти України надала інформаційній політиці безпосереднього безпекового значення, а європейська інтеграція актуалізувала необхідність узгодження національної практики з принципами свободи вираження, медіаплюралізму, захисту персональних даних, кіберстійкості, прозорості платформ і належного врядування.

На основі історико-генетичного аналізу систематизовано еволюцію наукових поглядів на державну інформаційну політику через державоцентричну, організаційно-правову, демократично-комунікаційну, інформаційно-суспільну, безпекову та цифрово-платформну парадигми. Доведено, що їх розвиток має кумулятивний характер: кожна наступна парадигма не заперечувала попередню, а розширювала предмет політики, склад суб'єктів, інструментарій і критерії результативності. Від розуміння інформації як об'єкта правового регулювання і державного контролю науковий дискурс перейшов до трактування інформаційної сфери як відкритої екосистеми, у якій правові гарантії, комунікація, дані, платформи, безпека, довіра та суспільна участь утворюють взаємозалежну систему.

Запропоновано авторське визначення державної інформаційної політики як цілеспрямованої, нормативно впорядкованої, інституційно скоординованої та технологічно підтриманої діяльності публічної влади у партнерстві з громадянами, медіа, громадянським суспільством, бізнесом, науковим середовищем, органами місцевого самоврядування, цифровими платформами та міжнародними партнерами, спрямованої на гарантування інформаційних прав і свобод, формування якісної публічної комунікації, розвиток цифрового врядування, захист інформаційного простору, зміцнення суспільної стійкості та створення вимірюваної публічної цінності. Таке трактування поєднує управлінський, правовий, комунікаційний, цифровий і безпековий виміри та розширює відповідальність держави від вироблення повідомлення до перевірки його суспільного результату.

Систематизовано правозахисну, регуляторну, комунікаційну, сервісну, аналітичну, просвітницьку, безпекову, координаційну та оціночну функції

державної інформаційної політики. Обґрунтовано функціонально-цільову архітектуру за логікою «цінності – функції – цілі – пріоритети – механізми – результати – зворотний зв'язок». Генеральною метою визначено створення відкритого, безпечного, стійкого й людиноцентричного інформаційного середовища. Її декомпозиція охоплює гарантування інформаційних прав і відкритості, зміцнення довіри та громадянської участі, забезпечення інформаційної безпеки, цифровий розвиток та інклюзію, а також європейську інтеграцію і міжнародну присутність України.

Уточнено, що пріоритети державної інформаційної політики мають визначатися не ситуативною медійною увагою, а прозорими критеріями масштабу й терміновості проблеми, ризику для прав людини та національної безпеки, очікуваної публічної цінності, вразливості цільових груп, нормативної обов'язковості, міжсекторального ефекту, ресурсної здійсненності та можливості вимірювання результату. До актуальних пріоритетів віднесено інформаційну доброчесність і протидію дезінформації, стратегічні та кризові комунікації, відкриті дані, кіберстійкість критичної інформаційної інфраструктури, свободу й плюралізм медіа, цифрову інклюзію та медіаграмотність, належне врядування даних і платформ, інформаційну реінтеграцію деокупованих територій та євроінтеграційну комунікацію.

Удосконалено методичні засади дослідження механізмів реалізації державної інформаційної політики через поєднання історико-генетичного, системного, інституційного, структурно-функціонального, процесного, мережевого, ризик-орієнтованого та результативно-оціночного підходів. Запропонований алгоритм комплексного дослідження передбачає операціоналізацію понять, аналіз нормативної бази, картування суб'єктів і ролей, опис процесів та інструментів, визначення ресурсів, оцінювання результатів, виявлення ризиків, моделювання змін, апробацію та валідацію рекомендацій. До базових принципів віднесено верховенство права, пріоритет інформаційних прав, доказовість, достовірність, відкритість, підзвітність, пропорційність обмежень, інклюзивність, політичну неупередженість інституційної комунікації,

субсидіарність, технологічну нейтральність, міжвідомчу узгодженість і стійкість.

Розроблено систему критеріїв комплексного оцінювання механізмів, що охоплює правомірність, стратегічну узгодженість, інституційну спроможність, доступність, оперативність, двосторонність взаємодії, якість і достовірність інформації, економність використання ресурсів, безпекову стійкість, суспільну довіру, вплив та адаптивність. Методичну логіку побудовано так, щоб оцінювання не завершувалося констатацією стану, а запускало визначену управлінську дію: продовження, коригування, додаткову перевірку, перерозподіл ресурсів або припинення неефективного інструменту.

Охарактеризовано систему суб'єктів формування та реалізації державної інформаційної політики як поліцентричну, багаторівневу й міжгалузеву. Її стратегічно-нормативне ядро утворюють Верховна Рада України, Президент України, Рада національної безпеки і оборони України та Кабінет Міністрів України; координаційні й виконавчо-функціональні ролі реалізують центральні та місцеві органи виконавчої влади й органи місцевого самоврядування; регуляторно-гарантійні та безпекові функції здійснюють уповноважені регулятори, контрольні органи й сектор безпеки; територіально-суспільний контур охоплює суспільні медіа, професійні редакції, громадські організації, науково-експертне середовище, бізнес, цифрові платформи, міжнародних партнерів і громадян.

Встановлено, що ключовою інституційною проблемою є не відсутність органів, а недостатня узгодженість їхніх ролей, даних і часових горизонтів. Запропоновано принцип координованої поліцентричності, за якого єдність забезпечується на рівні стратегічних цілей, фактологічної основи, стандартів, кризових протоколів і показників, тоді як предметні рішення приймаються уповноваженими суб'єктами з належною професійною компетентністю. Сформовано рольову матрицю, що розмежовує провідного суб'єкта, виконавців, погоджувальні, консультативні та незалежно-оціночні ролі, а також зони спільної відповідальності й процедури ескалації.

Проаналізовано сучасний стан інструментів інформаційної взаємодії органів публічної влади з громадянами та медіа. Їх класифіковано на інструменти офіційного інформування, доступу до публічної інформації та відкритих даних, сервісної комунікації, електронної демократії, взаємодії з медіа, соціальних мереж, кризових комунікацій, протидії дезінформації та аналітичного зворотного зв'язку. Доведено, що інструмент не може ототожнюватися лише з каналом: він має включати правову процедуру, відповідального суб'єкта, стандарти змісту, можливість відповіді, фіксацію результату та критерії оцінювання.

За результатами проведеного в роботі кількісного аналізу встановлено масове поширення цифрових форм взаємодії: у 2025 році державними послугами онлайн користувалися 59 % охопленого вимірюванням населення, а частка отримувачів послуг через застосунок або портал «Дія» становила 48 %, що на 6 відсоткових пунктів більше порівняно з попереднім роком. Понад 2,1 млн відповідей в одному із загальнодержавних цифрових опитувань засвідчили потенціал швидкого залучення великої аудиторії. Водночас доведено, що цифрове охоплення не дорівнює якості врядування: сервіс має забезпечувати зрозумілість правових наслідків, доступ до першоджерела, можливість оскарження, омніканальність і використання отриманого зворотного зв'язку для вдосконалення рішення.

Виявлено значну територіальну нерівність цифрової та комунікаційної спроможності. Середнє значення Індексу цифрової трансформації територіальних громад у першому вимірюванні 2025 року становило 16 балів зі 100, тоді як показники громад-лідерів перевищували 60 балів. Авторська оцінка зрілості основних груп інструментів перебувала в межах 3,0–4,0 бала за п'ятибальною шкалою: найвищу зрілість продемонстрували сервісні платформи та системи запитів і звернень, а найнижчу – соціальні мережі й інструменти електронної демократії. На цій підставі запропоновано мінімальний територіальний стандарт інформаційної взаємодії, що охоплює основний і резервний канали, доступні формати, єдиний облік звернень, локальний кризовий протокол, партнерство з медіа та регулярне навчання персоналу.

Уточнено поняття інформаційної стійкості держави як динамічної спроможності системи публічного управління, медіасередовища та суспільства завчасно виявляти ризики, зберігати безперервність законної й достовірної комунікації під час деструктивного впливу, адаптувати інституційні й технологічні механізми, відновлювати довіру та накопичувати досвід без непропорційного обмеження прав людини. На відміну від вузького трактування інформаційної безпеки, стійкість охоплює превентивність, функціональну безперервність, адаптивність, відновлюваність, суспільну участь і правову легітимність.

Гібридні загрози розкрито як ланцюг «джерело – контент – канал – вразливість – поведінковий або управлінський наслідок». До їх ключових проявів віднесено координовану дезінформацію, інформаційно-психологічні операції, кібератаки з комунікаційним ефектом, витоки й маніпуляції даними, синтетичний контент і deepfake, алгоритмічне підсилення, дискредитацію медіа та створення локальних інформаційних вакуумів. Авторська матриця залишкового ризику визначила координовану дезінформаційну кампанію як найбільш критичну загрозу з розрахунковим рівнем 80 %. Алгоритмічне підсилення маніпуляцій, синтетичний контент, дискредитація інституцій і кібератаки на комунікаційні канали отримали по 64 %, а локальні інформаційні вакууми та кадрове виснаження комунікаційних команд – 51,2 %. Ці оцінки використано як аналітичний інструмент пріоритезації, а не як офіційну статистику.

Системні проблеми інформаційної стійкості згруповано у п'ять взаємопов'язаних площин: стратегічну безперервність, інституційну координацію, технологічну адаптивність, суспільну довіру та правову легітимність. Для переходу від реактивної до стійкісної моделі запропоновано цикл «передбачення – моніторинг – раннє виявлення – верифікація – координація – публічна комунікація – пропорційне реагування – відновлення – інституційне навчання». Кожний етап має отримати визначеного власника, строки, критерії якості, захищені канали та процедуру документування.

Уперше обґрунтовано концептуальну архітектуру інтегрованого організаційно-управлінського механізму реалізації державної інформаційної політики як системи нормативно-стратегічного, інституційно-суб'єктного, функціонального, інструментально-комунікаційного, ресурсно-забезпечувального та моніторингово-оціночного контурів. Їх поєднання забезпечує перетворення стратегічних пріоритетів на узгоджені процеси, продукти, безпосередні результати та суспільний вплив. Механізм ґрунтується на верховенстві права, людиноцентричності, доказовості, субсидіарності, розподіленій відповідальності, інтероперабельності, безпеці й приватності за проєктуванням, інклюзивності, адаптивності та організаційному навчанні.

Організаційну цілісність запропоновано забезпечувати через інститут власника процесу, матрицю відповідальності, спільні стандарти метаданих, протоколи обміну, плановий і кризовий режими та федеративну цифрову інфраструктуру. Процесний вимір представлено замкненим восьмиетапним циклом: виявлення проблеми й ризиків; аналітична діагностика; проєктування рішення та комунікації; правове й ресурсне погодження; реалізація; взаємодія і кризове реагування; моніторинг; оцінювання та коригування. Запропонована дорожня карта охоплює інвентаризацію чинних процесів, розроблення стандартів, пілотування, масштабування, цифрову інтеграцію та нормативне закріплення результативних практик.

Уперше розроблено двоконтурний механізм стратегічних комунікацій і протидії дезінформації. Проактивний контур забезпечує довгострокове пояснення державної політики, наративне планування, заповнення інформаційних вакуумів, розвиток медіаграмотності, міжнародну комунікацію та постійний суспільний діалог. Захисний контур охоплює ситуаційний моніторинг, раннє попередження, виявлення координованих кампаній, предметну верифікацію, рівневу ескалацію, кризове реагування, взаємодію з медіа і цифровими платформами та післядієвий аналіз. Обидва контури об'єднано спільними цінностями, стандартами доказовості, аналітичною платформою, правовими запобіжниками й системою показників.

Для проактивного контуру сформовано каскад наративного планування, що поєднує державні цінності, стратегічні цілі, тематичні наративи, доказову базу, адаптовані повідомлення, канали й показники сприйняття. Результативність запропоновано вимірювати індексом якості стратегічної комунікації за критеріями доказовості, своєчасності, узгодженості, доступності та якості зворотного зв'язку. Для захисного контуру розроблено чотирирівневу класифікацію інформаційних інцидентів і алгоритм реагування, який включає реєстрацію сигналу, первинний скринінг, предметну перевірку, оцінювання ризику, вибір пропорційної відповіді, погодження фактологічної основи, оприлюднення, моніторинг наслідків та післядієвий розбір.

Обґрунтовано протокол цифрової автентичності офіційних повідомлень, що включає підтверджені канали, збереження оригіналів і метаданих, резервні способи перевірки, публічне повідомлення про виправлення та порядок дій у разі компрометації. Партнерська екосистема передбачає рівний доступ медіа до перевірених фактів, залучення незалежних фактчекерів і науковців, добровільну взаємодію з цифровими платформами та участь громадянського суспільства в тестуванні й оцінюванні. Правові й етичні запобіжники мають відокремлювати верифікацію фактів від політичної оцінки, забезпечувати можливість оскарження, захист персональних даних і недопустимість використання протидії дезінформації для обмеження законної критики.

Удосконалено систему моніторингу й оцінювання ефективності реалізації державної інформаційної політики. Її методичним ядром визначено теорію змін і логічну модель, що пов'язують ресурси, процеси, продукти, безпосередні результати, суспільні наслідки та стратегічний вплив. Сформовано три рівні показників: стратегічні індикатори довіри, доступу, участі та інформаційної стійкості; індикатори результатів окремих напрямів; операційні показники строків, якості процесів і використання ресурсів. Показники згруповано у вісім вимірів: інституційна узгодженість; правомірність і відкритість; якість та своєчасність інформації; доступність і охоплення; взаємодія та участь; довіра і стратегічні результати; інформаційна стійкість; якість даних та організаційне навчання.

Для узагальнення результатів запропоновано інтегральний індекс ефективності з правилом мінімального стандарту, яке не допускає компенсації критичного порушення інформаційних прав, маніпуляції даними або небезпечної вразливості високим охопленням чи значною кількістю інформаційних продуктів. Розроблено коефіцієнт якості даних за критеріями повноти, своєчасності, валідності, узгодженості, унікальності й простежуваності, паспорт індикатора, картку відхилення та цифрову інформаційно-аналітичну панель. Система передбачає багатоджерельний аналіз, незалежну верифікацію, диференційовані рівні доступу та формалізований перехід від показника до управлінського рішення.

Наукова новизна одержаних результатів полягає в поєднанні в єдиній моделі принципу координованої поліцентричності, шестиконтурної організаційно-управлінської архітектури, двоконтурного механізму стратегічних комунікацій і протидії дезінформації, замкненого управлінського циклу, федеративної цифрової інфраструктури та системи моніторингу й оцінювання з обов'язковим коригуванням політики. Це дозволяє розглядати реалізацію державної інформаційної політики не як сукупність розрізнених інформаційних заходів, а як повний цикл спільного вироблення, виконання, перевірки та вдосконалення публічних рішень.

Практичне значення результатів полягає у можливості їх використання центральними органами виконавчої влади, органами місцевого самоврядування, безпековими органами, регуляторами, комунікаційними підрозділами, державними й суспільними медіа, аналітичними центрами та закладами освіти. Концептуальна архітектура може бути покладена в основу положень про міжвідомчу координацію, регламентів обміну даними та цифрової координаційно-аналітичної платформи. Двоконтурна модель придатна для розроблення комунікаційних стратегій, протоколів раннього попередження й кризового реагування. Матриці ролей і ризиків, система індикаторів, індекс інформаційної стійкості, паспорти показників і цифрова панель можуть застосовуватися для організаційного аудиту, моніторингу програм, кампаній, електронних сервісів та заходів із протидії дезінформації.

Результати дисертаційного дослідження висвітлено у 12 наукових працях, зокрема у 6 статтях у наукових періодичних виданнях та 6 публікаціях у збірниках матеріалів міжнародних і всеукраїнських науково-практичних конференцій. Сукупність теоретичних положень, методичних розробок, концептуальних моделей та прикладних інструментів створює науково-практичне підґрунтя для переходу від реактивного й відомчо роз'єданого інформування до правомірної, адаптивної, підзвітної та стійкої державної інформаційної політики, спроможної одночасно захищати національні інтереси, гарантувати інформаційні права людини, підтримувати суспільну довіру та сприяти європейській інтеграції України.

Ключові слова: державна інформаційна політика, механізми реалізації, публічне управління, інформаційні права, стратегічні комунікації, дезінформація, інформаційна стійкість, цифрове врядування, публічна комунікація, цифрові платформи, медіа, гібридні загрози, моніторинг, оцінювання, суспільна довіра, європейська інтеграція.

ABSTRACT

Dubovyk D. Ye. *Mechanisms for Implementing State Information Policy.* – *Qualifying scientific work submitted as a manuscript.*

Dissertation for the degree of Doctor of Philosophy in specialty 281 “Public Management and Administration”.

The dissertation provides a theoretical generalisation and offers a solution to an important applied scientific problem consisting in the theoretical and methodological substantiation and development of scientific and practical foundations for improving the mechanisms of state information policy implementation in Ukraine under digital transformation, hybrid threats and European integration. A coherent vision is developed for the transition from fragmented departmental informing, situational coordination and reactive rebuttal of individual messages to integrated, evidence-based, human-centred and adaptive governance of the information sphere. The findings combine clarification of the conceptual framework, periodisation of the evolution of

scientific thought, functional and target-based systematisation, methodological support for evaluation, analysis of the current state of institutions and interaction tools, classification of hybrid risks, and development of an integrated organisational and managerial mechanism, a dual-contour model of strategic communications and a monitoring and evaluation system.

The relevance of the research is determined by the transformation of information into a strategic public resource on which the exercise of information rights, the legitimacy of public authorities, the validity of public decisions, the resilience of democratic institutions and society's ability to resist destructive influence depend. The spread of digital platforms, social networks, algorithmic systems, electronic registers and services has accelerated information exchange and expanded opportunities for civic participation, while increasing dependence on private digital infrastructure and the risks of opaque algorithmic amplification, data leakage, manipulative microtargeting and automated production of false content. Russia's full-scale armed aggression against Ukraine has given information policy direct security significance, while European integration has increased the need to align national practice with the principles of freedom of expression, media pluralism, personal data protection, cyber resilience, platform transparency and good governance.

Based on historical and genetic analysis, the evolution of scientific views on state information policy is systematised through state-centred, organisational and legal, democratic and communicative, information-society, security, and digital-platform paradigms. Their development is shown to be cumulative: each subsequent paradigm did not negate the previous one but expanded the scope of policy, the range of actors, the set of instruments and the criteria of effectiveness. Scientific discourse has therefore moved from understanding information mainly as an object of legal regulation and state control to treating the information sphere as an open ecosystem in which legal safeguards, communication, data, platforms, security, trust and public participation form an interdependent whole.

An original definition is proposed: state information policy is a purposeful, normatively ordered, institutionally coordinated and technologically supported activity of public authorities, carried out in partnership with citizens, the media, civil society,

business, academia, local self-government bodies, digital platforms and international partners, aimed at guaranteeing information rights and freedoms, ensuring high-quality public communication, developing digital governance, protecting the information space, strengthening societal resilience and creating measurable public value. This definition integrates managerial, legal, communicative, digital and security dimensions and extends state responsibility from producing a message to verifying its public outcome.

The rights-protecting, regulatory, communicative, service, analytical, educational, security, coordination and evaluation functions of state information policy are systematised. A functional and target architecture is substantiated according to the sequence ‘values – functions – objectives – priorities – mechanisms – results – feedback’. The overarching objective is defined as the creation of an open, secure, resilient and human-centred information environment. It is decomposed into the protection of information rights and openness, strengthening trust and civic participation, ensuring information security, advancing digital development and inclusion, and supporting Ukraine’s European integration and international presence.

The dissertation clarifies that policy priorities should be determined not by short-term media attention but by transparent criteria: the scale and urgency of a problem; risk to human rights and national security; expected public value; vulnerability of target groups; legal obligations; cross-sector effects; resource feasibility; and measurability of results. Current priorities include information integrity and countering disinformation, strategic and crisis communications, open data, cyber resilience of critical information infrastructure, media freedom and pluralism, digital inclusion and media literacy, responsible governance of data and platforms, information reintegration of de-occupied territories, and communication on European integration.

The methodological foundations for studying state information policy implementation mechanisms are improved by combining historical-genetic, systemic, institutional, structural-functional, process, network, risk-oriented and performance-evaluation approaches. The proposed comprehensive research algorithm includes operationalisation of concepts, analysis of the regulatory framework, mapping of actors and roles, description of processes and instruments, identification of resources,

evaluation of results, risk detection, modelling of changes, piloting and validation of recommendations. The basic principles comprise the rule of law, priority of information rights, evidence, accuracy, openness, accountability, proportionality of restrictions, inclusion, political neutrality of institutional communication, subsidiarity, technological neutrality, inter-agency coherence and resilience.

A system of criteria for comprehensive evaluation is developed, covering legality, strategic alignment, institutional capacity, accessibility, timeliness, two-way interaction, information quality and accuracy, economy of resource use, security resilience, public trust, impact and adaptability. The evaluation logic is designed so that assessment does not end with a description of the current state but triggers a defined management response: continuation, correction, additional verification, reallocation of resources or termination of an ineffective instrument.

The system of actors involved in shaping and implementing state information policy is characterised as polycentric, multi-level and cross-sectoral. Its strategic and regulatory core consists of the Verkhovna Rada of Ukraine, the President of Ukraine, the National Security and Defence Council of Ukraine and the Cabinet of Ministers of Ukraine. Coordination and executive roles are performed by central and local executive authorities and local self-government bodies. Regulatory, safeguard and security functions are carried out by authorised regulators, oversight bodies and the security sector. The territorial and societal contour includes public service media, professional newsrooms, civil society organisations, academia and expert communities, business, digital platforms, international partners and citizens.

The central institutional problem is shown to be not the absence of actors but insufficient coherence of their roles, data and time horizons. The principle of coordinated polycentricity is proposed: unity is ensured at the level of strategic objectives, the factual basis, common standards, crisis protocols and performance indicators, while substantive decisions remain with legally empowered and professionally competent actors. A role matrix is developed to distinguish the lead actor, implementers, approving and advisory bodies, independent evaluators, shared responsibility zones and escalation procedures.

The current state of information interaction tools used by public authorities with citizens and the media is analysed. They are classified into official informing, access to public information and open data, service communication, e-democracy, media relations, social media, crisis communication, counter-disinformation tools and analytical feedback. An instrument is shown to be more than a technical channel: it must include a legal procedure, a responsible actor, content standards, a possibility of response, documentation of outcomes and evaluation criteria.

The quantitative analysis conducted in the dissertation confirms the broad use of digital interaction. In 2025, 59 per cent of the population covered by the measurement used public services online, while 48 per cent received services through the Diia application or portal, six percentage points more than in the previous year. More than 2.1 million responses in one nationwide digital survey demonstrated the potential for rapid large-scale engagement. At the same time, digital reach is not equated with quality of governance: a service should also ensure understandable legal consequences, access to the primary source, appeal mechanisms, omnichannel availability and the use of feedback to improve public decisions.

Significant territorial inequality in digital and communication capacity is identified. The average value of the Digital Transformation Index of Territorial Communities in the first 2025 measurement was 16 out of 100 points, while leading communities scored above 60. The original assessment of maturity across the main tool groups ranged from 3.0 to 4.0 on a five-point scale: service platforms and request/appeal systems demonstrated the highest maturity, whereas social media and e-democracy tools showed the lowest. A minimum territorial standard for information interaction is therefore proposed, including primary and backup channels, accessible formats, unified handling of appeals, a local crisis protocol, partnerships with media and regular staff training.

Information resilience of the state is clarified as the dynamic capacity of public governance, the media environment and society to anticipate risks, maintain continuous lawful and accurate communication during destructive influence, adapt institutional and technological mechanisms, restore trust and accumulate learning without disproportionate restrictions on human rights. Unlike a narrow understanding of

information security, resilience includes prevention, functional continuity, adaptability, recoverability, public participation and legal legitimacy.

Hybrid threats are disclosed through the chain ‘source – content – channel – vulnerability – behavioural or managerial consequence’. Their principal manifestations include coordinated disinformation, information and psychological operations, cyberattacks with communicative effects, data leaks and manipulation, synthetic content and deepfakes, algorithmic amplification, discrediting of media and institutions, and local information vacuums. The original residual-risk matrix identifies a coordinated disinformation campaign as the most critical threat with an estimated risk level of 80 per cent. Algorithmic amplification, synthetic content, institutional discrediting and cyberattacks against communication channels each received 64 per cent, while local information vacuums and exhaustion of communication teams received 51.2 per cent. These values are used as analytical prioritisation tools rather than official statistics.

Systemic resilience problems are grouped into five interrelated areas: strategic continuity, institutional coordination, technological adaptability, public trust and legal legitimacy. A transition from a reactive to a resilience-oriented model is proposed through the cycle ‘foresight – monitoring – early detection – verification – coordination – public communication – proportionate response – recovery – institutional learning’. Each stage should have a designated owner, time limits, quality criteria, protected channels and documentation procedures.

For the first time, a conceptual architecture of an integrated organisational and managerial mechanism for state information policy implementation is substantiated as a system of regulatory-strategic, institutional-actor, functional, instrumental-communication, resource-support and monitoring-evaluation contours. Their integration converts strategic priorities into coordinated processes, outputs, outcomes and public impact. The mechanism is based on the rule of law, human-centredness, evidence, subsidiarity, distributed responsibility, interoperability, security and privacy by design, inclusion, adaptability and organisational learning.

Organisational integrity is to be ensured through process ownership, a responsibility matrix, common metadata standards, exchange protocols, planned and

crisis modes and a federated digital infrastructure. The process dimension is represented as a closed eight-stage cycle: problem and risk identification; analytical diagnosis; design of the decision and communication; legal and resource approval; implementation; interaction and crisis response; monitoring; and evaluation with correction. The implementation roadmap includes an inventory of current processes, development of standards, piloting, scaling, digital integration and legal institutionalisation of effective practices.

For the first time, a dual-contour mechanism of strategic communications and countering disinformation is developed. The proactive contour provides long-term explanation of public policy, narrative planning, prevention of information vacuums, media literacy, international communication and continuous public dialogue. The protective contour covers situational monitoring, early warning, detection of coordinated campaigns, subject-matter verification, tiered escalation, crisis response, interaction with media and digital platforms, and after-action review. Both contours share common values, evidence standards, an analytical platform, legal safeguards and performance indicators.

For the proactive contour, a narrative-planning cascade is developed that links public values, strategic objectives, thematic narratives, evidence, adapted messages, channels and perception indicators. Performance is proposed to be assessed through a Strategic Communication Quality Index based on evidence, timeliness, coherence, accessibility and feedback quality. For the protective contour, a four-level classification of information incidents and a response algorithm are developed, including signal registration, initial screening, subject-matter verification, risk assessment, selection of a proportionate response, approval of the factual basis, publication, impact monitoring and after-action analysis.

A protocol for the digital authenticity of official messages is substantiated. It includes verified channels, preservation of originals and metadata, alternative verification methods, public correction notices and procedures for compromised accounts or systems. The partnership ecosystem provides equal media access to verified facts, participation of independent fact-checkers and researchers, voluntary cooperation with digital platforms, and civil society involvement in testing and

evaluation. Legal and ethical safeguards must separate fact verification from political judgment, ensure avenues for appeal, protect personal data and prevent counter-disinformation measures from being used to suppress legitimate criticism.

The monitoring and evaluation system for state information policy implementation is improved. Its methodological core is a theory of change and a logical model linking inputs, processes, outputs, immediate outcomes, broader social effects and strategic impact. Three indicator levels are formed: strategic indicators of trust, access, participation and information resilience; outcome indicators for individual policy areas; and operational indicators of timing, process quality and resource use. The indicators are grouped into eight dimensions: institutional coherence; legality and openness; information quality and timeliness; accessibility and reach; interaction and participation; trust and strategic results; information resilience; and data quality with organisational learning.

An integrated effectiveness index with a minimum-standard rule is proposed so that critical violations of information rights, data manipulation or dangerous vulnerabilities cannot be offset by high reach or a large number of information products. A data-quality coefficient is developed based on completeness, timeliness, validity, consistency, uniqueness and traceability, together with an indicator passport, a deviation card and a digital analytical dashboard. The system provides for multi-source analysis, independent verification, differentiated access levels and a formal transition from an indicator to a management decision.

The scientific novelty of the findings lies in combining within a single model the principle of coordinated polycentricity, a six-contour organisational and managerial architecture, a dual-contour mechanism for strategic communications and countering disinformation, a closed management cycle, a federated digital infrastructure and a monitoring and evaluation system with mandatory policy correction. This makes it possible to understand implementation not as a collection of isolated information activities but as a complete cycle of co-production, execution, verification and continuous improvement of public decisions.

The practical significance of the findings lies in their applicability to central executive authorities, local self-government bodies, security agencies, regulators,

communication units, state and public service media, analytical centres and educational institutions. The conceptual architecture can underpin inter-agency coordination regulations, data-exchange procedures and a digital coordination and analytical platform. The dual-contour model can be used to design communication strategies, early-warning protocols and crisis-response procedures. Role and risk matrices, indicator systems, the information resilience index, indicator passports and the digital dashboard may support organisational audits and monitoring of public programmes, campaigns, electronic services and counter-disinformation measures.

The dissertation findings are presented in 12 scientific works, including six articles in scientific periodicals and six papers in proceedings of international and national scientific and practical conferences. The theoretical provisions, methodological developments, conceptual models and applied instruments establish a scientific and practical foundation for the transition from reactive and institutionally fragmented informing to lawful, adaptive, accountable and resilient state information policy capable of protecting national interests, guaranteeing information rights, maintaining public trust and supporting Ukraine's European integration.

Keywords: state information policy, implementation mechanisms, public governance, information rights, strategic communications, disinformation, information resilience, digital governance, public communication, digital platforms, media, hybrid threats, monitoring, evaluation, public trust, European integration.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Праці, які відображають основні наукові результати дисертації

Публікації у наукових фахових виданнях України з державного управління

1. Дубовик Д. Інформаційна політика як інструмент державного управління в умовах цифровізації. Вісник Хмельницького національного університету. 2026. № 1. С. 572-578. (0,5 д.а)

2. Дубовик Д. Інституційний механізм реалізації державної інформаційної політики в умовах цифрової трансформації. Вісник Хмельницького національного університету. 2025. № 6. С. 496-502. (0,5 д.а)

3. Гривко С.Д., **Дубовик Д.Є.** Вплив цифровізації на зайнятість та ринок праці в інформаційному суспільстві. Економічний простір. 2025. № 208. С. 203-209. (0,5 д.а) (внесок автора – визначені особливості впливу цифровізації на зайнятість та ринок праці, (0,3 д.а))

4. Дубовик Д.Є. Цифрові трансформації в інформаційному суспільстві. Публічне управління і адміністрування в Україні. 2024. Випуск 44. С. 231-235. (0,5 д.а)

5. Shestakovska T., **Dubovyk D.** Formation of a transparent information policy in the context of decentralization: challenges and prospects. RFI Scientific Papers. 2025. № 4. С. 89-100. (0,5 д.а) (внесок автора – обґрунтовані напрямки розвитку інформаційної політики в Україні, (0,3 д.а))

***Публікації у виданнях, внесених до наукометричних баз даних
Web of Science та Scopus:***

6. Nikoliuk O., Shestakovska T., Hayduk A., Pinezhko A., **Dubovyk D.** Marketing Strategies for Project Management in the Digital Age. Ad Alta: Journal of Interdisciplinary Research. 2025. Vol. 14. Issue 1. Pp. 151-155. (0,7 д.а) (внесок автора – оцінено вплив цифровізації на розвиток маркетингових стратегій, (0,2 д.а))

***Публікації в наукових виданнях іноземних держав за напрямом,
з якого підготовлено дисертацію:***

7. Denys Dubovyk. Organizational and economic mechanism of implementation of state information policy. Modern Science – Moderní věda. Praha. Česká republika, Nemoros. 2023. № 1. P.22-27. (0,5 д.а)

Опубліковані праці апробаційного характеру:

8. Дубовик Д.Є. Оптимізація реалізації державної інформаційної політики в умовах глобальних викликів. Березневий науковий дискурс 2025 на тему: «Синергія освіти, науки та бізнесу в епоху глобальних трансформацій»: збірник матеріалів III Міжнародної науково-практичної конференції (м. Чернігів, 27 лютого 2025 р.). Чернігів: ГО «Науково-освітній інноваційний центр суспільних трансформацій», 2025. С. 241-242. (0,1 д.а)

9. Дубовик Д.Є. Перспективи державної інформаційної політики в Україні. Актуальні питання управління та адміністрування: регіональний, міжнародний та глобалізаційний аспекти: Збірник тез міжнародної науково-практичної конференції (22-23 травня 2025 р.). Під загальною редакцією доктора економічних наук Дуки Анастасії Петрівни, доктора економічних наук Філіпової Наталії Володимирівни. Чернігів: ЗВО «Університет трансформації майбутнього», 2025. С.43-44. *(0,1 д.а)*

10. Дубовик Д.Є. Особливості публічного управління соціальними конфліктами в Україні. Матеріали І Науково-практичної конференції з міжнародною участю (м. Чернігів, 06-08 березня 2024р.) / Під загальною редакцією д.н.держ. упр., професорки Гбур З.В. – Чернігів, ППЗО «ІПТ», 2024. С. 100-102. *(0,1 д.а)*

11. Дубовик Д.Є. Удосконалення підходів до впровадження державної інформаційної політики в умовах глобальних трансформацій. Людина в системі управління: гендерні та психологічні аспекти менеджменту та адміністрування: Збірник тез І Науково-практичної конференції з міжнародною участю (28-29 листопада 2024 р.). Під загальною редакцією доктора економічних наук Філіпової Наталії Володимирівни. Чернігів, ППЗО «ІПТ», 2024. С. 197-199. *(0,1 д.а)*

12. Дубовик Д.Є. Удосконалення процесів втілення державної інформаційної стратегії в контексті глобальних змін. Всеукраїнської науково-практичної конференції «Національна безпека в умовах війни, післявоєнної відбудови та глобальних викликів ХХІ століття» (м. Житомир, 7-8 грудня 2023 року). – Житомир: Житомирська політехніка, 2023. С.63-66.

13. Дубовик Д.Є. Організаційний механізм реалізації інформаційної політики. Стійкість освіти і науки в умовах трансформації: матеріали Міжнародної науково-практичної конференції до 30-річчя створення Закладу вищої освіти «Міжнародний науково-технічний університет імені академіка Юрія Бугая», м. Київ, 23–24 трав. 2023 р. : [зб. тез]. Київ : [ЗВО «МНТУ»], 2023. С.281-283.

14. Дубовик Д.Є. Удосконалення державної інформаційної політики в Україні. Державне й муніципальне управління у ХХІ столітті: організаційно-економічні, правові та інформаційні аспекти : Збірник тез I Міжнародної науково-практичної конференції здобувачів вищої освіти та молодих вчених (27 квітня 2023 р.) / За наук. ред. д.е.н., проф. Капленко Г.В. – Львів : ЛНУ імені Івана Франк. 2023. С. 53-55.

15. Дубовик Д.Є. Оптимізація механізмів реалізації державної інформаційної політики в умовах глобалізації. Актуальні питання сучасної стратегії розвитку України: виклики, пріоритети та прогнози: збірник наукових праць / Кадлубович Т.І., Савич В.О., Дабіжа В. В. та ін. м. Київ, 22 листопада 2023 р. К.: Університет «Україна», 2023 р. С. 54-56.

16. Дубовик Д.Є., Солодовник П.В. Оптимізація методів реалізації державної інформаційної політики у рамках світових трансформацій. Вища освіта – студентська наука – сучасне суспільство: напрями розвитку: матеріали VII Всеукр. студ. наук.-практ. конф., м. Київ, 12 груд. 2023 р.: [зб. тез] / ЗВО «МНТУ», каф-ра ЮНЕСКО «Інформ.-комунікат. технол. в освіті». Київ : [б. в.], 2023.С. 67-69. (0,1 д.а).

ЗМІСТ

ВСТУП	24
РОЗДІЛ 1. КОНЦЕПТУАЛЬНІ ОСНОВИ ДЕРЖАВНОЇ ІНФОРМАЦІЙНОЇ ПОЛІТИКИ	34
1.1 Еволюція наукових поглядів на формування державної інформаційної політики	34
1.2 Функції, цілі та пріоритети державної інформаційної політики в системі публічного управління	54
1.3 Методичні засади дослідження механізмів реалізації державної інформаційної політики	73
Висновки до розділу 1	92
РОЗДІЛ 2 ОСОБЛИВОСТІ ФУНКЦІОНУВАННЯ ДЕРЖАВНОЇ ІНФОРМАЦІЙНОЇ ПОЛІТИКИ В УКРАЇНІ	97
2.1 Система суб'єктів формування та реалізації державної інформаційної політики	97
2.2 Інструменти інформаційної взаємодії органів публічної влади з громадянами та медіа	115
2.3 Проблеми забезпечення інформаційної стійкості держави в умовах гібридних загроз	133
Висновки до розділу 2	149
РОЗДІЛ 3 РОЗВИТОК МЕХАНІЗМІВ РЕАЛІЗАЦІЇ ДЕРЖАВНОЇ ІНФОРМАЦІЙНОЇ ПОЛІТИКИ	153
3.1 Формування інтегрованого організаційно-управлінського механізму реалізації державної інформаційної політики	153
3.2 Удосконалення механізмів стратегічних комунікацій та протидії дезінформації	171
3.3 Система моніторингу й оцінювання ефективності реалізації державної інформаційної політики	188
Висновки до розділу 3	207
ВИСНОВКИ	210
СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ	214
ДОДАТКИ	230

ВСТУП

Актуальність теми. Інформація в сучасній державі набула значення стратегічного ресурсу, від якості управління яким залежать легітимність публічної влади, обґрунтованість управлінських рішень, реалізація прав людини, стійкість демократичних інститутів і спроможність суспільства протидіяти зовнішнім та внутрішнім загрозам. Державна інформаційна політика вже не обмежується оприлюдненням офіційних повідомлень або регулюванням діяльності медіа. Актуальність дослідження посилюється цифровою трансформацією публічного управління. Поширення платформ, алгоритмічних систем, соціальних мереж, електронних реєстрів і сервісів змінило швидкість, масштаб та архітектуру інформаційної взаємодії. Громадяни очікують безперервного доступу до перевіреної інформації, можливості отримувати послуги дистанційно, брати участь у консультаціях і впливати на рішення. Тому механізми державної інформаційної політики мають поєднувати відкритість із безпекою, оперативність із достовірністю, технологічність із правовими гарантіями, а централізовану координацію – з автономією демократичних інститутів, незалежних медіа та громадянського суспільства. Особливої ваги зазначена проблематика набула в умовах повномасштабної збройної агресії проти України та тривалого гібридного протиборства. Інформаційні операції, дезінформаційні кампанії, кібератаки з комунікаційними наслідками, спроби підірвати довіру до державних інституцій, посіяти паніку, поляризувати суспільство й дискредитувати міжнародну підтримку безпосередньо впливають на національну безпеку. За цих обставин держава повинна діяти швидко, однак зберігати правову визначеність, пропорційність обмежень, повагу до свободи вираження поглядів і право громадян на достовірну інформацію. Невиважене ототожнення протидії дезінформації з контролем над суспільною дискусією створює ризик порушення демократичних стандартів, тоді як запізніле або неузгоджене реагування залишає інформаційний простір вразливим. Отже, ключовою науковою і практичною проблемою є побудова такого механізму, який одночасно забезпечує інформаційну стійкість, результативну державну комунікацію, захист прав людини та публічну підзвітність.

Наукові основи дослідження державної інформаційної політики сформовано у працях українських учених, які розкрили її організаційно-правову, управлінську, комунікаційну, безпекову та цифрову природу. Організаційно-правові засади інформаційної сфери досліджували І. Арістова, О. Баранов, К. Беляков, В. Брижко, А. Марущак та інші. Теоретико-методологічні положення державної інформаційної політики й інформаційної складової публічного управління розробляли Ю. Нестеряк, С. Соловійов, О. Бухтатий, Ю. Турченко, Т. Савосько, К. Захаренко, О. Пушкар. Питання інформаційної безпеки, гібридних впливів та інформаційної стійкості висвітлено у працях В. Горбуліна, Д. Дубова, Г. Почепцова, О. Курбана, О. Золотар, О. Олійника, В. Шемчука, А. Марущака, Л. Рудник. Інституційні й правові механізми протидії дезінформації досліджували О. Дяковський, К. Животова, Н. Новицька, В. Малярєнко, Н. Уханова та інші. Значущими є також праці, присвячені стратегічним комунікаціям, євроінтеграційному виміру інформаційної політики, цифровому врядуванню та взаємодії держави з громадянами.

Зарубіжний науковий дискурс представлений дослідженнями С. Браман щодо взаємозв'язку інформації, політики й влади; М. Х. Канель і К. Сандерс – щодо урядових комунікацій; К. Халлахана, Д. Хольцхаузен, Б. ван Рулер, Д. Верчича та К. Срірамеша – щодо стратегічної комунікації; А. Чедвіка – щодо гібридної медіасистеми; В. Беннета і С. Лівінгстон – щодо інституційних наслідків дезінформаційного порядку; К. Вордл і Х. Дерахшана – щодо інформаційного безладу; Е. Гумпрехт, Ф. Ессера та П. ван Аелста – щодо стійкості до онлайн-дезінформації. Важливе методичне та нормативне значення мають документи OECD, UNESCO, ООН, Ради Європи та Європейського Союзу, у яких публічна комунікація розглядається як функція належного врядування, а протидія дезінформації – як багатосторонній процес, що має ґрунтуватися на доказовості, пропорційності, прозорості та захисті прав людини.

Попри значний науковий доробок, недостатньо вирішеними залишаються питання інтеграції нормативного, інституційного, організаційного, цифрового, комунікаційного, безпекового й оціночного складників у єдиний механізм реалізації державної інформаційної політики; розмежування ролей суб'єктів за

етапами політичного циклу; поєднання проактивних стратегічних комунікацій із захисним реагуванням на дезінформаційні інциденти; формування системи показників, що вимірює не лише активність органів влади, а й суспільний результат; забезпечення обов'язкового зворотного зв'язку між моніторингом, оцінюванням та коригуванням рішень. Необхідність комплексного розв'язання цих питань зумовила вибір теми, мети, завдань і структури дисертаційної роботи.

Зв'язок роботи з науковими програмами, планами, темами.

Дисертаційну роботу виконано в межах науково-дослідної теми «Трансформація механізмів публічного управління в умовах діджиталізації» (номер державної реєстрації 0125U002400). Особистий внесок здобувача в межах теми полягає в обґрунтуванні концептуальних і методичних засад державної інформаційної політики, розробленні інтегрованого організаційно-управлінського механізму її реалізації, формуванні двоконтурної моделі стратегічних комунікацій і протидії дезінформації, а також системи моніторингу й оцінювання результативності відповідних управлінських рішень.

Мета і завдання дослідження. Метою дисертаційної роботи є теоретико-методологічне обґрунтування та розробка науково-практичних засад удосконалення механізмів реалізації державної інформаційної політики України в умовах цифрової трансформації, гібридних загроз і європейської інтеграції.

Досягнення поставленої мети передбачає розв'язання таких завдань:

- узагальнити еволюцію наукових поглядів на формування державної інформаційної політики;
- систематизувати функції, цілі та пріоритети державної інформаційної політики в системі публічного управління;
- розробити методичні засади дослідження механізмів реалізації державної інформаційної політики;
- охарактеризувати систему суб'єктів формування та реалізації державної інформаційної політики;
- проаналізувати сучасний стан інструментів інформаційної взаємодії органів публічної влади з громадянами та медіа,

- сформувати концептуальну архітектуру інтегрованого організаційно-управлінського механізму реалізації державної інформаційної політики;
- удосконалити механізми стратегічних комунікацій і протидії дезінформації;
- розробити систему моніторингу й оцінювання ефективності реалізації державної інформаційної політики.

Об’єкт дослідження. Процеси формування та реалізації державної інформаційної політики в системі публічного управління України.

Предмет дослідження. Теоретико-методологічні, інституційно-правові, організаційно-управлінські, комунікаційні, цифрові та безпекові засади, механізми й інструменти реалізації державної інформаційної політики.

Методи дослідження. Методологічну основу дисертації становить комплекс загальнонаукових і спеціальних методів, добір яких зумовлено міждисциплінарною природою державної інформаційної політики. Історико-генетичний і ретроспективний методи застосовано для встановлення етапів еволюції наукових поглядів та зміни домінуючих парадигм. Абстрактно-логічний метод, аналіз, синтез, індукцію, дедукцію, порівняння й наукове узагальнення використано для уточнення понятійно-категоріального апарату, розмежування функцій, цілей, пріоритетів і механізмів. Системний, структурно-функціональний, процесний та інституційний підходи дали змогу розкрити державну інформаційну політику як багаторівневу систему суб’єктів, повноважень, функцій, ресурсів, процедур та зворотних зв’язків.

Формально-юридичний метод і контент-аналіз нормативно-правових актів застосовано для дослідження правових засад доступу до інформації, діяльності медіа, захисту даних, кібербезпеки, стратегічних комунікацій і протидії дезінформації. Інституційне картування, суб’єктно-рольовий аналіз і елементи мережевого підходу використано для побудови системи суб’єктів та визначення вертикальних і горизонтальних зв’язків між ними. Статистико-аналітичний, порівняльний і трендовий методи застосовано під час оцінювання сучасного стану цифрових каналів, електронних послуг, відкритих даних, взаємодії з громадянами та медіа. Класифікацію, типологізацію, причинно-наслідковий

аналіз, ризик-аналіз і матричний метод використано для систематизації гібридних загроз, визначення вразливостей і побудови матриці залишкового ризику.

Методи концептуального та логіко-структурного моделювання, декомпозиції, алгоритмізації, рольового й сценарного проектування застосовано для побудови інтегрованого організаційно-управлінського механізму, двоконтурної моделі стратегічних комунікацій та алгоритму реагування на інформаційні інциденти. Теорію змін, індикативний метод, експертно-бальне оцінювання, нормування показників і метод інтегрального індексу використано для формування системи моніторингу й оцінювання. Компаративний метод і функціональний бенчмаркінг дали змогу узагальнити міжнародні підходи та визначити можливості їх адаптації в Україні. Сукупність зазначених методів забезпечила взаємну перевірку висновків і поєднання теоретичного, нормативного, емпіричного та проектного рівнів дослідження.

Інформаційна база дослідження. Інформаційну основу роботи становили Конституція України, закони України, укази Президента України, постанови й розпорядження Кабінету Міністрів України, стратегічні та концептуальні документи у сферах інформаційної безпеки, кібербезпеки, цифровізації, європейської та євроатлантичної інтеграції; нормативні й методичні матеріали центральних органів виконавчої влади, регуляторів та органів місцевого самоврядування; офіційні адміністративні й статистичні дані, матеріали державних цифрових платформ і відкритих реєстрів; документи Європейського Союзу, Ради Європи, OECD, UNESCO та ООН; наукові праці українських і зарубіжних учених; аналітичні звіти, матеріали моніторингу медіасередовища та публічних комунікацій. Інформаційну базу сформовано з дотриманням принципів релевантності, перевірюваності, порівнюваності та актуальності даних.

Наукова новизна одержаних результатів. Наукова новизна полягає в теоретико-методологічному обґрунтуванні та розробленні цілісної системи механізмів реалізації державної інформаційної політики, що забезпечує перехід від фрагментарного відомчого інформування й реактивного спростування

окремих повідомлень до інтегрованого, доказового, людиноцентричного та адаптивного управління інформаційною сферою. Основні положення, що характеризують наукову новизну та виносяться на захист, полягають у такому:

удосконалено:

– концептуальну архітектуру інтегрованого організаційно-управлінського механізму реалізації державної інформаційної політики як багаторівневої системи нормативно-стратегічного, інституційно-суб'єктного, функціонального, інструментально-комунікаційного, ресурсно-забезпечувального та моніторингово-оціночного контурів. На відміну від існуючих підходів, запропонований механізм передбачає єдину стратегічну мету, розподіл ролей, спільні стандарти, плановий і кризовий режими, цифрову координаційну платформу та обов'язковий зворотний зв'язок між результатами оцінювання і коригуванням політики;

– двоконтурний механізм стратегічних комунікацій та протидії дезінформації, у якому проактивний контур забезпечує наративне планування, пояснення державної політики, заповнення інформаційних вакуумів, суспільний діалог і розвиток медіаграмотності, а захисний контур – моніторинг, раннє виявлення, верифікацію, рівневу ескалацію, кризове реагування, взаємодію з платформами та післядієвий аналіз. Відмінністю моделі є поєднання обох контурів спільними ціннісними орієнтирами, стандартами доказовості, правовими запобіжниками, партнерською екосистемою та системою показників результативності.

– методичні засади дослідження механізмів реалізації державної інформаційної політики через поєднання історико-генетичного, системного, інституційного, структурно-функціонального, мережевого, ризик-орієнтованого та результативно-оціночного підходів, а також розроблення послідовного алгоритму від операціоналізації понять і картування суб'єктів до оцінювання механізмів, моделювання змін і валідації рекомендацій;

– систему моніторингу й оцінювання ефективності реалізації державної інформаційної політики, що, на відміну від переважно кількісної звітності про проведені заходи, ґрунтується на теорії змін, ієрархії показників ресурсів,

продуктів, результатів та впливу, стандартах якості даних, інтегральному оцінюванні, цифровій аналітичній панелі, незалежній верифікації й обов'язковості управлінського реагування на встановлені відхилення.

дістали подальшого розвитку:

– понятійно-категоріальний апарат науки публічного управління в частині уточнення змісту державної інформаційної політики як цілеспрямованої, нормативно впорядкованої, інституційно скоординованої та технологічно підтриманої діяльності публічної влади у партнерстві із суспільством, спрямованої на забезпечення інформаційних прав, формування якісної публічної комунікації, розвиток цифрового врядування, захист інформаційного простору та досягнення вимірюваної публічної цінності;

– науково-методичний підхід до забезпечення інформаційної стійкості держави шляхом поєднання оцінки загроз, вразливостей і спроможностей, застосування матриці залишкового ризику, визначення вимірів інтегрального індексу інформаційної стійкості та організації циклу «моніторинг – раннє попередження – реагування – відновлення – навчання»;

– функціонально-цільова архітектура державної інформаційної політики шляхом узгодження її правозахисної, регуляторної, комунікаційної, сервісної, аналітичної, просвітницької, безпекової, координаційної та оціночної функцій із деревом цілей, динамічними пріоритетами, механізмами реалізації та критеріями суспільної результативності. Дана архітектура включає удосконалену класифікацію інструментів інформаційної взаємодії органів публічної влади з громадянами та медіа, яку доповнено критеріями цифрової зрілості, інклюзивності, двосторонності, довіри, доказовості, оперативності та придатності до кризового використання.

Практичне значення одержаних результатів. Практичне значення полягає у можливості безпосереднього використання запропонованих моделей, методичних положень та інструментів центральними органами виконавчої влади, органами місцевого самоврядування, безпековими органами, регуляторами, комунікаційними підрозділами, державними й суспільними медіа, аналітичними

центрами та закладами освіти. Так, оригінальні методики та практичні рекомендації, що містяться в дисертаційній роботі, використано в діяльності:

– Народним депутатом України під час опрацювання законодавчих ініціатив щодо вдосконалення інституційно-правового забезпечення формування та реалізації державної інформаційної політики, розмежування повноважень її суб'єктів, розвитку стратегічних комунікацій, протидії дезінформації та запровадження системи моніторингу й оцінювання результативності державних інформаційно-комунікаційних заходів (довідка № 116д7/11-2025/196124 від 23.09.2025 р.);

– Менською міською радою під час удосконалення інформаційної взаємодії органів місцевого самоврядування з громадянами та медіа, організації офіційного інформування населення, проведення публічних консультацій, використання цифрових каналів комунікації, підвищення інформаційної відкритості та формування механізмів оперативного реагування на дезінформаційні й кризові інформаційні впливи (довідка № 05-23/2116 від 07.11.2025 р.);

– Громадською організацією «Освітній компас» під час розроблення та реалізації інформаційно-просвітницьких і громадських ініціатив, організації взаємодії із зацікавленими сторонами, проведення моніторингу інформаційного середовища, підготовки інформаційних матеріалів, розвитку медіаграмотності, перевірки достовірності повідомлень та оцінювання результативності комунікаційних заходів (довідка про впровадження № 08/25 від 24.12.2025 р.);

– ЗВО «Університет трансформації майбутнього» у навчальній і науковій діяльності, зокрема під час викладання освітніх компонентів із державної інформаційної політики, публічних комунікацій, цифрового врядування та інформаційної безпеки, підготовки навчально-методичних матеріалів, організації наукових досліджень, проведення практичних занять із моніторингу інформаційного простору, оцінювання ефективності комунікацій і протидії дезінформації (довідка № 19/25 від 18.10.2025 р.).

Особистий внесок здобувача. Дисертація є самостійно виконаною науковою працею. Наукові положення, теоретичні узагальнення, авторські

визначення, класифікації, методичні підходи, концептуальні моделі, алгоритми, матриці, системи показників, практичні рекомендації та висновки сформульовано здобувачем особисто. У наукових працях, підготовлених у співавторстві, використано лише ті положення й результати, які належать здобувачеві.

Апробація результатів дисертації. Основні теоретичні положення, методичні підходи та практичні рекомендації дисертаційного дослідження доповідалися й обговорювалися на науково-практичних заходах, зокрема: III Міжнародній науково-практичній конференції «Березневий науковий дискурс 2025: Синергія освіти, науки та бізнесу в епоху глобальних трансформацій» (Чернігів, 27 лютого 2025 р.); Міжнародній науково-практичній конференції «Актуальні питання управління та адміністрування: регіональний, міжнародний та глобалізаційний аспекти» (Чернігів, 22-23 травня 2025 р.); I Науково-практичній конференції з міжнародною участю (Чернігів, 6-8 березня 2024 р.); I Науково-практичній конференції з міжнародною участю «Людина в системі управління: гендерні та психологічні аспекти менеджменту та адміністрування» (Чернігів, 28-29 листопада 2024 р.); Всеукраїнській науково-практичній конференції «Національна безпека в умовах війни, післявоєнної відбудови та глобальних викликів XXI століття» (Житомир, 7-8 грудня 2023 р.); Міжнародній науково-практичній конференції «Стійкість освіти і науки в умовах трансформації» (Київ, 23-24 травня 2023 р.); I Міжнародній науково-практичній конференції здобувачів вищої освіти та молодих учених «Державне й муніципальне управління у XXI столітті: організаційно-економічні, правові та інформаційні аспекти» (Львів, 27 квітня 2023 р.); науково-практичній конференції «Актуальні питання сучасної стратегії розвитку України: виклики, пріоритети та прогнози» (Київ, 22 листопада 2023 р.); VII Всеукраїнській студентській науково-практичній конференції «Вища освіта – студентська наука – сучасне суспільство: напрями розвитку» (Київ, 12 грудня 2023 р.).

Публікації. Результати дисертаційного дослідження опубліковано у 16 наукових працях, зокрема: 7 статтях, із яких 5 оприлюднено у наукових фахових виданнях України та 2 – у наукових періодичних виданнях інших держав, а також

9 публікаціях у збірниках матеріалів міжнародних, всеукраїнських і регіональних науково-практичних конференцій.

Структура та обсяг дисертації. Дисертація складається зі вступу, трьох розділів, висновків до розділів, загальних висновків, списку використаних джерел і додатків. Повний обсяг дисертації становить 230 сторінок, основний текст викладено на 195 сторінках. Робота містить 46 таблиць та 32 рисунки. Список використаних джерел налічує 161 найменувань.

РОЗДІЛ 1. КОНЦЕПТУАЛЬНІ ОСНОВИ ДЕРЖАВНОЇ ІНФОРМАЦІЙНОЇ ПОЛІТИКИ

1.1. Еволюція наукових поглядів на формування державної інформаційної політики

Дослідження механізмів реалізації державної інформаційної політики потребує попереднього з'ясування того, як змінювалися наукові уявлення про її природу, цілі, суб'єктний склад та інструментарій. Історико-еволюційний ракурс дає змогу уникнути спрощеного трактування цієї політики лише як сукупності заходів із поширення офіційної інформації. У різні періоди її розглядали як напрям правового регулювання інформаційних відносин, інституційну функцію держави, засіб демократичної комунікації, складову національної безпеки, механізм розвитку інформаційного суспільства, а нині – як інтегровану систему управління даними, платформами, публічною комунікацією та інформаційною стійкістю. Відповідно, еволюція поглядів відображає не тільки накопичення знань, а й зміну самого об'єкта державного впливу.

Поняття державної інформаційної політики належить до категорій, зміст яких формується на перетині правової науки, теорії публічного управління, політології, комунікаційних студій, безпекознавства та досліджень цифрової трансформації. Така міждисциплінарність зумовлює різні дослідницькі акценти. Правознавці переважно аналізують інформаційні права, режими доступу, захист інформації та компетенцію публічних інституцій; фахівці з державного управління – механізми вироблення, координації й оцінювання політики; політологи – вплив інформаційних процесів на демократію та легітимність; дослідники комунікації – взаємодію влади з аудиторіями; представники безпекових студій – загрози, інформаційні операції та стійкість суспільства [6; 17; 124; 136; 137].

Еволюційний аналіз передбачає розмежування двох взаємопов'язаних процесів. Перший полягає у розвитку нормативної та інституційної основи інформаційної сфери: закріпленні права на інформацію, формуванні медійного

законодавства, визначенні режимів захисту даних, створенні органів і процедур доступу до публічної інформації. Другий процес пов'язаний зі зміною наукової парадигми – переходом від державоцентричного управління інформаційними потоками до людиноцентричної, мережевої та партнерської моделі, у якій держава не володіє монополією на комунікацію, а координує взаємодію численних учасників інформаційного середовища [4; 8; 43; 136].

Для української науки особливе значення має залежність інформаційної політики від державотворчих і безпекових викликів. У 1990-х роках пріоритетом було створення національної системи законодавства та інституцій, здатних забезпечити функціонування незалежного інформаційного простору. У 2000-х роках домінували питання розвитку інформаційного суспільства, європейської інтеграції та електронного урядування. Після 2014 року центральними стали інформаційна безпека, гібридна війна, стратегічні комунікації й протидія дезінформації. Повномасштабне вторгнення Російської Федерації поглибило безпековий вимір, але водночас актуалізувало вимоги до довіри, точності, координації та суспільно-мобілізаційної ефективності державної комунікації [21; 28; 71; 114].

У межах цього дослідження пропонується розглядати еволюцію наукових поглядів як послідовність п'яти взаємопов'язаних етапів: правового та інституційного становлення; розвитку концепції інформаційного суспільства й електронного урядування; безпекової переорієнтації; воєнно-комунікаційної моделі; цифрово-платформної та людиноцентричної парадигми. Межі між ними є умовними, оскільки окремі наукові підходи виникали раніше або продовжували домінувати пізніше, проте така періодизація відображає зміну провідної дослідницької проблематики [69; 126].

Узагальнену логіку переходу між провідними науковими парадигмами подано на рис. 1.1. Схема демонструє, що кожний наступний етап не заперечує попередній, а розширює предмет державної інформаційної політики та ускладнює її механізми.



Рис. 1.1. Еволюційний ланцюг наукових поглядів на державну інформаційну політику

Джерело: систематизовано автором на основі [3; 24; 28; 69; 71; 115; 120; 126].

Наведена послідовність засвідчує рух від відносно вузького бачення державної інформаційної політики як правового та організаційного впорядкування медійної сфери до розуміння її як багаторівневої системи публічного врядування. У такій системі нормативні правила, інституційна координація, стратегічні комунікації, цифрові інструменти, захист інформаційного простору та оцінювання суспільної довіри утворюють єдиний цикл. Саме ця інтеграція є найбільш виразним результатом розвитку наукової думки останніх років.

Теоретичні витоки державної інформаційної політики пов'язані з ширшими уявленнями про взаємозв'язок інформації, влади та суспільного порядку. Інформація тривалий час розглядалася як ресурс управління, необхідний для прийняття рішень, підтримання організаційної цілісності та легітимації політичної влади. Проте в умовах демократизації до ресурсного виміру додався правовий: інформація стала сприйматися не лише як об'єкт володіння чи поширення державою, а як суспільне благо та предмет фундаментального права людини. Саме поєднання управлінського й правового

вимірів створило передумови для виокремлення державної інформаційної політики як самостійної сфери [43; 48; 93; 127].

У класичній державоцентричній моделі комунікація переважно мала вертикальний характер: органи влади визначали зміст повідомлень, канали їх поширення та допустимі межі доступу до відомостей. Науковий аналіз за таких умов концентрувався на організації інформаційної діяльності державних установ і правових режимах інформації. Демократична модель змінила вихідну точку дослідження: легітимність публічної комунікації почала пов'язуватися з відкритістю, можливістю громадян отримувати відомості, висловлювати позицію та контролювати діяльність влади. Відтак інформаційна політика стала осмислюватися як механізм забезпечення публічності та підзвітності [4; 7; 79; 84].

Організаційно-правовий підхід, системно представлений у працях І. Арістової, заклав основу для розуміння державної інформаційної політики як цілеспрямованої діяльності держави, що здійснюється через взаємопов'язані нормативні та організаційні засоби. Його принципова перевага полягає у переході від опису окремих інформаційних процесів до аналізу цілісної системи: цілей, принципів, суб'єктів, повноважень, правових режимів та процедур. Така логіка надалі була розвинена в дослідженнях правового забезпечення інформаційної сфери, інформаційного права та механізмів реалізації права на доступ до інформації [3; 4; 6; 62].

Істотний вплив на категоріальне оформлення державної інформаційної політики справила концепція інформаційної держави, представлена у зарубіжній літературі. С. Браман показує, що інформація є не окремим сектором політики, а системоутворювальним чинником, який змінює форми влади, регуляторні спроможності та взаємодію держави з громадянами. За такого підходу інформаційна політика охоплює не лише медіа або доступ до відомостей, а правила створення, збирання, оброблення, зберігання, поширення та використання інформації в усіх сферах публічного життя.

У сучасній українській науці поняття державної інформаційної політики дедалі частіше розкривається через сукупність її змістових функцій. До них

відносять гарантування інформаційних прав, створення умов для розвитку інформаційного суспільства, забезпечення відкритості влади, регулювання медійної сфери, розвиток цифрової інфраструктури, підтримання інформаційної безпеки та формування ефективної публічної комунікації. Такий функціональний підхід дає змогу з'єднати в одній категорії правові, управлінські, технологічні й безпекові складові [68; 120; 121].

Отже, початкове категоріальне оформлення державної інформаційної політики відбувалося шляхом поєднання чотирьох базових ідей: інформації як управлінського ресурсу; інформації як об'єкта правового регулювання; доступу до інформації як права людини; публічної комунікації як умови демократичної легітимності. Подальша еволюція не скасувала ці ідеї, а доповнила їх категоріями цифрового врядування, інформаційної безпеки, стійкості та доброчесності інформаційного середовища.

Категоріальна визначеність державної інформаційної політики має принципове значення для подальшого аналізу механізмів її реалізації, оскільки зміст поняття окреслює межі державного впливу, коло суб'єктів, набір інструментів і критерії результативності. У науковій літературі відсутнє цілком уніфіковане визначення цієї категорії. Розбіжності зумовлені тим, що правознавці акцентують на нормативному регулюванні та гарантіях прав, фахівці з публічного управління – на цілях, інституціях і процедурах, дослідники комунікацій – на взаємодії держави із суспільством, а представники безпекових і цифрових студій – на захисті інформаційного простору, даних, мереж і платформ.

У межах організаційно-правової традиції І. В. Арістова розкриває державну інформаційну політику як цілеспрямовану діяльність держави з упорядкування інформаційних відносин, визначення компетенції уповноважених інституцій, створення правових умов для функціонування інформаційної сфери та забезпечення прав її учасників [3]. Такий підхід сформував фундаментальне уявлення про політику не як сукупність окремих інформаційних заходів, а як системно організовану державно-владну діяльність. Близьке за логікою трактування представлене В. О. Негодченком, який

наголошує на комплексі правових, організаційних, економічних та інших заходів держави, спрямованих на розвиток і належне функціонування інформаційної сфери [68].

Публічно-управлінський вимір найбільш послідовно простежується у працях Ю. В. Нестеряка та Ю. В. Турченка. Ю. В. Нестеряк пов'язує державну інформаційну політику із системним управлінням інформаційними процесами, формуванням національного інформаційного простору, координацією діяльності суб'єктів та забезпеченням національних інтересів [69; 70]. Ю. В. Турченко розглядає її як складову демократичного державотворення, у межах якої держава має створювати умови для реалізації інформаційних прав, відкритості влади, розвитку суспільної комунікації та участі громадян [127]. У цих позиціях державна інформаційна політика набуває ознак безперервного управлінського процесу, що охоплює не лише нормативне встановлення правил, а й організацію їх практичного виконання.

Комунікаційний та інтеграційний аспекти поняття розкрито у колективній монографії Л. В. Губерського, Є. Є. Камінського, Є. А. Макаренка, М. А. Ожевана та О. І. Шниркова, де інформаційна політика пов'язується з демократизацією інформаційної сфери, європейською інтеграцією, розвитком міжнародної комунікації та позиціонуванням держави у світовому інформаційному просторі [24]. Т. О. Савосько, узагальнюючи зміст і функції досліджуваної категорії, акцентує на цілеспрямованій діяльності органів публічної влади щодо регулювання інформаційних відносин, інформування суспільства, підтримання комунікації, розвитку інформаційного середовища та забезпечення його безпеки [120; 121]. Отже, комунікація постає не допоміжною функцією, а одним із системоутворювальних компонентів політики.

Безпековий і цифрово-інституційний поворот розширив попередні трактування. Д. В. Дубов обґрунтовує необхідність розглядати державну інформаційну політику з урахуванням одночасної дії мирних і воєнних механізмів, гібридних загроз та потреби у стратегічних комунікаціях [28]. Д. Дубовик визначає інформаційну політику як інструмент державного управління в умовах цифровізації та наголошує на інституційному механізмі її реалізації,

який має забезпечувати узгоджену діяльність органів влади, цифрових каналів і суб'єктів інформаційної взаємодії [29; 30]. У ширшій теоретичній перспективі С. Брамман трактує інформаційну політику як сукупність законів, правил, доктрин і практик, що визначають створення, оброблення, рух, доступ і використання інформації та безпосередньо пов'язані з реалізацією влади [136].

Зіставлення наведених позицій свідчить про поступове розширення змісту поняття: від організаційно-правового регулювання інформаційних відносин – до системного публічного управління інформаційною екосистемою. Інваріантними ознаками державної інформаційної політики у більшості наукових трактувань є цілеспрямованість, нормативна визначеність, інституційна забезпеченість, орієнтація на інформаційні права, розвиток інформаційного простору та захист суспільно значущих інтересів. Новітні підходи доповнюють цей перелік багатосуб'єктною взаємодією, стратегічними комунікаціями, цифровим врядуванням, платформним регулюванням, інформаційною доброчесністю, стійкістю та оцінюванням суспільних результатів [28; 29; 45; 120; 136; 150; 159; 160].

Для більш чіткого розмежування етапів доцільно систематизувати їх за домінуючою парадигмою, предметом наукового інтересу та характерними обмеженнями. Результати такого узагальнення наведено в табл. 1.1.

Таблиця 1.1 підтверджує, що зміна домінуючих парадигм зумовлювалася не лише розвитком науки, а й практичними викликами державотворення. Поява нових загроз або технологій змінювала пріоритети, однак не усувала значення попередніх інституцій. Зокрема, воєнна комунікація залишається правомірною лише за умови дотримання конституційних гарантій, а цифрова трансформація потребує чітких правил доступу, захисту даних і відповідальності суб'єктів [48; 84; 91; 119].

Етапи еволюції наукових поглядів на формування державної інформаційної політики

Етап	Домінуюча парадигма	Ключовий предмет наукового аналізу	Характерні здобутки та обмеження
1991–2000	Правова та інституційна	Інформаційні права, медійне законодавство, компетенції органів влади, режими інформації	Створено базові категорії й нормативний каркас; недостатньо уваги приділялося партнерській комунікації та цифровим мережам
2001–2013	Інформаційне суспільство, електронне урядування, європеїзація	Інформатизація, доступ до публічної інформації, електронна взаємодія, стандарти ЄС	Розширено технологічний та інтеграційний вимір; безпекові ризики часто розглядалися відокремлено від комунікаційної політики
2014–2021	Безпекова та стратегічно-комунікаційна	Гібридна війна, дезінформація, кібербезпека, координація стратегічних комунікацій	Сформовано комплексне бачення інформаційних загроз; існував ризик надмірної сек'юритизації та звуження правозахисного підходу
2022–2024	Воєнно-комунікаційна та стійкісна	Кризове інформування, суспільна мобілізація, захист інформаційного простору, довіра	Посилено оперативну координацію та стійкість; загострено проблему балансу відкритості й обмежень в умовах воєнного стану
2025–2026	Цифрово-платформна та людиноцентрична	Дані, платформи, алгоритми, ШІ, інформаційна доброчесність, оцінювання результативності	Інтегруються права, технології, безпека та комунікація; потребують розвитку механізми підзвітності алгоритмів і міжсекторального партнерства

Джерело: систематизовано автором на основі [3; 24; 28; 69; 71; 105; 115; 126; 136; 160].

Періодизація також дає підстави стверджувати, що найбільш стійкою тенденцією є розширення суб'єктного складу державної інформаційної політики. Від моделі, у якій держава виступала головним виробником і розпорядником суспільно значущої інформації, наука перейшла до визнання мережі учасників: органів публічної влади, медіа, цифрових платформ, громадянського суспільства, наукових установ, бізнесу та міжнародних організацій. Це обумовлює перехід від командного управління до координації, співрегулювання та партнерства [138; 150; 151; 159].

Перший етап розвитку української наукової думки був безпосередньо пов'язаний із формуванням правових засад незалежної держави. Відсутність усталеної системи національного регулювання вимагала визначити базові категорії інформації, суб'єктів інформаційних відносин, види інформації, принципи доступу та юридичні підстави обмежень. Закон України «Про

інформацію» заклав рамкову основу цієї сфери, а Конституція України надала інформаційним правам найвищого рівня юридичного захисту [48; 93].

У наукових працях 1990-х – початку 2000-х років державна інформаційна політика переважно аналізувалася через співвідношення правового статусу особи й повноважень держави. У центрі були свобода думки і слова, право вільно збирати, зберігати, використовувати та поширювати інформацію, а також можливість установа законних обмежень. Такий підхід був закономірним, оскільки становлення демократичної державності потребувало подолання практик закритості та адміністративного контролю над публічною комунікацією [7; 43; 79].

Значний внесок у систематизацію організаційно-правових засад зробила І. Арістова, яка розглядала державну інформаційну політику як цілеспрямовану діяльність, що потребує узгодження законодавчих норм, компетенцій органів держави та організаційних процедур. У цій концепції державна політика набуває ознак системності: вона має бути заснована на визначених принципах, охоплювати процес формування і реалізації рішень, передбачати інституційну відповідальність та правові гарантії [3].

Важливим напрямом наукового пошуку стало співвідношення відкритості й охорони інформації. З одного боку, демократична держава має забезпечувати доступ до суспільно значущих відомостей; з іншого – зберігати державну таємницю, захищати персональні дані, інформаційні системи й інші законні інтереси. Уже на ранньому етапі стало очевидно, що державна інформаційна політика не може бути зведена ані до максимальної відкритості, ані до переважно обмежувальної моделі. Її зміст визначається пошуком пропорційного балансу [4; 83; 90; 91].

Попри це, правова та інституційна парадигма зберегла фундаментальне значення. Саме вона встановила межі допустимого державного втручання, визначила права й обов'язки учасників, сформувала принципи законності та юридичної відповідальності. Усі наступні підходи – безпековий, цифровий або комунікаційний – можуть бути легітимними лише в межах цього фундаменту [48; 93].

На початку 2000-х років розвиток інформаційно-комунікаційних технологій змінив предмет наукового аналізу. Інформація почала розглядатися не тільки як об'єкт правового режиму, а й як стратегічний ресурс економічного, соціального та адміністративного розвитку. Поняття інформаційного суспільства поєднало технологічні, інституційні й гуманітарні аспекти: доступ до мереж, цифрові навички, електронні послуги, відкритість даних, інноваційність і нові форми участі громадян [100; 122; 136].

Законодавче закріплення Основних засад розвитку інформаційного суспільства в Україні на 2007–2015 роки стало важливим чинником переорієнтації наукової думки. Державна інформаційна політика дедалі частіше пов'язувалася з модернізацією публічного управління, подоланням цифрової нерівності, розвитком національних інформаційних ресурсів і впровадженням електронної взаємодії. У цій парадигмі держава виступає не лише регулятором, а й інвестором, організатором інфраструктури та постачальником цифрових послуг.

Концепція електронного урядування конкретизувала управлінський вимір інформаційного суспільства. Йшлося про переведення адміністративних процедур у цифрову форму, інтеграцію інформаційних систем, електронну ідентифікацію, документообіг і нові канали комунікації з громадянами. Науковий акцент змістився з інформування про діяльність влади до цифрової взаємодії, у якій інформація стає частиною самої публічної послуги [85; 87; 111].

Європейська інтеграція стала окремим каталізатором розвитку державної інформаційної політики. Монографічні дослідження підкреслювали необхідність узгодження українських підходів із європейськими стандартами свободи вираження поглядів, медіаплюралізму, захисту персональних даних і доступу до інформації. Водночас інформаційні кампанії розглядалися як механізм пояснення євроінтеграційних реформ та формування суспільної підтримки [23; 24].

У межах євроінтеграційної парадигми державна інформаційна політика набула двох взаємопов'язаних вимірів. Внутрішній вимір передбачав приведення законодавства, інституцій і практик комунікації у відповідність до

європейських норм. Зовнішній – формування міжнародного образу України, представлення її інтересів у світовому інформаційному просторі та протидію стереотипам. Надалі ці напрями були закріплені в Угоді про асоціацію та спеціальних комунікаційних стратегіях [110; 112; 128].

Вагомим теоретико-методологічним узагальненням цього етапу стала праця Ю. Нестеряка, у якій державна інформаційна політика розглядається як системний напрям діяльності держави, пов'язаний із формуванням інформаційного простору, забезпеченням прав, розвитком інфраструктури та безпекою. Такий підхід відображав уже не галузеве, а комплексне бачення, придатне для аналізу взаємозв'язку правових, організаційних і технологічних механізмів [69].

Отже, парадигма інформаційного суспільства істотно розширила наукове розуміння державної інформаційної політики. До прав і регулювання додалися інфраструктура, цифрові послуги, електронна взаємодія, відкриті дані, європейські стандарти та міжнародна комунікація. Водночас вона підготувала концептуальний ґрунт для наступного безпекового повороту, оскільки мережева відкритість виявилася нерозривно пов'язаною з новими ризиками [24; 69; 100; 128].

Для зіставлення основних наукових позицій доцільно систематизувати їх за змістом визначення, домінуючим акцентом і внеском у розвиток категорії. У табл. 1.2 подано змістове узагальнення авторських концепцій, а не дослівне відтворення формулювань, що дає змогу коректно порівняти різні дисциплінарні підходи до державної інформаційної політики.

Дані табл. 1.2 засвідчують, що зміст державної інформаційної політики еволюціонував шляхом накопичення взаємодоповнювальних ознак. Організаційно-правовий підхід закріпив системність і законність державної діяльності; управлінський – цілепокладання, координацію та механізми реалізації; демократичний – права людини, відкритість і участь; комунікаційний – діалог та довіру; безпековий – захист від деструктивних впливів; цифрово-платформний – управління даними, алгоритмами й технологічними посередниками. Отже, сучасне визначення має бути інтегрованим і водночас не

зводити політику ані до державного інформування, ані до медійного регулювання, ані виключно до інформаційної безпеки.

Таблиця 1.2

Узагальнення наукових трактувань поняття «державна інформаційна політика»

Автор / джерело	Узагальнений зміст наукового трактування	Домінуючий акцент	Еволюційне значення
І. В. Арістова [3]	Цілеспрямована організаційно-правова діяльність держави з упорядкування інформаційних відносин, визначення компетенції інституцій і гарантування прав учасників.	Правове та інституційне регулювання	Сформовано базову системну модель державної діяльності в інформаційній сфері.
Л. В. Губерський та ін. [24]	Стратегічний напрям державної діяльності, що поєднує внутрішній розвиток інформаційної сфери з європейською інтеграцією та позиціонуванням держави.	Європеїзація і зовнішня комунікація	Розширено поняття міжнародним та інтеграційним вимірами.
Ю. В. Нестеряк [69]	Системна публічно-управлінська діяльність щодо формування інформаційного простору, координації суб'єктів і забезпечення національних інтересів.	Системність та механізми управління	Перенесено увагу з правових норм на управлінський процес і взаємодію суб'єктів.
Ю. В. Турченко [127]	Складова демократичного державотворення, спрямована на реалізацію інформаційних прав, відкритість влади, суспільну комунікацію та участь громадян.	Демократичний і правозахисний підхід	Посилено людиноцентричний та учасниковий зміст політики.
В. О. Негодченко [68]	Комплекс правових, організаційних, економічних та інших заходів держави, спрямованих на розвиток і належне функціонування інформаційної сфери.	Комплекс державних заходів	Конкретизовано багатокомпонентний інструментарій державного впливу.
Т. О. Савосько [120; 121]	Цілеспрямована діяльність органів публічної влади з регулювання інформаційних відносин, інформування, комунікації, розвитку інформаційного середовища та його захисту.	Функціонально-комунікаційний підхід	Поєднано регулятивні, комунікаційні, розвиткові й безпекові функції.
Д. В. Дубов; Д. Дубовик [28; 29; 30]	Інструмент державного управління і безпеки, який за умов війни та цифровізації потребує інституційної координації, стратегічних комунікацій і цифрових механізмів.	Безпековий і цифрово-інституційний підхід	Адаптовано поняття до гібридних загроз, цифрової трансформації та мережевої взаємодії.
S. Braman [136]	Сукупність законів, правил, доктрин і практик, що визначають створення, оброблення, потоки, доступ та використання інформації і пов'язані з реалізацією влади.	Інформація, політика і влада	Розширено аналіз до всієї інформаційної екосистеми та владних відносин.

Джерело: узагальнено автором за [3; 24; 28; 29; 30; 68; 69; 120; 121; 127; 136].

Російська агресія проти України, що розпочалася у 2014 році, стала переломним чинником розвитку наукових поглядів на державну інформаційну політику. Інформаційний простір почав розглядатися як середовище ведення гібридного протиборства, у якому використовуються пропаганда, дезінформація,

психологічний вплив, маніпуляція історичною пам'яттю, кібератаки та мережеві операції. Відповідно, політика вже не могла обмежуватися розвитком медіа чи електронних сервісів [21; 28; 38; 50].

Безпековий поворот мав глибше значення, ніж просте додавання нового напрямку до існуючої політики. Він змінив уявлення про об'єкт державного захисту. Якщо раніше йшлося переважно про інформаційні ресурси та системи, то надалі увага поширилася на суспільну свідомість, довіру до інституцій, здатність громадян розпізнавати маніпуляції та функціонування демократичного публічного простору. Інформаційна безпека стала осмислюватися одночасно як безпека держави, суспільства й людини [17; 41; 42; 72].

Поняття дезінформації поступово набуло самостійного значення у правових і управлінських дослідженнях. Науковці звернули увагу на її цілеспрямованість, маніпулятивний характер, здатність завдавати шкоди національній безпеці та водночас складність правового обмеження через необхідність захисту свободи вираження поглядів. Унаслідок цього сформувався запит на пропорційні механізми, що поєднують спростування, медіаграмотність, прозорість платформ, відповідальність за координовані операції та судовий захист [35; 40; 61; 63; 64; 76].

Важливим результатом безпекового повороту стало виокремлення стратегічних комунікацій. На відміну від ситуативного інформування, вони передбачають узгодження дій і повідомлень державних інституцій із довгостроковими цілями, аналіз аудиторій, використання різних каналів, координацію цивільних і безпекових органів та оцінювання ефекту. Концепція стратегічної комунікації спрямована не лише на передачу інформації, а й на формування послідовної поведінки держави, що підтверджує її повідомлення.

У науковому дискурсі України стратегічні комунікації почали розглядатися як міст між інформаційною політикою та національною безпекою. Вони поєднують публічну дипломатію, урядові комунікації, взаємодію з медіа, кризове інформування, протидію дезінформації та внутрішню координацію. Така інтеграція сприяла подоланню розриву між політикою розвитку інформаційного суспільства й політикою захисту інформаційного простору [28; 36; 45].

Разом із тим сек'юритизація інформаційної політики створила ризик надмірного розширення обмежувальних повноважень держави. Наукові дослідження конституційного й адміністративно-правового забезпечення інформаційної безпеки наголошують, що будь-які обмеження мають бути встановлені законом, переслідувати легітимну мету, бути необхідними та пропорційними. Особливої ваги набуває розмежування шкідливого інформаційного впливу, помилкової інформації, критики влади та законного вираження поглядів [58; 75; 130; 131].

Отже, безпековий поворот розширив державну інформаційну політику трьома взаємопов'язаними компонентами: системним аналізом інформаційних загроз, стратегічними комунікаціями та концепцією суспільної стійкості. Водночас він актуалізував фундаментальну проблему балансу між захистом інформаційного простору й гарантіями свободи інформації. Саме цей баланс став центральним для подальшої воєнної та цифрової парадигми.

Зміст безпекового повороту неможливо розкрити в межах однієї наукової дисципліни. Сучасне дослідження державної інформаційної політики утворює міждисциплінарну архітектуру, у якій різні галузі формують взаємодоповнювальні аналітичні блоки (рис. 1.2).

Правова наука права, свободи, режими доступу	Теорія публічного управління інституції, компетенції, механізми	Комунікаційні студії діалог, довіра, стратегічні повідомлення
Безпекові студії загрози, стійкість, протидія впливам	ДЕРЖАВНА ІНФОРМАЦІЙНА ПОЛІТИКА інтегрована сфера формування й реалізації публічних рішень	Цифрове врядування дані, платформи, електронні послуги
Соціологія та психологія поведінка аудиторій, сприйняття, медіаграмотність	Політична наука влада, демократія, публічна сфера	Міжнародні та європейські студії стандарти, координація, транснаціональні ризики

Рис. 1.2. Міждисциплінарна архітектура дослідження державної інформаційної політики

Джерело: розроблено автором на основі [6; 17; 42; 69; 124; 136; 137; 144; 146].

Рисунок 1.2 відображає інтегративний характер сучасної наукової проблематики. Правові засади визначають межі втручання, теорія публічного управління пояснює механізми реалізації, комунікаційні студії – взаємодію з аудиторіями, безпекові науки – загрози й стійкість, цифрове врядування – інфраструктуру та дані, а соціальні й політичні науки – поведінкові та демократичні наслідки. Відсутність хоча б одного з цих блоків призводить до однобічного розуміння політики.

Повномасштабне вторгнення Російської Федерації у 2022 році перевело державну інформаційну політику в режим одночасного кризового реагування та довгострокової трансформації. Наукова увага зосередилася на здатності держави оперативно інформувати населення, підтримувати суспільну мобілізацію, протидіяти ворожим наративам, захищати чутливі дані та забезпечувати безперервність цифрових сервісів. Інформаційна політика стала безпосередньою складовою життєстійкості держави [71; 114].

Воєнна комунікація підвищила вимоги до точності, швидкості та узгодженості офіційних повідомлень. Суперечлива або несвоєчасна інформація може створювати паніку, підривати довіру й полегшувати поширення дезінформації. Водночас надмірне обмеження відомостей або відсутність пояснення управлінських рішень породжують інформаційний вакуум. Тому сучасна наука розглядає довіру не як побічний результат, а як стратегічний ресурс інформаційної політики.

Правові дослідження воєнного періоду детально аналізують допустимі обмеження доступу до інформації. Воєнний стан об'єктивно вимагає захисту даних про оборону, критичну інфраструктуру, переміщення сил та інші чутливі відомості. Однак обмеження мають бути конкретними, обґрунтованими й тимчасовими, а не перетворюватися на загальну практику закритості. Ця позиція продовжує правозахисну лінію ранньої парадигми в новому безпековому контексті [19; 119; 131].

Одночасно з воєнними викликами відбувається поглиблення цифрової трансформації публічного управління. Електронні послуги, цифрові документи, реєстри та мобільні платформи стали ключовими каналами взаємодії держави з

громадянами. Наукові дослідження дедалі більше розглядають цифровізацію як зміну самої моделі управління, а не як просте переведення паперових процедур в електронну форму.

Інституційний механізм державної інформаційної політики в цифровому середовищі охоплює координацію органів влади, управління даними, взаємодію реєстрів, стандарти безпеки, комунікацію з користувачами та партнерство з приватним сектором. Його ефективність залежить від розподілу відповідальності й здатності уникати дублювання функцій. Саме тому сучасні дослідження повертаються до інституційної проблематики, але вже в контексті мережевої держави [30; 44].

Платформізація інформаційного простору створює новий рівень посередництва між державою та громадянами. Соціальні мережі й пошукові системи визначають видимість повідомлень за допомогою алгоритмів, правила яких не завжди є прозорими. Державна інформаційна політика повинна враховувати не тільки зміст офіційної комунікації, а й технічні та комерційні умови її поширення. Це зумовлює потребу в регулюванні платформ, дослідницькому доступі до даних і прозорості алгоритмічних рішень.

Європейське регулювання цифрового середовища суттєво впливає на сучасні наукові підходи. Digital Services Act установлює вимоги до відповідальності платформ і управління системними ризиками, Data Governance Act розвиває механізми доступу та обміну даними, European Media Freedom Act формує гарантії незалежності й плюралізму медіа, а Artificial Intelligence Act закладає ризик-орієнтовану модель регулювання штучного інтелекту [154; 155; 156; 157].

Особливого значення набуває поняття інформаційної доброчесності. Глобальні принципи ООН пов'язують її з точністю, надійністю, плюралізмом і безпечністю інформаційного середовища, а рекомендації ЮНЕСКО наголошують на багатосторонньому врядуванні цифрових платформ. Наукова новизна цього підходу полягає в переході від боротьби з окремими проявами дезінформації до підтримання якості всієї інформаційної екосистеми [159; 160].

В українських дослідженнях 2024–2026 років зростає увага до механізмів цифрової комунікації органів публічної влади, інформаційної стійкості, нормативного забезпечення стратегічних комунікацій і взаємодії державних та правоохоронних органів у протидії дезінформації [2; 36; 45; 55]. Це свідчить про перехід від опису загроз до пошуку організаційних моделей реалізації політики.

Паралельно розвивається напрям оцінювання державної інформаційної політики. Традиційні кількісні показники – кількість повідомлень, охоплення або відвідування ресурсів – не відображають суспільного результату. Доцільно вимірювати рівень довіри, доступність і зрозумілість інформації, швидкість реагування, стійкість до дезінформації, якість координації, захищеність даних і ступінь участі громадян. Такий підхід переводить наукову дискусію від активності органів влади до публічної цінності [120; 121; 150].

Таким чином, парадигма 2022–2026 років інтегрує воєнну стійкість, цифрове врядування, платформне регулювання, права людини та публічну комунікацію. Її відмінність від попередніх етапів полягає у переході від галузевої політики до управління інформаційною екосистемою. У цій екосистемі результат залежить від взаємодії держави, медіа, платформ, громадянського суспільства, наукової спільноти та міжнародних партнерів.

Зміни, що відбулися на різних етапах, можна простежити за основними параметрами механізму державної інформаційної політики. Порівняльну характеристику наведено в табл. 1.3.

Дані табл. 1.3 демонструють якісний перехід від переважно нормативного механізму до інтегрованого управління інформаційною екосистемою. Найвиразніше змінюються об'єкт і критерії результативності. Якщо на ранніх етапах достатнім вважалося створення норм та інформаційних ресурсів, то нині політика має доводити здатність формувати довіру, знижувати суспільні ризики, підтримувати права та забезпечувати стійкість у цифровому середовищі.

Трансформація основних параметрів механізму державної інформаційної політики

Параметр	1991–2013 роки	2014–2021 роки	2022–2026 роки
Провідна мета	Правове впорядкування, забезпечення доступу, розвиток інформаційного суспільства	Захист інформаційного простору, протидія гібридним загрозам, стратегічні комунікації	Інформаційна стійкість, довіра, безперервність цифрової держави, доброчесність інформаційної екосистеми
Основний об'єкт	Інформація, медіа, державні ресурси та системи	Інформаційний простір, наративи, мережі впливу, критична інфраструктура	Дані, платформи, алгоритми, поведінка аудиторій, суспільна спроможність до відновлення
Суб'єктний склад	Переважно органи державної влади та традиційні медіа	Органи влади, безпекові інституції, медіа, громадські організації, міжнародні партнери	Багаторівнева мережа: держава, громади, платформи, бізнес, медіа, наука, громадяни, міжнародні організації
Домінуючі інструменти	Нормативне регулювання, інформатизація, офіційне інформування, електронні послуги	Моніторинг, спростування, кіберзахист, стратегічні комунікації, санкційні та інституційні заходи	Управління даними, платформне співрегулювання, ризик-орієнтований нагляд, цифрова участь, превентивна комунікація, медіаграмотність
Критерії результативності	Виконання норм, доступність інформації, кількість цифрових сервісів	Швидкість реагування, зниження впливу загроз, узгодженість повідомлень	Довіра, стійкість, якість інформації, захищеність прав, інклюзивність, підзвітність алгоритмів і партнерств

Джерело: систематизовано автором за [3; 24; 28; 29; 45; 69; 71; 105; 115; 120; 150; 159; 160].

Проведений аналіз дає підстави стверджувати, що сучасне наукове розуміння державної інформаційної політики сформувалося внаслідок інтеграції, а не послідовного заперечення підходів. Правова парадигма визначає ціннісні й нормативні межі; інституційна – суб'єктів та процедури; комунікаційна – принципи взаємодії з аудиторіями; безпекова – ризики й механізми захисту; цифрово-платформна – інфраструктуру та технологічних посередників; людиноцентрична – кінцевий суспільний результат.

Узагальнення поглядів дає змогу виділити кілька наскрізних закономірностей. Перша – розширення предмета політики від регулювання

інформації до врядування інформаційної екосистеми. Друга – перехід від монополії держави на формування повідомлень до багатосуб’єктної взаємодії. Третя – зміна домінуючих інструментів від адміністративно-правових до комбінованих, що включають партнерство, комунікацію, технологічне регулювання й розвиток стійкості. Четверта – переорієнтація оцінювання з формального виконання заходів на суспільні ефекти.

Водночас наукова еволюція не усунула фундаментальних дилем. Найважливішою залишається суперечність між відкритістю та безпекою. Держава повинна забезпечувати доступ до інформації, але водночас захищати чутливі дані й реагувати на ворожі операції. Вирішення цієї дилеми можливе не через вибір одного полюса, а через правові критерії необхідності, пропорційності, обґрунтованості та підзвітності [48; 84; 105; 119].

На думку автора, державна інформаційна політика – це ціннісно орієнтована, нормативно врегульована, інституційно скоординована та суспільно підзвітна система цілей, принципів, управлінських рішень, механізмів і дій держави у взаємодії з громадянами, медіа, інститутами громадянського суспільства, бізнесом, науковим середовищем, органами місцевого самоврядування та цифровими платформами, спрямована на гарантування інформаційних прав і свобод, розвиток відкритого та інклюзивного інформаційного простору, забезпечення достовірної публічної комунікації, цифрового розвитку, інформаційної безпеки й суспільної стійкості, а також на досягнення вимірюваних суспільних результатів на основі постійного зворотного зв’язку.

Наукова новизна запропонованого визначення полягає у поєднанні шести взаємопов’язаних характеристик: ціннісно-правової, що визначає пріоритет прав і свобод; інституційно-управлінської, яка фіксує систему суб’єктів, компетенцій і відповідальності; комунікаційної, орієнтованої на діалог, довіру та участь; цифрово-платформної, що враховує дані, алгоритми й технологічних посередників; безпеково-стійкісної, пов’язаної із запобіганням загрозам і здатністю до відновлення; результативної, яка вимагає оцінювати не лише

виконані заходи, а й зміни у доступності інформації, довірі, захищеності прав та стійкості суспільства.

Похідним від наведеного є авторське розуміння механізму реалізації державної інформаційної політики як впорядкованої сукупності нормативно-правових, інституційно-організаційних, комунікаційних, цифрових, економічних, безпекових і контрольних-аналітичних засобів, процедур та взаємодій, за допомогою яких цілі й принципи політики трансформуються у скоординовані дії, публічні послуги, правила інформаційного обігу, заходи захисту та вимірювані суспільні результати.

Авторське узагальнення інтегрованого механізму, що сформувався внаслідок еволюції наукових поглядів, представлено на рис. 1.3.



Рис. 1.3. Циклічна модель інтегрованого механізму державної інформаційної політики

Джерело: розроблено автором на основі узагальнення [3; 29; 42; 45; 69; 120; 150; 151; 159; 160].

Рисунок 1.3 фіксує принципову зміну логіки державної інформаційної політики. Її механізм не починається з вибору каналу поширення повідомлення, а з визначення публічних цінностей, прав та суспільної проблеми. Лише після цього формуються інституційні правила, комунікаційні й цифрові інструменти

та заходи безпеки. Завершальним елементом є не формальний звіт про виконані дії, а оцінювання впливу й коригування політики.

У контексті подальшого дослідження механізмів реалізації державної інформаційної політики особливого значення набуває розмежування формування та реалізації політики. Формування охоплює діагностику проблем, визначення цілей, нормативне закріплення й вибір інструментів. Реалізація передбачає організацію виконання, координацію суб'єктів, ресурсне забезпечення, комунікацію, моніторинг та коригування. Еволюційний аналіз свідчить, що слабкість політики часто виникає саме на етапі переходу від стратегічних документів до узгоджених практичних дій [30; 69; 115].

Отже, становлення наукових поглядів на державну інформаційну політику пройшло шлях від переважно правового й державоцентричного бачення до інтегрованої, мережевої та людиноцентричної концепції. Сучасна політика одночасно гарантує інформаційні права, забезпечує цифрову взаємодію, підтримує демократичну комунікацію, захищає інформаційний простір і розвиває суспільну стійкість. Її об'єктом є вже не окремий інформаційний ресурс, а взаємопов'язана екосистема даних, медіа, платформ, інституцій та аудиторій.

Таким чином, еволюція наукової думки підтверджує перехід від моделі «держава інформує» до моделі «держава створює правила, координує взаємодію, гарантує права, управляє ризиками та забезпечує спільне формування публічної цінності в інформаційній сфері». Цей висновок визначає подальшу логіку дисертаційного дослідження: від категоріального аналізу – до оцінювання інституційних і практичних механізмів реалізації політики в сучасній Україні.

1.2. Функції, цілі та пріоритети державної інформаційної політики в системі публічного управління

Наукове осмислення державної інформаційної політики потребує переходу від загального визначення її сутності до з'ясування функціонального призначення, цільової спрямованості та пріоритетів реалізації. У системі

публічного управління ця політика не обмежується поширенням офіційних повідомлень або регулюванням діяльності медіа. Вона охоплює формування правил інформаційної взаємодії, гарантування прав людини, координацію органів влади, розвиток цифрових сервісів, захист інформаційного простору, підтримання суспільної довіри та представлення інтересів держави у міжнародному середовищі.

Функції, цілі та пріоритети відображають різні, хоча й взаємопов'язані характеристики державної інформаційної політики. Функції розкривають сталі напрями її впливу на суспільні відносини та управлінські процеси; цілі визначають бажані результати, яких має досягти держава; пріоритети фіксують напрями першочергової концентрації уваги, ресурсів і відповідальності в конкретних умовах. Змішування цих категорій ускладнює проєктування механізмів реалізації політики, оскільки інструменти починають підміняти цілі, а поточні заходи – стратегічні результати.

Управлінська цінність такого розмежування полягає в можливості вибудувати логічний зв'язок між суспільною проблемою, функцією держави, сформульованою метою, обраним пріоритетом і конкретним механізмом реалізації. Наприклад, поширення дезінформації активізує захисну та аналітичну функції; метою стає підвищення інформаційної стійкості; пріоритетами – раннє виявлення маніпулятивних впливів, узгоджена кризова комунікація та розвиток медіаграмотності; механізмами – правові, організаційні, цифрові й комунікаційні інструменти [37; 45; 105; 150].

Державна інформаційна політика формується в середовищі, де одночасно діють демократичні вимоги відкритості, безпекові обмеження, технологічні зміни та очікування громадян щодо швидких і зрозумілих комунікацій. Тому її функціональна система має бути багаторівневою, а цілі – узгодженими з публічними цінностями. Пріоритети не можуть визначатися винятково ситуативною політичною доцільністю: вони повинні спиратися на закон, оцінювання ризиків, суспільні потреби, міжнародні зобов'язання та інституційну спроможність держави [48; 84; 93; 97; 108].

У межах дослідження доцільно застосувати поняття «функціонально-цільова архітектура державної інформаційної політики». Під ним пропонується розуміти впорядковану систему функцій, ієрархічно пов'язаних цілей і ранжованих пріоритетів, реалізація яких забезпечується комплексом правових, організаційних, економічних, цифрових і комунікаційних механізмів. Така архітектура поєднує відносно сталі елементи політики з адаптивними рішеннями, що переглядаються відповідно до змін інформаційного середовища.

Схематичне відображення взаємозв'язку функцій, цілей, пріоритетів і механізмів подано на рис. 1.4. Центральне місце в моделі посідають цінності публічного врядування, оскільки саме вони визначають межі допустимого державного впливу та критерії суспільної результативності інформаційної політики.

ФУНКЦІЇ сталі напрями державного впливу	ЦІННОСТІ ПУБЛІЧНОГО ВРЯДУВАННЯ права людини • відкритість • довіра • безпека	ЦІЛІ бажані суспільні результати
Нормативна • координаційна • комунікаційна • сервісна • захисна • аналітична	ФУНКЦІОНАЛЬНО-ЦІЛЬОВА АРХІТЕКТУРА ДЕРЖАВНОЇ ІНФОРМАЦІЙНОЇ ПОЛІТИКИ	Стратегічні • середньострокові • операційні
МЕХАНІЗМИ правові • організаційні • економічні • цифрові • комунікаційні	ЗВОРОТНИЙ ЗВ'ЯЗОК І ОЦІНЮВАННЯ дані • участь • моніторинг • коригування	ПРІОРИТЕТИ ранжовані напрями концентрації ресурсів

Рис. 1.4. Функціонально-цільова архітектура державної інформаційної політики в системі публічного управління

Джерело: розроблено автором на основі [69; 115; 120; 124; 136; 151].

Запропонована модель засвідчує, що функції не існують ізольовано від цілей, а пріоритети не можуть формуватися без урахування механізмів реалізації та зворотного зв'язку. Відсутність хоча б одного з цих зв'язків призводить до фрагментарності політики. Надмірна кількість декларативних цілей без пріоритетизації розпорошує ресурси; механізми без чітких цілей

перетворюються на сукупність процедур; пріоритети без ціннісних обмежень створюють ризик непропорційного втручання у свободу вираження поглядів і доступ до інформації.

Функціональний підхід дає змогу досліджувати державну інформаційну політику через її призначення у відтворенні та розвитку системи публічного управління. Функція в цьому контексті є не окремою дією органу влади, а відносно стійким напрямом впливу, що реалізується багатьма суб'єктами та інструментами. Так, комунікаційна функція здійснюється не лише пресслужбами, а й керівниками органів влади, цифровими платформами, підрозділами стратегічних комунікацій, центрами надання послуг і механізмами громадської участі [137; 144; 151].

Функцію також не слід ототожнювати з компетенцією конкретної інституції. Компетенція окреслює юридично визначене коло повноважень певного суб'єкта, тоді як функція характеризує загальний напрям діяльності держави та може вимагати міжвідомчої, міжсекторальної й багаторівневої координації. Саме тому інформаційна безпека, відкритість даних або міжнародна комунікація не можуть бути результативно забезпечені одним органом; вони потребують розподіленої відповідальності та узгоджених процедур [16; 30; 44; 55].

У науковій літературі функціональне призначення інформаційної політики розкривається через різні концептуальні акценти. Організаційно-правовий підхід зосереджується на регулюванні інформаційних відносин і визначенні повноважень; системно-управлінський – на координації ресурсів, інститутів і процесів; комунікаційний – на взаємодії держави із суспільством; безпековий – на протидії загрозам; цифровий – на управлінні даними, платформами й електронними сервісами [3; 6; 29; 42; 69].

Для систематизації підходів до функціонального призначення державної інформаційної політики доцільно зіставити їхній зміст і управлінське значення. Узагальнення подано в табл. 1.4.

Наукові підходи до визначення функціонального призначення державної інформаційної політики

Підхід	Зміст функціонального призначення	Значення для публічного управління	Основні джерела
Організаційно-правовий	Нормативне впорядкування інформаційних відносин; гарантування прав; визначення режимів доступу, обігу й захисту інформації.	Створює легітимні межі державного впливу, розподіляє повноваження та відповідальність.	[3; 6; 62; 93]
Інституційно-координаційний	Узгодження діяльності органів влади, місцевого самоврядування, медіа, громадянського суспільства та цифрових платформ.	Зменшує дублювання рішень, забезпечує єдність повідомлень і спільне використання ресурсів.	[30; 44; 55; 115]
Комунікаційно-діалогічний	Інформування, пояснення рішень, стратегічні комунікації, консультації та зворотний зв'язок.	Підвищує зрозумілість політики, довіру, участь громадян і спроможність до спільних дій.	[23; 137; 144; 151]
Сервісно-цифровий	Забезпечення доступу до даних, електронних послуг, реєстрів і каналів взаємодії; цифрова інклюзія.	Перетворює інформацію на ресурс надання послуг і прийняття рішень, знижує трансакційні витрати.	[29; 32; 55; 98]
Безпеково-захисний	Виявлення загроз, захист інформаційної та критичної інфраструктури, протидія дезінформації, кризова комунікація.	Підтримує безперервність державного управління, стійкість суспільства та захист національних інтересів.	[9; 37; 45; 105]
Соціально-гуманітарний	Підтримка культурної ідентичності, медіаграмотності, соціальної згуртованості та захисту вразливих аудиторій.	Посилює здатність громадян критично сприймати інформацію та брати участь у демократичних процесах.	[8; 25; 42; 147]
Аналітично-адаптивний	Моніторинг інформаційного середовища, прогнозування ризиків, оцінювання результатів і коригування політики.	Забезпечує доказовість управлінських рішень і своєчасне реагування на зміни.	[115; 121; 146; 150]
Міжнародно-інтеграційний	Гармонізація стандартів, зовнішня комунікація, просування інтересів України та співпраця з міжнародними партнерами.	Інтегрує державу в європейський інформаційний простір і зміцнює міжнародну суб'єктність.	[12; 24; 112; 128]

Джерело: систематизовано автором за [3; 6; 9; 12; 23; 24; 29; 30; 32; 37; 42; 44; 45; 55; 62; 93; 98; 105; 112; 115; 121; 137; 144; 146; 147; 150; 151].

Зміст функцій змінюється під впливом суспільних трансформацій. У період становлення інформаційного законодавства домінували нормативна, правозахисна та інституційна функції. Розвиток електронного урядування посилив сервісну, технологічну та координаційну складові. Російська агресія надала особливого значення захисній, мобілізаційній, кризово-комунікаційній та відновлювальній функціям. Поширення алгоритмічних платформ і штучного інтелекту актуалізує функції нагляду, управління даними, забезпечення прозорості цифрових рішень і захисту інформаційної автономії людини [28; 32; 71; 157].

Функціональна система державної інформаційної політики має поєднувати стабільність і адаптивність. Стабільними є функції, що впливають із конституційних прав, природи демократичного врядування та необхідності забезпечувати національну безпеку. Адаптивною є конкретна конфігурація завдань, інструментів і суб'єктів, за допомогою яких ці функції реалізуються. У кризових умовах захисна функція посилюється, однак не скасовує правозахисну; цифровізація розширює сервісну функцію, проте одночасно вимагає посилення захисту персональних даних.

Наведене узагальнення показує, що жоден із підходів не є самодостатнім. Нормативне регулювання без комунікації не гарантує розуміння й прийняття державних рішень; цифрові сервіси без захисту даних можуть знижувати довіру; протидія дезінформації без медіаграмотності створює залежність від постійного адміністративного реагування; міжнародне просування без внутрішньої узгодженості повідомлень втрачає переконливість. Отже, функції повинні реалізовуватися як взаємодоповнювальна система.

Водночас функціональна багатоманітність не означає необмеженого розширення державного втручання. Демократична інформаційна політика має діяти в межах принципів законності, необхідності, пропорційності й підзвітності. Захисна функція не повинна перетворюватися на монополізацію інформаційного простору, а комунікаційна – на пропагандистське нав'язування позицій. Їхня легітимність визначається здатністю одночасно захищати публічні інтереси та зберігати свободу вираження, плюралізм і право на доступ до інформації [7; 84; 95; 156].

На основі аналізу наукових підходів доцільно виокремити дев'ять базових функцій державної інформаційної політики: нормативно-регуляторну, правозахисну, інституційно-координаційну, інформаційно-комунікаційну, партисипативну, сервісно-цифрову, аналітично-прогностичну, безпеково-захисну та соціально-інтеграційну. Додаткового значення набуває міжнародно-репутаційна функція, яка забезпечує зовнішню комунікацію та включення України до європейського інформаційного простору [24; 69; 115; 120].

Для практичного застосування зазначені функції доцільно згрупувати за рівнями публічного управління та очікуваними результатами. Авторську класифікацію наведено в табл. 1.5.

Таблиця 1.5

Авторська класифікація функцій державної інформаційної політики за рівнями публічно-управлінського впливу

Рівень	Групи функцій	Основний зміст реалізації	Очікуваний публічний результат
Ціннісно-правовий	Нормативно-регуляторна; правозахисна	Установлення правил, гарантування прав, визначення допустимих обмежень і процедур відповідальності.	Законність, передбачуваність, захищеність прав людини.
Системно-управлінський	Інституційно-координаційна; аналітично-прогностична	Розподіл повноважень, міжвідомча взаємодія, планування, моніторинг, оцінювання та коригування.	Узгодженість рішень, спроможність і підзвітність інституцій.
Комунікаційно-демократичний	Інформаційно-комунікаційна; партисипативна	Інформування, пояснення, консультації, діалог, залучення громадян і робота зі зворотним зв'язком.	Довіра, поінформованість, участь і легітимність рішень.
Сервісно-технологічний	Сервісно-цифрова	Відкриті дані, електронні послуги, реєстри, цифрова ідентифікація, доступні канали взаємодії.	Зручність, доступність, прозорість і ефективність публічних сервісів.
Безпеково-стійкісний	Безпеково-захисна	Протидія дезінформації та кібератакам, захист інфраструктури, кризова комунікація, відновлення.	Безперервність управління, інформаційна стійкість і захист національних інтересів.
Суспільно-інтеграційний	Соціально-інтеграційна; освітня	Медіаграмотність, інклюзія, підтримка ідентичності, робота з вразливими групами та територіями.	Згуртованість, критичне мислення, рівний доступ до інформації.
Зовнішньополітичний	Міжнародно-репутаційна; інтеграційна	Зовнішні комунікації, гармонізація стандартів, міжнародне партнерство, просування інтересів держави.	Міжнародна довіра, підтримка та інтеграція в європейський інформаційний простір.

Джерело: розроблено автором на основі [24; 29; 45; 55; 69; 105; 115; 120; 137; 150; 151; 159].

Нормативно-регуляторна функція полягає у встановленні загальнообов'язкових правил створення, збирання, зберігання, поширення, використання й захисту інформації. Вона охоплює визначення правових режимів, стандартів відкритості, вимог до медіа та електронних комунікацій, процедур доступу до публічної інформації, принципів захисту персональних даних і відповідальності за порушення. Її результативність залежить не лише від кількості нормативних актів, а від їхньої узгодженості, зрозумілості та придатності до застосування [84; 86; 91; 93; 95].

Правозахисна функція виражає людиноцентричну спрямованість політики. Держава має не тільки утримуватися від неправомірного обмеження інформаційних прав, а й створювати умови для їх практичної реалізації. Це передбачає доступність інформації для різних груп населення, захист приватності, недискримінаційний доступ до цифрових каналів, механізми оскарження рішень і правову визначеність обмежень в умовах воєнного стану [4; 7; 43; 79; 119].

Інституційно-координаційна функція спрямована на формування цілісної системи суб'єктів політики. Вона охоплює розподіл компетенцій, встановлення процедур міжвідомчої взаємодії, узгодження центрального та місцевого рівнів, залучення незалежних регуляторів, експертного середовища, медіа й громадських організацій. В умовах мережевого інформаційного середовища державний центр не спроможний одноосібно керувати всіма потоками інформації, тому координація має будуватися на спільних стандартах, обміні даними та чіткій відповідальності [30; 34; 44; 158].

Інформаційно-комунікаційна функція включає своєчасне надання суспільно значущої інформації, пояснення цілей і наслідків управлінських рішень, формування послідовних наративів, організацію кризової комунікації та підтримання постійного діалогу з громадянами. Її результатом є не максимальна кількість повідомлень, а зрозумілість державних дій, зниження невизначеності та формування підстав для обґрунтованої довіри [36; 45; 137; 151].

Партисипативна функція забезпечує включення громадян та інших заінтересованих сторін у формування й оцінювання інформаційної політики. Зворотний зв'язок у цьому разі не зводиться до реакції на вже ухвалені рішення. Він має охоплювати консультації, громадську експертизу, спільне вироблення правил, аналіз запитів, скарг і поведінкових даних. Такий підхід дає змогу виявляти інформаційні потреби до того, як вони переростають у кризу довіри [121; 151; 159].

Сервісно-цифрова функція відображає трансформацію інформації на інфраструктурний ресурс публічного управління. Відкриті дані, електронні документи, реєстри, системи ідентифікації та цифрові послуги мають

забезпечувати зручну взаємодію людини з державою. Водночас цифровізація не є самоціллю: її суспільний сенс полягає у доступності, швидкості, надійності й прозорості процедур. Тому поряд із технологічною модернізацією необхідні цифрова інклюзія, захист даних і альтернативні канали для осіб, які не можуть повноцінно користуватися онлайн-сервісами [85; 87; 88; 98; 102].

Аналітично-прогностична функція забезпечує інформаційну основу управлінських рішень. Вона передбачає моніторинг медіа та цифрових платформ, аналіз суспільних настроїв, оцінювання доступності інформації, виявлення вразливостей, прогнозування інформаційних ризиків і дослідження результатів комунікацій. Принципово важливо відокремлювати аналітику від політичного контролю над думками громадян: її метою має бути підвищення якості рішень і раннє виявлення проблем, а не маніпулятивне управління поведінкою [136; 146; 148; 150].

Безпеково-захисна функція охоплює протидію інформаційним операціям, дезінформації, кібератакам, витоку даних і порушенню безперервності критичних інформаційних систем. У сучасних умовах вона включає не лише технічний захист, а й стійкість суспільства до маніпуляцій, здатність держави швидко спростовувати неправдиві повідомлення, підтримувати достовірні канали комунікації та координувати дії під час криз [9; 22; 37; 45; 105].

Соціально-інтеграційна функція пов'язана з підтриманням суспільної згуртованості, культурної ідентичності, взаємної поваги та інформаційної включеності різних груп. Вона особливо важлива для дітей і молоді, внутрішньо переміщених осіб, ветеранів, жителів деокупованих територій та громадян, які перебувають за кордоном. Держава має забезпечувати не уніфікацію поглядів, а спільний простір достовірної інформації, демократичних цінностей і можливостей для участі [25; 42; 71; 129].

Міжнародно-репутаційна функція забезпечує системне представлення позиції України, пояснення її рішень міжнародним аудиторіям, протидію зовнішнім інформаційним впливам і розвиток партнерств. Вона тісно пов'язана з європейською та євроатлантичною інтеграцією, культурною дипломатією,

взаємодією з діаспорою та формуванням довіри до України як демократичної й спроможної держави [24; 107; 110; 112].

Класифікація відображає не адміністративну підпорядкованість, а рівні суспільного ефекту. Одна й та сама інституція може брати участь у реалізації кількох груп функцій, а одна функція – потребувати діяльності багатьох суб'єктів. Така побудова корисна для визначення відповідальності: за кожною групою повинні бути встановлені головний координатор, партнери, ресурси, показники результату та процедури звітування.

Між функціями існують відносини взаємного підсилення та потенційного конфлікту. Відкритість даних підтримує прозорість і сервісність, але потребує захисту персональної та службової інформації. Швидкість кризової комунікації може суперечити вимозі перевірки фактів. Протидія інформаційним загрозам вимагає оперативності, проте повинна залишатися підконтрольною праву. Завдання публічного управління полягає не в усуненні цих суперечностей, а в установленні процедур їх збалансування.

З огляду на це функціональна система має бути доповнена принципами реалізації: верховенством права, людиноцентричністю, відкритістю, достовірністю, пропорційністю, субсидіарністю, технологічною нейтральністю, інклюзивністю, координацією та вимірюваністю результатів. Принципи визначають якість виконання функцій і запобігають ситуації, коли формальне досягнення показника суперечить суспільному інтересу.

Цілі державної інформаційної політики відображають бажаний стан інформаційної сфери та публічних відносин, якого держава прагне досягти за допомогою визначених функцій і механізмів. На відміну від функцій, що характеризують сталі напрями діяльності, цілі мають часові межі, очікувані результати та критерії досягнення. Їх формулювання повинно виходити не з внутрішніх потреб апарату управління, а з проблем і потреб громадян, суспільства та держави.

Генеральною метою державної інформаційної політики пропонується визначити створення відкритого, безпечного, стійкого та людиноцентричного інформаційного середовища, у якому громадяни можуть реалізовувати

інформаційні права, отримувати достовірну інформацію й публічні послуги, брати участь у виробленні рішень, а держава – захищати національні інтереси та підтримувати демократичний розвиток. Таке формулювання поєднує правовий, комунікаційний, цифровий, безпековий і соціальний виміри.

Дерево цілей, яке поєднує генеральну мету зі стратегічними напрямками та основними групами результатів, подано на рис. 1.5.

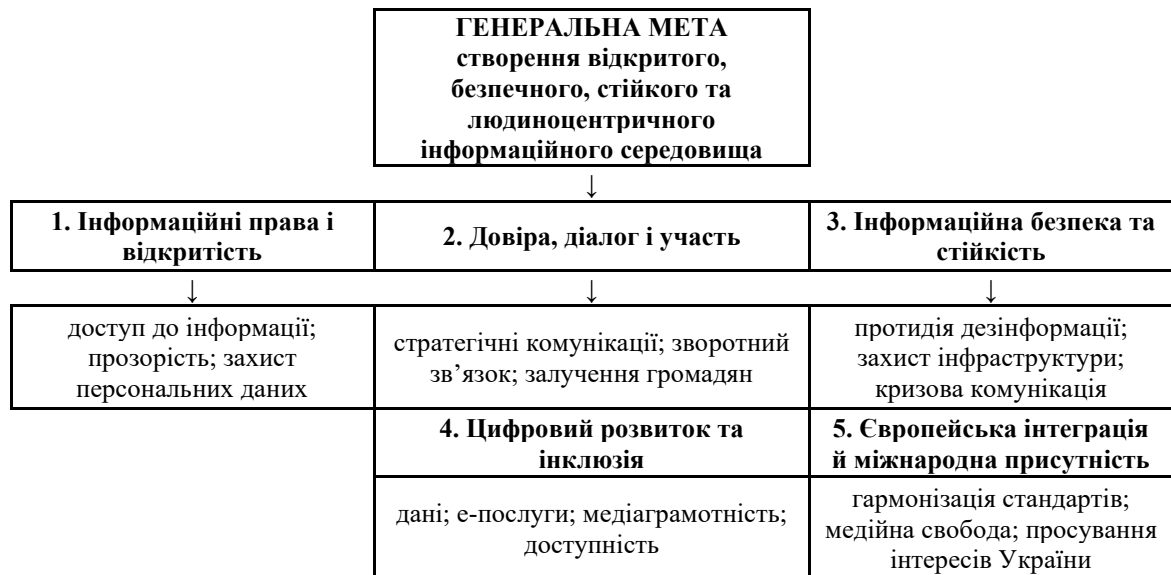


Рис. 1.5. Дерево цілей державної інформаційної політики

Джерело: розроблено автором на основі [48; 84; 91; 93; 105; 112; 151; 159; 160].

Генеральна мета конкретизується у стратегічних цілях. Першою є гарантування інформаційних прав, відкритості й підзвітності влади. Вона охоплює доступ до публічної інформації, відкриті дані, прозорість використання коштів, захист персональних даних і правові засоби оскарження. Її досягнення оцінюється не лише обсягом оприлюдненої інформації, а доступністю, повнотою, своєчасністю та придатністю відомостей для практичного використання [81; 84; 88; 91].

Другою стратегічною ціллю є зміцнення довіри, діалогу та участі. Довіра не може бути безпосередньо «створена» інформаційною кампанією; вона формується через послідовність рішень, чесне пояснення обмежень, визнання помилок, відповідність повідомлень реальним діям і можливість громадян впливати на політику. Тому комунікаційні показники мають доповнюватися

показниками якості зворотного зв'язку, зрозумілості рішень і врахування суспільних пропозицій.

Третьою стратегічною ціллю є забезпечення інформаційної безпеки та суспільної стійкості. Вона передбачає захист інформаційної інфраструктури, зниження вразливості до маніпулятивних впливів, підтримання достовірних каналів комунікації, готовність до криз і здатність швидко відновлювати інформаційні процеси. Стійкість слід розуміти як спроможність не лише відбити атаку, а й адаптуватися, зберегти довіру та продовжити виконання ключових функцій.

Четверта стратегічна ціль пов'язана з цифровим розвитком та інклюзією. Вона охоплює доступні електронні послуги, якісні державні дані, сумісність реєстрів, безпечну електронну ідентифікацію, цифрову грамотність і запобігання новим формам нерівності. У центрі має перебувати не технологія, а користувач, його життєва ситуація та право отримати послугу незалежно від місця проживання, віку чи рівня цифрових навичок.

П'ятою стратегічною ціллю є європейська інтеграція та посилення міжнародної інформаційної присутності України. Вона включає гармонізацію правових і професійних стандартів, забезпечення свободи та плюралізму медіа, розвиток співпраці у сфері кібербезпеки, належне врядування цифрових платформ і послідовне представлення інтересів України зовнішнім аудиторіям.

Стратегічні цілі мають бути декомпозовані на середньострокові та операційні. Середньострокові цілі визначають результати програм і планів на кількарічний період: створення системи стратегічних комунікацій, удосконалення координації суб'єктів інформаційної безпеки, розширення відкритих даних, підвищення медіаграмотності або наближення регулювання до права Європейського Союзу. Операційні цілі стосуються конкретних продуктів і змін, що можуть бути забезпечені відповідальними інституціями у визначені строки.

Якість цілепокладання залежить від чіткого розмежування продуктів, результатів і суспільного впливу. Створення вебпорталу є продуктом; зростання частки громадян, які отримують потрібну інформацію без додаткових звернень,

– безпосереднім результатом; підвищення відкритості та довіри – довгостроковим впливом. Якщо оцінювання обмежується кількістю публікацій, заходів або технічних систем, воно не показує, чи змінилася якість публічного управління.

Цілі мають бути взаємно узгодженими. Прагнення до максимальної відкритості не повинно ігнорувати захист персональних даних і безпекові режими; цифрова ефективність – створювати бар'єри для людей без цифрових навичок; швидке спростування дезінформації – призводити до поширення неперевіраних відомостей. Узгодження здійснюється через правові критерії, оцінювання ризиків, консультації із заінтересованими сторонами та попередній аналіз можливих наслідків.

Пріоритети є динамічною складовою функціонально-цільової архітектури. Вони відображають управлінський вибір щодо того, які проблеми, цілі та групи заходів мають отримати першочергову увагу в умовах обмежених ресурсів. На відміну від стратегічних цілей, пріоритети можуть змінюватися швидше – відповідно до безпекової ситуації, технологічних новацій, суспільних очікувань і міжнародних зобов'язань.

Пріоритетизація повинна здійснюватися за прозорими критеріями. До них належать масштаб і терміновість проблеми; рівень ризику для прав людини, безпеки та безперервності державного управління; очікувана публічна цінність; кількість і вразливість груп, на які впливатиме рішення; нормативна обов'язковість; міжсекторальний ефект; наявність інституційної спроможності; ресурсна здійсненність; можливість виміряти результат. Застосування критеріїв знижує залежність політики від короткострокових медійних коливань.

Ієрархічне співвідношення цілей, пріоритетів і результатів систематизовано в табл. 1.6.

Таблиця 1.6

Ієрархія цілей і пріоритетів державної інформаційної політики

Рівень	Характер цілей	Типові пріоритети	Очікуваний результат
Стратегічний (довгостроковий)	Відкрите, безпечне, стійке та людиноцентричне інформаційне середовище.	Права й відкритість; довіра й участь; безпека; цифрова інклюзія; європейська інтеграція.	Стійкі зміни у якості врядування, правах громадян і суспільній спроможності.
Середньостроковий (програмний)	Інституційні та поведінкові зміни в окремих сферах політики.	Стратегічні комунікації; система протидії дезінформації; відкриті дані; медіаграмотність; стійкі цифрові сервіси.	Узгоджені процедури, спроможні інституції, покращення доступу та довіри.
Операційний (річний / проєктний)	Конкретні продукти й безпосередні результати відповідальних суб'єктів.	Плани комунікацій; протоколи кризового реагування; набори даних; навчальні програми; оновлення систем захисту.	Виконані заходи, доступні сервіси, своєчасні повідомлення, зменшення виявлених вразливостей.
Кризовий (невідкладний)	Збереження безперервності управління та захист населення в умовах інформаційної загрози.	Оперативне сповіщення; перевірка фактів; координація повідомлень; резервні канали; захист критичних систем.	Зниження шкоди, збереження довіри та швидке відновлення інформаційних процесів.
Переглядовий (адаптивний)	Коригування політики за результатами моніторингу, оцінювання й зворотного зв'язку.	Оновлення цілей, індикаторів, ресурсів, нормативних правил і відповідальності.	Відповідність політики новим ризикам, технологіям і суспільним потребам.

Джерело: розроблено автором на основі [27; 45; 84; 105; 112; 115; 150; 151; 159; 160].

Першим актуальним пріоритетом є забезпечення інформаційної доброчесності та протидія дезінформації. Йдеться не лише про спростування неправдивих повідомлень, а про створення системи раннього виявлення, координацію офіційних комунікацій, підтримку незалежної журналістики, прозорість цифрових платформ, розвиток фактчекінгу та медіаграмотності. Такий підхід поєднує державні заходи із суспільною спроможністю критично оцінювати інформацію.

Другим пріоритетом є розвиток стратегічних і кризових комунікацій. Органи влади мають перейти від переважно реактивного інформування до системного планування комунікації навколо суспільних цілей. Це передбачає єдині принципи, підготовку комунікаційних кадрів, визначення аудиторій, координацію повідомлень, використання достовірних даних, готовність до криз і оцінювання того, як громадяни розуміють державні рішення [36; 45; 144; 151].

Третім пріоритетом є забезпечення відкритості, доступу до інформації та якісних відкритих даних. В умовах воєнного стану окремі обмеження можуть бути необхідними, однак вони мають бути правомірними, обґрунтованими та переглядатися після зникнення ризику. Паралельно потрібно розвивати проактивне оприлюднення інформації, стандарти якості наборів даних, доступні формати та механізми контролю за відповідями на запити [4; 84; 88; 119].

Четвертим пріоритетом виступає кібербезпека та стійкість критичної інформаційної інфраструктури. Цей напрям включає захист державних реєстрів і комунікацій, резервування даних, безперервність цифрових послуг, управління інцидентами, обмін інформацією про загрози та наближення до європейських вимог. Інформаційна політика повинна забезпечувати зрозумілу комунікацію кіберризиків і поведінкових правил, а не залишати проблему лише технічним підрозділам [90; 94; 99; 106; 139].

П'ятим пріоритетом є забезпечення свободи, плюралізму та професійної спроможності медіа. Незалежні медіа виконують функцію суспільного контролю, забезпечують конкуренцію інтерпретацій і сприяють викриттю дезінформації. Державна підтримка має бути прозорою та недискримінаційною, а регулювання – не створювати непропорційних обмежень. Особливого значення набувають сталість суспільних медіа, безпека журналістів і відповідність європейським стандартам [82; 95; 109; 156].

Шостим пріоритетом є цифрова інклюзія, медіа- та інформаційна грамотність. Поширення цифрових сервісів і платформ створює можливості, але водночас поглиблює нерівність між групами з різним доступом, освітою та навичками. Політика має поєднувати навчальні програми, доступні інтерфейси, підтримку локальних мереж допомоги, спеціальні рішення для дітей і молоді та розвиток критичного мислення протягом життя [8; 25; 147; 159].

Сьомим пріоритетом є належне управління даними, цифровими платформами й алгоритмічними системами. Держава повинна забезпечувати якість і сумісність даних, прозорість їх використання, захист приватності, відповідальність за автоматизовані рішення та оцінювання ризиків штучного інтелекту. Зростання ролі платформ вимагає поєднання національних механізмів

із європейськими правилами цифрових послуг, управління даними та штучного інтелекту [153; 154; 155; 157].

Восьмим пріоритетом є інформаційна реінтеграція деокупованих територій і підтримка зв'язку з громадянами, які пережили окупацію або вимушене переміщення. Політика має враховувати різний досвід, рівень доступу до українських медіа, травматичні наслідки війни та потребу в достовірній інформації про права, послуги й відновлення. Комунікація не повинна стигматизувати аудиторії; її основою мають бути повага, безпека та залучення місцевих громад [25; 71].

Дев'ятим пріоритетом є європейська інтеграція інформаційної сфери. Йдеться про послідовне наближення законодавства, інституційних практик і професійних стандартів до права Європейського Союзу, а також про комунікацію змісту реформ для громадян. Євроінтеграційна інформаційна політика повинна пояснювати не лише політичну мету, а конкретні зміни у правах, послугах, медійному середовищі, цифровій безпеці та відповідальності платформ [12; 27; 112; 128].

Таблиця демонструє, що пріоритети мають різний часовий горизонт. Кризовий рівень не може повністю витіснити стратегічний: навіть під час війни необхідно підтримувати розвиток інституцій, відкритість, медійну свободу та цифрову інклюзію. Водночас стратегічні документи повинні передбачати можливість швидкого переходу до режиму кризового управління із заздалегідь визначеними каналами, відповідальними суб'єктами та процедурами перевірки інформації.

Пріоритети мають бути диференційованими за рівнями врядування. На центральному рівні переважають нормативне регулювання, координація, міжнародна взаємодія та захист загальнодержавної інфраструктури. На регіональному й місцевому рівнях особливого значення набувають комунікація конкретних послуг, доступність інформації, взаємодія з локальними медіа, робота з громадами та виявлення інформаційних потреб. Децентралізація не повинна призводити до інформаційної фрагментації; вона потребує спільних стандартів і простору для адаптації повідомлень.

Європейська інтеграція змінює логіку державної інформаційної політики: від переважно національного регулювання окремих каналів – до комплексного врядування інформаційною екосистемою. Європейські підходи поєднують захист прав, свободу та плюралізм медіа, відповідальність цифрових платформ, кібербезпеку, захист даних і прозорість алгоритмічних систем. Для України це означає необхідність координувати реформи, які традиційно належать до різних секторів публічної політики [139; 153; 154; 156; 157].

Важливою є орієнтація на інформаційну цілісність, а не лише на боротьбу з окремими проявами дезінформації. Інформаційна цілісність передбачає умови, за яких суспільно значуща інформація є доступною, достовірною та плюралістичною, а маніпулятивні впливи не руйнують демократичне волевиявлення. Відповідно, пріоритетами стають прозорість джерел і реклами, підзвітність платформ, підтримка професійної журналістики, дослідницький доступ до даних і розвиток суспільної стійкості [140; 141; 160].

Підхід OECD до публічної комунікації акцентує її відмінність від політичної реклами та пропаганди. Комунікація має служити політиці, бути заснованою на фактах, орієнтуватися на потреби аудиторій, забезпечувати інклюзивність, координуватися між інституціями та оцінюватися за результатами. Для України цей підхід важливий як основа професіоналізації комунікаційної функції та розмежування інституційної інформації від партійно-політичних інтересів [150; 151].

Рекомендації UNESCO щодо врядування цифровими платформами підкреслюють багатосторонній характер регулювання. Держава повинна встановлювати правові гарантії та наглядові механізми, але розроблення й реалізація рішень мають включати платформи, медіа, дослідників, громадянське суспільство та користувачів. Така модель знижує ризик як безконтрольності приватних платформ, так і надмірного державного контролю.

Демократичний вимір вимагає, щоб цілі політики формувалися публічно й були підзвітними. Стратегічні документи мають містити не лише перелік заходів, а логіку проблеми, очікувані результати, індикатори, відповідальних суб'єктів і механізми участі. Звітування повинно пояснювати не лише те, що зроблено, а й

те, який суспільний результат отримано, які ризики залишилися та чому пріоритети були переглянуті.

Європеїзація також передбачає взаємне навчання та використання порівняльних даних. Механічне перенесення іноземних інструментів без урахування війни, інституційної культури та медійної структури України може бути неефективним. Адаптація повинна зберігати європейські цінності й стандарти, але враховувати національні ризики, спроможність органів влади та потреби різних громад.

Функції, цілі та пріоритети набувають практичного значення лише тоді, коли інтегруються у повний цикл публічного управління. Початковим етапом є діагностика проблеми, що спирається на правові дані, статистику, моніторинг інформаційного середовища, дослідження потреб аудиторій і консультації. Важливо відокремлювати реальну суспільну проблему від її медійної видимості: висока кількість згадок не завжди означає найбільший ризик, а малопомітні вразливості можуть мати системні наслідки.

На етапі цілепокладання проблема перетворюється на опис бажаного суспільного результату. Після цього здійснюється відбір пріоритетів за визначеними критеріями, формуються альтернативи механізмів, оцінюються правові наслідки, ризики для прав людини, вартість і спроможність виконавців. Планування повинно встановлювати відповідальних суб'єктів, строки, ресурси, індикатори продукту, результату та впливу.

Реалізація потребує міжвідомчої координації та єдиного інформаційного супроводу. Органи влади мають розуміти не тільки власне завдання, а й його місце у досягненні спільної цілі. Це особливо важливо під час криз, коли суперечливі повідомлення різних інституцій швидко знижують довіру. Координація не означає повної централізації: місцеві суб'єкти повинні мати можливість адаптувати комунікацію до контексту, зберігаючи достовірність і спільні стандарти.

Моніторинг має відбуватися паралельно з реалізацією, а не лише після завершення програми. Він включає відстеження виконання заходів, охоплення аудиторій, доступності інформації, якості зворотного зв'язку, змін у знаннях і

поведінці, динаміки ризиків та небажаних наслідків. У сфері протидії дезінформації особливо важливо оцінювати не тільки кількість спростувань, а й швидкість реагування, довіру до джерела та зменшення повторного поширення маніпулятивного повідомлення.

Оцінювання завершує один цикл і відкриває наступний. Воно повинно встановлювати причинний зв'язок між застосованими механізмами та отриманими результатами, порівнювати альтернативи й пояснювати відхилення. На цій основі здійснюється перегляд пріоритетів, перерозподіл ресурсів, оновлення індикаторів і, за потреби, коригування нормативного регулювання. Отже, адаптивність є не ознакою непослідовності, а необхідною властивістю політики в умовах швидких змін.

Цикл формування, реалізації та перегляду пріоритетів представлено на рис.

1.6.

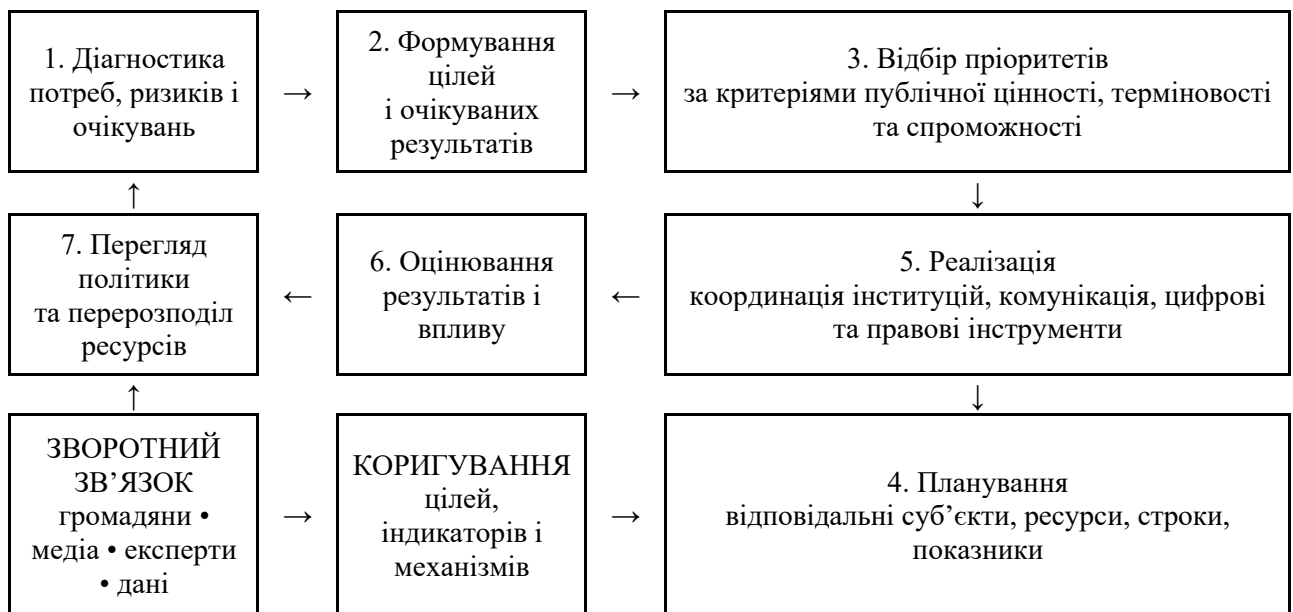


Рис. 1.6. Цикл формування, реалізації та перегляду пріоритетів державної інформаційної політики

Джерело: розроблено автором на основі [115; 121; 150; 151; 159; 160].

Зворотний зв'язок у запропонованому циклі має системоутворювальне значення: він показує, чи відповідає політика реальним потребам, чи є повідомлення зрозумілими, а цифрові й безпекові рішення – правомірними та доступними. Для забезпечення узгодженості доцільно застосовувати функціонально-цільову матрицю, у якій для кожної цілі визначаються функції,

пріоритетні аудиторії, відповідальні та партнерські суб'єкти, механізми, ресурси, індикатори й ризики. Це унеможлиблює формальне віднесення заходів до цілей без доказового внеску в результат.

Результативність політики залежить від професійної, фінансової та організаційної спроможності. Підготовка кадрів має поєднувати право, комунікації, аналіз даних, кібербезпеку, поведінкові науки й роботу з громадами, а фінансування – спрямовуватися на суспільно значущі результати за прозорими критеріями [45; 151]. Центральні органи повинні формувати нормативні рамки та загальнонаціональні спроможності, тоді як регіональні й місцеві – забезпечувати контекстну комунікацію, доступ до інформації та виявлення потреб громад, зберігаючи спільні стандарти [55; 158].

Отже, функціонально-цільова архітектура державної інформаційної політики вибудовується за логікою «цінності – функції – цілі – пріоритети – механізми – результати – зворотний зв'язок». Її генеральною метою є формування відкритого, безпечного, стійкого та людиноцентричного інформаційного середовища. Авторський підхід полягає у трактуванні функцій, цілей і пріоритетів як взаємопов'язаної управлінської системи, що забезпечує баланс відкритості й безпеки, обґрунтовану концентрацію ресурсів та регулярне коригування рішень на основі даних і суспільного діалогу. Це створює методологічну основу для подальшого аналізу механізмів реалізації та критеріїв результативності державної інформаційної політики.

1.3. Методичні засади дослідження механізмів реалізації державної інформаційної політики

Дослідження механізмів реалізації державної інформаційної політики потребує методичного інструментарію, здатного одночасно охопити нормативну, інституційну, організаційну, комунікаційну, цифрову та безпекову природу цього явища. Його складність зумовлюється тим, що інформаційна політика не локалізується в межах одного органу влади або однієї галузі регулювання. Вона формується на перетині публічного управління, права,

політичної комунікації, медіасистеми, цифрових технологій, національної безпеки та суспільної участі.

Методичні засади в цьому дослідженні розуміються як упорядкована сукупність принципів, наукових підходів, методів, процедур, критеріїв і показників, за допомогою яких забезпечуються постановка дослідницької проблеми, добір емпіричних даних, їх перевірка, інтерпретація та формування обґрунтованих пропозицій. Таке трактування дає змогу відмежувати методичний рівень від загальної методології: методологія визначає світоглядну й концептуальну логіку пізнання, тоді як методичне забезпечення конкретизує послідовність аналітичних дій та правила застосування відповідних методів.

У працях І. Арістової державна інформаційна політика розглядається крізь організаційно-правовий вимір, що орієнтує дослідження на аналіз компетенцій, правових норм і структур взаємодії [3]. О. Баранов акцентує на єдності теорії, методології та практики правового забезпечення інформаційної сфери [6]. Ю. Нестеряк обґрунтовує теоретико-методологічне бачення державної інформаційної політики як системного напрямку державного управління [69], а О. Пушкар поєднує методологічні підходи з аналізом практичних механізмів її розвитку [115]. Сукупність цих позицій підтверджує необхідність інтегрованого дослідницького дизайну.

В умовах воєнного стану методичний інструментарій повинен забезпечувати баланс між дослідженням інформаційної безпеки та дотриманням прав людини. Оцінювання механізмів протидії дезінформації не може обмежуватися підрахунком заблокованих ресурсів або спростованих повідомлень. Необхідно аналізувати правову визначеність втручання, його пропорційність, інституційну підзвітність, вплив на доступ до інформації, довіру, суспільну стійкість і здатність громадян приймати обґрунтовані рішення.

Метою підрозділу є обґрунтування цілісної методичної конструкції дослідження механізмів реалізації державної інформаційної політики. Для її досягнення необхідно визначити логіку дослідницького процесу; систематизувати методологічні підходи й принципи; сформувати комплекс загальнонаукових і спеціальних методів; конкретизувати джерельну та

емпіричну базу; запропонувати критерії й показники оцінювання; окреслити процедури забезпечення достовірності, етичності та відтворюваності результатів.

Вихідним елементом методичної конструкції є чітке визначення об'єкта і предмета дослідження. Об'єктом виступають процеси формування та реалізації державної інформаційної політики у системі публічного управління. Предмет охоплює сукупність теоретичних, нормативно-правових, інституційних, організаційних, комунікаційних, цифрових і безпекових засад функціонування відповідних механізмів, а також закономірності їх взаємодії, результативності та адаптації до змін інформаційного середовища. Таке розмежування запобігає надмірному розширенню дослідницького поля.

Категорія «механізм реалізації» використовується для позначення не окремого засобу або управлінської дії, а впорядкованої системи суб'єктів, норм, ресурсів, процедур, методів, інструментів і зворотних зв'язків, які забезпечують перетворення цілей державної інформаційної політики на конкретні публічні результати. Відповідно, методика повинна досліджувати не лише формальну наявність елементів, а й причинно-наслідкові зв'язки між ними, спроможність до координації та фактичний вплив на інформаційні права, довіру, стійкість і якість державної комунікації [30; 37; 115].

Для аналітичної точності доцільно відрізнити механізм від суміжних понять. Інструмент є конкретним засобом впливу, наприклад нормативним актом, інформаційною кампанією, цифровою платформою або процедурою спростування. Метод характеризує спосіб застосування інструмента. Технологія описує послідовність операцій та технічних рішень. Процедура встановлює формалізований порядок дій. Механізм інтегрує ці елементи, визначає суб'єктів, ресурси й правила їх узгодженого функціонування. Таке розмежування має бути закріплене в операціональній моделі дослідження.

Методичне забезпечення доцільно вибудовувати на чотирьох взаємопов'язаних рівнях. Перший, концептуальний, формує уявлення про інформацію як ресурс публічного управління, право людини, складову влади та чинник безпеки. Другий, загальнонауковий, охоплює системний аналіз,

діалектичну логіку, індукцію, дедукцію, абстрагування, моделювання та порівняння. Третій, спеціально-науковий, включає інституційний, правовий, комунікаційний, мережевий, ризик-орієнтований і політико-управлінський аналіз. Четвертий, операційний, містить конкретні процедури збирання й оброблення даних.

Концептуальний рівень повинен поєднувати публічно-управлінську та правозахисну перспективи. У першій інформаційна політика розглядається як цілеспрямована діяльність держави, що організує інформаційні потоки, комунікації та цифрові сервіси. У другій вона оцінюється з позицій свободи вираження поглядів, доступу до інформації, захисту персональних даних і допустимості обмежень. Конституція України та профільне законодавство формують нормативну рамку, яка має бути не просто описана, а використана як система критеріїв оцінювання механізмів [48; 84; 91; 93].

Загальнонауковий рівень забезпечує встановлення зв'язків між елементами механізму. Системний аналіз дозволяє досліджувати входи, процеси, результати, середовище і зворотний зв'язок; структурно-функціональний підхід – співвідносити інституції з виконуваними функціями; процесний – відстежувати реалізацію політики від постановки проблеми до оцінювання; порівняння – виявляти спільні та відмінні ознаки моделей; моделювання – формувати цільову конфігурацію механізму. Їх застосування повинно бути взаємодоповнювальним, а не механічно паралельним.

Спеціально-науковий рівень визначається природою предмета. Правовий аналіз встановлює нормативні повноваження, прогалини та колізії. Інституційний аналіз виявляє формальні й неформальні правила, розподіл ролей і ресурси. Комунікаційний аналіз оцінює зміст, канали, аудиторії та зворотний зв'язок. Мережевий підхід досліджує взаємозалежності державних і недержавних суб'єктів. Безпековий підхід виявляє загрози, вразливості та спроможність до реагування. Цифрово-екосистемний підхід враховує платформи, дані, алгоритми та інфраструктурні залежності [45; 136; 138; 159].

Операційний рівень перетворює теоретичні категорії на вимірювані ознаки. Наприклад, інституційна спроможність може бути операціоналізована

через наявність чітких повноважень, кадрових компетентностей, бюджетних ресурсів, процедур координації та системи оцінювання. Відкритість – через доступність даних, строк реагування, повноту інформації та зрозумілість комунікації. Інформаційна стійкість – через здатність виявляти загрози, зберігати безперервність комунікації, підтримувати довіру й швидко відновлювати функції [45; 70; 146].

Операціоналізація повинна здійснюватися до початку збору даних. Для кожного поняття визначаються аналітичні компоненти, емпіричні індикатори, джерела інформації, шкала оцінювання та правила інтерпретації. Це зменшує ризик підміни аналізу ілюстративним описом. Якщо показники формуються після ознайомлення з результатами, виникає небезпека вибіркового підтвердження попередніх припущень.

Авторська позиція полягає в тому, що методичні засади дослідження державної інформаційної політики повинні будуватися не навколо одного домінуючого методу, а навколо дослідницької проблеми. Метод обирається відповідно до характеру питання: правова визначеність досліджується нормативно-правовим аналізом; координація – інституційним картуванням і аналізом процесів; суспільний ефект – соціологічними та поведінковими показниками; інформаційні загрози – контентним, мережевим і ризик-аналізом; адаптивність – порівнянням рішень у часі та кейс-стаді.

Структуру методичного забезпечення, яка поєднує концептуальний, загальнонауковий, спеціально-науковий та операційний рівні, представлено на рис. 1.7. Схема показує, що результати кожного рівня слугують підставою для наступного, а зворотний зв'язок забезпечує коригування вихідних припущень.

Запропонована архітектура не допускає редукції дослідження до аналізу законодавства або, навпаки, лише до вимірювання комунікаційних ефектів. Нормативна модель показує, як механізм повинен функціонувати; інституційний та процесний аналіз – як він організований фактично; емпіричні показники – яких результатів досягнуто; порівняння – які альтернативні рішення можливі. Поєднання цих перспектив створює підстави для пояснювальних, а не лише описових висновків.

КОНЦЕПТУАЛЬНИЙ РІВЕНЬ	ЗАГАЛЬНОНАУКОВИЙ РІВЕНЬ
інформація як право, ресурс, влада, публічна цінність і чинник безпеки	системний аналіз, індукція, дедукція, порівняння, моделювання
↓ формування категорій і гіпотез	↓ встановлення зв'язків і закономірностей
СПЕЦІАЛЬНО-НАУКОВИЙ РІВЕНЬ	ОПЕРАЦІЙНИЙ РІВЕНЬ
правовий, інституційний, комунікаційний, мережевий, цифровий і ризик-аналіз	індикатори, джерела даних, шкали, процедури збору й перевірки
ЗВОРОТНИЙ ЗВ'ЯЗОК: емпіричні результати уточнюють поняття, гіпотези та модель	ЗВОРОТНИЙ ЗВ'ЯЗОК: емпіричні результати уточнюють поняття, гіпотези та модель

Рис. 1.7. Рівнева архітектура методичного забезпечення дослідження

механізмів реалізації державної інформаційної політики

Джерело: розроблено автором на основі [3; 6; 69; 115; 124].

Таблиця 1.7

Методологічні підходи до дослідження механізмів реалізації державної інформаційної політики

Підхід	Аналітичний фокус	Дослідницькі можливості	Методичні обмеження
Системний	Розглядає механізм як цілісність із входами, процесами, результатами, середовищем і зворотним зв'язком	Цілісність, взаємозалежність, виявлення системних розривів	Ризик надмірної абстракції без емпіричної операціоналізації
Інституційний	Аналізує формальні й неформальні правила, суб'єктів, компетенції, ресурси та стимули	Виявлення дублювання, прогалин, конфліктів повноважень	Необхідність враховувати неформальні практики
Структурно-функціональний	Співвідносить елементи системи з функціями, які вони повинні виконувати	Оцінювання функціональної повноти та відповідальності	Може недооцінювати процеси змін і мережеві зв'язки
Процесний	Досліджує послідовність формування, виконання, моніторингу й коригування політики	Встановлення вузьких місць, затримок і розривів циклу	Потребує доступу до внутрішніх процедур і даних
Правовий	Оцінює нормативні підстави, законність, пропорційність, узгодженість і гарантії прав	Визначення правових колізій та меж втручання	Формальна відповідність не дорівнює фактичній ефективності
Комунікаційний	Аналізує зміст, канали, аудиторії, доступність, зворотний зв'язок і довіру	Оцінювання якості публічної взаємодії	Складність встановлення причинного впливу комунікації
Мережевий	Виявляє структуру взаємодії держави, медіа, платформ, науки та громадянського суспільства	Аналіз координації, центрів впливу й залежностей	Динамічність мереж і неповнота цифрових даних
Ризик-орієнтований	Встановлює загрози, вразливості, імовірність, наслідки та спроможність реагування	Пріоритезація ресурсів і сценарне планування	Ризик сек'юритизації та звуження правозахисної перспективи
Порівняльний	Зіставляє національні, європейські й міжнародні моделі та практики	Виявлення альтернатив і меж адаптації досвіду	Неприпустимість механічного перенесення інституцій
Цифрово-екосистемний	Охоплює дані, платформи, алгоритми, інфраструктуру та технологічне врядування	Врахування платформізації й автоматизованих рішень	Швидке старіння показників та обмежена прозорість алгоритмів

Джерело: систематизовано автором за [3; 6; 30; 45; 69; 115; 136; 146; 159].

Наведені підходи не є взаємовиключними. Системний підхід формує загальну рамку, інституційний і правовий деталізують структуру, процесний відтворює послідовність дій, комунікаційний і мережевий пояснюють взаємодію, ризик-орієнтований визначає безпекові пріоритети, а цифрово-екосистемний враховує технологічні залежності. Їх інтеграція повинна здійснюватися за принципом функціональної доцільності: кожний підхід відповідає на визначене дослідницьке питання.

Особливе значення має поєднання нормативного й емпіричного вимірів. Закон або стратегія можуть декларувати координацію, однак аналіз реальних процедур виявляє фрагментацію. Орган може мати формальне повноваження, але не володіти ресурсами. Публічна комунікація може бути регулярною, але не зрозумілою для цільових груп. Тому висновок про дієвість механізму повинен спиратися на зіставлення принаймні трьох рівнів: нормативно передбачено, інституційно забезпечено, фактично досягнуто.

Методологічна багатовимірність не означає накопичення максимальної кількості методів. Надлишковий інструментарій ускладнює інтерпретацію й може породити несумісні результати. Доцільно застосовувати принцип методичної достатності: обирати мінімально необхідний набір методів, який дає змогу перевірити ключові припущення з різних джерел. У межах цього дослідження базовими є аналіз документів, інституційне картування, порівняльний аналіз, контент-аналіз, експертне оцінювання та моделювання.

Методичну якість дослідження визначають принципи, які регулюють вибір даних, способи їх інтерпретації та межі висновків. Принцип об'єктивності вимагає відокремлювати аналітичні судження від політичних оцінок і перевіряти твердження через декілька джерел. Принцип системності орієнтує на дослідження взаємозв'язків, а не ізольованих елементів. Принцип історизму передбачає врахування етапу розвитку інституцій та контексту ухвалення рішень. Принцип комплексності зобов'язує поєднувати правові, управлінські, комунікаційні, цифрові й безпекові характеристики.

Принцип правової визначеності має особливу вагу, оскільки механізми інформаційної політики можуть впливати на фундаментальні права. Дослідник повинен оцінювати наявність чіткої нормативної підстави, передбачуваність процедур, визначеність компетенцій, можливість оскарження та контроль за дискрецією. Для обмежень доступу або поширення інформації додатково застосовуються критерії легітимної мети, необхідності та пропорційності [48; 84; 93; 119].

Принцип людиноцентричності зміщує фокус від адміністративної активності до досвіду громадянина. Ефективність цифрової комунікації не можна визначати лише кількістю опублікованих матеріалів або відвідувань вебсайту. Необхідно встановлювати, чи отримала людина потрібну інформацію, чи зрозуміла її, чи могла скористатися правом, чи не була виключена через цифрові, мовні або фізичні бар'єри. Цей принцип узгоджується з підходами UNESCO до врядування цифрових платформ та міжнародними принципами інформаційної доброчесності [159; 160].

Принцип міждисциплінарності вимагає узгодження правових, комунікаційних і безпекових понять. Дезінформація, інформаційний розлад та інформаційна операція не є тотожними категоріями, тому перед емпіричним аналізом необхідно сформулювати глосарій операційних понять і визначити правила їх використання [76; 142; 161].

Принцип триангуляції передбачає зіставлення різних видів даних і методів. Нормативні документи показують формальні правила; організаційні положення – розподіл функцій; звіти – задекларовані результати; цифрові дані – фактичну активність; експертні оцінки – приховані процеси й обмеження; соціологічні дані – суспільне сприйняття. Збіг результатів посилює обґрунтованість висновків, а розбіжність стає окремим предметом аналізу, а не приводом відкинути незручне джерело.

Принцип відтворюваності означає можливість повторити основні аналітичні процедури. Для цього фіксуються критерії добору документів, часові межі, одиниці аналізу, кодувальна схема, правила оцінювання, шкали та алгоритм розрахунку. У дослідженні цифрових комунікацій також необхідно

зазначати дату збору, параметри пошуку та обмеження доступу, оскільки онлайн-контент може редагуватися або видалятися. Відтворюваність не гарантує тотожного результату, але робить процес прозорим.

Принцип етичності охоплює захист персональних даних, мінімізацію шкоди, добровільність участі експертів і респондентів, безпечне зберігання матеріалів та відповідальне представлення результатів. У воєнний період необхідно уникати оприлюднення деталей, які можуть розкрити вразливості інформаційної інфраструктури або внутрішні процедури реагування. Водночас посилення на безпеку не повинно використовуватися для приховування методики, критеріїв і загальної логіки оцінювання [83; 90; 91].

З урахуванням визначених принципів дослідницький процес доцільно організовувати як послідовність взаємопов'язаних блоків: постановка проблеми; формування концептуальної моделі; визначення запитань і припущень; операціоналізація; добір джерел і методів; збір даних; аналіз; перевірка; моделювання вдосконаленого механізму; апробація рекомендацій. Логічну модель такого процесу подано на рис. 1.8.

1. ПРОБЛЕМА І КОНТЕКСТ	→	2. КОНЦЕПТУАЛЬНА МОДЕЛЬ	→	3. ПИТАННЯ ТА ПРИПУЩЕННЯ
↓		↓		↓
4. ОПЕРАЦІОНАЛІЗАЦІЯ	→	5. ДЖЕРЕЛА І МЕТОДИ	→	6. ЗБІР ТА ВЕРИФІКАЦІЯ ДАНИХ
↓		↓		↓
7. АНАЛІЗ І ПОЯСНЕННЯ	→	8. ОЦІНЮВАННЯ МЕХАНІЗМІВ	→	9. МОДЕЛЮВАННЯ ТА РЕКОМЕНДАЦІЇ
ЗВОРОТНИЙ ЗВ'ЯЗОК І УТОЧНЕННЯ ВИХІДНИХ ПРИПУЩЕНЬ	ЗВОРОТНИЙ ЗВ'ЯЗОК І УТОЧНЕННЯ ВИХІДНИХ ПРИПУЩЕНЬ	ЗВОРОТНИЙ ЗВ'ЯЗОК І УТОЧНЕННЯ ВИХІДНИХ ПРИПУЩЕНЬ	ЗВОРОТНИЙ ЗВ'ЯЗОК І УТОЧНЕННЯ ВИХІДНИХ ПРИПУЩЕНЬ	ЗВОРОТНИЙ ЗВ'ЯЗОК І УТОЧНЕННЯ ВИХІДНИХ ПРИПУЩЕНЬ

Рис. 1.8. Логічна модель організації дослідження механізмів реалізації державної інформаційної політики

Джерело: авторська розробка.

Постановка проблеми повинна спиратися на розрив між нормативно бажаним і фактичним станом. Формулювання на кшталт «недостатня ефективність інформаційної політики» є надто загальним. Необхідно визначити, у чому саме проявляється недостатність: дублюванні повноважень, відсутності координації, низькій доступності, неузгодженості комунікації, вразливості цифрової інфраструктури, слабкому зворотному зв'язку або відсутності показників результату. Точність проблеми визначає релевантність методів.

Концептуальна модель задає попередній набір елементів і зв'язків. Вона може включати суб'єктів, нормативну основу, цілі, функції, ресурси, інструменти, процеси, продукти, результати, зовнішні фактори та механізми зворотного зв'язку. На цьому етапі формуються дослідницькі припущення, наприклад: чим чіткіше розподілені функції, тим вищою є координаційна спроможність; чим відкритішою є комунікація, тим вищою є довіра; чим більша залежність від однієї платформи, тим вищою є системна вразливість. Такі припущення потребують перевірки, а не приймаються як аксіоми.

Добір джерел повинен бути цілеспрямованим і прозорим. До нормативного корпусу включаються закони, укази, постанови, розпорядження, стратегії та плани заходів. До інституційного – положення про органи, регламенти, структури, бюджетні програми й звіти. До комунікаційного – офіційні повідомлення, кампанії, вебсайти, соціальні мережі та матеріали для різних аудиторій. До результативного – статистика, соціологічні дослідження, оцінки міжнародних організацій, судова практика, експертні висновки та дані моніторингу.

Методи мають відповідати типу даних. Тексти нормативних актів досліджуються формально-юридичним, порівняльно-правовим і контент-аналітичним методами; організаційні структури – інституційним картуванням; управлінські процеси – процес-трейсингом і кейс-стаді; цифрові повідомлення – кількісним і якісним контент-аналізом; взаємодія суб'єктів – мережевим аналізом; сприйняття – опитуваннями та інтерв'ю; перспективні конфігурації – сценарним і структурно-логічним моделюванням.

Комплекс методів дослідження та очікувані аналітичні результати

Метод	Джерельна база	Основна процедура	Очікуваний результат
Аналіз і синтез	Наукові концепції, нормативні й аналітичні матеріали	Розкладання механізму на складові та їх подальше інтегрування	Структурована модель механізму
Історико-логічний метод	Нормативні акти, стратегії, інституційні зміни у часі	Відтворення етапів і причин трансформації	Періодизація та виявлення закономірностей
Формально-юридичний аналіз	Закони, підзаконні акти, положення, процедури	Тлумачення норм, компетенцій, гарантій та обмежень	Оцінка правової визначеності й узгодженості
Порівняльно-правовий метод	Українські, європейські та міжнародні акти	Зіставлення моделей регулювання й гарантій	Визначення можливостей адаптації
Контент-аналіз	Офіційні повідомлення, стратегії, медіа- та цифровий контент	Кодування тем, тональності, аудиторій, рамок і закликів	Кількісна та якісна характеристика комунікації
Інституційне картування	Положення, структури, компетенції, взаємодія	Візуалізація суб'єктів, ролей, ресурсів і зв'язків	Виявлення дублювання, прогалин і залежностей
Кейс-стаді та процес-трейсинг	Окремі рішення, кампанії, кризи або реформи	Відстеження послідовності рішень і причинних механізмів	Пояснення успіху або невдачі реалізації
Експертне оцінювання	Думки фахівців публічного управління, права, медіа й безпеки	Ранжування проблем, критеріїв і варіантів рішень	Уточнення ваг і практичної здійсненості
Соціологічні методи	Опитування, інтерв'ю, фокус-групи	Вимірювання доступності, довіри, розуміння і поведінки	Оцінювання суспільних результатів
Структурно-логічне та сценарне моделювання	Узагальнені результати всіх етапів	Побудова цільової конфігурації та сценаріїв	Авторська модель і рекомендації

Джерело: сформовано автором із урахуванням [22; 37; 69; 115; 124; 150; 151; 161].

Контент-аналіз у дослідженні державної інформаційної політики доцільно здійснювати за попередньо сформованою кодувальною книгою. Одиницею аналізу може бути документ, повідомлення, тематичний фрагмент, візуальний елемент або комунікаційна дія. Категорії повинні охоплювати ціль, тему, суб'єкта, аудиторію, канал, доказову основу, рівень доступності, наявність зворотного зв'язку, безпекову рамку та заклик до дії. Для підвищення надійності частину матеріалів доцільно кодувати незалежно двома дослідниками.

Інституційне картування має включати не лише перелік органів, а й матрицю відповідальності. Для кожної функції визначаються суб'єкт, який ухвалює рішення; виконавець; орган, що погоджує; постачальник даних; партнер; суб'єкт контролю та адресат звітування. Така матриця дає змогу виявити ситуації, коли одна функція має декількох неузгоджених виконавців або, навпаки, не закріплена за жодним суб'єктом. Практичну цінність має також картування потоків даних і каналів кризової комунікації [30; 34; 113].

Експертне оцінювання може застосовуватися для визначення ваг критеріїв, ранжування проблем і перевірки реалістичності рекомендацій. Добір експертів повинен забезпечувати різноманітність секторів і компетенцій, а не лише статусність учасників. Доцільно включати представників органів влади, місцевого самоврядування, медіа, громадських організацій, науковців, фахівців із цифрових технологій, права та безпеки. Розбіжності оцінок не слід штучно усереднювати; вони можуть відображати конфлікт цінностей або різний досвід реалізації.

Порівняльний аналіз зарубіжного досвіду повинен орієнтуватися не на копіювання організаційних форм, а на порівняння функцій, принципів і умов ефективності. Європейські правила щодо цифрових послуг, медіасвободи, кібербезпеки, даних і штучного інтелекту формують релевантну нормативну рамку [139; 154; 155; 156; 157]. Проте їх адаптація залежить від адміністративної спроможності, медіасистеми, рівня цифровізації, безпекового контексту та правової культури України.

Оцінювання механізмів повинно відрізняти ресурси, процеси, продукти, результати та суспільний вплив. Ресурси відображають кадрове, фінансове, технологічне й нормативне забезпечення. Процеси характеризують координацію, швидкість, прозорість і дотримання процедур. Продукти є безпосередніми результатами діяльності – нормативними актами, наборами даних, повідомленнями, сервісами, навчаннями. Результати показують зміни у доступності, узгодженості, спроможності та поведінці. Вплив стосується довіри, демократичної стійкості, інформаційної безпеки та якості публічного управління.

Поширеною помилкою є ототожнення активності з ефективністю. Велика кількість повідомлень не свідчить про якісну комунікацію; наявність стратегії – про її реалізацію; збільшення фінансування – про досягнення суспільного результату; швидкість реагування – про достовірність; обмеження контенту – про підвищення стійкості. Методика повинна встановлювати логічний зв'язок між витраченими ресурсами, виконаними діями та змінами в інформаційному середовищі.

Критерій нормативної узгодженості характеризує повноту, ієрархічну несуперечливість і актуальність правового регулювання. Його показниками можуть бути визначеність цілей, компетенцій і процедур; відповідність Конституції та міжнародним зобов'язанням; наявність механізмів оскарження; узгодженість стратегій із планами заходів. Цей критерій оцінюється через формально-юридичний, порівняльно-правовий та контент-аналітичний методи [48; 84; 93; 105; 128].

Критерій інституційної спроможності відображає здатність суб'єктів виконувати покладені функції. До його індикаторів належать чіткість повноважень, наявність професійного персоналу, сталість фінансування, доступ до даних, технологічна оснащеність, внутрішні процедури й система навчання. Важливо аналізувати не тільки центральні органи, а й місцевий рівень, оскільки доступність і кризова комунікація значною мірою реалізуються територіально [16; 30; 158].

Критерій координаційної якості оцінює взаємодію між суб'єктами. Показниками є наявність визначеного координатора, спільних протоколів, сумісних інформаційних систем, регулярного обміну даними, механізмів вирішення суперечностей та узгодженої публічної позиції. При цьому уніфікація повідомлень не повинна підміняти плюралізм або приховувати невизначеність. Координація є якісною тоді, коли вона зменшує дублювання й затримки, зберігаючи відповідальність кожного суб'єкта [2; 34; 45].

Критерій відкритості та доступності включає юридичну, технічну, змістову й когнітивну доступність інформації. Вимірюються повнота оприлюднення, своєчасність, машиночитаність, доступність для людей з

інвалідністю, зрозумілість мови, можливість повторного використання даних і якість відповідей на запити. Відкритість має оцінюватися разом із законністю обмежень і захистом персональних даних [4; 81; 84; 88; 91].

Критерій комунікаційної результативності охоплює відповідність повідомлень потребам аудиторій, узгодженість змісту і каналу, доказовість, оперативність, двосторонність і рівень довіри. Можливими показниками є розуміння ключових повідомлень, здатність відрізнити офіційну інформацію, охоплення пріоритетних груп, частка запитань, на які надано змістовну відповідь, та зміна поведінки. Міжнародні підходи наголошують на відмежуванні публічної комунікації від політичної пропаганди [137; 150; 151].

Критерій цифрової зрілості характеризує інтегрованість даних і сервісів, інтероперабельність, надійність електронної ідентифікації, захищеність систем, доступність цифрових каналів і прозорість автоматизованих рішень. Оцінювання повинно враховувати не лише впровадження технологій, а й управління даними, резервування, безперервність, алгоритмічні ризики та людський контроль [85; 87; 98; 102; 139; 155; 157].

Критерій інформаційної безпеки та стійкості передбачає оцінювання спроможності виявляти загрози, запобігати їм, реагувати, відновлюватися й навчатися. Індикатори можуть охоплювати швидкість верифікації, наявність кризових протоколів, резервні канали, міжвідомчу взаємодію, захист критичної інфраструктури, підтримку медіаграмотності та суспільної довіри. Стійкість не зводиться до оборонної реакції; вона включає здатність інформаційної екосистеми зберігати демократичні функції під тиском [22; 45; 94; 105; 146].

Критерій адаптивності показує здатність механізму змінювати інструменти й пріоритети на основі даних, не руйнуючи правових принципів і інституційної пам'яті. Його ознаками є регулярний перегляд стратегій, сценарне планування, навчання за результатами криз, експериментування з подальшим оцінюванням, залучення незалежної експертизи та коригування показників. Адаптивність особливо важлива для протидії дезінформації, оскільки тактики, платформи й технології швидко змінюються [37; 141; 150; 161].

**Критеріально-індикаторна матриця оцінювання механізмів реалізації
державної інформаційної політики**

Критерій	Ключові індикатори	Основні джерела даних	Методи перевірки
Нормативна узгодженість	Чіткість цілей і компетенцій; несуперечливість; гарантії прав; наявність процедур оскарження	Нормативні акти, стратегії, судова практика	Формально-юридичний і порівняльно-правовий аналіз
Інституційна спроможність	Кадри; бюджет; технології; дані; внутрішні процедури; навчання	Положення, структури, бюджети, звіти, інтерв'ю	Інституційне картування, експертне оцінювання
Координаційна якість	Координатор; протоколи; обмін даними; сумісність; вирішення суперечностей	Регламенти, протоколи, кейси взаємодії	Процес-трейсинг, мережевий аналіз, кейс-стаді
Відкритість і доступність	Повнота; своєчасність; машиночитаність; інклюзивність; зрозумілість	Портали, відповіді на запити, набори даних	Аудит доступності, контент-аналіз, тестування користувачами
Комунікаційна результативність	Доказовість; сегментація; охоплення; розуміння; зворотний зв'язок; довіра	Повідомлення, кампанії, аналітика каналів, опитування	Контент-аналіз, соціологічні та поведінкові методи
Цифрова зрілість	Інтероперабельність; надійність; захист; прозорість алгоритмів; безперервність	ІТ-архітектура, реєстри, аудити, журнали інцидентів	Техніко-організаційний аудит, аналіз ризиків
Інформаційна безпека і стійкість	Виявлення; превенція; реагування; відновлення; навчання; резервування	Плани, протоколи, кейси криз, звіти про загрози	Ризик-аналіз, сценарний метод, порівняння кейсів
Адаптивність і підзвітність	Перегляд політики; оцінювання; публічне звітування; незалежний контроль	Плани моніторингу, звіти, рекомендації, рішення про коригування	Оцінювання політики, експертна валідація, аналіз зворотного зв'язку

Джерело: розроблено автором на основі [4; 30; 45; 70; 84; 105; 146; 150; 151; 159].

Для інтегрованого оцінювання запропоновані критерії можуть переводитися у нормовану шкалу від 0 до 1, де 0 означає відсутність або критичну неспроможність відповідного елемента, а 1 – повне нормативне, інституційне та результативне забезпечення. Проміжні значення мають визначатися через описані рівні, а не довільне експертне судження. Наприклад, рівень 0,5 може означати формальне запровадження механізму за нестабільного ресурсного забезпечення та часткової реалізації процедур.

Узагальнений індекс дієвості механізмів може бути представлений як $I = \sum(w_i \times k_i)$, де k_i – нормована оцінка окремого критерію, w_i – його ваговий коефіцієнт, а сума ваг дорівнює одиниці. Ваги доцільно визначати шляхом експертного оцінювання та перевіряти аналізом чутливості. Інтегральний індекс

не замінює якісного аналізу: однакове значення може бути сформоване різними комбінаціями сильних і слабких сторін, тому поряд із підсумковою оцінкою обов'язково подається профіль критеріїв.

Інтегральний індекс доцільно використовувати переважно для порівняння у часі або між механізмами. Його слід супроводжувати профілем критеріїв, описом якості даних і рівнем узгодженості експертних оцінок, щоб кількісне узагальнення залишалось інструментом діагностики, а не формальним рейтингом.

Емпірична база повинна бути достатньо різноманітною, щоб охопити формальні й фактичні практики. Нормативні акти та офіційні звіти є необхідними, але можуть відображати переважно позицію інституцій. Їх слід доповнювати незалежними моніторингами, судовими рішеннями, даними про використання цифрових сервісів, оцінками користувачів, експертними інтерв'ю та аналізом конкретних кризових ситуацій. Особливо важливо відокремлювати відсутність проблеми від відсутності даних про неї.

Послідовність застосування критеріїв і методів доцільно оформити як алгоритм, що починається з визначення меж механізму та завершується валідацією рекомендацій. Авторський алгоритм представлено на рис. 1.9.



Рис. 1.9. Алгоритм комплексного оцінювання та проєктування механізмів реалізації державної інформаційної політики

Джерело: авторська розробка.

Перший етап алгоритму передбачає встановлення функціональних, інституційних, територіальних і часових меж механізму. Без цього дослідження може змішувати механізм політики з усією інформаційною сферою. Другий етап

формує карту суб'єктів, норм, ресурсів, інструментів і потоків даних. На третьому етапі загальні критерії адаптуються до конкретного об'єкта, після чого визначаються джерела та правила вимірювання.

Четвертий етап об'єднує збір даних із їх попередньою верифікацією. П'ятий спрямований на виявлення розривів між нормативним, інституційним і фактичним станом та встановлення причин. Причини доцільно класифікувати як правові, організаційні, ресурсні, технологічні, комунікаційні, мотиваційні або зовнішні. Така класифікація запобігає універсальним рекомендаціям: правова прогалина потребує іншого рішення, ніж нестача компетентностей або технічна несумісність.

На шостому етапі порівнюються альтернативи з урахуванням витрат, ризиків, правових обмежень, строків і очікуваної публічної цінності. Сценарний аналіз має включати щонайменше базовий, оптимістичний і кризовий сценарії. Сьомий етап формує цільову модель механізму, у якій визначаються функції, відповідальність, ресурси, процедури, показники та зворотний зв'язок. Восьмий етап передбачає експертну валідацію, перевірку внутрішньої узгодженості та коригування.

Валідація рекомендацій повинна оцінювати не лише бажаність, а й здійсненність. Для кожної пропозиції визначаються нормативні зміни, відповідальні суб'єкти, ресурсні потреби, ризики реалізації, часовий горизонт і критерії успіху. Окремо перевіряється можливість непередбачених наслідків: надмірної централізації, дублювання, обмеження прав, технологічної залежності або зростання адміністративного навантаження. Тільки після такої перевірки рекомендація може вважатися методично обґрунтованою.

Запропонований алгоритм може застосовуватися на різних рівнях: для оцінювання національної системи інформаційної політики, окремого інституційного механізму, регіональної комунікації, цифрового сервісу або політики протидії дезінформації. Незмінними залишаються логіка від визначення меж до валідації та вимога зіставляти правові, інституційні й результативні дані. Зміст індикаторів адаптується до об'єкта й доступної емпіричної бази.

Достовірність дослідження визначається якістю даних, логічною узгодженістю процедур і адекватністю інтерпретації. Для документальних джерел необхідно перевіряти чинність, офіційне походження та редакцію акта. Для статистичних даних – методику формування, повноту й порівнюваність. Для цифрових метрик – правила платформи й часовий зріз. Для експертних оцінок – компетентність, незалежність і різноманітність учасників. Якість кожного джерела доцільно фіксувати у паспорті даних.

Внутрішня валідність стосується обґрунтованості причинних висновків. Збіг у часі між інформаційною кампанією та зміною довіри не доводить причинності, тому слід враховувати альтернативні пояснення, часову послідовність і контекст. Процес-трейсинг, порівняння до і після та якісні інтерв'ю посилюють аргументацію.

Рефлексивність дослідника є важливою через політично чутливий характер інформаційної політики. Дослідник повинен усвідомлювати власні нормативні припущення, професійний досвід і можливі конфлікти інтересів. Доцільно відокремлювати опис факту, його оцінювання за встановленим критерієм та авторську рекомендацію. Така структура тексту зменшує ризик прихованої політизації й дозволяє читачеві простежити шлях від даних до висновку.

Етична робота з експертами й респондентами передбачає інформовану згоду, можливість відмови, пояснення мети використання даних і способів анонімізації. У разі дослідження службових процесів необхідно розмежовувати інформацію, що підтверджує науковий висновок, та деталі, публікація яких створює безпековий ризик. Принцип мінімізації даних означає збір лише тієї інформації, яка безпосередньо потрібна для дослідницького питання [91; 153].

Узагальнення розглянутих підходів дає підстави запропонувати авторську методичну модель, побудовану на принципах системності, людиноцентричності, правової визначеності, доказовості, адаптивності, триангуляції та відтворюваності. Її відмінністю є одночасне дослідження трьох площин механізму: нормативно спроектованої, інституційно реалізованої та суспільно

сприйнятої. Розрив між цими площинами розглядається як ключове джерело управлінської проблеми.

Методичні засади дослідження механізмів реалізації державної інформаційної політики – це цілісна система принципів, наукових підходів, методів, процедур, критеріїв, індикаторів і правил верифікації, за допомогою якої здійснюється багаторівневе вивчення нормативної конструкції, інституційної спроможності, управлінських процесів, комунікаційних практик, цифрової інфраструктури, безпекової стійкості та суспільних результатів інформаційної політики з метою пояснення причин її дієвості або недієвості та проєктування обґрунтованих напрямів удосконалення.

Основною одиницею аналізу в авторській моделі є функціональний зв'язок «ціль – суб'єкт – повноваження – ресурс – процедура – інструмент – продукт – результат – зворотний зв'язок». Якщо будь-який елемент відсутній або не узгоджений з іншими, виникає функціональний розрив. Така одиниця аналізу дозволяє перейти від загального опису інституцій до діагностики конкретного механізму та встановити, на якому етапі політична ціль втрачає реалізаційну спроможність.

Модель передбачає побудову профілю механізму за вісьмома критеріями, наведеними в табл. 1.9. Профіль поєднує кількісні оцінки з якісним поясненням. Пріоритет удосконалення визначається не лише найнижчою оцінкою, а й системним значенням критерію. Наприклад, неузгодженість нормативних повноважень може блокувати ресурсно забезпечений механізм, а недостатня відкритість – знижувати легітимність технічно ефективного рішення.

Для перевірки рекомендацій вводиться принцип подвійної відповідності. По-перше, рішення повинно відповідати встановленій причині проблеми. По-друге, воно має відповідати правовим принципам, ресурсним можливостям і контексту. Пропозиція вважається методично слабкою, якщо вона лише описує бажаний стан, але не встановлює відповідального суб'єкта, нормативну підставу, ресурси, послідовність впровадження та показники результату.

Наукова новизна методичної моделі полягає в поєднанні функціонально-цільової логіки з критеріями правової якості, інституційної спроможності,

комунікаційної результативності, цифрової зрілості та інформаційної стійкості. Вона дозволяє оцінити механізм не як статичний набір органів і нормативних актів, а як адаптивний цикл створення публічної цінності. Зворотний зв'язок і коригування розглядаються як обов'язкові елементи, а не завершальна формальність.

Практичне значення моделі полягає у можливості її використання для аналізу чинної системи державної інформаційної політики України, оцінювання окремих інституційних механізмів, розроблення стратегічних документів і планів заходів, проведення функціонального аудиту та формування системи моніторингу. Методика також створює основу для порівняння національної практики з європейськими й міжнародними принципами інформаційної доброчесності, цифрового врядування та публічної комунікації [140; 150; 151; 159; 160].

Таким чином, методичні засади дослідження механізмів реалізації державної інформаційної політики повинні забезпечувати цілісність, доказовість і практичну спрямованість аналізу. Їх структура охоплює рівневу методологічну архітектуру, систему принципів, комплекс взаємодоповнювальних методів, критерії та індикатори, алгоритм оцінювання, процедури валідації й авторську модель інтерпретації. Застосування цієї конструкції дає змогу перейти від опису інформаційної політики до пояснення її інституційної дієвості та науково обґрунтованого проєктування механізмів удосконалення.

Висновки до розділу 1

Установлено, що еволюція наукових поглядів на формування державної інформаційної політики має послідовний, але кумулятивний характер. Запропонована періодизація охоплює п'ять взаємопов'язаних етапів: правове та інституційне становлення у 1991–2000 роках; розвиток парадигми інформаційного суспільства, електронного урядування та європеїзації у 2001–2013 роках; безпекову переорієнтацію і становлення стратегічних комунікацій у 2014–2021 роках; воєнно-комунікаційну та стійкісну модель у 2022–2024 роках; цифрово-платформну й людиноцентричну парадигму у 2025–2026 роках.

Кожний наступний етап не заперечував попередній, а розширював предмет політики, склад її суб'єктів, інструментарій і критерії оцінювання.

Обґрунтовано міждисциплінарну природу державної інформаційної політики. Її належне наукове пояснення потребує поєднання організаційно-правового, інституційного, публічно-управлінського, комунікаційного, безпекового, цифрово-екосистемного, соціологічного та міжнародно-інтеграційного підходів. Правова наука визначає межі допустимого державного втручання і гарантії прав; теорія публічного управління розкриває систему суб'єктів, компетенцій, ресурсів та процедур; комунікаційні студії пояснюють взаємодію з аудиторіями, довіру і зворотний зв'язок; безпекові дослідження зосереджуються на загрозах і стійкості; цифровий підхід охоплює дані, платформи, алгоритми та інфраструктуру.

На основі інтеграції цих підходів уточнено авторське розуміння державної інформаційної політики як ціннісно орієнтованої, нормативно врегульованої, інституційно скоординованої та суспільно підзвітної системи цілей, принципів, рішень і дій держави у взаємодії з громадянами, медіа, громадянським суспільством, бізнесом, науковим середовищем, органами місцевого самоврядування, цифровими платформами та міжнародними партнерами.

Уточнено принципову основу формування та реалізації державної інформаційної політики. До базових принципів віднесено верховенство права, пріоритет інформаційних прав і свобод, достовірність, відкритість, підзвітність, пропорційність обмежень, інклюзивність, політичну неупередженість інституційної комунікації, технологічну нейтральність, субсидіарність, доказовість, міжвідомчу узгодженість і стійкість.

Доведено, що предмет державної інформаційної політики розширився від регулювання інформації, медіа та державних інформаційних ресурсів до управління цілісною інформаційною екосистемою. Її складовими є дані, реєстри, традиційні й цифрові медіа, платформи, алгоритмічні системи, комунікаційні мережі, інституції, суспільні наративи та поведінка аудиторій. Відповідно, суб'єктний склад не може обмежуватися центральними органами виконавчої влади: реалізація політики залежить від узгодженої взаємодії державних і

місцевих органів, медіа, наукових установ, громадських організацій, бізнесу, технологічних компаній, громадян і міжнародних інституцій.

Уточнено поняття механізму реалізації державної інформаційної політики як впорядкованої сукупності нормативно-правових, інституційно-організаційних, комунікаційних, цифрових, економічних, безпекових і контрольних-аналітичних засобів, процедур та взаємодій, за допомогою яких стратегічні цілі перетворюються на узгоджені управлінські дії та суспільні результати. Визначальною характеристикою такого механізму є циклічність: публічні цінності й права задають межі політики; нормативні правила та компетенції забезпечують її легітимність; координація суб'єктів і ресурсів створює спроможність; комунікаційні, цифрові та безпекові інструменти забезпечують виконання; моніторинг і зворотний зв'язок стають підставою для перегляду рішень.

Систематизовано функції державної інформаційної політики та встановлено, що вони є відносно сталими напрямками державного впливу, які повинні бути пов'язані з конкретними публічними результатами. Виокремлено організаційно-правову, інституційно-координаційну, комунікаційно-діалогічну, сервісно-цифрову, безпеково-захисну, соціально-гуманітарну, аналітично-адаптивну та міжнародно-інтеграційну функціональні групи.

Визначено функціонально-цільову архітектуру державної інформаційної політики, що вибудовується за логікою «цінності – функції – цілі – пріоритети – механізми – результати – зворотний зв'язок». Генеральною метою політики обґрунтовано створення відкритого, безпечного, стійкого та людиноцентричного інформаційного середовища. Її декомпозиція охоплює п'ять взаємопов'язаних напрямів: гарантування інформаційних прав і відкритості; зміцнення довіри, діалогу та участі; забезпечення інформаційної безпеки й стійкості; цифровий розвиток та інклюзію; європейську інтеграцію і міжнародну присутність.

Обґрунтовано, що пріоритети державної інформаційної політики є динамічним управлінським вибором щодо концентрації ресурсів і відповідальності, а тому повинні визначатися за прозорими критеріями. До таких критеріїв віднесено масштаб і терміновість проблеми, рівень ризику для прав

людини та національної безпеки, очікувану публічну цінність, охоплення і вразливість цільових груп, нормативну обов'язковість, міжсекторальний ефект, інституційну спроможність, ресурсну здійсненність і можливість вимірювання результату. Застосування цих критеріїв зменшує вплив ситуативної політичної доцільності та короточасних медійних коливань на формування державних рішень.

Сформовано рівневу методологічну архітектуру дослідження механізмів реалізації державної інформаційної політики. Вона охоплює концептуальний рівень, на якому інформація розглядається як право, ресурс, форма влади, публічна цінність і чинник безпеки; загальнонауковий рівень із використанням системного аналізу, індукції, дедукції, порівняння та моделювання; спеціально-науковий рівень, що поєднує правовий, інституційний, структурно-функціональний, процесний, комунікаційний, мережевий, ризик-орієнтований, порівняльний і цифрово-екосистемний підходи; операційний рівень, на якому категорії перетворюються на критерії, індикатори, шкали та процедури перевірки.

Розроблено систему комплексного оцінювання механізмів реалізації державної інформаційної політики, яка охоплює нормативну узгодженість, інституційну спроможність, координаційну якість, відкритість і доступність, комунікаційну результативність, цифрову зрілість, інформаційну безпеку та стійкість, адаптивність і підзвітність. Для кожного критерію визначено групи індикаторів, джерела даних і методи перевірки. Принциповим є оцінювання не лише нормативно спроектованого механізму, а трьох його площин: формально встановленої, інституційно реалізованої та суспільно сприйнятої. Розриви між ними розглядаються як джерела управлінської неефективності й підстава для цільових змін.

Таким чином, загальним результатом першого розділу є формування цілісної концептуально-методичної основи дослідження механізмів реалізації державної інформаційної політики. Вона поєднує еволюційну періодизацію, інтегроване авторське визначення політики й механізму її реалізації, функціонально-цільову архітектуру, систему пріоритетів та багаторівневу

методику оцінювання. Отримані результати дають підстави перейти від загальнотеоретичного опису інформаційної сфери до аналізу реальної системи суб'єктів, інструментів взаємодії та проблем інформаційної стійкості України, що становить зміст другого розділу дисертації.

РОЗДІЛ 2. ОСОБЛИВОСТІ ФУНКЦІОНУВАННЯ ДЕРЖАВНОЇ ІНФОРМАЦІЙНОЇ ПОЛІТИКИ В УКРАЇНІ

2.1. Система суб'єктів формування та реалізації державної інформаційної політики

Державна інформаційна політика набуває практичного змісту лише через діяльність суб'єктів, які визначають суспільно значущі інформаційні проблеми, формують цілі, ухвалюють нормативні та управлінські рішення, забезпечують їх виконання, здійснюють контроль і підтримують зворотний зв'язок із громадянами. Тому дослідження її інституційної будови не може обмежуватися переліком органів влади. Воно має розкривати розподіл компетенцій, характер взаємозалежностей, механізми координації та реальну спроможність учасників перетворювати політичні наміри на публічні результати.

Складність суб'єктної системи зумовлена міжгалузевою природою інформаційної політики. Вона охоплює гарантування права на інформацію, функціонування медіасередовища, стратегічні комунікації, цифрову трансформацію, відкриті дані, захист персональних даних, кібербезпеку, протидію дезінформації, зовнішнє інформаційне представництво та інформаційне забезпечення управлінських рішень. Кожен із цих напрямів має власне нормативне поле й коло відповідальних інституцій, однак суспільний результат залежить від їх узгодженої дії.

Воєнні та гібридні загрози додатково посилили значення інституційної узгодженості. Оперативне виявлення інформаційних атак, перевірка даних, вироблення спільної позиції, донесення достовірних повідомлень до різних аудиторій та захист критичної інформаційної інфраструктури потребують взаємодії політичного керівництва, органів виконавчої влади, сектору безпеки й оборони, регуляторів, публічних медіа та громадського середовища. Фрагментована система за таких умов створює ризик суперечливих повідомлень, дублювання функцій і втрати довіри [2; 28; 37; 45; 71].

У категоріальному сенсі суб'єктом державної інформаційної політики є учасник суспільно-владних відносин, який на підставі правового статусу, публічного мандата, професійної компетентності або суспільної ролі здатний впливати на зміст, інструменти й результати політики. Ознакою суб'єктності є не сама організаційна наявність, а можливість здійснювати цілеспрямовані дії, нести відповідальність, вступати у взаємодію з іншими учасниками та змінювати параметри інформаційного середовища [3; 6; 127].

Поняття «система суб'єктів» ширше за поняття «система органів державної влади». Перше охоплює як носіїв владних повноважень, так і регуляторів, публічні установи, органи місцевого самоврядування, суспільні медіа, недержавних виробників інформації, експертні мережі та громадян. Водночас включення недержавних учасників не означає розмивання відповідальності держави. Саме публічна влада зберігає обов'язок гарантувати права, визначати прозорі правила, захищати національні інтереси та забезпечувати підзвітність політики [48; 84; 93; 159].

Організаційно-правовий підхід акцентує увагу на компетенціях, процедурах і підпорядкованості. У його межах система постає як нормативно впорядкована сукупність інституцій, кожна з яких має встановлений предмет відання, повноваження та юридичні форми діяльності. Перевагою цього підходу є можливість перевірити законність рішень і уникнути довільного втручання в інформаційну сферу; обмеженням – недостатня увага до неформальних мереж, цифрових платформ і фактичних центрів впливу [3; 5; 6; 56].

Функціональний підхід виходить із того, що один напрям політики може забезпечуватися кількома суб'єктами, а одна інституція – виконувати різні функції. Тому аналіз спрямовується на встановлення ролей: нормотворчої, стратегічної, координаційної, регуляторної, сервісної, комунікаційної, аналітичної, безпекової та контрольної. Функціональна карта дає змогу виявити дублювання, прогалини та точки необхідної взаємодії, які не завжди помітні з формальної організаційної схеми [69; 115; 120; 124].

Мережевий підхід розглядає політику як результат постійної взаємодії взаємозалежних учасників, жоден із яких не володіє всіма ресурсами. Держава

має правові й примусові інструменти, медіа – професійні канали та аудиторну довіру, громадські організації – доступ до окремих груп і незалежну експертизу, наука – методи аналізу, цифрові платформи – технологічну інфраструктуру й дані. За таких умов ключовою управлінською функцією стає організація правил співпраці [138; 150; 151; 159].

Безпековий підхід групує суб'єктів залежно від їх участі у виявленні загроз, захисті інформаційних ресурсів, протидії ворожим впливам і відновленні стійкості. Він особливо важливий в умовах воєнного стану, проте потребує правових запобіжників. Надмірне домінування логіки закритості може звужувати доступ до суспільно необхідної інформації, тоді як відсутність обґрунтованих обмежень створює загрози для оборони, приватності та критичної інфраструктури [19; 42; 97; 105; 119].

З урахуванням наведених підходів суб'єктну систему доцільно досліджувати як багаторівневу інституційно-мережеву конструкцію. Її вертикальний вимір відображає рівні публічної влади, горизонтальний – взаємодію органів із різною компетенцією, а суспільний – участь недержавних партнерів і громадян. Інтеграція цих вимірів дозволяє уникнути протиставлення ієрархічного управління та мережевої співпраці: вони мають застосовуватися відповідно до характеру завдання.

I. Конституційно-стратегічний рівень	Верховна Рада України; Президент України; Рада національної безпеки і оборони України; Кабінет Міністрів України.
II. Політико-координаційний рівень	Профільне міністерство; урядові координаційні механізми; міжвідомчі робочі групи; Центр протидії дезінформації.
III. Виконавчо-функціональний рівень	Міністерство цифрової трансформації; Міністерство закордонних справ; Держкомтелерадіо; інші центральні органи виконавчої влади.
IV. Регуляторно-гарантійний рівень	Національна рада України з питань телебачення і радіомовлення; Уповноважений Верховної Ради України з прав людини; судові та контрольні механізми.
V. Безпековий і кризовий рівень	Держспецзв'язку; Служба безпеки України; органи сектору безпеки і оборони; спеціалізовані аналітичні центри.
VI. Територіально-суспільний рівень	Місцеві державні та військові адміністрації; органи місцевого самоврядування; суспільні й професійні медіа; громадські, наукові та міжнародні партнери; громадяни.

Рис. 2.1. Рівні системи суб'єктів формування та реалізації державної інформаційної політики

Джерело: розроблено автором.

Подана на рис. 2.1 модель відображає різну природу інституційних ролей. Перші два рівні визначають політичний курс і забезпечують міжвідомче узгодження. Виконавчо-функціональний рівень перетворює стратегічні установки на програми, сервіси та управлінські дії. Регуляторно-гарантійний і безпековий рівні встановлюють межі допустимого втручання, контролюють дотримання правил та реагують на загрози. Територіально-суспільний рівень забезпечує адаптацію загальнодержавних рішень до конкретних аудиторій і повертає до центру інформацію про реальні потреби та наслідки політики.

Таблиця 2.1

Класифікація суб'єктів державної інформаційної політики

Критерій	Основні групи	Аналітичне значення
Правовий статус	Органи державної влади; органи місцевого самоврядування; регулятори; публічні установи; приватні та громадські організації	Дає змогу встановити межі повноважень, юридичні форми діяльності та підзвітність.
Масштаб діяльності	Загальнодержавні; регіональні; місцеві; транснаціональні	Показує просторовий рівень прийняття рішень та охоплення аудиторій.
Характер компетенції	Загальна; галузева; спеціальна; допоміжна	Виявляє центри відповідальності, дублювання і прогалини.
Функціональна роль	Стратегічні; нормотворчі; виконавчі; регуляторні; сервісні; безпекові; контрольні	Дозволяє зіставити організаційну структуру з фактично виконуваними завданнями.
Стадія політичного циклу	Діагностика; проектування; ухвалення; реалізація; моніторинг; коригування	Фіксує зміну ваги суб'єкта залежно від етапу політики.
Тип взаємодії	Ієрархічна; координаційна; договірна; консультативна; мережева	Характеризує спосіб узгодження рішень і обміну ресурсами.
Ресурсний внесок	Правові повноваження; дані; фінанси; технології; експертиза; канали довіри	Пояснює взаємозалежність учасників і необхідність партнерства.

Джерело: систематизовано автором на основі [3; 69; 115; 136; 150; 151].

Класифікація засвідчує, що одна інституція може одночасно належати до кількох груп. Наприклад, центральний орган виконавчої влади є суб'єктом загальнодержавного рівня, виконує галузеві функції, бере участь у проектуванні та реалізації рішень і використовує правові, організаційні та комунікаційні інструменти. Відтак для оцінювання системи важливо аналізувати не назви органів, а їхні ролі в конкретному управлінському процесі. Такий підхід зберігає наукову придатність моделі навіть у разі адміністративних реорганізацій.

Верховна Рада України забезпечує демократичну легітимацію інформаційної політики. Через закони визначаються зміст інформаційних прав, правила доступу до публічної інформації, основи діяльності медіа, режими захисту інформації, засади цифрових комунікацій та межі державного втручання. Парламентські комітети готують законодавчі рішення, організовують консультації, аналізують практику застосування норм і здійснюють контроль за діяльністю виконавчої влади. Ця роль принципово відрізняється від оперативного управління: парламент формує нормативну рамку та перевіряє її суспільну обґрунтованість. [48; 84; 93; 95; 97]

Парламентський контроль має особливе значення в умовах воєнного стану, коли частина інформації обґрунтовано обмежується з міркувань безпеки. Контрольні процедури повинні підтверджувати, що такі обмеження мають законну мету, є необхідними й пропорційними, а також не використовуються для приховування помилок чи уникнення підзвітності. Водночас надмірна публічність окремих відомостей може створювати ризики для оборони, критичної інфраструктури або персональних даних. Отже, парламент виступає інституційним гарантом балансу між відкритістю та захистом.

Президент України у межах конституційних повноважень визначає стратегічні орієнтири національної безпеки, вводить у дію рішення Ради національної безпеки і оборони України та забезпечує політичне узгодження дій у кризових ситуаціях. У сфері інформаційної політики ця роль проявляється передусім через затвердження стратегічних документів, визначення пріоритетів інформаційної безпеки та підтримання єдності державної позиції щодо загроз, які мають міжвідомчий характер. Рада національної безпеки і оборони України функціонує як координаційний центр з питань, що безпосередньо стосуються національної безпеки. Її місце в системі не полягає у підміні міністерств або регуляторів, а в узгодженні оцінок загроз, формуванні стратегічних рішень і визначенні спільних завдань для органів сектору безпеки та цивільних інституцій. При РНБО діє Центр протидії дезінформації, який спеціалізується на моніторингу інформаційного простору, аналітиці та координації протидії деструктивним впливам. [2; 34; 113]

Кабінет Міністрів України забезпечує перехід від стратегічних установок до організованого виконання. Уряд затверджує плани заходів, розподіляє ресурси, визначає завдання центральним органам виконавчої влади та створює міжвідомчі механізми. Для інформаційної політики особливо важливо, щоб урядові рішення містили не лише перелік заходів, а й чітко визначені результати, відповідальних виконавців, строки, джерела даних і процедури оцінювання. Інакше стратегія залишається сукупністю декларацій, а взаємодія залежить від ситуативних домовленостей. [27; 89; 112]

Взаємодія між парламентом, Президентом, РНБО та Кабінетом Міністрів повинна будуватися на функціональному розмежуванні. Законодавець встановлює правила та здійснює контроль, Президент і РНБО забезпечують стратегічне лідерство у безпековій площині, а Уряд організовує реалізацію. Порушення цього розподілу створює два протилежні ризики: надмірну політизацію виконавчих процедур або розпорошення стратегічної відповідальності між багатьма органами.

Таблиця 2.2

Ролі суб'єктів конституційно-стратегічного рівня

Суб'єкт	Ключова роль	Основні інструменти	Очікуваний результат
Верховна Рада України	Нормативне визначення правил і парламентський контроль	Закони, слухання, депутатські запити, бюджетний контроль	Правова визначеність, гарантії прав, підзвітність виконавчої влади
Президент України	Стратегічне політичне лідерство в межах конституційних повноважень	Укази, введення в дію рішень РНБО, публічна стратегічна комунікація	Єдність загальнодержавних пріоритетів
РНБО України	Координація безпекової політики та оцінювання загроз	Рішення, міжвідомча координація, аналітичні механізми	Узгоджене реагування на системні інформаційні загрози
Кабінет Міністрів України	Організація виконання та ресурсне забезпечення	Постанови, розпорядження, плани заходів, державні програми	Перетворення стратегій на спільні дії органів виконавчої влади

Джерело: систематизовано автором на основі [48; 89; 105; 108; 113].

Сильна сторона конституційно-стратегічного рівня полягає у здатності забезпечувати легітимність і загальнодержавну спрямованість політики. Його слабкість проявляється тоді, коли стратегічні документи не супроводжуються робочими процедурами міжвідомчої взаємодії. Тому на наступному рівні вирішальними стають компетентність спеціалізованих органів, сумісність їхніх інформаційних систем і наявність спільного календаря планування.

На центральному виконавчому рівні провідне місце посідає Міністерство культури України як профільний орган у сферах інформаційної безпеки, медіа, інформаційної та видавничої політики. Його системна роль полягає у формуванні пріоритетів, розробленні нормативних пропозицій, координації державних комунікацій, розвитку медіаграмотності та організації виконання відповідних стратегій. Водночас ефективність міністерства залежить від спроможності не концентрувати всі функції, а створювати правила взаємодії між органами з різною спеціалізацією. [29; 30; 36; 115]

Державний комітет телебачення і радіомовлення України реалізує окремі напрями політики у сфері медіа, інформації та видавничої справи. Його практичне значення пов'язане з виконанням адміністративних і галузевих завдань, веденням відповідних реєстраційних та координаційних процедур, взаємодією з підприємствами й установами інформаційної сфери. У системній моделі Держкомтелерадіо доцільно розглядати як виконавчий компонент, функції якого мають бути узгоджені з політико-формувальною роллю профільного міністерства та регуляторними повноваженнями Національної ради.

Міністерство цифрової трансформації України забезпечує технологічну основу сучасної інформаційної політики. Електронні послуги, цифрова ідентифікація, відкриті дані, публічні реєстри, взаємодія інформаційних систем і цифрові канали участі визначають фактичну доступність держави для громадян. Тому Мінцифри є не лише сервісним органом, а співформувачем правил щодо управління державними даними та цифрової комунікації. Його рішення повинні узгоджуватися з вимогами інформаційної безпеки, захисту персональних даних і недискримінаційної доступності. [32; 86; 87; 88; 98; 102]

Міністерство закордонних справ України формує зовнішній вимір інформаційної політики. Воно забезпечує публічну дипломатію, комунікацію з міжнародними аудиторіями, реагування на зовнішні інформаційні кампанії та узгодження позицій України з міжнародними партнерами. У цьому напрямі важливо поєднувати дипломатичну точність із сучасними форматами комунікації, а також забезпечувати єдність повідомлень між закордонними дипломатичними установами, урядовими органами та спеціалізованими центрами стратегічних комунікацій.

Національна рада України з питань телебачення і радіомовлення виконує роль незалежного регулятора у сфері медіа. Її завданням є застосування правил, передбачених законодавством, ведення реєстрів, нагляд за дотриманням вимог, сприяння співрегулюванню та забезпечення прозорого медіасередовища. Незалежність регулятора є принциповою умовою, оскільки поєднання функцій вироблення державної інформаційної позиції та контролю за медіа в одному центрі створювало б конфлікт інтересів.

Уповноважений Верховної Ради України з прав людини виконує гарантійну функцію щодо доступу до інформації та захисту персональних даних. Його участь у системі відрізняється від управлінської або регуляторної: йдеться про незалежний контроль за дотриманням прав людини, реагування на порушення та формування практики, яка обмежує надмірне втручання органів влади. Ця функція особливо важлива під час цифровізації, коли зростають обсяги оброблення даних і ризики непрозорих рішень.

Суспільні медіа України посідають окреме місце між державою та ринком. Вони створені законом, виконують суспільну місію і фінансуються за участю держави, але мають зберігати редакційну незалежність. Їх не слід розглядати як канал урядової агітації. Функція суспільних медіа полягає у забезпеченні універсального доступу до достовірної, збалансованої та суспільно значущої інформації, представленні різних груп і підтриманні публічної дискусії. [95; 109]

Нормативне поле Верховна Рада, Президент, Кабінет Міністрів	Стратегічні цілі РНБО, Уряд, профільне міністерство	Публічна комунікація органи влади, речники, державні установи
Цифрова інфраструктура Мінцифри, реєстри, відкриті дані	КООРДИНАЦІЙНЕ ЯДРО спільне планування, обмін даними, узгодження позицій, відповідальність	Медіарегулювання Національна рада, співрегулювання, професійні стандарти
Інформаційна безпека Держспецзв'язку, ЦПД, сектор безпеки	Територіальна реалізація області, громади, місцеві мережі комунікації	Суспільний контроль медіа, громадськість, наука, громадяни

Рис. 2.2. Функціональна мережа взаємодії ключових суб'єктів

Джерело: розроблено автором.

Рисунок 2.2 демонструє, що виконавчо-функціональний контур не має єдиного центру, здатного самотійно охопити всі завдання. Координаційне ядро повинно поєднувати нормативні рішення, цифрові дані, регуляторну практику, безпекову аналітику та публічну комунікацію. Його змістом є не адміністративне підпорядкування незалежних інституцій, а узгодження планів, термінології, форматів даних і меж відповідальності.

Наведений розподіл показує, що функції формування політики, її виконання, незалежного регулювання, гарантування прав і безпекового реагування не повинні змішуватися. Водночас їх організаційне відокремлення потребує постійних процедур взаємодії. Найбільш проблемними є питання обміну даними, погодження кризових повідомлень, визначення головного виконавця у міжгалузевих проєктах та оцінювання результатів, коли один орган одночасно планує, виконує і звітує про власну діяльність.

Функціональна компетенція ключових державних суб'єктів

Суб'єкт	Основна функція	Типові інструменти	Критична умова ефективності
Міністерство культури України	Формування політики у сферах інформаційної безпеки, медіа та інформації	Стратегії, нормативні пропозиції, координація комунікацій, програми медіаграмотності	Чітке розмежування політичної комунікації та суспільного інформування
Держкомтелерадіо	Реалізація галузевих та адміністративних завдань	Реєстраційні, організаційні, видавничі й координаційні процедури	Узгодженість з міністерством і регулятором
Міністерство цифрової трансформації	Цифрова інфраструктура публічної взаємодії	Е-послуги, реєстри, відкриті дані, електронна ідентифікація	Безпека, сумісність систем і захист даних
Міністерство закордонних справ	Зовнішня комунікація та публічна дипломатія	Дипломатичні канали, міжнародні кампанії, робота із зарубіжними медіа	Єдність повідомлень і адаптація до аудиторій
Національна рада з питань телебачення і радіомовлення	Незалежне регулювання медіа	Реєстрація, нагляд, санкції, співрегулювання, консультації	Інституційна незалежність і прозорість рішень
Уповноважений ВРУ з прав людини	Гарантування інформаційних прав і захисту даних	Моніторинг, реагування, рекомендації, контрольні провадження	Реальна доступність механізмів захисту
Суспільні медіа	Суспільно значуще незалежне інформування	Новини, аналітика, освітній і культурний контент	Редакційна автономія та стабільне фінансування
Держспецзв'язку	Кіберзахист і захист державних інформаційних ресурсів	Стандарти, координація кіберзахисту, спеціальний зв'язок, реагування	Обмін інформацією про інциденти й готовність інфраструктури
Центр протидії дезінформації	Моніторинг, аналіз і координація протидії дезінформації	Аналітичні матеріали, попередження, міжвідомча взаємодія	Верифіковані дані та правова визначеність
Центр стратегічних комунікацій та інформаційної безпеки	Методична й комунікаційна підтримка інформаційної стійкості	Роз'яснення, методики, навчання, інформаційні продукти	Системна взаємодія з комунікаційними підрозділами органів влади

Джерело: систематизовано автором на основі [2; 29; 30; 36; 44; 55; 84; 95; 99; 105; 113].

Безпековий контур є складовою системи державної інформаційної політики, але не поглинає її повністю. Інформаційна безпека охоплює захист інформаційних ресурсів, протидію кібератакам і ворожим інформаційним операціям, збереження стійкості комунікацій та недопущення використання інформаційного простору на шкоду національним інтересам. Водночас загальна інформаційна політика включає також доступ до інформації, розвиток медіа, цифрові послуги та демократичну участь. Зведення всіх завдань до безпеки послаблює права людини і довіру до держави.

Державна служба спеціального зв'язку та захисту інформації України відповідає за організацію захищеного урядового зв'язку, кіберзахист державних інформаційних ресурсів і координацію відповідних заходів. Її роль має інфраструктурний характер: без захищених мереж, резервування, управління вразливостями та обміну інформацією про інциденти неможливі ні цифрові послуги, ні стійка кризова комунікація. Тому вимоги кібербезпеки повинні враховуватися на етапі проєктування інформаційних систем, а не лише після виникнення інциденту.

Служба безпеки України, розвідувальні органи, Міністерство оборони, інші складові сектору безпеки й оборони здійснюють спеціальні функції щодо виявлення та нейтралізації загроз. Їхня діяльність пов'язана з режимною інформацією, оперативними даними й обмеженнями, установленими законом. Для системи інформаційної політики важливо, щоб висновки цих органів своєчасно трансформувалися у рішення цивільних інституцій і зрозумілі публічні повідомлення без розкриття відомостей, здатних зашкодити безпеці.

Центр протидії дезінформації при РНБО та Центр стратегічних комунікацій та інформаційної безпеки виконують взаємодоповнювальні, але не тотожні функції. Перший орієнтований на моніторинг, оцінювання загроз і координацію протидії дезінформаційним впливам. Другий забезпечує роз'яснювальні матеріали, методичну підтримку, навчання та розвиток спроможностей державних комунікацій. Чітке розмежування аналітичної, координаційної та комунікаційної ролей зменшує ризик дублювання і підвищує персональну відповідальність. [2; 36; 37; 45; 113]

Кризове реагування потребує заздалегідь визначеного протоколу. У ньому мають бути зафіксовані джерела первинної верифікації, провідний орган за типом події, строки погодження, уповноважені речники, резервні канали та порядок виправлення помилкових повідомлень. Система, що починає визначати ролі вже після виникнення атаки, неминуче втрачає час. Водночас надмірна централізація може спричинити затримку та одноманітність повідомлень, які не враховують потреби різних аудиторій.

Правовим запобіжником у безпековому контурі має бути принцип пропорційності. Обмеження доступу, блокування ресурсів, оброблення персональних даних або застосування санкцій повинні мати визначену законом підставу, бути необхідними для конкретної мети й підлягати контролю. У демократичній державі ефективність протидії дезінформації не вимірюється кількістю заборон; вона визначається здатністю зменшувати шкоду, зберігаючи свободу вираження поглядів і можливість незалежної перевірки рішень.

На регіональному рівні завдання державної інформаційної політики виконують обласні державні адміністрації, а в умовах воєнного стану - відповідні військові адміністрації та територіальні органи центральних органів виконавчої влади. Вони адаптують загальнодержавні повідомлення до місцевого контексту, координують інформування під час надзвичайних ситуацій, збирають дані про інформаційні потреби населення та забезпечують взаємодію з громадами. Саме тут перевіряється практична придатність рішень, ухвалених на центральному рівні.

Органи місцевого самоврядування є найближчим до громадян елементом системи. Вони інформують про місцеві послуги, бюджетні рішення, безпеку, відновлення, соціальну підтримку та участь у прийнятті рішень. Їхня комунікація не повинна обмежуватися публікацією документів на вебсайті. Необхідно поєднувати відкриті дані, зрозумілі пояснення, консультації, звернення, локальні медіа та офлайн-канали для груп, які мають обмежений цифровий доступ. [81; 84; 88; 158]

Територіальна спроможність є нерівномірною. Великі міста можуть утримувати професійні комунікаційні підрозділи, проводити дослідження аудиторій і розвивати цифрові сервіси, тоді як малим громадам бракує кадрів, техніки та методичної підтримки. Через це однакові нормативні вимоги породжують різну якість виконання. Державна політика має передбачати типові стандарти, навчання, спільні цифрові рішення та можливість міжмуніципальної співпраці, не позбавляючи громади права адаптувати комунікацію до локальних умов.

Центральний рівень	↓ стандарти, дані, ресурси	Уряд, міністерства, регулятори, безпекові органи
Регіональний рівень	↑ координація і адаптація	Обласні державні / військові адміністрації, територіальні органи
Місцевий рівень	↑ сигнали, потреби, оцінка	Органи місцевого самоврядування, комунальні установи, локальні медіа
Суспільний контур	↔ участь і зворотний зв'язок	Громадяни, громадські організації, професійні спільноти, бізнес

Рис. 2.3. Вертикально-горизонтальна взаємодія суб'єктів на територіальному рівні

Джерело: розроблено автором.

Модель на рис. 2.3 передбачає двосторонній рух інформації. З центру надходять правові норми, стандарти, ресурси й підтверджені дані; з територій - сигнали про проблеми, запити аудиторій, локальні ризики та оцінка наслідків. Горизонтальні зв'язки між громадами й регіонами дають змогу швидше поширювати успішні практики та спільно реагувати на інформаційні атаки, що охоплюють кілька територій. За відсутності зворотного зв'язку центральна комунікація стає формальною і втрачає релевантність. Особливої уваги потребує взаємодія місцевої влади з комунальними медіа. Фінансова залежність не повинна перетворювати такі медіа на інструмент персонального просування посадових осіб. Їхня діяльність має відповідати правилам прозорості фінансування, професійним стандартам і чіткому розмежуванню між офіційним повідомленням органу влади та редакційним матеріалом. Це безпосередньо впливає на довіру до локального інформаційного середовища. Професійні медіа виконують у системі дві взаємопов'язані функції: поширюють суспільно значущу інформацію та здійснюють незалежний контроль за владою. Вони не є виконавцями державної політики у владному розумінні, проте є необхідними партнерами для досягнення її демократичних цілей. Держава повинна гарантувати доступ журналістів до інформації, безпеку професійної діяльності та прозорі правила, не втручаючись у редакційні рішення. [82; 84; 95; 101]

Цифрові платформи стали інфраструктурними учасниками інформаційного середовища. Вони визначають видимість контенту, застосовують правила модерації, накопичують дані про поведінку користувачів і впливають на швидкість поширення дезінформації. Національна держава має обмежені можливості одноосібного регулювання таких компаній, тому необхідними є європейські механізми відповідальності платформ, прозорість алгоритмічних рішень та співпраця з регуляторами і дослідниками. [140; 141; 154; 157]

Громадські організації, фактчекінгові ініціативи та професійні об'єднання забезпечують незалежний моніторинг, медіаосвіту, адвокацію прав і роботу з вразливими аудиторіями. Їхня цінність полягає у гнучкості та довірі до окремих спільнот. Водночас партнерство з державою повинно бути прозорим: джерела фінансування, критерії відбору виконавців і очікувані результати мають бути відкритими, щоб співпраця не перетворювалася на приховане делегування політичної комунікації.

Наукові установи й експертні центри формують доказову основу політики. Вони досліджують медіаспоживання, інформаційні ризики, рівень довіри, ефективність кампаній та вплив цифрових технологій. Наукова участь потрібна не лише під час підготовки концепцій, а й для незалежного оцінювання наслідків. Практика, за якої орган сам визначає показники, збирає дані та оцінює власний успіх, створює ризик підтверджувального упередження і приховує невдалі рішення. [149; 150; 151]

Громадяни є не пасивними адресатами, а носіями інформаційних прав і співучасниками політики. Через звернення, запити, петиції, консультації, громадський контроль і створення контенту вони впливають на порядок денний та оцінку рішень. Водночас участь потребує доступної інформації, цифрових навичок і зрозумілих процедур. Коли держава обмежується повідомленням уже прийнятого рішення, зворотний зв'язок перетворюється на формальність.

Міжнародні організації та партнери підтримують гармонізацію законодавства, розвиток інституційної спроможності, обмін даними про транскордонні загрози та професійне навчання. Європейська інтеграція посилює значення стандартів незалежності медіарегулятора, свободи вираження, захисту даних, кіберстійкості й відповідальності платформ. Проте запозичення моделей має враховувати український воєнний контекст і не зводитися до механічного копіювання інституцій.

Таблиця 2.4

Роль недержавних і суспільних учасників у реалізації політики

Група учасників	Основний внесок	Необхідні умови взаємодії з державою
Професійні медіа	Незалежне інформування, перевірка фактів, журналістський контроль	Доступ до інформації, безпека журналістів, невтручання в редакційну політику
Суспільні медіа	Універсальний доступ, збалансоване представлення суспільних інтересів	Редакційна автономія, передбачуване фінансування, публічна підзвітність
Цифрові платформи	Технологічне поширення контенту, модерація, дані про інформаційні потоки	Прозорість правил, співпраця з регуляторами, захист прав користувачів
Громадські та фактчекінгові організації	Моніторинг, просвіта, робота з цільовими групами, незалежні оцінки	Прозорий добір партнерів, відкритість фінансування, відсутність політичного контролю
Наукові й експертні установи	Дослідження, прогнозування, методики та незалежне оцінювання	Доступ до даних, професійна автономія, використання результатів у рішеннях
Громадяни	Визначення потреб, участь, зворотний зв'язок, контроль	Зрозуміла інформація, доступні процедури, цифрова й медійна грамотність
Міжнародні партнери	Стандарти, обмін досвідом, технічна підтримка, транскордонна координація	Урахування національного контексту та чітка відповідальність українських інституцій

Джерело: систематизовано автором на основі [95; 109; 140; 150; 151; 154; 159; 160].

Суспільний контур підвищує якість політики за умови, що участь має процедурний, а не декоративний характер. Консультації повинні проводитися до ухвалення рішення, експертні висновки - супроводжуватися відповіддю органу влади, а дані моніторингу - використовуватися для коригування програм. Такий формат дає змогу поєднати владну відповідальність із розподіленою експертизою та зменшує розрив між офіційним баченням проблеми й досвідом конкретних аудиторій.

Функціональність системи найкраще виявляється через аналіз політичного циклу. На стадії діагностики провідне значення мають статистичні дані, моніторинг медіасередовища, соціологічні дослідження, звернення громадян, сигнали з регіонів і безпекова аналітика. Жодне джерело не є достатнім саме по собі: адміністративні дані показують масштаби процесів, медіамоніторинг - динаміку наративів, а участь громадськості - проблеми, які не відображені в офіційній звітності.

На стадії проєктування рішень необхідне поєднання політичної відповідальності та професійної експертизи. Міністерства готують альтернативи, регулятори оцінюють їх відповідність галузевим правилам, безпекові органи визначають ризики, а громадські й наукові учасники перевіряють пропорційність і можливі побічні наслідки. Відкриті консультації особливо важливі для рішень, що впливають на свободу вираження, доступ до даних або правила роботи медіа.

На стадії ухвалення рішення відповідальність концентрується в органі, наділеному відповідними повноваженнями. Колегіальне обговорення не повинно розмивати персональну відповідальність. У документі мають бути визначені провідний виконавець, співвиконавці, джерела фінансування, інформаційні ресурси, показники та порядок звітування. Відсутність такого розподілу спричиняє ситуацію, коли кілька органів формально відповідають за напрям, але жоден не керує результатом.

Реалізація охоплює правове регулювання, публічну комунікацію, цифрові сервіси, нагляд, навчання, виробництво суспільно значущого контенту та заходи безпеки. Координація повинна відбуватися не лише на рівні керівників, а й між аналітичними, юридичними, технічними та комунікаційними підрозділами. Саме на робочому рівні виявляються несумісність даних, різні визначення показників та суперечливі строки.

Оцінювання завершує один цикл і одночасно розпочинає наступний. Воно має відрізнити виконані дії від суспільних результатів. Кількість публікацій, заходів або створених ресурсів характеризує активність, але не підтверджує зростання довіри, доступності, медіаграмотності чи інформаційної стійкості. До оцінювання доцільно залучати незалежні установи, а результати робити доступними в обсязі, сумісному з вимогами безпеки.

Практичним інструментом розподілу ролей може бути матриця відповідальності, у якій для кожного завдання визначаються суб'єкт, що ухвалює остаточне рішення, безпосередній виконавець, консультовані учасники та отримувачі інформації. Така матриця не замінює законодавства, але робить міжвідомчу взаємодію операційною. Її слід переглядати після зміни компетенцій або виявлення нових ризиків, а не зберігати як формальний додаток до плану.

Першою системною проблемою є фрагментація. Окремі напрями інформаційної політики розвивалися в межах різних секторів - медійного, цифрового, безпекового, зовнішньополітичного та територіального. Це забезпечило професійну спеціалізацію, але не завжди супроводжувалося інтегрованим плануванням. Унаслідок цього органи можуть застосовувати різні поняття, часові горизонти та критерії успіху. Вирішення проблеми потребує спільної рамки цілей і результатів, а не механічного об'єднання установ.

Другою проблемою є поєднання дублювання з компетенційними прогалинами. Декілька інституцій можуть одночасно готувати роз'яснення щодо однієї події, тоді як відповідальність за аналіз довгострокового впливу або роботу з окремою аудиторією залишається невизначеною. Для усунення такого дисбалансу необхідно періодично проводити функціональний аудит: зіставляти нормативні повноваження, фактичні процеси, ресурси та очікувані результати.

Третьою проблемою є домінування реактивної логіки. Під час масштабних інформаційних атак державні інституції вимушені оперативно спростовувати повідомлення, однак постійна концентрація на реакції зменшує ресурси для превентивної комунікації, розвитку медіаграмотності та пояснення політик. Стійка система має працювати на випередження: виявляти інформаційні вразливості, готувати сценарії, формувати довготривалі наративи та регулярно перевіряти готовність каналів.

Четверта проблема полягає у недостатній інтеграції територіального зворотного зв'язку. Центральні органи часто оцінюють успіх за кількістю оприлюднених матеріалів або охопленням, але ці показники не відображають зрозумілість, доступність і довіру в конкретних громадах. Система повинна агрегувати звернення, результати консультацій, локальні опитування та дані про використання сервісів, перетворюючи їх на підставу для коригування змісту й каналів комунікації.

П'ята проблема пов'язана з підзвітністю у відносинах із цифровими платформами та зовнішніми партнерами. Співпраця потрібна для доступу до даних і реагування на транскордонні загрози, але державні органи не повинні передавати приватним компаніям право непрозоро визначати межі допустимого висловлювання. Необхідні документовані процедури, можливість оскарження, захист прав користувачів і публічне пояснення критеріїв взаємодії. [154; 157; 159; 160].

Шоста проблема - слабе розмежування суспільного інформування та політичного просування. Комунікаційні ресурси органів влади мають використовуватися для пояснення рішень, попередження ризиків і забезпечення доступу до послуг, а не для персоналізованої реклами посадових осіб. Інституційним запобіжником є стандарти державної комунікації, прозорість бюджетних витрат, відокремлення офіційних каналів від партійної агітації та незалежний контроль. [81; 101; 103; 151]

За результатами проведеного аналізу систему суб'єктів доцільно оцінювати за сімома параметрами: нормативна визначеність ролей; повнота функціонального покриття; якість горизонтальної координації; сумісність даних і технологій; територіальна спроможність; відкритість до суспільної участі; наявність незалежного контролю й оцінювання. Ці параметри дозволяють перейти від опису організаційної структури до вимірювання її управлінської дієздатності.

Отже, сучасна система суб'єктів формування та реалізації державної інформаційної політики має поліцентричний характер. Її ядро утворюють органи публічної влади, що визначають правила, стратегії та ресурси. Спеціалізовані виконавчі, регуляторні, гарантійні та безпекові інституції забезпечують професійну реалізацію. Територіальні органи адаптують рішення, а медіа, громадськість, наука, цифрові платформи та міжнародні партнери формують середовище участі, експертизи й контролю. Результативність залежить від узгодженості цих ролей, а не від кількості створених органів.

Подальший аналіз інструментів інформаційної взаємодії органів публічної влади з громадянами та медіа повинен спиратися саме на таке розуміння суб'єктної архітектури. Інструмент набуває управлінського змісту лише тоді, коли визначено його власника, цільову аудиторію, джерело даних, правила використання, механізм зворотного зв'язку та критерії результативності. Відповідно, інституційна визначеність є передумовою переходу від фрагментарного інформування до системної державної інформаційної політики.

2.2. Інструменти інформаційної взаємодії органів публічної влади з громадянами та медіа

Практична результативність державної інформаційної політики визначається не лише змістом нормативних актів або наявністю профільних інституцій, а передусім якістю інструментів, через які публічна влада вступає у взаємодію з громадянами та медіа. Саме інструментальний рівень перетворює

стратегічні цілі відкритості, підзвітності, інформаційної стійкості й участі на конкретні процедури: оприлюднення даних, надання відповідей, організацію консультацій, проведення брифінгів, роботу цифрових сервісів, реагування на дезінформацію та вимірювання суспільної реакції. За відсутності належно інтегрованої системи каналів навіть змістовно обґрунтована політика залишається переважно декларативною.

Сучасна інформаційна взаємодія виходить за межі одностороннього інформування. Громадяни дедалі частіше очікують не лише доступу до офіційного повідомлення, а й можливості перевірити його походження, поставити запитання, подати звернення, вплинути на рішення та отримати аргументовану відповідь. Медіа, своєю чергою, виконують подвійну роль: є каналом масового поширення суспільно значущої інформації й незалежним посередником, який перевіряє факти, формує порядок денний і контролює владу. Тому інструменти взаємодії мають одночасно забезпечувати швидкість, точність, правову визначеність, інклюзивність і можливість зворотного зв'язку [84; 93; 95; 101; 137].

В умовах воєнного стану інструментарій взаємодії набуває додаткового безпекового виміру. Публічна влада повинна своєчасно інформувати про ризики, спростовувати маніпуляції та підтримувати суспільну стійкість, але водночас не допускати розголошення відомостей, здатних завдати шкоди обороні, критичній інфраструктурі або персональній безпеці. Отже, актуальним є не механічне максимізування відкритості, а встановлення пропорційного балансу між доступом, захистом і суспільною потребою в достовірному поясненні.

Метою підрозділу є систематизація інструментів інформаційної взаємодії органів публічної влади з громадянами та медіа, оцінювання сучасного стану їх використання на основі кількісних показників 2025–2026 років, визначення диспропорцій між технологічною доступністю та реальною інтерактивністю, а також обґрунтування авторського підходу до формування інтегрованого комунікаційного контуру.

Інструмент інформаційної взаємодії доцільно визначати як нормативно врегульований або організаційно закріплений спосіб створення, передавання,

отримання, обговорення та оцінювання суспільно значущої інформації, що забезпечує комунікаційний зв'язок між суб'єктами публічної влади, громадянами й медіа. У цьому визначенні принципово важливими є три ознаки. По-перше, інструмент не зводиться до технічного каналу, оскільки передбачає процедуру, відповідальність і очікуваний результат. По-друге, взаємодія має включати щонайменше потенційну можливість відповіді. По-третє, результатом є не лише охоплення аудиторії, а зміна рівня поінформованості, довіри, участі або якості управлінського рішення [3; 69; 120; 124].

За функціональним призначенням варто розрізняти інструменти інформування, доступу, сервісної комунікації, участі, медійної взаємодії, кризового реагування, протидії дезінформації та аналітичного зворотного зв'язку. Таке групування є продуктивнішим за перелік окремих платформ, оскільки одна платформа може виконувати кілька функцій. Наприклад, державний портал одночасно оприлюднює інформацію, надає послуги, збирає звернення й формує дані по поведінку користувачів. Водночас одна функція може реалізовуватися через різні канали, що потребує узгоджених стандартів змісту.

Важливим критерієм є рівень цифрової зрілості. Базовий рівень характеризується наявністю вебсторінки та публікацією повідомлень; транзакційний – можливістю подати документ або звернення онлайн; інтерактивний – двосторонньою комунікацією й відстеженням статусу; партисипативний – залученням до підготовки рішень; аналітично адаптивний – використанням даних про реакції громадян для коригування політики. Перехід між рівнями потребує не тільки технологій, а зміни управлінських процедур і професійних компетентностей.

Таблиця 2.4.

Класифікація інструментів інформаційної взаємодії органів публічної влади

Група інструментів	Типові форми	Провідна функція	Ключовий показник результативності
Офіційне інформування	вебсайти, пресрелізи, звіти, офіційні канали	оперативне поширення перевіреної інформації	повнота, своєчасність, охоплення
Доступ до інформації	запити, відкриті дані, публічні реєстри	реалізація права знати й повторне використання даних	частка своєчасних відповідей, якість наборів
Сервісна комунікація	Дія, е-кабінети, чат-боти, контакт-центри	отримання послуг і персоналізованих повідомлень	частка завершених онлайн-взаємодій
Електронна демократія	петиції, консультації, опитування, бюджети участі	залучення громадян до підготовки рішень	частка пропозицій, що отримали мотивовану відповідь
Медійна взаємодія	брифінги, інтерв'ю, акредитація, пресцентри	масове пояснення політики та незалежна перевірка	швидкість надання коментаря, доступ медіа
Соціальні мережі	дописи, прямі ефіри, коментарі, модерація	діалог у реальному часі та сегментація аудиторій	час реагування, частка відповідей, залученість
Кризові комунікації	попередження, сповіщення, кризові штаби, гарячі лінії	зменшення невизначеності й координація поведінки	час першого повідомлення, узгодженість каналів
Протидія дезінформації	спростування, фактчекінг, медіамоніторинг	захист інформаційної стійкості	час виявлення і спростування, повторне охоплення
Аналітичний зворотний зв'язок	CRM, опитування, медіааналітика, дашборди	коригування рішень на основі даних	частка рішень, змінених за результатами аналізу

Джерело: систематизовано автором на основі [29; 55; 84; 88; 95; 101; 115; 137; 150; 151].

Узагальнену архітектуру такої взаємодії подано на рис. 2.4. Її центральним елементом є єдина аналітична основа, що поєднує моніторинг інформаційного середовища, дані про звернення, показники використання цифрових сервісів і медійну реакцію. Без цього комунікація залишається набором розрізнених активностей, які складно оцінити за впливом на рішення та суспільну довіру.

ІНТЕГРОВАНА ЕКОСИСТЕМА ІНФОРМАЦІЙНОЇ ВЗАЄМОДІЇ				
ОРГАНИ ПУБЛІЧНОЇ ВЛАДИ рішення, дані, офіційні повідомлення	→	ЦИФРОВИЙ КОНТУР вебсайти • Дія • е- звернення • відкриті дані	→	ГРОМАДЯНИ отримання інформації, участь, оцінювання
↓		↕		↑
КОМУНІКАЦІЙНИЙ КОНТУР брифінги • пресрелізи • консультації • гарячі лінії	↔	ЄДИНА АНАЛІТИЧНА ОСНОВА моніторинг • CRM звернень • медіааналітика • показники	↔	МЕДІА ТА ГРОМАДСЬКІ ПОСЕРЕДНИКИ перевірка, пояснення, публічний контроль
↑		↕		↓
БЕЗПЕКОВИЙ КОНТУР верифікація • кризові протоколи • захист даних	→	ЗВОРОТНИЙ ЗВ'ЯЗОК відповіді • петиції • опитування • аналітика реакцій	←	ПУБЛІЧНИЙ РЕЗУЛЬТАТ довіра • доступність • підзвітність • участь
ПРИНЦИПИ: законність • достовірність • оперативність • доступність • інклюзивність • двосторонність • безпека				

Рис. 2.4. Інтегрована екосистема інформаційної взаємодії органів публічної влади з громадянами та медіа

Джерело: розроблено автором на основі [55; 115; 137; 150; 151; 158; 159].

Нормативна основа інформаційної взаємодії має багаторівневий характер. Конституційні гарантії свободи думки і слова, права збирати, зберігати, використовувати та поширювати інформацію задають базову рамку [48]. Законодавство про інформацію визначає основні принципи інформаційних відносин, а закон про доступ до публічної інформації встановлює процедури запитів, строки відповідей, обов'язки розпорядників та засади відкритих даних [84; 93]. Для взаємодії з медіа важливими є норми щодо статусу медіа, гарантій професійної діяльності журналістів і порядку висвітлення роботи органів влади [82; 95; 101].

Цифровий контур спирається на законодавство про електронні документи, електронну ідентифікацію, публічні електронні реєстри, Національну програму інформатизації та захист інформації в інформаційно-комунікаційних системах [85; 87; 90; 98; 102]. Сукупність цих актів створює підстави для юридично значущої взаємодії без фізичної присутності особи. Однак нормативна

сумісність ще не означає організаційної інтегрованості: у практиці громадянин нерідко повторно подає дані, які вже містяться в іншому реєстрі, або отримує різні повідомлення від пов'язаних органів.

Право на інформацію не є абсолютним. Захист персональних даних, державної таємниці, критичної інфраструктури та національної безпеки встановлює межі оприлюднення [83; 91; 94; 97]. Проблема полягає у правильному застосуванні принципів необхідності та пропорційності. Надмірне засекречування знижує довіру і створює простір для чуток, тоді як необґрунтоване розкриття може спричинити реальну шкоду. Тому кожен інструмент має містити процедуру правової перевірки, але така перевірка не повинна перетворюватися на механізм необмеженого затягування відповіді [19; 119].

Організаційною передумовою є закріплення відповідального підрозділу та маршруту обробки інформаційного запиту. Комунікаційна служба не може самостійно готувати змістовні відповіді без доступу до профільних даних, а галузевий підрозділ не завжди володіє навичками зрозумілого пояснення. Ефективна модель передбачає розподіл ролей: власник даних відповідає за точність, юридичний підрозділ – за правомірність, комунікаційний – за форму й адаптацію, керівник – за політичну відповідальність, а аналітичний – за оцінювання реакції.

Для медійної взаємодії необхідні прозорі правила акредитації, рівний доступ до суспільно значущих подій, передбачуваний календар брифінгів, реєстр офіційних контактів і протокол надання коментарів. Вибіркове надання інформації лише лояльним редакціям суперечить публічній природі державної комунікації та послаблює конкуренцію інтерпретацій. Водночас у кризових умовах можуть бути обґрунтовані часові або змістові обмеження, якщо вони однаково застосовуються, мають правову підставу й пояснюються медіаспільноті [82; 95; 101].

Нормативно-організаційне забезпечення доцільно оцінювати не за кількістю прийнятих актів, а за наявністю повного циклу: правила оприлюднення, стандарт відповіді, механізм оскарження, облік виконання,

публічна звітність і коригування процедури. Якщо хоча б одна ланка відсутня, інструмент втрачає сталість і залежить від неформальної практики конкретної установи.

Станом на 2025–2026 роки цифрові канали стали основним напрямом розширення взаємодії громадян із державою. За актуальними вимірюваннями, 59% українців користувалися державними послугами онлайн, а 48% отримували їх через застосунок або портал Дія. Порівняно з попереднім роком частка користувачів Дії зросла на 6 відсоткових пунктів, тобто орієнтовно з 42% до 48%. Це свідчить про перехід цифрових сервісів із додаткового каналу до масового інструменту повсякденної взаємодії [29; 32; 55].

Структура популярних послуг показує, що громадяни найактивніше використовують цифрову взаємодію для отримання витягів і довідок з реєстрів та пенсійних послуг – по 15% користувачів. Сервіси для водіїв становили 13%, оформлення субсидій і податкові послуги – по 12%. Отже, найбільший попит формується у сферах, де раніше існувала значна паперова, часова або територіальна складність. Цифровізація тут виконує не лише сервісну, а й інформаційну функцію, оскільки особа отримує персоналізоване повідомлення про статус права або адміністративної процедури.

Водночас цифрова взаємодія залишається нерівномірною територіально. У першому вимірюванні 2025 року середній Індекс цифрової трансформації територіальних громад становив лише 16 балів зі 100. Найвищі результати мали Криворізька громада – 62,97 бала, Вінницька – 62,75, Тернопільська – 60,35, Львівська – 55,61 і Харківська – 54,57. Розрив між середнім значенням і лідерами перевищує 38 балів, що свідчить про значну диференціацію спроможності громад [30; 32; 158].

Окремим показником суспільного потенціалу цифрових інструментів є масовість електронних опитувань. В одному з найбільших загальнодержавних опитувань у застосунку Дія взяли участь понад 2,1 млн користувачів: понад 1,3 млн підтримали один варіант, понад 703 тис. – альтернативний, близько 110 тис. не визначилися. Хоча такі опитування не тотожні юридично врегульованому референдуму або репрезентативному соціологічному дослідженню, вони

демонструють спроможність швидко залучати значну аудиторію та виявляти спектр позицій.

Для відкритих даних на 2025–2027 роки визначено кількісні орієнтири розвитку: приріст переглядів сторінок Єдиного державного вебпорталу відкритих даних на 13% у 2025 році та по 15% у 2026 і 2027 роках; зменшення частки наборів, що не відповідають критеріям якості, на 15% у 2026 році та на 20% у 2027 році. Ці показники важливі тим, що зміщують увагу з формального розміщення наборів до їх доступності, якості та повторного використання [84; 88; 155].

Таблиця 2.5.

Ключові кількісні показники цифрової інформаційної взаємодії в Україні

Показник	Період	Значення	Аналітичне значення
Користування державними послугами онлайн	2025	59% населення, охопленого вимірюванням	онлайн-канал став масовим способом взаємодії
Отримання послуг через Дію	2024 / 2025	42% / 48%	зростання на 6 відсоткових пунктів за рік
Участь у масовому опитуванні в Дії	2023	понад 2,1 млн відповідей	високий потенціал швидкої цифрової мобілізації
Середній Індекс цифрової трансформації громад	I кв. 2025	16 зі 100 балів	низький середній рівень і значна територіальна нерівність
Найвищий індекс громади	I кв. 2025	62,97 бала	лідери перевищують середній рівень майже у 4 рази
Плановий приріст переглядів порталу відкритих даних	2025 / 2026 / 2027	13% / 15% / 15%	орієнтація на фактичне використання даних
Планове зменшення неякісних наборів	2026 / 2027	15% / 20%	перехід від кількості публікацій до стандартів якості

Джерело: узагальнено автором за актуальними офіційними цифровими вимірюваннями 2025–2026 років; аналітична інтерпретація здійснена на основі [29; 30; 32; 55; 84; 88; 98; 151; 158].

Динаміку основних показників користування онлайн-каналами відображено на рис. 2.5. Порівняння показує, що частка користувачів Дії наближається до половини охопленої аудиторії, тоді як загальне користування онлайн-послугами вже перевищило половину. Різниця між 59% і 48% відображає існування інших державних та муніципальних цифрових платформ, однак водночас підтверджує центральну роль Дії як єдиного впізнаваного входу до сервісної держави.

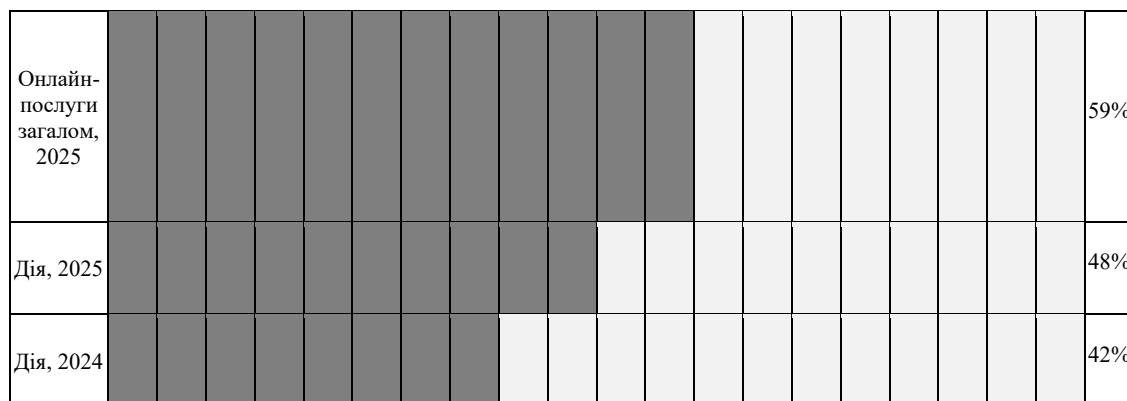


Рис. 2.5. Поширення цифрових каналів взаємодії з державою, %

Джерело: побудовано автором за актуальними вимірюваннями 2024–2025 років; методологічна основа [29; 32; 55; 151].

Сервісна платформа відрізняється від звичайного інформаційного сайту тим, що комунікація завершується адміністративною дією: реєстрацією заяви, отриманням документа, зміною статусу, нарахуванням виплати або підтвердженням права. У такій моделі інформація є складовою послуги, а не окремим продуктом. Користувач повинен розуміти умови, перелік даних, послідовність кроків, строк виконання та причини можливої відмови. Непрозорість будь-якого з цих елементів породжує повторні звернення й знижує довіру навіть за технічно успішної транзакції [29; 98].

Персоналізовані повідомлення мають особливу цінність, оскільки зменшують інформаційну асиметрію між державою та людиною. Повідомлення про строк дії документа, зміну статусу заяви, можливість отримання виплати або необхідність уточнення даних переводить взаємодію з реактивної у проактивну. Водночас персоналізація повинна спиратися на законні підстави обробки даних, принцип мінімізації й можливість користувача контролювати налаштування повідомлень.

Офіційний вебсайт зберігає значення первинного джерела навіть за домінування мобільних застосунків і соціальних мереж. Саме на ньому мають міститися нормативні акти, повні тексти рішень, набори даних, контакти, звіти, архіви повідомлень і порядок оскарження. Соціальний допис повинен вести до повного першоджерела, а не замінювати його. Така модель знижує ризик викидання інформації з контексту та полегшує перевірку для журналістів.

Популярність окремих категорій онлайн-послуг подано в табл. 2.6. Вона показує, що п'ять найбільш затребуваних напрямів формують 67 відсоткових пунктів за сумою часток респондентів. Це не означає, що решта послуг не потрібні, але вказує на доцільність пріоритетного вдосконалення саме тих процесів, які мають найбільше щоденне навантаження і впливають на широкі групи населення.

Таблиця 2.6.

Найпопулярніші категорії державних онлайн-послуг у 2025 році

Категорія послуг	Частка користувачів, %	Інформаційна потреба користувача	Пріоритет удосконалення
Витяги та довідки з реєстрів	15	достовірність запису, статус документа, можливість завантаження	інтероперабельність реєстрів і пояснення реквізитів
Пенсійні послуги	15	право на виплату, розмір, стаж, статус звернення	проактивні повідомлення та доступність для старших груп
Сервіси для водіїв	13	дійсність документа, штрафи, реєстраційні дії	оперативне оновлення та інтеграція даних
Оформлення субсидій	12	критерії права, перелік даних, рішення і причина відмови	зрозуміла мова та супровід складних випадків
Податкові послуги	12	нарахування, строки, борг, підтвердження сплати	єдине повідомлення та узгодження між системами

Джерело: представлено автором за актуальним дослідженням користування онлайн-послугами у 2025 році; інтерпретація на основі [29; 32; 55; 98].

Порівняння свідчить, що сервісний попит концентрується навколо достовірності державних даних і підтвердження індивідуального статусу. Це дає підстави розглядати реєстрову комунікацію як окремий напрям інформаційної політики. Громадянин повинен мати можливість не тільки отримати витяг, а й зрозуміти джерело запису, дату оновлення, відповідальний орган та порядок виправлення помилки. Без такого пояснювального шару цифровізація переносить бюрократичну непрозорість у електронний формат.

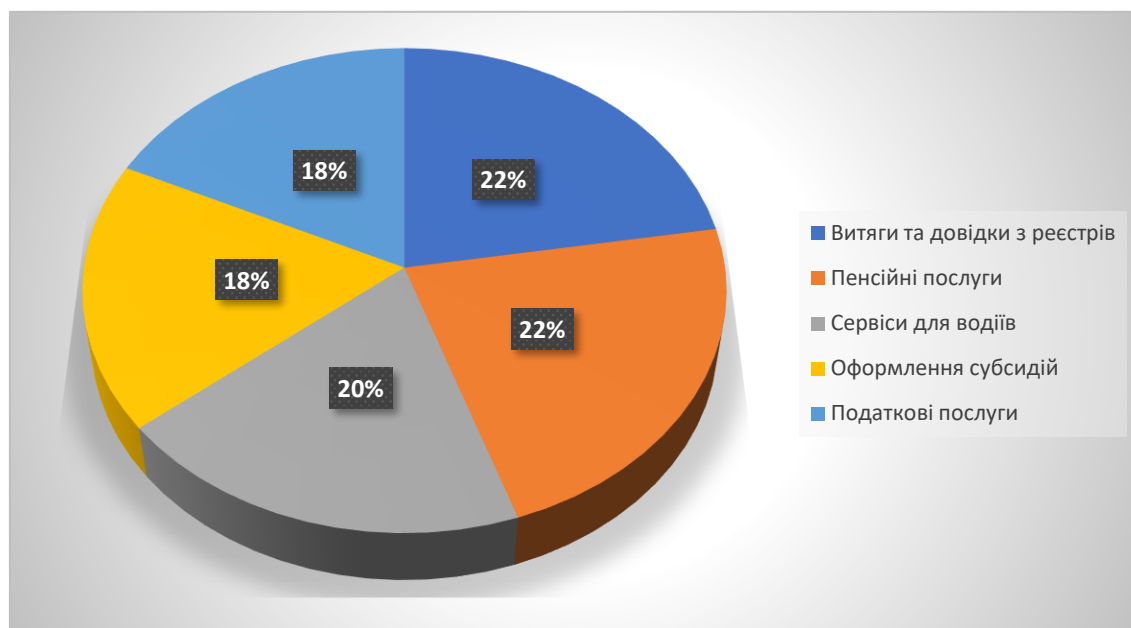


Рис. 2.6. Структура найпопулярніших державних онлайн-послуг у 2025 році, % користувачів

Джерело: побудовано автором; аналітична основа [29; 55; 98].

Відкриті дані є інструментом опосередкованої багатосторонньої взаємодії. Орган влади оприлюднює структурований набір, а громадяни, журналісти, дослідники та бізнес повторно використовують його для аналізу, створення сервісів, виявлення проблем і контролю рішень. На відміну від пресрелізу, дані дають змогу перевірити офіційну інтерпретацію та сформулювати альтернативні висновки. Саме тому якість набору безпосередньо пов'язана з реальністю підзвітності [84; 88; 158].

Найпоширенішими проблемами залишаються несвоєчасне оновлення, різні назви однакових показників, відсутність метаданих, публікація у непридатних для машинного опрацювання форматах і надмірне обмеження доступу з міркувань безпеки. В умовах війни частина наборів обґрунтовано обмежується, однак рішення повинно бути предметним і періодично переглядатися. Суцільне закриття цілих категорій без оцінки конкретного ризику послаблює антикорупційний та управлінський потенціал даних [19; 119].

Запит на публічну інформацію зберігає значення персоналізованого правового інструменту, який компенсує неповноту проактивного оприлюднення.

Якість відповіді слід оцінювати не лише за дотриманням строку, а й за повнотою, зрозумілістю, форматом і можливістю подальшого використання. Пересилання посилання на великий масив документів без вказівки на релевантний фрагмент може формально відповідати процедурі, але фактично не задовольняти інформаційну потребу.

Кількісні цілі розвитку порталу відкритих даних демонструють поступову зміну підходу: очікуване зростання переглядів на 13–15% щороку та зниження частки неякісних наборів на 15–20% мають поєднуватися з вимірюванням фактичного впливу. Важливо відстежувати не тільки перегляди, а завантаження, API-запити, цитування у медіа, створені сервіси, виявлені помилки та рішення, змінені внаслідок аналізу даних [88; 155].

Електронна демократія охоплює інструменти, за допомогою яких громадяни не лише отримують інформацію, а формулюють позицію та беруть участь у підготовці рішень. До них належать електронні петиції, консультації, опитування, громадські обговорення, бюджети участі й цифрові платформи співтворення. Їхня демократична цінність виникає лише тоді, коли процедура пов'язана з мотивованою відповіддю та видимим впливом на управлінський цикл [55; 151].

Публічна консультація є глибшим інструментом, оскільки дозволяє обговорити проблему, варіанти рішення та наслідки. Якісна консультація має містити зрозумілий документ, достатній строк, кілька форматів участі, оприлюднення всіх релевантних пропозицій і звіт про врахування. Поширеною вадою є проведення консультації після фактичного ухвалення політичного рішення, коли участь набуває символічного характеру.

Звернення громадян, гарячі лінії та електронні приймальні формують найбільш деталізований масив повсякденних проблем. Для перетворення звернень на інструмент політики потрібна CRM-система, єдина класифікація тем, контроль повторних звернень і аналітика причин. Показником якості має бути не кількість закритих карток, а частка проблем, вирішених по суті, та кількість процедурних змін, запроваджених після виявлення системної проблеми.

Взаємодія через соціальні мережі потребує окремого стандарту. Доцільно визначати час першої реакції, частку коментарів, що отримали змістовну відповідь, порядок перенаправлення персональних даних у захищений канал, правила модерації та архівування. Видалення критичного коментаря лише через негативну тональність руйнує довіру; водночас мова ворожнечі, розкриття персональних даних або координовані маніпулятивні атаки потребують правомірного обмеження [55; 159].

Медіа забезпечують масштабування офіційної інформації, але не є технічним ретранслятором державних повідомлень. Їхня професійна функція передбачає перевірку, контекстуалізацію, зіставлення позицій і постановку незручних запитань. Тому ефективна взаємодія влади з медіа має ґрунтуватися на доступності першоджерел, рівності редакцій, оперативності коментарів і повазі до редакційної незалежності [82; 95; 109].

Брифінги й пресконференції є інструментами синхронного пояснення. Їх перевага – можливість уточнювальних запитань і публічної відповідальності речника. Для збереження довіри необхідно заздалегідь повідомляти тему, забезпечувати трансляцію й архів, надавати матеріали після заходу та не обмежувати питання лише попередньо погодженим переліком. За кризової ситуації частота брифінгів має відповідати швидкості зміни обставин.

Офіційний коментар повинен надаватися у строк, сумісний з медійним циклом. Відповідь через кілька днів може бути юридично коректною, але інформаційно запізнілою. Доцільно застосовувати дворівневу модель: коротке підтвердження отримання запиту й попереднє фактичне повідомлення, а після перевірки – розгорнутий коментар. Це зменшує інформаційний вакуум і водночас не змушує речника повідомляти неперевірені дані.

В умовах воєнного стану взаємодія з медіа потребує спеціальних протоколів. Обмеження щодо місць зйомки, переміщення військ, наслідків атак або критичної інфраструктури мають бути чіткими, однаково застосовуваними та регулярно оновлюваними. Пояснення логіки обмеження сприяє добровільному дотриманню й зменшує конфлікти. Одночасно державні органи

повинні забезпечувати достатній обсяг перевіреної інформації, щоб безпековий режим не перетворювався на інформаційний вакуум.

Таблиця 2.7.

Інструменти взаємодії з медіа та критерії їх належного застосування

Інструмент	Оптимальна практика	Кількісний індикатор	Ризик неналежного застосування
Пресреліз	факт, дані, документ, контакт, зрозумілі наслідки	частка релізів із посиланням на першоджерело	рекламність, бюрократична мова, неповнота
Офіційний коментар	підтвердження запиту та відповідь у межах медійного циклу	медіанний час першої реакції та повної відповіді	запізнення, шаблонність, уникнення суті
Брифінг / пресконференція	відкриті запитання, трансляція, архів, матеріали	частота, кількість редакцій, частка відповідей по суті	контрольованість, вибірковий доступ
Медіакіт / дата-рум	структуровані дані, хронологія, словник, візуалізації	кількість завантажень і посилань у матеріалах	підміна первинних документів
Медіамоніторинг	виявлення інформаційних розривів і фактичних помилок	час від виявлення помилки до уточнення	оцінювання лояльності та тиск на редакції
Кризовий протокол	єдиний речник, регулярні оновлення, правила безпеки	час першого повідомлення; узгодженість каналів	суперечливі дані або надмірне замовчування

Джерело: розроблено автором на основі [71; 82; 95; 101; 105; 109; 137].

Соціальні мережі й месенджери забезпечують найвищу швидкість поширення, але водночас є середовищем алгоритмічної конкуренції, емоційної поляризації та дезінформації. Офіційна присутність органу влади має бути верифікована, пов'язана з вебсайтом і захищена багатофакторною автентифікацією. Кожен канал повинен мати визначеного адміністратора, резервного відповідального та процедуру дій у разі компрометації акаунта [9; 45; 59].

Кризова комунікація повинна починатися до повного з'ясування всіх обставин. Перше повідомлення може містити підтверджений мінімум: факт події, дії влади, правила безпеки, час наступного оновлення та офіційні канали. Відсутність інформації заповнюється припущеннями, тому чесне позначення невизначеності є кращим за мовчання або надмірно категоричну заяву. Кожне наступне оновлення має фіксувати, що змінилося.

Протидія дезінформації потребує вибору форми реагування. Не кожне неправдиве повідомлення слід повторювати, оскільки спростування може збільшити його охоплення. Реагування доцільне, коли інформація має значне поширення, здатна спричинити шкідливу поведінку або підриває критично важливе рішення. Ефективне спростування спочатку подає правильний факт, потім коротко називає маніпуляцію, пояснює техніку й завершується повторенням перевіреної інформації [18; 35; 150].

Територіальний рівень є критичним для інформаційної взаємодії, оскільки саме громада повідомляє про локальні послуги, безпекові ризики, відновлення інфраструктури, соціальну допомогу й участь у місцевих рішеннях. Загальнодержавна цифрова платформа не може повністю замінити місцевий контент. Водночас громади істотно різняться за кадровими, фінансовими й технічними можливостями, що підтверджується показниками Індексу цифрової трансформації [30; 158].

Результати п'яти громад-лідерів і середнє значення наведено у табл. 2.8 та на рис. 2.7. Порівняння візуалізує не тільки розрив, а й обмеженість абсолютного рівня: найвищий показник становить 62,97 бала. Це обґрунтовує необхідність переходу від рейтингового змагання до програм розвитку конкретних компонентів цифрової спроможності.

Таблиця 2.8.

Результати Індексу цифрової трансформації окремих територіальних громад у 2025 році

Позиція	Територіальна громада	Індекс, балів зі 100	Перевищення середнього рівня, бала
1	Криворізька	62,97	46,97
2	Вінницька	62,75	46,75
3	Тернопільська	60,35	44,35
4	Львівська	55,61	39,61
5	Харківська	54,57	38,57
—	Середнє значення громад	16,00	—

Джерело: узагальнено автором за результатами вимірювання 2025 року; інтерпретація на основі [30; 32; 158].

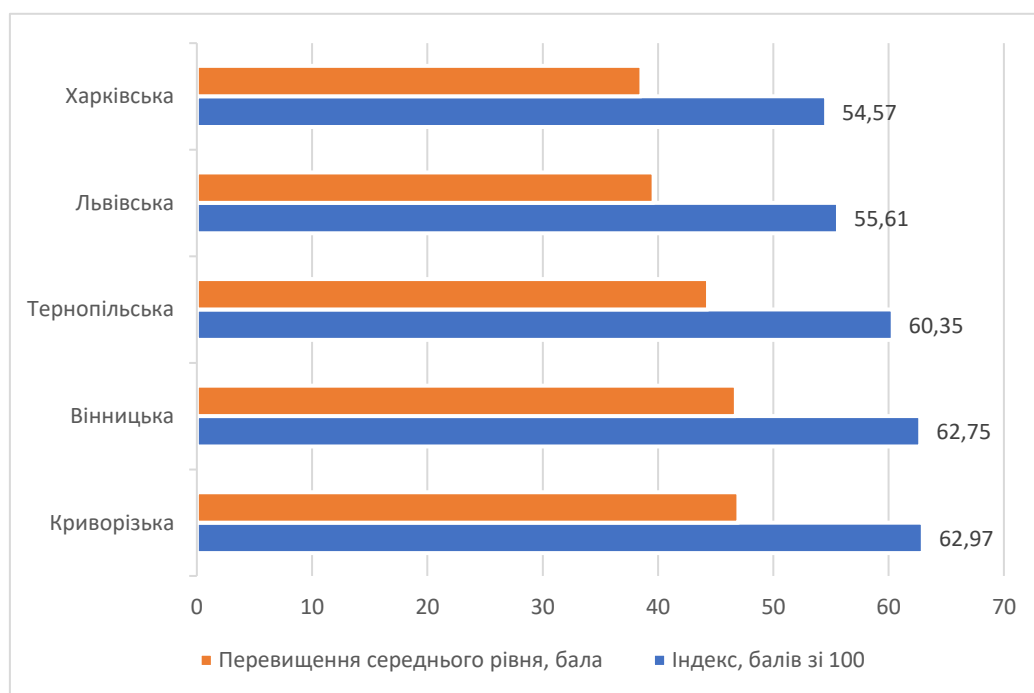


Рис. 2.7. Порівняння Індексу цифрової трансформації громад у 2025 році, балів зі 100

Джерело: побудовано автором; аналітична основа [30; 158].

Графік підтверджує, що диференціація має системний характер. Значення громад-лідерів у 3,4–3,9 раза перевищують середній показник. Якщо не враховувати цю різницю, загальнонаціональні цифрові інструменти можуть формально існувати, але не забезпечувати рівного доступу. Тому оцінювання механізмів державної інформаційної політики повинно містити територіальний коефіцієнт, який відображає реальну спроможність місцевого рівня підтримувати канал, обробляти зворотний зв'язок і захищати дані.

Для комплексної оцінки сучасного стану пропонується п'ятикомпонентна модель зрілості: нормативна визначеність, технологічна доступність, інтерактивність, аналітичність і стійкість. Кожен компонент оцінюється від 1 до 5 балів, де 1 означає фрагментарність, а 5 – системне застосування з публічними стандартами та вимірюванням результату. Така модель не замінює емпіричного аудиту окремого органу, але дозволяє порівнювати типи інструментів.

Першим напрямом удосконалення має стати омніканальність: незалежно від каналу, звернення повинно потрапляти до єдиного обліку, а користувач –

бачити його статус. Другим є стандартизація часу реагування та якості відповіді. Третім – відкриті дашборди, що показують не лише охоплення, а строки, частку вирішених питань, повторні звернення і зміни політики. Четвертим – системна доступність для осіб з інвалідністю, старших людей і користувачів з низькими цифровими навичками.

Узагальнену авторську оцінку наведено в табл. 2.9. Її значення відображають не рейтинг конкретних платформ, а поточний рівень розвитку груп інструментів у системі публічного управління України. Найбільший резерв зосереджений у перетворенні даних про комунікацію на управлінські рішення та в забезпеченні однакового рівня якості між центральними й місцевими органами.

Таблиця 2.9.

Авторська оцінка зрілості основних груп інструментів інформаційної взаємодії, балів від 1 до 5

Група інструментів	Нормативна визначеність	Технологічна доступність	Інтерактивність	Аналітичність	Стійкість	Середній бал
Офіційні вебресурси	4	4	2	3	4	3,4
Сервісні платформи	4	5	3	4	4	4,0
Запити й звернення	5	4	4	3	4	4,0
Відкриті дані	5	3	2	4	3	3,4
Електронна демократія	3	4	4	2	3	3,2
Соціальні мережі	2	5	3	3	2	3,0
Взаємодія з медіа	4	4	4	3	3	3,6
Кризові комунікації	4	4	3	3	4	3,6

Джерело: авторська експертно-аналітична оцінка на основі [29; 30; 55; 71; 84; 88; 95; 105; 115; 150; 151; 158; 159].

Середні значення від 3,0 до 4,0 бала підтверджують проміжний характер сучасного етапу: базова нормативна й технологічна інфраструктура сформована, але діалогічні та аналітичні механізми не досягли однакової інституційної зрілості. Найвищий результат сервісних платформ і систем звернень пояснюється їх процедурною визначеністю та безпосередньою орієнтацією на завершення конкретної дії. Найнижчий результат соціальних мереж відображає залежність від зовнішніх платформ і нестачу єдиних стандартів.

З урахуванням проведеного аналізу інструменти інформаційної взаємодії органів публічної влади з громадянами та медіа пропонується визначати як

взаємопов'язану сукупність правових процедур, організаційних практик, цифрових і традиційних каналів, сервісів, форматів участі та аналітичних засобів, за допомогою яких забезпечуються створення, перевірка, поширення, отримання й обговорення суспільно значущої інформації, фіксується зворотний зв'язок і здійснюється його використання для коригування управлінських рішень за умов дотримання прав людини, безпеки, доступності та підзвітності.

Сучасний стан характеризується поєднанням значних цифрових досягнень і структурних диспропорцій. Позитивними ознаками є користування онлайн-послугами 59% охопленої аудиторії, зростання частки користувачів Дії до 48%, масова участь у цифрових опитуваннях і наявність кількісних цілей розвитку відкритих даних. Проблемними залишаються середній індекс цифрової трансформації громад на рівні 16 зі 100, нерівна інтерактивність каналів, фрагментарна аналітика й недостатня публічність результатів зворотного зв'язку.

Практичне впровадження інтегрованої моделі доцільно розпочинати з формування єдиного реєстру інформаційних контактів. У ньому мають фіксуватися канал надходження звернення, тематична категорія, відповідальний структурний підрозділ, строк першої реакції, дата остаточного вирішення та оцінка користувача. Такий реєстр не підмінює системи електронного документообігу, а створює аналітичний шар, що дає змогу виявляти повторювані проблеми, зіставляти навантаження каналів і контролювати перехід запиту між комунікаційною та управлінською процедурами [55; 84; 93; 102; 151].

Оцінювання результативності потребує переходу від обліку кількості публікацій і підписників до збалансованої системи індикаторів. Її доцільно будувати за п'ятьма групами: охоплення цільових аудиторій; своєчасність повідомлень і відповідей; повнота та зрозумілість змісту; частка звернень, завершених практичним результатом; рівень довіри й задоволеності користувачів. Показники мають розкриватися за каналами, територіями та групами населення, оскільки усереднені значення можуть приховувати цифрову нерівність і бар'єри доступності.

Для взаємодії з медіа необхідно інституціоналізувати стандарт інформаційного супроводу управлінського рішення. Разом із повідомленням мають оприлюднюватися першоджерело, коротке пояснення наслідків, структуровані дані, контакт уповноваженої особи та порядок виправлення неточностей. У кризових ситуаціях цей стандарт доповнюється регламентом регулярних оновлень і чітким розмежуванням підтверджених фактів, попередніх оцінок та інформації, розкриття якої обмежене з міркувань безпеки.

Отже, пріоритетом наступного етапу має бути не просте збільшення кількості каналів, а інтеграція наявних інструментів у єдиний комунікаційний цикл. Для цього необхідні омніканальний облік звернень, стандарти часу та якості відповіді, єдина аналітична основа, доступні формати, прозорі правила взаємодії з медіа, кризові протоколи та публічні показники результативності. Така система дозволить перейти від цифрової присутності до інформаційно відповідального врядування.

2.3. Проблеми забезпечення інформаційної стійкості держави в умовах гібридних загроз

Забезпечення інформаційної стійкості держави належить до найбільш складних завдань сучасного публічного управління, оскільки об'єктом управлінського впливу є не лише захищеність інформаційних ресурсів, а й здатність інституцій, медіасистеми та суспільства функціонувати в умовах тривалого деструктивного впливу. Повномасштабна війна, цифровізація комунікацій, алгоритмічне поширення контенту та трансформація медіаспоживання створюють середовище, у якому інформаційна атака може одночасно впливати на суспільну довіру, процес ухвалення рішень, поведінку окремих груп, міжнародне сприйняття України та стійкість критичної інфраструктури. Саме тому дослідження проблем інформаційної стійкості має виходити за межі вузького розуміння протидії фейкам або технічного захисту інформації.

Гібридна природа сучасних загроз виявляється у поєднанні інформаційно-психологічних операцій, кібератак, маніпулювання фактами, використання справжньої інформації в шкідливому контексті, економічного тиску на медіа, дипломатичного впливу та експлуатації соціальних суперечностей. Відокремлене реагування на кожний із цих компонентів не забезпечує стійкого результату, оскільки противник використовує взаємне підсилення каналів: кібератака створює подію, дезінформаційна кампанія нав'язує її інтерпретацію, мережі координованої поведінки забезпечують масштабування, а дефіцит офіційної інформації підвищує сприйнятливість аудиторії до маніпуляцій [22; 38; 46; 51; 54; 74].

У науковому дискурсі інформаційна стійкість поступово утверджується як динамічна категорія. На відміну від інформаційної безпеки, яка переважно описує стан захищеності інтересів особи, суспільства і держави, стійкість акцентує здатність передбачати загрозу, витримувати її вплив, зберігати критичні функції, швидко відновлюватися та навчатися на основі отриманого досвіду. Такий підхід узгоджується з міжнародними моделями суспільної резильєнтності до дезінформації, принципами інформаційної цілісності та людиноцентричним регулюванням цифрових платформ [42; 105; 146; 159; 160].

У межах цього дослідження під інформаційною стійкістю держави пропонується розуміти інтегральну спроможність системи публічного управління, медіасередовища та суспільства завчасно виявляти й оцінювати гібридні інформаційні загрози, поглинати їхній деструктивний вплив без втрати критичних функцій, забезпечувати узгоджену та правомірну комунікаційну відповідь, відновлювати довіру і якість інформаційного середовища, а також інституціоналізувати отриманий досвід. Авторське визначення поєднує захисний, адаптивний, відновлювальний і навчальний компоненти та передбачає обов'язкове дотримання прав людини [42; 105; 146; 159; 160].

Інформаційна безпека захист інтересів і ресурсів	—	Інформаційна цілісність якість та надійність екосистеми	—	Інформаційна стійкість адаптація та відновлення
---	---	--	---	--

Рис. 2.8. Співвідношення інформаційної безпеки, інформаційної цілісності та інформаційної стійкості держави

Джерело: розроблено автором на основі [42; 69; 105; 146; 159; 160].

Таблиця 2.10.

Наукові підходи до розуміння інформаційної стійкості держави та суміжних категорій

Підхід	Змістовий акцент	Управлінський результат	Релевантні джерела
Безпековий	захист національних інтересів, інформаційних ресурсів і прав особи	зниження ймовірності та масштабу шкідливого впливу	[42; 67; 75; 105]
Інституційний	спроможність суб'єктів діяти узгоджено в межах визначених повноважень	безперервність координації та відповідальності	[30; 34; 37; 44]
Комунікаційний	своєчасна, прозора й доказова взаємодія держави з аудиторіями	збереження довіри та зменшення інформаційного вакууму	[36; 45; 137; 150]
Медіаекосистемний	плюралізм, незалежність медіа, професійні стандарти й доступ до даних	стале виробництво суспільно значущої інформації	[95; 109; 147; 156]
Соціально-когнітивний	медіаграмотність, критичне мислення, опір маніпулятивним наративам	зниження сприйнятливості громадян до дезінформації	[8; 41; 129; 146]
Технологічний	стійкість цифрових платформ, мереж, реєстрів і каналів комунікації	збереження доступності та цілісності інформації	[90; 94; 99; 139]
Адаптивний	поглинання впливу, відновлення, корекція процедур і навчання	перетворення досвіду криз на інституційну спроможність	[146; 150; 159; 160]

Джерело: систематизовано автором за [8; 30; 36; 42; 90; 95; 105; 129; 137; 139; 146; 150; 156; 159; 160].

Порівняння підходів засвідчує, що інформаційна стійкість не може бути забезпечена окремим органом або одним видом інструментів. Вона виникає як системна властивість, коли нормативні правила, інституційна координація, професійна комунікація, незалежне медіасередовище, технологічна надійність і суспільна компетентність діють взаємопов'язано. Наявність слабкої ланки знижує сукупний результат: технічно захищений канал не гарантує довіри до повідомлення, а високий рівень медіаграмотності не компенсує відсутності достовірних даних або затримку офіційної реакції [45; 105; 146; 150; 160].

Проблемність гібридних загроз зумовлена тим, що вони не мають стабільної форми й легко адаптуються до змін політичного порядку денного, технологічного середовища та суспільних настроїв. Їхнім змістом може бути повністю сфабриковане повідомлення, маніпулятивне поєднання справжніх фактів, витік конфіденційних даних, підроблене аудіо або відео, маскування пропагандистського матеріалу під журналістику, псевдоекспертна інтерпретація чи координована кампанія дискредитації. Відповідно, реагування лише на окремий матеріал не усуває мережі його виробництва, мотивацію поширювачів і вразливості цільової аудиторії.

Особливої небезпеки набуває конвергенція інформаційних і кібернетичних операцій. Порушення роботи реєстру, сайту чи телекомунікаційної мережі формує дефіцит перевіреної інформації; одночасно в соціальних мережах поширюється версія, що пояснює збій неспроможністю держави або навмисним приховуванням даних. У такому випадку технічне відновлення системи без комунікаційного супроводу не ліквідує репутаційних наслідків, а спростування без усунення технічної причини не відновлює довіри.

Мережеве середовище змінює масштаб і швидкість гібридного впливу. Алгоритмічна логіка платформ винагороджує контент, що викликає сильні емоції, швидкі реакції та конфліктну взаємодію. Це створює економічні й політичні стимули для виробництва низькоякісної інформації, а також дозволяє невеликій кількості координованих акторів створювати видимість масової підтримки певного наративу. У результаті органи влади змушені реагувати не лише на зміст повідомлення, а й на його мережеву траєкторію, аудиторні сегменти та механізми алгоритмічного підсилення.

1. Джерело	державний або недержавний актор
↓ 2. Контент	фейк, маніпуляція, витік, deepfake
↓ 3. Канал	медіа, платформи, месенджери, кібератака
↓ 4. Вразливість	дефіцит довіри, страх, поляризація
↓ 5. Наслідок	поведінкова зміна, дезорганізація, репутаційна шкода

Рис. 2.9. Ланцюг формування гібридного інформаційного впливу

Джерело: розроблено автором на основі [22; 46; 51; 134; 138; 145; 161].

Класифікація гібридних інформаційних загроз для системи публічного управління

Вид загрози	Типовий механізм	Об'єкт впливу	Основний наслідок для держави
Координована дезінформаційна кампанія	масове повторення неправдивого або маніпулятивного наративу	суспільна думка, довіра до інституцій	спотворення сприйняття рішень і зниження легітимності
Інформаційно-психологічна операція	поєднання страху, тиску, деморалізації та селективного використання фактів	військові, цивільне населення, посадові особи	порушення здатності до раціонального рішення
Кібератака з інформаційним супроводом	порушення доступності ресурсу та нав'язування вигідного пояснення	реєстри, сервіси, канали оповіщення	операційна дезорганізація й репутаційна шкода
Витік або маніпуляція даними	оприлюднення автентичних чи змінених даних поза контекстом	державні органи, посадовці, громадяни	компрометація, правові ризики, недовіра
Синтетичний контент і deepfake	генерування реалістичного аудіовізуального матеріалу	керівництво держави, медіа, кризові повідомлення	ускладнення перевірки та заперечення автентичних доказів
Алгоритмічне підсилення	рекомендаційні системи, мережі ботів і координована неавтентична поведінка	цифрові аудиторії	штучне масштабування радикального або хибного змісту
Дискредитація незалежних медіа	кампанії недовіри, економічний тиск, загрози журналістам	медіаєкосистема	зменшення плюралізму та якості перевірки
Маніпулювання зовнішніми аудиторіями	локалізація наративів під політичні й культурні контексти інших держав	міжнародні партнери та діаспора	послаблення підтримки України та репутаційні втрати
Експлуатація соціальних розколів	посилення конфліктів за мовними, регіональними, політичними чи соціальними ознаками	окремі групи населення	поляризація та зниження суспільної згуртованості

Джерело: узагальнено автором за [21; 22; 38; 46; 51; 54; 74; 118; 123; 134; 138; 143; 145; 157; 161].

Класифікація показує, що об'єктом гібридного впливу дедалі частіше є не окремий інформаційний ресурс, а здатність держави визначати порядок денний, пояснювати рішення та підтримувати єдине розуміння критичної ситуації. Це вимагає переходу від моделі реакції на контент до моделі управління ризиком, у якій аналізуються суб'єкт, намір, канал, аудиторна вразливість, можливий каскад наслідків і правові межі втручання.

Україна сформувала розгалужену нормативну основу інформаційної безпеки, що охоплює національну безпеку, кібербезпеку, медіа, захист

інформації, критичну інфраструктуру, персональні дані, доступ до інформації та стратегічні комунікації. Водночас значна кількість актів не автоматично утворює цілісну систему стійкості. Документи відрізняються за термінологією, об'єктами регулювання, суб'єктами виконання, часовими горизонтами та наборами індикаторів, що ускладнює координацію і створює дублювання функцій.

Окремою проблемою у 2026 році є часовий розрив між рамковою Стратегією інформаційної безпеки та операційним плануванням: план заходів, затверджений у 2023 році, був розрахований на період до 2025 року. За відсутності безперервного циклу оновлення показників, відповідальних виконавців і ресурсного забезпечення стратегічний документ ризикує виконувати переважно декларативну функцію. Гібридні загрози змінюються швидше, ніж традиційний цикл державного планування, тому щорічне коригування ризиків має бути вбудованою процедурою, а не разовою реакцією [89; 105; 115].

Удосконалення нормативної основи має відбуватися без необґрунтованого розширення обмежень свободи вираження поглядів. Під час війни держава має легітимний обов'язок захищати національну безпеку, однак будь-яке обмеження інформаційних прав повинно бути передбачене законом, переслідувати визначену мету, бути необхідним і пропорційним. Нечіткі формулювання щодо шкідливого контенту або надмірно широкі повноваження можуть створювати ризик вибіркового застосування, знижувати довіру та послаблювати саме ту стійкість, яку покликані захищати [7; 19; 43; 48; 79; 119; 130; 131].

Інституційна архітектура інформаційної політики включає органи сектору безпеки і оборони, центральні органи виконавчої влади, регуляторів, правоохоронні органи, органи місцевого самоврядування, суспільні та приватні медіа, громадські організації, дослідницькі центри й цифрові платформи. Така багатосуб'єктність відповідає складності проблеми, проте створює ризики дублювання моніторингу, конкуренції за повноваження, несумісності інформаційних систем і різних стандартів оцінки загроз [2; 30; 34; 37; 44; 77; 113].

Критичним недоліком є відсутність стабільного міжвідомчого циклу, який поєднує раннє попередження, верифікацію, правову кваліфікацію, вибір аудиторій, підготовку єдиної позиції, розподіл спікерів та оцінювання ефекту. На практиці кожний орган здатен реагувати в межах власної компетенції, але складна кампанія потребує синхронізації часових рішень. Запізнення одного суб'єкта може нівелювати оперативність інших, а суперечливі формулювання створюють додатковий матеріал для маніпуляції.

Таблиця 2.12.

Системні проблеми забезпечення інформаційної стійкості держави

Проблема	Коренева причина	Наслідок	Першочерговий напрям реагування
Нормативна фрагментарність	розбіжність термінів, цілей і часових горизонтів документів	неузгоджені рішення та формальне виконання заходів	єдина рамка стійкості й щорічне оновлення ризиків
Часовий розрив планування	операційний план завершився раніше, ніж рамкова стратегія	втрата безперервності цілей, індикаторів і відповідальності	новий середньостроковий план із річними циклами
Розпорошеність повноважень	дублювання моніторингу та відсутність єдиного протоколу	затримка або суперечливість реагування	міжвідомчий координаційний контур і матриця ролей
Реактивність комунікацій	відповідь після масштабування наративу	інформаційний вакуум і втрата порядку денного	сценарне планування та випереджальне інформування
Платформна залежність	обмежений доступ до алгоритмічних і рекламних даних	неможливість оцінити походження та масштаби кампанії	прозорість платформ і доступ дослідників до даних
Вразливість медіа	економічна нестабільність, тиск, дефіцит локального контенту	звуження плюралізму й перевірки інформації	підтримка незалежності та суспільно значущих медіа
Нерівність спроможностей громад	дефіцит кадрів, резервних каналів і стандартів	локальні інформаційні вакууми	типові протоколи, навчання і міжмуніципальна підтримка
Низька вимірюваність результатів	перевага показників кількості повідомлень над показниками впливу	неможливість навчання та корекції політики	інтегральний індекс і незалежне оцінювання
Ризик надмірних обмежень	нечіткі критерії шкідливого контенту	правова невизначеність і падіння довіри	тести законності, необхідності та пропорційності
Кадрове виснаження	тривала кризова робота, ротація, дефіцит аналітиків	втрата інституційної пам'яті та помилки	резервні команди, стандарти й психологічна підтримка

Джерело: розроблено автором на основі [2; 16; 30; 36; 37; 44; 45; 55; 89; 105; 119; 137; 150; 158; 160].

Систематизація проблем підтверджує, що більшість із них має міжсекторальний характер. Наприклад, платформна залежність одночасно є технологічною, правовою, аналітичною та комунікаційною проблемою;

вразливість локальних медіа має економічний вимір, але безпосередньо впливає на здатність громад протистояти чуткам; надмірне обмеження інформації може зменшити короткостроковий ризик витоку, проте збільшити довгостроковий дефіцит довіри. Отже, державна політика має оцінювати не лише прямий ефект окремого рішення, а й його системні побічні наслідки [42; 95; 119; 150; 159].

Однією з центральних проблем є переважання реактивної моделі комунікації. Органи влади часто починають публічне спростування після того, як маніпулятивний наратив уже отримав значне охоплення, був адаптований до різних платформ і закріпився в емоційному сприйнятті аудиторії. За таких умов спростування змушене повторювати хибне твердження, а отже частково сприяє його впізнаваності. Більш стійкою є модель превентивного пояснення, коли держава завчасно комунікує очікувані ризики, процедури та критерії рішень.

Реактивність пов'язана з повільним погодженням інформації, страхом посадових осіб помилитися, недостатнім доступом комунікаційних підрозділів до первинних даних та відсутністю підготовлених сценаріїв. У кризі швидкість не повинна протиставлятися точності: стійка система використовує двоетапну комунікацію – оперативне підтвердження факту події та наступне деталізоване повідомлення після верифікації. Мовчання або формула про відсутність коментарів без пояснення процесу створює інформаційний вакуум.

Недостатньою є сегментація аудиторій. Єдине повідомлення не може однаково ефективно працювати для мешканців прифронтової громади, внутрішньо переміщених осіб, міжнародних партнерів, молоді, старших людей, журналістів і професійних спільнот. Ворожі кампанії, навпаки, дедалі частіше використовують локалізовані меседжі, що враховують страхи й інформаційні звички конкретної групи. Тому стійкість потребує карти аудиторій, перевірки зрозумілості повідомлень і використання довірених посередників [25; 45; 145; 150].

Проблемою залишається й недостатня оцінка результативності. Кількість пресрелізів, публікацій або переглядів не показує, чи змінилося розуміння ситуації, чи зросла довіра та чи зменшилася готовність поширювати неперевірену інформацію. Показники повинні охоплювати швидкість першої

реакції, частку виправлених помилкових уявлень, сталість ключового повідомлення між інституціями, доступність для різних груп і рівень відновлення довіри після кризи [45; 150; 151; 160].

Значна частина публічної комунікації відбувається на приватних цифрових платформах, правила функціонування яких визначаються корпоративними політиками та алгоритмами. Держава не контролює порядок рекомендації контенту, має обмежений доступ до даних про координовану поведінку й залежить від процедур модерації, що можуть застосовуватися нерівномірно до різних мов і контекстів. Це перетворює платформну залежність на структурну проблему інформаційної стійкості.

Поширення генеративного штучного інтелекту знижує вартість створення переконливого синтетичного контенту, автоматизованого перекладу та персоналізації маніпулятивних повідомлень. Deepfake створює подвійний ризик: дозволяє підробляти заяви та одночасно дає можливість заперечувати автентичні матеріали як нібито згенеровані. За відсутності надійної системи підтвердження офіційних повідомлень це може вплинути на кризове оповіщення, дипломатичні комунікації та довіру до доказів [157; 160].

Управлінська відповідь має включати резервні офіційні канали, цифрове маркування та верифікацію автентичних матеріалів, протоколи швидкого спростування підробок, підготовку журналістів і державних службовців, а також стандарти збереження доказів координованої кампанії. Важливо, щоб технічні засоби перевірки не створювали ілюзії абсолютної надійності: стійкість забезпечується поєднанням технологій, авторитету джерела, узгодженості повідомлень і попередньо сформованої довіри.

Інформаційна стійкість неможлива без незалежної, професійної та економічно життєздатної медіаекосистеми. Медіа виконують функцію перевірки офіційних тверджень, пояснення складних рішень, представлення різних позицій і виявлення маніпуляцій. Якщо журналістика послаблена фінансово, кадрово або політично, суспільство стає більш залежним від неформальних каналів і платформних рекомендацій, де стандарти достовірності є нижчими.

Особливо вразливими є локальні медіа, які працюють найближче до громад, але мають обмежені доходи та людські ресурси. Зникнення місцевого джерела перевіреної інформації створює інформаційні пустелі, у яких чутки та анонімні канали отримують статус фактичного монополіста. Підтримка таких медіа повинна бути прозорою, конкурентною та захищеною від впливу органів влади на редакційну політику [95; 109; 156; 159].

Державна підтримка інформаційної стійкості не повинна перетворюватися на заміщення незалежної журналістики офіційною комунікацією. Влада повідомляє про свої рішення й не може виконувати функцію зовнішнього контролю за собою. Тому стійка модель передбачає відкритий доступ журналістів до даних, регулярні брифінги, захист професійної діяльності, прозорість власності та фінансування медіа, а також незалежне суспільне мовлення.

Суспільна стійкість до дезінформації формується не лише знанням окремих способів перевірки фактів. Вона залежить від довіри до інституцій, якості освіти, політичної поляризації, соціально-економічної стабільності, доступності незалежних медіа та звички громадян брати участь у публічному обговоренні. За високої недовіри навіть достовірне офіційне повідомлення може бути відхилене, а контент, що підтверджує попередні переконання, поширюється без перевірки.

Нерівність медіаграмотності має віковий, освітній, територіальний і цифровий виміри. Частина громадян не має стабільного доступу до якісного інтернету, не використовує офіційні сервіси або покладається на вузьке коло джерел. Діти та молодь стикаються з ризиками алгоритмічно сформованого контенту, тоді як старші групи можуть бути вразливими до пересилання повідомлень у закритих месенджерах. Універсальна кампанія не усуває цих відмінностей.

Медіаосвіта повинна перейти від одноразових тренінгів до системи безперервного навчання, що охоплює школи, заклади вищої освіти, державну службу, громади та професійні спільноти. Її зміст має включати не лише виявлення фейків, а й розуміння алгоритмічної логіки платформ, рекламних

моделей, методів психологічного впливу, правил захисту персональних даних і відповідального поширення інформації під час криз.

Цифрова держава залежить від безперервної роботи реєстрів, телекомунікаційних мереж, систем електронної ідентифікації, державних вебресурсів і каналів оповіщення. Порушення доступності або цілісності цих систем має не лише технічний, а й інформаційно-психологічний ефект. Громадяни, які не можуть отримати послугу або перевірити дані, швидше сприймають чутки про масштаб проблеми, а противник використовує збій як доказ неспроможності держави [11; 16; 90; 94; 99; 106].

Особливо небезпечною є маніпуляція даними. Якщо інформація в реєстрі змінена непомітно, наслідки можуть бути тривалими й проявитися пізніше у вигляді помилкових управлінських рішень, порушення прав громадян або компрометації офіційної статистики. Тому стійкість вимагає не лише резервного копіювання, а й контролю походження даних, журналювання змін, незалежної верифікації та комунікації щодо відновлення цілісності.

Захист критичної інфраструктури має включати комунікаційний план на випадок перебоїв. Технічні команди повинні заздалегідь визначити, які повідомлення можна оприлюднювати без шкоди для безпеки, хто є уповноваженим спікером, які резервні канали використовуються та як громадяни можуть перевірити справжність інструкції. Інакше навіть правильно локалізована кібератака може спричинити масштабну паніку або поширення небезпечних рекомендацій.

Умови воєнного стану об'єктивно потребують обмеження доступу до окремих відомостей, захисту військової таємниці, персональних даних і критичної інфраструктури. Проте стійкість держави залежить від того, наскільки такі обмеження є зрозумілими, передбачуваними та підконтрольними. Невмотивоване приховування інформації або нерівномірне застосування правил може стимулювати припущення, недовіру та альтернативні неофіційні версії [19; 83; 84; 91; 119].

Пропорційність має оцінюватися за чотирма питаннями: чи передбачене обмеження законом; чи переслідує легітимну мету; чи існує менш

обмежувальний засіб; чи співмірна суспільна користь із шкодою для права. Важливо розрізняти інформацію, оприлюднення якої реально створює оперативний ризик, і дані, приховування яких лише зменшує підзвітність органу влади.

Боротьба з дезінформацією не повинна спиратися на оцінювання політичної зручності висловлювання. Предметом державного реагування мають бути встановлені правопорушення, координована ворожа діяльність, маніпуляція платформними механізмами, незаконне використання даних або реальна загроза національній безпеці. Критика державного рішення, навіть різка або помилкова, не тотожна ворожій операції [35; 63; 64; 130].

Відкритість сама по собі є інструментом стійкості, оскільки зменшує простір для спекуляцій і дозволяє журналістам, дослідникам та громадськості перевіряти офіційні твердження. Водночас відкриті дані потребують оцінювання ризику повторної ідентифікації, поєднання наборів і використання ворожими суб'єктами. Отже, політика має поєднувати принцип максимальної відкритості з ризик-орієнтованим захистом чутливої інформації.

Оцінювання інформаційної стійкості часто зводиться до переліку проведених заходів: кількості спростувань, публікацій, тренінгів або заблокованих ресурсів. Такі показники відображають активність, але не доводять зміну суспільної сприйнятливості, якості координації чи швидкості відновлення після інциденту. Необхідний перехід до результативних індикаторів, які вимірюють стан системи до загрози, перебіг реагування та наслідки після завершення гострої фази.

Ключовим є інституціоналізоване навчання. Після значної інформаційної атаки має проводитися міжвідомчий розбір, що фіксує часову шкалу подій, рішення, використані дані, координаційні розриви, ефективні формулювання та помилки. Результатом повинно бути оновлення протоколу, навчальних матеріалів і сценаріїв, а не лише звіт про виконані дії.

Відсутність незалежного оцінювання створює ризик самооцінки за зручними критеріями. До аналізу стійкості доцільно залучати наукові установи, професійні медійні організації, громадянське суспільство та представників

громад. Багатосторонній підхід підвищує якість даних і зменшує ризик використання безпекової риторики для приховування проблем [159; 160].

Таблиця 2.13.

Авторська матриця залишкового ризику гібридних інформаційних загроз

Загроза	Імовіріс ть Р 1–5	Вплив І 1–5	Вразливіс ть V 1–5	R, %	Рівень
Координовані дезінформаційні кампанії	5	5	4	80.0	дуже високий
Алгоритмічне підсилення маніпуляцій	5	4	4	64.0	високий
Синтетичний контент і deepfake	4	4	5	64.0	високий
Дискредитація медіа та інституцій	5	4	4	64.0	високий
Кібератаки на комунікаційні канали	4	5	4	64.0	високий
Локальні інформаційні вакууми	4	4	4	51.2	високий
Кадрове виснаження комунікаційних команд	4	4	4	51.2	високий
Маніпуляція зовнішніми аудиторіями	5	4	3	48.0	середній
Витік або підміна даних	4	5	3	48.0	середній
Надмірні обмеження інформаційних прав	3	4	3	28.8	помірний

Примітка: $R = P \times I \times V / 125 \times 100$. Оцінка є авторською діагностичною моделлю, а не офіційною статистикою. Джерело: розроблено автором на основі [37; 45; 105; 146; 150; 159; 160].

Авторська матриця показує, що найвищий залишковий ризик формують координовані дезінформаційні кампанії, оскільки вони поєднують високу ймовірність, значний суспільний вплив і наявні інституційні вразливості. До групи високого ризику також належать алгоритмічне підсилення, синтетичний контент, дискредитація медіа та кібератаки на комунікаційні канали. Методика не претендує на заміну емпіричного моніторингу, але дозволяє порівнювати різні загрози за єдиною логікою й визначати пріоритети розподілу ресурсів [37; 146; 150].

Міжнародні підходи дедалі частіше розглядають дезінформацію не як ізольовану проблему контенту, а як порушення інформаційної цілісності. Глобальні принципи ООН поєднують суспільну довіру і стійкість, незалежні медіа, прозорість, відповідальні стимули та можливість дослідження інформаційного середовища. Така модель важлива для України, оскільки

проти дія ворожого впливу повинна зміцнювати демократичні інститути, а не звужувати їх [160].

Рекомендації OECD наголошують на інституціоналізації публічної комунікації, прозорості, своєчасності, координації, професійних стандартах, розумінні аудиторій і регулярному оцінюванні. Їхня цінність полягає в переході від разових інформаційних кампаній до сталої управлінської функції. Для України особливо релевантними є стандарти раннього попередження, міжвідомчої взаємодії та відокремлення публічної комунікації від політичного маркетингу [150; 151].

Право Європейського Союзу формує взаємодоповнювальний контур: NIS2 посилює кіберризик-менеджмент; Digital Services Act встановлює обов'язки щодо системних ризиків платформ; European Media Freedom Act захищає медіаплюралізм та редакційну незалежність; Artificial Intelligence Act вводить ризик-орієнтовані правила щодо ШІ. Адаптація цих підходів має враховувати інституційну спроможність України та уникати механічного перенесення процедур [139; 154; 156; 157].

Зарубіжний досвід протидії дезінформації підтверджує, що стійкість не створюється лише централізованою державною структурою. Необхідні мережі співпраці між органами влади, платформами, медіа, дослідниками, освітніми установами та громадянським суспільством. Водночас держава зберігає відповідальність за правові гарантії, координацію, захист критичних функцій і доступ громадян до достовірної інформації.

Для подолання виявлених проблем пропонується оцінювати інформаційну стійкість як цикл із семи взаємопов'язаних стадій: передбачення, виявлення, верифікація, координація, відповідь, відновлення та навчання. Порушення будь-якої стадії збільшує залишковий ризик. Наприклад, якісне виявлення без узгодженої відповіді не зменшує охоплення загрози, а швидка відповідь без подальшого навчання призводить до повторення помилок.

Передбачення охоплює сценарний аналіз, моніторинг вразливостей і підготовку аудиторій; виявлення – технічний і змістовий моніторинг; верифікація – перевірку фактів, джерел і масштабу; координація – розподіл

ролей та узгодження позицій; відповідь – комунікаційні, правові, технічні й дипломатичні заходи; відновлення – повернення доступності каналів і суспільної довіри; навчання – оновлення протоколів і підготовки персоналу [45; 105; 150; 160].

Циклічна модель відрізняється від лінійного реагування тим, що результат кожної кризи стає вхідними даними для наступного етапу передбачення. Вона також дозволяє розмежувати короткострокові та довгострокові цілі: спростування може зупинити конкретний наратив, але довгострокова стійкість потребує зміцнення медіа, довіри, освіти та платформної підзвітності.

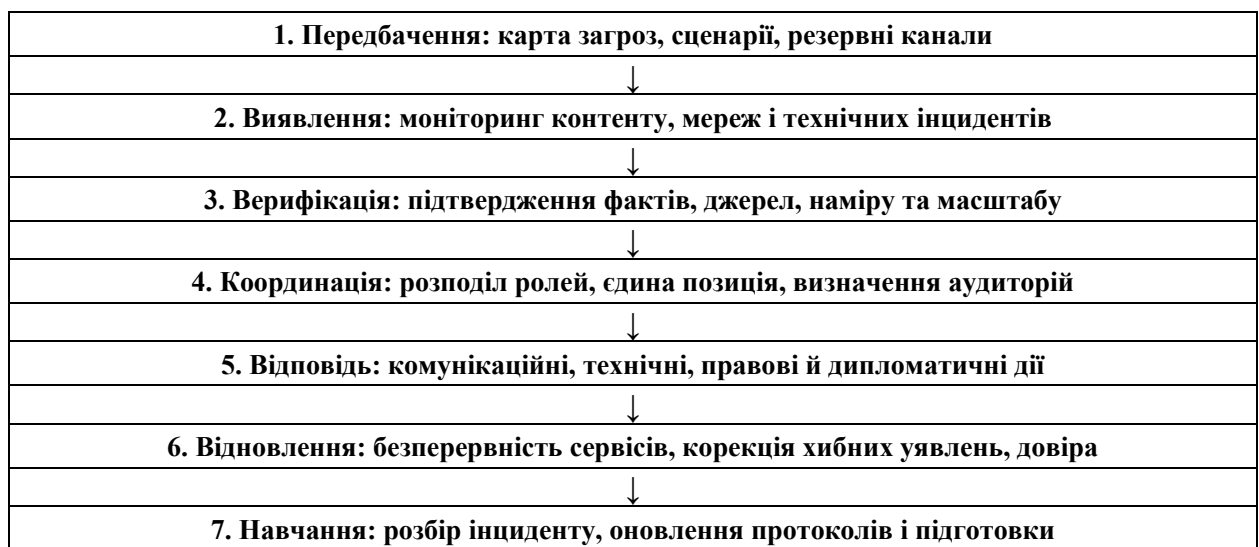


Рис. 2.10. Авторський цикл забезпечення інформаційної стійкості держави

Джерело: розроблено автором на основі [37; 45; 105; 146; 150; 160].

Для інтегрального оцінювання пропонується використовувати вісім вимірів зі встановленими вагами. Нормоване значення кожного виміру z_j визначається у межах від 0 до 100 балів, після чого інтегральний індекс розраховується за формулою $I_{\text{ст}} = \sum w_j \times z_j$, де w_j – ваговий коефіцієнт, сума яких дорівнює одиниці. Такий індекс не замінює аналіз окремих ризиків, але дозволяє порівнювати динаміку, регіони або інституції за однаковою методикою.

Таблиця 2.14.

Система вимірів авторського індексу інформаційної стійкості держави

Вимір	Вага, %	Приклади індикаторів	Ключове джерело даних
Стратегічне врядування і координація	15	наявність актуального плану; час міжвідомчого погодження; чіткість ролей	аудит документів і протоколів
Моніторинг та раннє попередження	15	час виявлення; охоплення платформ; частка загроз із підтвердженим походженням	моніторингові системи та звіти інцидентів
Публічна і кризова комунікація	15	час першої реакції; узгодженість повідомлень; доступність для аудиторій	контент-аналіз, опитування, журнали реагування
Стійкість медіаекосистеми	15	плюралізм; економічна життєздатність локальних медіа; доступ журналістів до даних	медіамоніторинг і галузеві дослідження
Платформна та алгоритмічна підзвітність	10	доступ до даних; прозорість реклами; швидкість взаємодії з платформами	звіти платформ, регулятора і дослідників
Суспільна стійкість і медіаграмотність	15	довіра до перевірених джерел; здатність розпізнавати маніпуляції; відповідальне поширення	репрезентативні опитування й освітні вимірювання
Кібер- та інфраструктурна стійкість	10	безперервність каналів; резервування; час відновлення; цілісність даних	технічні аудити та звіти про інциденти
Права людини та інклюзивність	5	правова визначеність обмежень; доступність інформації; механізми оскарження	правовий аудит і моніторинг доступності

Джерело: розроблено автором на основі [42; 45; 70; 105; 119; 139; 146; 150; 156; 159; 160].

Запропонована система дає змогу виявити ситуацію, коли високі технічні показники маскують слабку довіру або недостатню правову визначеність. Інтегральне значення слід доповнювати профілем вимірів: два суб'єкти з однаковим підсумковим балом можуть мати різні вразливості й потребувати різних управлінських рішень. Для забезпечення достовірності методика повинна передбачати відкритий опис індикаторів, незалежну перевірку та регулярне оновлення ваг з урахуванням зміни загроз.

Проведений аналіз свідчить, що головна проблема забезпечення інформаційної стійкості полягає не у відсутності окремих інструментів, а в недостатній інтегрованості нормативних, інституційних, технологічних, медійних і соціальних компонентів. Україна має значний досвід протидії

інформаційній агресії, створені спеціалізовані інституції та розвинене громадянське суспільство, однак система залишається вразливою до часових розривів планування, дублювання функцій, реактивної комунікації, платформної непрозорості та нерівності місцевих спроможностей.

Гібридні загрози вимагають поєднання чотирьох логік державної політики. Захисна логіка зменшує можливість проникнення та масштабування впливу; адаптивна – забезпечує безперервність функцій; відновлювальна – повертає якість інформаційного середовища й довіру; трансформаційна – усуває структурні вразливості через реформу інституцій, підтримку медіа, освіту та платформну підзвітність. Перевага лише однієї логіки створює тимчасовий, але нестійкий результат.

Пріоритетами мають стати оновлення стратегічного й операційного планування після завершення періоду дії плану до 2025 року; запровадження постійного міжвідомчого циклу раннього попередження та реагування; професіоналізація публічної комунікації; інтеграція кібербезпеки з кризовими комунікаціями; захист незалежних і локальних медіа; розвиток медіаграмотності; формування механізмів прозорості платформ та оцінювання впливу ІІІ.

Отже, інформаційна стійкість демократичної держави має поєднувати безпекову спроможність із правовою пропорційністю, відкритістю та підзвітністю. Запропоновані авторське визначення, матриця залишкового ризику, цикл реагування й індекс із восьми вимірів утворюють методичну основу для подальшого обґрунтування механізмів удосконалення державної інформаційної політики.

Висновки до розділу 2

Встановлено, що система суб'єктів формування та реалізації державної інформаційної політики має поліцентричний і міжгалузевий характер. Її ядро утворюють Верховна Рада України, Президент України та Рада національної безпеки і оборони України, Кабінет Міністрів України, центральні органи виконавчої влади, регуляторні, контрольні й безпекові інституції, органи

місцевого самоврядування. Водночас фактична спроможність політики залежить також від суспільних медіа, професійних редакцій, громадських організацій, науково-експертного середовища, суб'єктів цифрового ринку, платформ і громадян. Участь недержавних акторів не зменшує відповідальності держави, а змінює спосіб її реалізації: від одностороннього адміністративного впливу до організації прозорих правил співпраці, обміну інформацією, незалежної перевірки та суспільного контролю.

Обґрунтовано, що ключова інституційна проблема полягає не у відсутності суб'єктів, а в недостатній узгодженості їхніх дій. Виявлені ризики охоплюють дублювання функцій, розрив між стратегічними документами й операційним виконанням, використання несумісних показників, затримки міжвідомчого обміну, суперечливість публічних повідомлень та недостатню інституціоналізацію зворотного зв'язку. Додатковим чинником є небезпека змішування суспільно необхідної державної комунікації з політичним просуванням посадових осіб, що послаблює довіру і спотворює цільове призначення бюджетних ресурсів. За таких умов навіть значна активність окремих органів не гарантує цілісного публічного результату.

Систематизовано інструменти інформаційної взаємодії органів публічної влади з громадянами та медіа за їх функціональним призначенням. До основних груп віднесено офіційне інформування, доступ до публічної інформації та відкритих даних, сервісну комунікацію, інструменти електронної демократії, взаємодію з медіа, соціальні мережі, кризові комунікації, механізми протидії дезінформації та аналітичний зворотний зв'язок. Доведено, що інструмент не слід ототожнювати з технічним каналом: його зміст включає правову процедуру, відповідального суб'єкта, стандарти змісту, можливість відповіді, механізм фіксації результату та критерії оцінювання. Саме такий підхід дозволяє перейти від цифрової присутності органу влади до повноцінної інформаційної взаємодії.

З'ясовано, що взаємодія органів публічної влади з медіа та громадянами поступово переходить від моделі одностороннього повідомлення до діалогічної моделі, однак цей перехід залишається нерівномірним. Належний стандарт інформаційного супроводу управлінського рішення повинен включати

першоджерело, стислий виклад змісту, пояснення очікуваних наслідків, структуровані дані, контакт уповноваженої особи, порядок уточнення або виправлення та регулярне оновлення інформації. У кризовій ситуації до цього додаються час наступного повідомлення, чітке розмежування підтверджених фактів і попередніх оцінок, а також обґрунтування відомостей, доступ до яких тимчасово обмежено з міркувань безпеки.

Виявлено істотну територіальну нерівність цифрової та комунікаційної спроможності. Середнє значення Індексу цифрової трансформації територіальних громад у першому вимірюванні 2025 року становило 16 балів зі 100, тоді як показники громад-лідерів досягали 62,97; 62,75; 60,35; 55,61 і 54,57 бала. Отже, найкращі результати у 3,4–3,9 раза перевищували середній рівень. Такий розрив означає, що однакове нормативне право на інформацію, участь і цифрову послугу фактично реалізується за різної кадрової, технічної та організаційної спроможності місцевих органів.

Уточнено зміст інформаційної стійкості держави як динамічної спроможності системи публічного управління, медіасередовища та суспільства завчасно виявляти ризики, зберігати безперервність законної й достовірної комунікації під час деструктивного впливу, адаптувати інституційні й технологічні механізми, відновлювати довіру та накопичувати досвід без непропорційного обмеження прав людини. На відміну від вузького розуміння інформаційної безпеки як захисту ресурсів або блокування шкідливого контенту, стійкість охоплює превентивність, функціональну безперервність, адаптивність, відновлюваність і правову легітимність.

Авторська матриця залишкового ризику засвідчила, що найбільш критичною загрозою є координована дезінформаційна кампанія із розрахунковим рівнем ризику 80 %. Алгоритмічне підсилення маніпуляцій, синтетичний контент і deepfake, дискредитація медіа та інституцій, а також кібератаки на комунікаційні канали отримали по 64 %, що відповідає високому рівню. Локальні інформаційні вакууми та кадрове виснаження комунікаційних команд оцінено у 51,2 %. Наведені значення мають експертно-аналітичний, а не

офіційно-статистичний характер, проте вони демонструють взаємозалежність технологічних, організаційних, медійних і кадрових ризиків.

Загальним результатом другого розділу є висновок про те, що Україна вже сформувала значний нормативний, інституційний і цифровий фундамент державної інформаційної політики, однак її сучасний стан характеризується нерівномірною зрілістю. Сильними сторонами є розгалужена система суб'єктів, масове використання електронних послуг, розвиток відкритих даних, наявність спеціалізованих безпекових і комунікаційних інституцій, активність суспільного та експертного середовища. Слабкі сторони виявляються у фрагментарності координації, переважанні процесних показників над показниками суспільного результату, територіальній нерівності, залежності від зовнішніх цифрових платформ, недостатній інтеграції зворотного зв'язку та реактивному характері частини заходів протидії загрозам.

Пріоритетами подальшого вдосконалення визначено: забезпечення безперервності стратегічного планування та щорічного перегляду ризиків; запровадження єдиного класифікатора інформаційних інцидентів і матриці відповідальності; створення спільної інформаційно-аналітичної основи; інтеграцію звернень і каналів в омніканальний контур; установлення стандартів часу, змісту та доступності відповіді; відкриті дашборди результативності; мінімальний стандарт спроможності громад; сталі правила взаємодії з медіа і платформами; розвиток медіаграмотності; правові та етичні запобіжники використання штучного інтелекту; незалежне оцінювання пропорційності обмежень і впливу політики на права людини.

Таким чином, результативність державної інформаційної політики доцільно визначати як здатність багаторівневої системи суб'єктів узгоджено перетворювати достовірні дані, публічний діалог і безпекову аналітику на своєчасні, зрозумілі, правомірні та вимірювані управлінські дії. Саме перехід від розрізнених інституцій і каналів до інтегрованого циклу «діагностика – рішення – комунікація – зворотний зв'язок – оцінювання – адаптація» створює основу для розроблення у третьому розділі практичної моделі розвитку механізмів реалізації державної інформаційної політики України.

РОЗДІЛ 3. РОЗВИТОК МЕХАНІЗМІВ РЕАЛІЗАЦІЇ ДЕРЖАВНОЇ ІНФОРМАЦІЙНОЇ ПОЛІТИКИ

3.1. Формування інтегрованого організаційно-управлінського механізму реалізації державної інформаційної політики

Система державної інформаційної політики охоплює сукупність суб'єктів, норм, ресурсів, зв'язків і суспільних відносин. Організаційна структура відображає формальний розподіл повноважень. Механізм характеризує спосіб приведення системи в дію: послідовність операцій, правила координації, інструменти впливу, ресурси, контроль і коригування. Тому його удосконалення можливе без механічного збільшення кількості органів, якщо змінюються взаємозв'язки, стандарти й відповідальність.

Інтеграція означає функціональне поєднання процесів, які нині часто здійснюються паралельно: аналіз інформаційного середовища, прогнозування ризиків, розроблення політики, правова експертиза, сегментація аудиторій, планування комунікації, створення контенту, кризове реагування, оцінювання та накопичення організаційного досвіду. Відсутність зв'язку між ними призводить до того, що аналітичні дані не впливають на рішення, комунікаційні підрозділи залучаються запізно, а результати кампаній не використовуються для перегляду політики.

Методологічною основою моделі є поєднання системного, інституційного, процесного, мережевого та ризик-орієнтованого підходів. Системний підхід дозволяє бачити інформаційну політику частиною архітектури публічного управління; інституційний – визначити формальні та неформальні правила; процесний – побудувати відтворюваний цикл; мережевий – включити недержавних партнерів; ризик-орієнтований – диференціювати режими роботи залежно від масштабу загрози [37; 45; 69; 137; 144; 150; 151].

Важливо не зводити державну інформаційну політику лише до протидії дезінформації. Безпековий компонент є критично важливим, проте механізм повинен також забезпечувати доступ до публічної інформації, відкриті дані, комунікацію реформ, медійну політику, цифрову інклюзію, міжнародне

позиціонування, медіаграмотність і участь громадян. Надмірна сек'юритизація звужує предмет політики й створює ризик підміни діалогу адміністративним контролем.

Управлінською формулою запропонованої моделі є координована поліцентричність. Спільними мають бути стратегічні цілі, стандарти даних, базові протоколи, критерії оцінювання та правила кризової взаємодії, тоді як рішення в межах компетенції приймаються на рівні, де наявні потрібні знання, повноваження та близькість до цільової аудиторії. Такий підхід запобігає як фрагментації, так і надмірній централізації.

Модель передбачає два взаємопов'язані режими функціонування. Плановий режим охоплює розроблення політики, комунікаційні кампанії, відкриті дані, медіаграмотність та міжнародну комунікацію. Кризовий режим активується у разі інформаційної атаки, кібератаки з комунікаційними наслідками, масштабної дезінформаційної кампанії або надзвичайної події. Для обох режимів застосовуються спільні стандарти й інфраструктура, але різняться строки, рівень централізації та порядок залучення безпекових суб'єктів.

За результатами узагальнення наукових підходів інтегрований організаційно-управлінський механізм реалізації державної інформаційної політики пропонується визначати як інституційно закріплену, багаторівневу й технологічно підтриману систему узгоджених повноважень, процесів, стандартів, ресурсів та зворотних зв'язків, за допомогою якої суб'єкти публічного управління спільно з медіа, громадянським суспільством, науковими установами, цифровими платформами та міжнародними партнерами здійснюють аналіз інформаційного середовища, формування рішень, стратегічну комунікацію, запобігання загрозам, кризове реагування, оцінювання та коригування політики з дотриманням прав людини, законності й підзвітності.

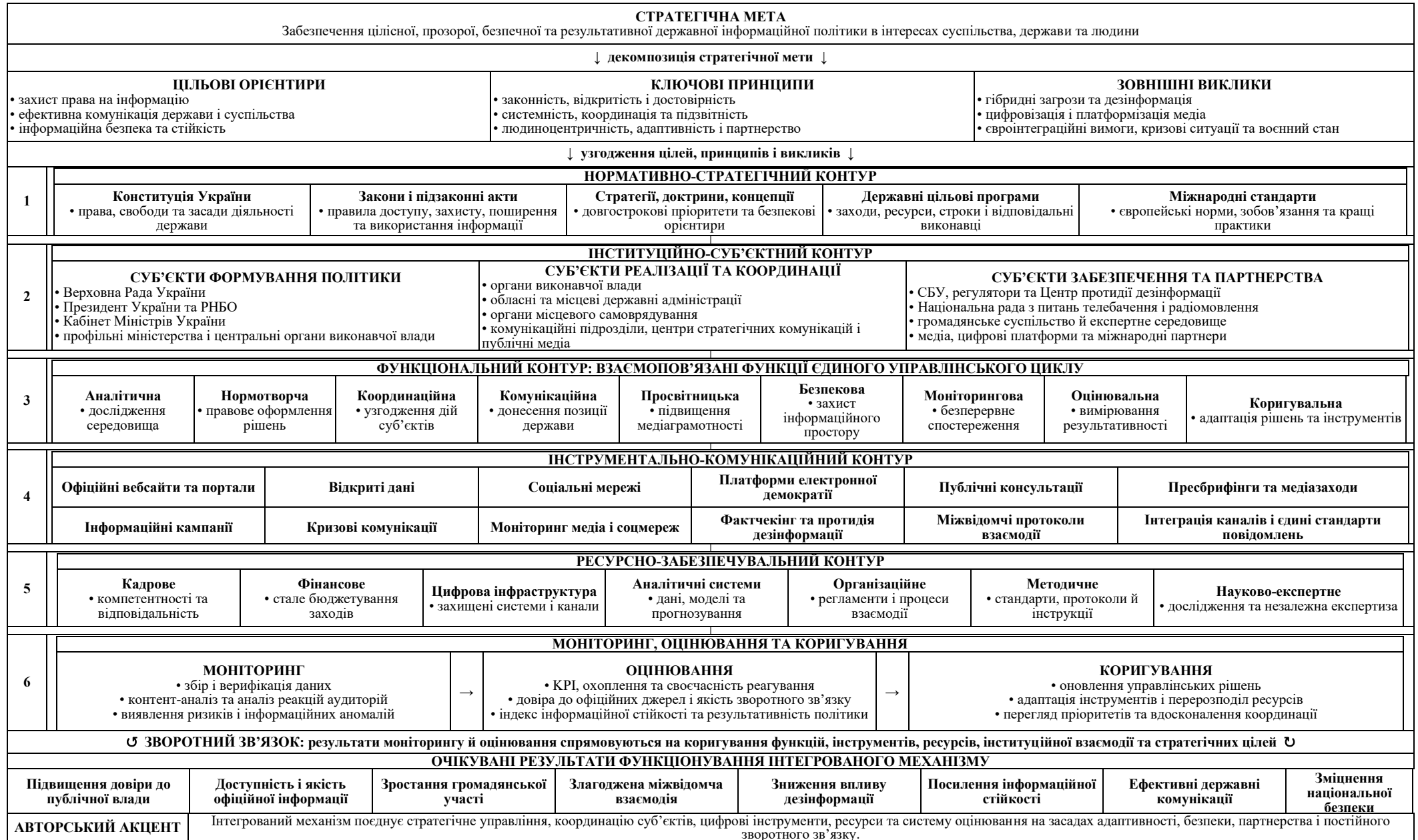


Рис. 3.1. Концептуальна архітектура інтегрованого організаційно-управлінського механізму реалізації державної інформаційної політики Джерело: розроблено автором.

Базовими принципами механізму визначено верховенство права, людиноцентричність, достовірність і доказовість, стратегічну узгодженість, розподілену відповідальність, субсидіарність, оперативність, інтероперабельність, безпеку за проєктуванням, відкритість, інклюзивність, адаптивність та організаційне навчання. Це означає, що управлінська доцільність не може виправдовувати непропорційне обмеження інформаційних прав, а швидке реагування має спиратися на визначені процедури, джерела даних і механізми перевірки [35; 48; 79; 84; 91; 150; 156; 160].

Окремо пропонується закріпити принцип комунікації за задумом політики. Комунікаційні наслідки, потреби аудиторій, ризики нерозуміння та індикатори сприйняття мають аналізуватися до ухвалення рішення. Це дозволяє виявляти складні для пояснення положення, оцінювати доступність для різних груп, планувати відповіді та визначати канали зворотного зв'язку. Державна комунікація стає складовою якості рішення, а не способом його одностороннього просування.

Таблиця 3.1.

Відмінності фрагментарної та інтегрованої моделей реалізації державної інформаційної політики

Вимір	Фрагментарна модель	Інтегрована модель	Очікуваний ефект
Стратегічне планування	Окремі відомчі плани, різні горизонти та показники	Єдина рамка цілей, взаємоузгоджені операційні плани	Менший розрив між стратегією і виконанням
Розподіл повноважень	Перетин функцій або невизначеність відповідального	Матриця ролей, власник процесу, процедура ескалації	Персоніфікація відповідальності
Аналітика	Розрізнені продукти та обмежений обмін даними	Спільні стандарти даних і ситуаційна картина	Швидше виявлення проблем
Комунікація	Реактивне інформування після ухвалення рішення	Раннє залучення комунікаційної функції й тестування	Зрозумілість і доступність
Кризове реагування	Ситуативні контакти та конкуренція повідомлень	Типові протоколи, рівні інцидентів, узгоджені факти	Скорочення часу реакції
Участь	Епізодичні консультації	Постійні партнерські формати та співтворення	Легітимність і якість політики
Оцінювання	Підрахунок охоплення та кількості матеріалів	Процесні, результативні, поведінкові й правозахисні індикатори	Оцінювання суспільного ефекту
Навчання	Досвід зберігається в окремих командах	Реєстр кейсів, післядієвий аналіз, стандартизація	Інституційна пам'ять

Джерело: систематизовано та розроблено автором за [29; 30; 37; 39; 45; 55; 115; 137; 144; 150; 151].

Інтегрована модель не передбачає уніфікації всіх повідомлень. Єдність має стосуватися фактів, стратегічних цілей, правових позицій і кризових протоколів, тоді як форма, мова, деталізація та канал адаптуються до потреб аудиторій. Так досягається поєднання цілісності державної позиції з комунікаційною релевантністю, особливо на регіональному й місцевому рівнях. Нормативно-стратегічна підсистема повинна забезпечувати узгодженість стратегій, концепцій, операційних планів і відомчих документів. Її продуктом має бути єдина карта цілей, у якій для кожної стратегічної цілі визначено очікувані результати, відповідальних, аудиторії, ризики, показники та джерела даних.

Інституційно-координаційна підсистема формує правила взаємодії та визначає власників ключових процесів. Її завданням є не погодження кожної публікації, а спільне планування, обмін даними, вирішення конфліктів компетенцій, ескалація інцидентів і міжвідомча оцінка. Інформаційно-аналітична підсистема забезпечує моніторинг, верифікацію, аналіз аудиторій і прогнозування, а комунікаційно-партисипативна перетворює висновки на діалогові формати, доступний контент і консультації [34; 37; 45; 55; 150; 151].

Таблиця 3.2.

Функціональні підсистеми інтегрованого організаційно-управлінського механізму

Підсистема	Основна функція	Ключові інструменти	Безпосередній результат
Нормативно-стратегічна	Узгодження цілей, принципів і планів	Стратегічна карта; операційні плани; правова експертиза	Несуперечлива рамка політики
Інституційно-координаційна	Розподіл ролей і синхронізація дій	Матриця повноважень; регламенти; групи; ескалація	Керованість багатосуб'єктної системи
Інформаційно-аналітична	Доказова основа рішень	Моніторинг; верифікація; дослідження аудиторій; прогнозування	Єдина ситуаційна картина
Комунікаційно-партисипативна	Пояснення політики й залучення громадян	Стратегії; консультації; кампанії; робота з медіа	Розуміння й легітимність
Цифрово-технологічна	Інтероперабельність і автоматизація	Захищена платформа; API; панелі; сповіщення	Безперервний обмін даними
Безпекова та кризова	Запобігання і реагування	Рівні загроз; сценарії; протоколи; резервні канали	Мінімізація наслідків
Кадрово-ресурсна	Формування спроможності	Компетентності; навчання; бюджетування; резерв	Професійність і сталість
Моніторингово-оціночна	Вимірювання та коригування	KPI; опитування; аудит; оцінка впливу	Підзвітність і навчання

Джерело: розроблено автором на основі [3; 30; 37; 44; 45; 55; 69; 105; 115; 150; 151].

Цифрово-технологічна підсистема має ґрунтуватися на інтероперабельності та принципі «безпека і приватність за проєктуванням». Обмін даними, контроль доступу, журналювання, класифікація інформації й захист персональних даних передбачаються на етапі розроблення процесів. Доцільною є федеративна архітектура, за якої установи зберігають власні ресурси, але надають стандартизовані метадані й визначені набори відомостей відповідно до повноважень [85; 87; 90; 91; 98; 99; 102; 139; 153; 155].

Безпекова та кризова підсистема повинна бути інтегрована з кібербезпекою, захистом критичної інфраструктури та стратегічними комунікаціями. Інформаційна загроза часто супроводжує технічний інцидент, а комунікаційна невизначеність посилює його наслідки. Для кожного класу інцидентів необхідно визначити джерела підтвердження, строки первинного повідомлення, порядок оновлення інформації, відповідального спікера, межі розкриття даних і процедуру спростування.

Пропонується дворівневий формат координації. Перший рівень – Міжвідомча рада з державної інформаційної політики як консультативно-координаційний орган при Кабінеті Міністрів України. Вона схвалює спільні пріоритети, розглядає результати оцінювання, вирішує системні конфлікти компетенцій і затверджує рамкові стандарти. Другий рівень – постійний операційний офіс або секретаріат, який підтримує щоденну взаємодію, адмініструє цифрову платформу, контролює виконання рішень та організовує навчання. Рада не отримує регуляторних, правоохоронних чи редакційних функцій.

Для запобігання політизації необхідно нормативно визначити предмет координації та межі втручання. Рада не повинна погоджувати редакційний контент незалежних медіа, давати обов'язкові вказівки регулятору щодо конкретних справ або використовувати моніторинг для спостереження за законною політичною активністю. Її компетенція стосується державних процесів, міжвідомчих стандартів, кризової взаємодії, публічної комунікації органів влади та добровільних партнерських механізмів [48; 84; 95; 109; 156; 159].

У межах операційного контуру пропонується інститут власника процесу. Для стратегічного планування, моніторингу інформаційного середовища, кризового реагування, комунікації європейської інтеграції, розвитку медіаграмотності та міжнародного позиціонування визначається орган, відповідальний не за всі дії, а за цілісність процесу, актуальність регламенту, координацію учасників і звітування. Це усуває ситуацію, коли всі формально залучені, але ніхто не відповідає за кінцевий результат.

Процесний вимір механізму пропонується реалізувати через замкнений цикл із восьми етапів. На відміну від лінійної моделі «рішення – повідомлення – поширення», цикл починається з виявлення суспільної проблеми та інформаційних ризиків, а завершується оцінюванням і коригуванням. Кожен етап має вхідні дані, відповідального координатора, строк, контрольну точку та результат, придатний для передачі наступному етапу.

1. МОНИТОРИНГ сигнали, потреби, ризики	2. ВЕРИФІКАЦІЯ факти, джерела, право	3. ПРОЄКТУВАННЯ цілі, аудиторії, сценарії	4. РІШЕННЯ ролі, ресурси, строки
8. КОРИГУВАННЯ уроки, стандарти, новий цикл	7. ОЦІНЮВАННЯ продукти, результати, вплив	6. ЗВОРОТНИЙ ЗВ'ЯЗОК реакції, запити, сигнали	5. РЕАЛІЗАЦІЯ контент, канали, партнерства

Рис. 3.2. Замкнений управлінський цикл реалізації державної інформаційної політики

Джерело: розроблено автором

Проєктування включає формулювання вимірюваної мети, визначення аудиторій, бар'єрів сприйняття, бажаної зміни, ключових фактів, каналів, партнерів і альтернативних сценаріїв. На цьому етапі проводиться оцінка впливу майбутнього рішення на інформаційні права та довіру. Якщо проблема полягає не у відсутності інформації, а у складності процедури або невідповідності політики потребам громадян, комунікаційна кампанія не може підміняти перегляд рішення.

Етап прийняття рішення формалізує ролі, строки, ресурси, порядок погодження фактологічної основи та критерії завершення. Для звичайних питань

застосовується децентралізований режим, для кризових – прискорений протокол із визначеним черговим складом, захищеним каналом і часовими нормативами. Рішення про обмеження доступу або інші правові заходи приймаються лише уповноваженими суб'єктами з документуванням підстав і можливістю оскарження [19; 65; 84; 119].

Реалізація охоплює поширення контенту, доступ до первинних даних, брифінги, відповіді на запити, гарячі лінії, консультації та локалізацію матеріалів. Для узгодженості пропонується фактологічна картка – структурований документ із підтвердженими фактами, джерелами, правовими межами, невідомими аспектами, датою оновлення та відповідальним експертом. Вона не уніфікує стилістику, але мінімізує суперечливі дані.

Зворотний зв'язок має впливати на рішення. Запитання громадян, журналістів і місцевих органів є даними про недоліки політики, складність процедур або інформаційну нерівність. Оцінювання порівнює базові й фактичні значення індикаторів, а коригування може охоплювати зміну повідомлень, каналів, строків, регламентів або самої політики. Так комунікація стає механізмом навчання держави [137; 150; 151].

Для кожного процесу пропонується адаптована матриця відповідальності, у якій визначаються суб'єкт, що затверджує рішення; власник процесу; виконавці; суб'єкти обов'язкової консультації; одержувачі інформації; незалежні контролери. Такий підхід відрізняється від простого переліку установ, оскільки показує, хто відповідає за проходження процесу від початкового сигналу до оцінки результату.

Стратегічний рівень встановлює цілі та межі політики, координаційне ядро підтримує процеси, секторальні органи забезпечують предметну достовірність, регіональні та місцеві органи адаптують комунікацію й надають дані про локальні потреби. Недержавні партнери виконують експертну, комунікаційну, освітню та контрольну функції, не підміняючи владних повноважень. Міжнародний рівень забезпечує обмін попередженнями й наближення до стандартів ЄС [12; 24; 47; 56; 128; 140; 156].

Матриця розподілу ролей у ключових процесах інтегрованого механізму

Управлінський процес	Стратегічний рівень	Координаційне ядро	Секторальний і територіальний рівні	Недержавні партнери та контроль
Стратегічні пріоритети	Схвалює рамку й цілі	Готує проєкт та узгоджує	Надають секторальні пропозиції	Консультації та незалежна експертиза
Моніторинг	Встановлює критерії ризику	Агрегує метадані й картину	Збирають профільні та регіональні дані	Медіа, науковці, фактчекери надають сигнали
Планування кампанії	Визначає політичний результат	Синхронізує учасників	Розробляють зміст, канали, локалізацію	Тестування й партнерське поширення
Кризове реагування	Визначає режим і межі розкриття	Активує протокол, координує факти	Надають дані та комунікують у компетенції	Незалежне інформування й перевірка
Медіаграмотність	Затверджує довгострокові цілі	Узгоджує програми та показники	Реалізують освітні й регіональні заходи	Освітні установи, медіа, громадські організації
Оцінювання	Розглядає висновки й коригує пріоритети	Зводить дані та організовує аналіз	Звітують за уніфікованими показниками	Незалежний аудит і громадський контроль
Нормативні зміни	Приймає політичне рішення	Формує пакет пропозицій	Правова та секторальна експертиза	Оцінка впливу на права людини

Джерело: розроблено автором на основі [30; 34; 37; 45; 55; 115; 150; 151; 159; 160].

Регіональний рівень доцільно включити через мережу координаторів державної інформаційної політики в обласних адміністраціях та типові координаційні групи при громадах або міжмуніципальних об'єднаннях. Їх завданням є локальний аналіз, адаптація матеріалів, взаємодія з місцевими медіа, комунікація ризиків і передавання зворотного зв'язку. Для прифронтових, деокупованих і тимчасово недоступних територій необхідні окремі сценарії та резервні канали.

Взаємодія з медіа має будуватися на рівному доступі до фактів і передбачуваності процедур: регулярних брифінгах, доступі до первинних документів, стандартизованих відповідях та можливості уточнення складних даних. Партнерство не означає погодження редакційних матеріалів; незалежна журналістська перевірка є елементом стійкого середовища. У кризах особливого значення набувають завчасно погоджені правила доступу, ембарго та захисту чутливої інформації.

Громадянське суспільство й наукові установи мають бути включені до експертних рад, тематичних лабораторій, оцінювання кампаній і розроблення методик. Цифрові платформи можуть брати участь у протоколах повідомлення про координовану неавтентичну поведінку, збереження доказів і надання агрегованих даних, але такі механізми потребують прозорості, можливості оскарження й дотримання свободи вираження.

Технологічною основою механізму пропонується зробити захищену цифрову платформу координації державної інформаційної політики. Її призначення полягає не у тотальному моніторингу контенту, а у підтримці законних управлінських процесів: спільного планування, обміну верифікованими даними, фіксації рішень, контролю строків, управління кризовими інцидентами та оцінювання результатів. Платформа має поєднувати закритий службовий контур із публічним модулем прозорості.

Архітектурно доцільною є федеративна модель. Джерельні дані залишаються у володільців, а платформа отримує лише необхідні метадані, показники або доступ за встановленими правилами. Розмежування здійснюється за ролями й рівнями чутливості; усі дії журналюються; автоматизовані рекомендації є допоміжними та не замінюють рішення уповноваженої особи. Для інформації з обмеженим доступом застосовуються окремі захищені сегменти.

ДЖЕРЕЛА ДАНИХ реєстри • звернення • медіамоніторинг • дослідження • регіональні сигнали		
Ситуаційна обізнаність сигнали • ризики • аудиторії	Планування і координація цілі • ролі • календар • завдання	Кризове реагування рівні інцидентів • протоколи • сповіщення
База верифікованих фактів джерела • актуальність • експерт	Реєстр кампаній версії • аудиторії • канали • доступність	Панель результатів KPI • відхилення • коригування
ЗАХИСНИЙ КОНТУР: рольовий доступ • журналювання • шифрування • резервування • оцінка приватності		
ПУБЛІЧНИЙ МОДУЛЬ: пріоритети • методики • відкриті показники • звіти • консультації • оскарження		

Рис. 3.3. Функціональна архітектура цифрової платформи координації державної інформаційної політики

Джерело: розроблено автором за [55; 85; 87; 90; 91; 98; 99; 102; 139; 153; 155; 157].

Модуль ситуаційної обізнаності має агрегувати сигнали за єдиною класифікацією: тема, джерело, територія, аудиторія, тип ризику, достовірність, вплив і терміновість. Система не повинна автоматично кваліфікувати законне висловлювання як загрозу. Остаточна оцінка здійснюється аналітиком за затвердженою методикою, а для рішень із правовими наслідками — уповноваженим органом [157; 159; 160].

Платформа має передбачати документування й оскарження рішень, пов'язаних із видаленням, обмеженням поширення або передаванням інформації цифровим платформам. Необхідно зберігати підстави, автора рішення, строк дії та результат перегляду. Це забезпечує сумісність із принципами прозорості платформного врядування та європейськими стандартами.

Оцінювання пропонується здійснювати за багаторівневою системою. Перший рівень відображає інституційну спроможність: наявність регламентів, підключення суб'єктів, підготовку персоналу та якість даних. Другий характеризує процес: швидкість верифікації, дотримання строків, міжвідомчу участь. Третій вимірює продукти: доступність матеріалів, охоплення та партнерські формати. Четвертий оцінює суспільні результати: розуміння політики, довіру до процедур, здатність знаходити перевірену інформацію та стійкість до маніпуляцій.

Таблиця 3.4.

Запропонована система показників результативності інтегрованого механізму

Вимір	Індикатор	Метод розрахунку / джерело	Цільовий орієнтир	Періодичність
Стратегічна узгодженість	Частка пріоритетних політик із комунікаційною та оціночною складовою	Політики з повним пакетом / усі пріоритетні політики	не менше 90 %	Щороку
Інституційне охоплення	Частка визначених суб'єктів, підключених до процедур і платформи	Підключені суб'єкти / перелік суб'єктів	не менше 95 %	Щокварталу
Якість даних	Частка записів із джерелом, датою та відповідальним експертом	Повні записи / перевірені записи	не менше 95 %	Щомісяця
Оперативність	Медіанний час первинної верифікації критичного сигналу	Від реєстрації до підтвердженої оцінки	до 30 хвилин	За інцидентом

Вимір	Індикатор	Метод розрахунку / джерело	Цільовий орієнтир	Періодичність
Кризова реакція	Час до першого підтвердженого публічного повідомлення	Від класифікації до повідомлення	до 60 хвилин	За інцидентом
Якість проектування	Частка великих кампаній із попереднім тестуванням	Кампанії з тестуванням / великі кампанії	не менше 70 %, надалі 90 %	Щопівроку
Доступність	Частка ключових матеріалів, що відповідають стандартам доступності	Матеріали, що пройшли перевірку / ключові матеріали	не менше 95 %	Щокварталу
Оцінювання	Частка пріоритетних кампаній із післядієвим звітом	Оцінені кампанії / завершені кампанії	100 %	Щокварталу
Суспільний результат	Зміна частки громадян, які правильно розуміють мету політики	Базове та підсумкове вимірювання	позитивна зміна за паспортом політики	За кампанією
Правові гарантії	Підтверджені випадки незаконного обмеження доступу або приватності	Рішення контролюючих органів	нульова толерантність	Постійно
Навчання	Частка рекомендацій післядієвого аналізу, виконаних у строк	Виконані / погоджені рекомендації	не менше 85 %	Щопівроку

Джерело: запропоновано автором з урахуванням [146; 150; 151; 159; 160].

Система оцінювання має використовувати змішані методи. Адміністративні дані платформи вимірюють строки й виконання; контент-аналіз – точність і доступність; опитування – розуміння й довіру; фокус-групи – причини реакцій; незалежний аудит – дотримання правових і етичних стандартів. Поєднання методів знижує ризик маніпулювання одним показником.

Раз на два роки доцільно проводити зовнішній аудит із залученням наукових установ, професійних об'єднань і громадських організацій. Предметом аудиту мають бути якість процедур, обґрунтованість даних, дотримання прав, ефективність координації та достовірність звітності. Рекомендації розглядаються стратегічним рівнем із публічним поясненням прийнятих або відхилених пропозицій.

Упровадження має бути поетапним, оскільки одночасна зміна нормативної бази, цифрової інфраструктури та організаційної культури створює ризик формалізації. На першому етапі проводиться інвентаризація повноважень, процесів, систем і показників; на другому – апробація моделі на обмеженій кількості міжвідомчих напрямів; на третьому – масштабування стандартів і

платформи; на четвертому – інституціоналізація через регулярне оцінювання й оновлення [30; 37; 115].

Таблиця 3.5.

Дорожня карта впровадження інтегрованого організаційно-управлінського механізму

Етап	Строк від запуску	Основні дії	Ключовий результат	Критерій переходу
I. Проектування	0–6 місяців	Інвентаризація; базове вимірювання; формування групи; положення; стандарти даних і протоколи	Нормативний пакет, карта процесів, технічне завдання	Затверджені ролі та врегульовані перетини компетенцій
II. Пілотування	7–18 місяців	Запуск операційного офісу; пілот платформи; апробація; навчання; післядієвий аналіз	Перевірені процеси, прототип платформи, уточнені регламенти	Не менше 80 % пілотних процесів завершено за контрольними точками
III. Масштабування	19–30 місяців	Підключення центральних і регіональних суб'єктів; спільні сервіси; панель індикаторів; публічний модуль	Національне охоплення, уніфікована звітність, регіональна мережа	Досягнення мінімальних значень охоплення та якості даних
IV. Інституціоналізація	31–48 місяців	Зовнішній аудит; коригування законодавства; стабільне бюджетування; навчальні програми	Сталий механізм із регулярним оновленням	Позитивна динаміка результатів і виконання не менше 85 % рекомендацій

Джерело: розроблено автором.

Кадрова модель має включати управлінські компетентності – стратегічне планування, координацію та оцінювання; аналітичні – роботу з даними, дослідження аудиторій, верифікацію й прогнозування; комунікаційні – створення доступного контенту, взаємодію з медіа, фасилітацію та кризову комунікацію. Для керівників потрібен окремий модуль, що формує розуміння комунікації як управлінської функції.

Постійна готовність до криз забезпечується міжвідомчими навчаннями. Сценарії мають моделювати одночасне виникнення технічного інциденту, інформаційного вакууму, дезінформаційної хвилі та високого суспільного запиту. Оцінюється здатність системи отримати підтверджені дані, прийняти рішення, визначити межі розкриття, підтримувати оновлення й фіксувати уроки.

ВХОДИ повноваження дані й ризики кадри та ресурси	ПРОЦЕСИ аналіз • координація проектування • реагування	ПРОДУКТИ узгоджені рішення верифіковані дані доступні повідомлення	РЕЗУЛЬТАТИ розуміння політики швидкість реакції довіра до процедур	ВПЛИВ інформаційна стійкість демократична легітимність якість управління
ЗВОРОТНИЙ ЗВ'ЯЗОК І НАВЧАННЯ: моніторинг → оцінювання → післядієвий аналіз → коригування стандартів і політики				

Рис. 3.4. Логічна модель впливу інтегрованого механізму на якість публічного управління

Джерело: розроблено автором.

Інтегрований механізм потребує не одного нормативного акта, а взаємоузгодженого пакета документів різного рівня. Рамковий акт має визначити мету, принципи, склад учасників, координаційний контур, порядок планування, базові вимоги до прозорості та захисту прав. Підзаконні акти й міжвідомчі регламенти повинні деталізувати процеси, строки, формати даних, рівні інформаційних інцидентів, порядок ескалації та післядієвого аналізу. Методичні документи забезпечують єдине тлумачення процедур, але не можуть установлювати нові обмеження прав поза законом [6; 84; 90; 93; 95; 105].

Особливого значення набуває стандартизація управлінських продуктів. Для кожного пріоритетного напрямку доцільно використовувати уніфікований паспорт політики, карту аудиторій, фактологічну картку, реєстр ризиків, комунікаційний план і звіт про результати. Уніфікація структури не означає шаблонності змісту: вона забезпечує порівнюваність даних, повноту обґрунтування та можливість контролю проходження процесу. Стандарти мають регулярно переглядатися на підставі практики, аудиту й технологічних змін.

У межах правового забезпечення необхідно встановити чіткий зв'язок між режимами відкритості та безпеки. За замовчуванням інформація про цілі, методики, публічні показники й використання ресурсів має бути відкритою. Обмеження застосовується лише до конкретних відомостей, якщо розкриття створює передбачений законом ризик, і супроводжується фіксацією підстав, строку та суб'єкта перегляду. Такий підхід підтримує довіру, зменшує простір для довільного засекречування та відповідає принципу пропорційності.

Пакет нормативно-організаційних документів для запуску інтегрованого механізму

Документ	Призначення	Ключовий зміст	Період перегляду
Рамкове положення про механізм	Закріплення архітектури та суб'єктів	Мета, принципи, рівні координації, повноваження, гарантії прав	Не рідше одного разу на три роки
Регламент міжвідомчої взаємодії	Організація повсякденних процесів	Власники процесів, строки, погодження, ескалація, документування	Щороку або після істотної зміни
Протокол кризового реагування	Уніфікація дій під час інцидентів	Рівні загроз, чергові групи, фактологічна картка, спікери, оновлення	Після кожного великого інциденту
Стандарт даних та інтероперабельності	Безпечний обмін і сумісність систем	Метадані, формати, API, доступ, журналювання, строки зберігання	Щороку з урахуванням технологічних змін
Методика оцінювання	Порівнюваність результатів	Індикатори, базові вимірювання, джерела, аудит, правила публікації	Раз на два роки
Кодекс професійної етики	Запобігання політизації та зловживанням	Розмежування державної та партійної комунікації, конфлікт інтересів, скарги	За результатами етичного аудиту

Джерело: розроблено автором на основі [6; 30; 84; 90; 93; 95; 105; 115; 150; 151].

Фінансове забезпечення має поєднувати базове утримання постійних функцій і програмне фінансування міжвідомчих проєктів. До базових витрат належать операційний офіс, кіберзахист, технічна підтримка платформи, навчання, дослідження аудиторій та незалежний аудит. Програмні кошти спрямовуються на кампанії, пілоти, локалізацію матеріалів, спільні сервіси й оцінювання. Міжнародна допомога може підтримувати розвиток, але критичні функції не повинні залежати від короткострокових грантів, оскільки це створює розриви в інституційній пам'яті та технологічному обслуговуванні.

Кожен міжвідомчий проєкт доцільно супроводжувати паспортом із визначенням проблеми, альтернатив, очікуваної зміни, аудиторій, бюджету, джерел даних, індикаторів і плану завершення. Закупівля комунікаційних послуг має оцінюватися не лише за кількістю контенту, а й за якістю методології, доступністю, планом вимірювання та передаванням державі даних і матеріалів, створених за публічні кошти. Це дозволяє пов'язати витрати з результатом і

зменшує ризик кампаній, які формально виконані, але не вплинули на розуміння політики [81; 150; 151].

Для вирівнювання спроможностей пропонується мережа регіональних центрів компетентностей або спільних сервісів. Вони можуть надавати громадам аналітичну, дизайнерську, перекладацьку, технологічну та кризово-комунікаційну підтримку, не забираючи в них відповідальність за локальний зміст. Така модель особливо важлива для малих громад, прифронтових територій і органів, які не можуть сформувати повноцінні спеціалізовані підрозділи.

Партнерська сталість забезпечується постійними, а не ситуативними форматами співпраці. Доцільно створити тематичні дорадчі панелі з медіа, громадських організацій, науковців, професійних асоціацій і представників платформ. Їх роль полягає в аналізі ризиків, тестуванні матеріалів, оцінюванні доступності та виробленні рекомендацій. Умови участі, джерела фінансування й можливі конфлікти інтересів мають бути публічними, щоб партнерство не перетворювалося на закритий канал привілейованого впливу.

Інтегрований механізм доцільно розвивати як інструмент наближення до європейських правил у сферах медіа, цифрових послуг, управління даними, кібербезпеки та штучного інтелекту. Йдеться не про механічне копіювання актів ЄС, а про вбудовування спільних принципів: прозорості платформ, незалежності медіа, захисту персональних даних, належного управління ризиками, людського контролю над автоматизованими системами та можливості оскарження.

Для цього в структурі операційного офісу доцільно передбачити функцію нормативного скринінгу. Вона аналізує нові акти ЄС і міжнародні рекомендації, визначає їхній вплив на національні процеси, готує таблиці відповідності та пропозиції до стандартів механізму. Результати скринінгу мають обговорюватися з регуляторами, медіа, платформами та громадянським суспільством, оскільки зміни в цифровому врядуванні одночасно стосуються безпеки, конкуренції, свободи вираження і приватності [140; 141; 154; 156; 159].

Міжнародна взаємодія має включати обмін попередженнями про транснаціональні інформаційні операції, спільні дослідження, навчання, взаємне визнання методик і координацію кризової комунікації. Водночас передавання

даних іноземним партнерам повинно мати правову підставу, визначену мету, мінімально необхідний обсяг і належні гарантії захисту. Європейська сумісність у запропонованій моделі розглядається як підвищення якості внутрішніх процедур, а не лише виконання зовнішніх зобов'язань.

Першим ризиком є надмірна централізація, за якої координаційний орган починає втручатися у зміст усіх комунікацій. Запобіжником має бути нормативне розмежування стратегічної координації, операційної підтримки, регуляторних повноважень і редакційної незалежності. Обов'язковому погодженню підлягають лише спільна фактологічна основа та дії у визначених кризових випадках; інші комунікації здійснюються суб'єктами самостійно.

Другим ризиком є політизація та використання державної комунікації для партійних або персональних інтересів. Мінімізація потребує професійного статусу операційного офісу, конкурсних процедур, публічної методики пріоритетів, розмежування інформування про політику й політичної реклами, незалежного аудиту та механізму скарг. Публічні ресурси мають пояснювати рішення і права громадян, а не створювати персоналізований імідж посадовців.

Третій ризик пов'язаний із надмірним накопиченням даних. Його зменшення потребує принципів мінімізації, цільового використання, обмеження строків зберігання, розподіленої архітектури та оцінки впливу на приватність. Аналітика має працювати переважно з агрегованими даними; ідентифікація особи можлива лише за наявності правової підстави та компетенції уповноваженого органу [91; 153; 155; 157].

Четвертим ризиком є технологічна залежність і алгоритмічна упередженість. Автоматизовані системи можуть помилково пріоритезувати емоційний контент, недостатньо враховувати регіональні та мовні особливості або відтворювати упередження даних. Тому алгоритми повинні проходити тестування, документування, періодичний аудит і людський перегляд, особливо коли результати впливають на права або розподіл ресурсів.

П'ятим ризиком є нерівність участі, коли великі центральні органи та впливові партнери домінують, а громади, вразливі групи й локальні медіа залишаються одержувачами інформації. До регламенту слід включити

регіональне представництво, обов'язкову оцінку доступності, підтримку локалізації, спільні сервіси для невеликих суб'єктів і механізм фіксації неврахованих позицій.

Наукова новизна полягає у розвитку теоретичних засад реалізації державної інформаційної політики через обґрунтування інтегрованого організаційно-управлінського механізму, побудованого на принципі координованої поліцентричності. На відміну від моделей, що акцентують нормативний, інституційний або комунікаційний аспект, авторська конструкція поєднує в одному циклі стратегічне планування, аналіз середовища, вироблення рішення, комунікацію, кризове реагування, участь стейкхолдерів, цифрову підтримку та оцінювання.

Практичний ефект моделі полягає у скороченні часу між виявленням проблеми та підтвердженням реагуванням; зменшенні дублювання й суперечливості повідомлень; ранньому включенні комунікаційної функції до вироблення політики; підвищенні якості даних; посиленні регіональної спроможності; формуванні інституційної пам'яті та переході від звітування про активність до оцінювання суспільного результату. Запобіжники обмежують ризики цензури, політизації, надмірного збору даних і технологічної дискримінації.

Отже, інтегрований механізм має функціонувати як адаптивна система спільного вироблення та виконання рішень, у якій координація не усуває автономію, технологія не підміняє відповідальність, а безпекові заходи не заперечують демократичні права. Його впровадження створює основу для переходу від розрізненого інформування до стратегічно узгодженої, доказової, підзвітної та стійкої державної інформаційної політики.

3.2. Удосконалення механізмів стратегічних комунікацій та протидії дезінформації

Результати попереднього аналізу засвідчили, що інституційна наявність органів, стратегій і комунікаційних каналів сама по собі не гарантує спроможності держави діяти узгоджено в умовах швидкоплинних інформаційних криз. Основними обмеженнями залишаються фрагментарність відповідальності, переважання реактивного спростування над превентивним поясненням, відокремленість аналітики від процесу прийняття рішень, нерівномірність комунікаційної спроможності між центральним, регіональним і місцевим рівнями, а також недостатньо формалізовані процедури взаємодії з медіа, громадянським суспільством і цифровими платформами.

За умов гібридної агресії стратегічні комунікації не можуть розглядатися як сукупність пресрелізів, брифінгів або інформаційних кампаній, що супроводжують уже прийняті рішення. Їх управлінська природа полягає у забезпеченні відповідності між державною політикою, фактичними діями, публічними поясненнями та очікуваннями цільових аудиторій. Коли слова органів влади не узгоджуються з практикою, комунікація втрачає переконливість незалежно від інтенсивності поширення повідомлень. Саме тому сучасні підходи пов'язують ефективність стратегічних комунікацій із цілісністю управлінського циклу, міжвідомчою координацією, доказовістю та довірою.

Протидія дезінформації є складовою, але не вичерпує зміст стратегічних комунікацій. Зосередження виключно на спростуваннях змушує державу діяти у порядку денному, сформованому противником, і витратити ресурси на кожне окреме неправдиве повідомлення. Більш результативною є модель, у якій держава завчасно пояснює політику, підтримує доступність перевірених даних, готує аудиторії до розпізнавання типових маніпуляцій, швидко заповнює інформаційні вакууми та коригує комунікацію на підставі зворотного зв'язку [74; 76; 149; 150; 159; 161].

Українська практика протидії інформаційним загрозам сформувала значний досвід оперативного інформування, фактчекінгу, міжнародної адвокації

та залучення громадянського суспільства. Водночас наукові дослідження 2024–2026 років наголошують на збереженні правової й інституційної фрагментарності, нечіткості розмежування компетенцій, недостатній інтеграції цифрової аналітики та потребі в переході від ситуативних дій до системного управління комунікаційними ризиками.

Удосконалення має відбуватися не шляхом створення універсального органу, що одноосібно визначає допустимий зміст суспільної дискусії, а через стандартизацію процесів і відповідальності. Централізувати доцільно правила координації, критерії оцінки ризику, формати обміну даними, базові вимоги до доказовості та процедури післядієвого аналізу. Водночас змістова компетенція повинна залишатися за органами, які володіють предметними знаннями, а незалежні медіа й громадські організації мають зберігати автономність.

Перехід до вдосконаленої моделі потребує поєднання двох логік. Перша є проактивною та спрямована на формування зрозумілих суспільних смислів, пояснення державної політики й підтримання довіри. Друга є захисною та забезпечує виявлення, оцінювання і нейтралізацію дезінформаційних впливів. Їх роз'єднання спричиняє або надмірну оборонність, або відірвану від ризиків іміджеву комунікацію. Інтеграція дозволяє використовувати аналітичні сигнали не лише для спростування, а й для коригування політики, повідомлень і сервісів [36; 45; 150; 151].

Систематизацію основних проблем і відповідних напрямів їх усунення подано в таблиці 3.7. Вона виконує функцію переходу від діагностичної частини дослідження до проєктування конкретних управлінських рішень.

Таким чином, удосконалення не зводиться до збільшення кількості повідомлень або посилення контролю над інформаційним простором. Його зміст полягає у зміні управлінської логіки: від епізодичної реакції – до постійної готовності; від відомчої ізольованості – до процесної координації; від комунікації як супроводу – до комунікації як складової політики; від оцінювання активності – до оцінювання суспільного результату.

Проблеми чинної практики та напрями вдосконалення стратегічних комунікацій і протидії дезінформації

Проблема	Управлінський прояв	Запропоноване рішення	Очікуваний результат
Реактивність	Переважання спростувань після вірусного поширення	Впровадження прогнозування, пребанкінгу, календаря ризиків і підготовлених сценаріїв	Скорочення інформаційного вакууму та випереджальне формування пояснень
Фрагментація	Різні органи надають несумісні або запізнілі повідомлення	Єдині протоколи координації, ролі провідного органу й предметних експертів	Узгодженість позицій без надмірної централізації
Відрив комунікації від політики	Комунікаційні підрозділи залучаються після ухвалення рішення	Обов'язкова комунікаційна оцінка на етапі розроблення політики	Відповідність між рішенням, діями та публічним поясненням
Недостатня доказовість	Спростування без відкритих джерел або зрозумілої аргументації	Реєстр доказів, маркування рівня впевненості, повторна верифікація	Підвищення довіри та можливість незалежної перевірки
Нерівномірність спроможностей	Регіони й громади не мають фахівців та резервних каналів	Мережа регіональних вузлів, спільні сервіси, типові пакети й навчання	Єдині мінімальні стандарти на всіх рівнях
Надмірна орієнтація на охоплення	Кількість переглядів підміняє оцінку розуміння й поведінкових наслідків	Система результативних індикаторів, опитування, експерименти й аудит	Оцінювання реального внеску комунікації у цілі політики
Правові ризики	Нечіткі підстави обмеження контенту та непрозорі рішення	Тест законності, необхідності, пропорційності, строковості й оскарження	Захист прав людини та легітимність протидії
Нові технологічні загрози	Deepfake, синтетичний контент, ботомережі, алгоритмічне підсилення	Протокол цифрової автентичності, людський контроль, партнерство з платформами	Швидша верифікація й зменшення помилкових рішень

Джерело: розроблено автором

На основі узагальнення наукових підходів пропонується авторське визначення: удосконалений механізм стратегічних комунікацій та протидії дезінформації – це нормативно визначена, інституційно узгоджена, аналітично керована й технологічно підтримана сукупність суб'єктів, процедур, ресурсів та партнерських зв'язків, яка забезпечує проактивне формування суспільно значущих наративів, своєчасне пояснення державної політики, раннє виявлення й верифікацію інформаційних загроз, пропорційне реагування, захист інформаційних прав громадян і безперервне організаційне навчання [36; 45; 105; 150; 159; 160].

Ключовою особливістю цього визначення є одночасне охоплення управлінської, комунікаційної, безпекової та правозахисної складових. Воно виключає ототожнення стратегічних комунікацій із пропагандою, оскільки передбачає доказовість, відкритість джерел у межах допустимого, можливість перевірки, повагу до свободи вираження та наявність механізмів оскарження. Дезінформація нейтралізується не прихованим маніпулюванням, а якіснішим поясненням, перевіреними фактами, підвищенням стійкості аудиторій і застосуванням правових заходів лише за наявності чітких підстав.

Механізм доцільно будувати як двоконтурну систему. Проактивний контур відповідає за довгострокові наративи, пояснення реформ, суспільний діалог, міжнародну комунікацію, медіаграмотність і запобігання інформаційним вакуумам. Захисний контур здійснює ситуаційний моніторинг, виявлення координованих кампаній, верифікацію, кризове реагування, взаємодію з платформами й післядієвий аналіз. Обидва контури використовують спільні ціннісні орієнтири, аналітичну платформу, стандарти доказовості та систему оцінювання.

Структуру двоконтурного механізму відображено на рис. 3.5. Усі його елементи оформлено як редаговану схему, що дає змогу адаптувати модель до конкретної інституційної архітектури.

ЦІННІСНО-ПРАВОВЕ ЯДРО права • верховенство права • свобода слова • відповідальність • національна стійкість		
ПРОАКТИВНИЙ КОНТУР	СПІЛЬНА АНАЛІТИКА І КООРДИНАЦІЯ	ЗАХИСНИЙ КОНТУР
Наративи й пояснення політики публічна дипломатія діалог і медіаграмотність	Карта аудиторій календар ризиків реєстр фактів ситуаційна панель	Виявлення й верифікація класифікація інцидентів оперативна реакція
Попереднє тестування доступні формати мережа партнерів	Єдині процедури рольова відповідальність журнал рішень	Взаємодія з медіа і платформами правові заходи відновлення довіри
ЗВОРОТНИЙ ЗВ'ЯЗОК: опитування • звернення • медіааналіз • громадські консультації • регіональні сигнали		
ОЦІНЮВАННЯ І НАВЧАННЯ: результати • аудит прав • післядієвий аналіз • оновлення сценаріїв і стандартів		

Рис. 3.5. Двоконтурний механізм стратегічних комунікацій та протидії дезінформації

Джерело: розроблено автором

Запропонована конструкція дозволяє уникнути протиставлення «комунікації» та «безпеки». Проактивний контур зменшує вразливість, а захисний – обмежує шкоду від конкретних атак. Спільний аналітичний центр не підміняє органи влади, а забезпечує єдину картину середовища, узгоджує критерії та фіксує рішення. Зворотний зв'язок повертає інформацію про сприйняття політики до етапу її проектування.

Для практичної реалізації механізму пропонується система принципів, кожен із яких має бути перетворений на операційну вимогу. Декларативність принципів долається через визначення конкретних процедур, відповідальних осіб і контрольних показників.

Таблиця 3.8.

Принципи вдосконаленого механізму та їх операційне втілення

Принцип	Зміст	Операційна вимога	Контрольний доказ
Правдивість і доказовість	Повідомлення ґрунтуються на перевірених даних, невизначеність не приховується	Щонайменше два незалежні джерела для критичних тверджень або мотивоване пояснення винятку	Картка верифікації, посилання на первинне джерело
Узгодженість слів і дій	Комунікація відповідає реальному змісту політики й поведінці інституцій	Комунікаційна експертиза проєкту рішення до його ухвалення	Паспорт політики та погоджена матриця повідомлень
Проактивність	Держава формує порядок денний і пояснює ризики до виникнення вакууму	Календар прогнозованих тем і підготовлені сценарії	Щомісячний план випереджальних комунікацій
Пропорційність	Інтенсивність реагування відповідає масштабу шкоди та достовірності сигналу	Рівні інцидентів і порогові критерії ескалації	Протокол класифікації та журнал рішень
Людиноцентричність	Враховуються потреби, мова, доступність, безпека та контекст аудиторій	Сегментація, тестування матеріалів і альтернативні формати	Звіт тестування й аудит доступності
Партнерство	Медіа, наука, громади й платформи залучаються без втрати автономії	Меморандуми, контактні мережі, спільні навчання	Реєстр партнерств та оцінка їх результативності
Підзвітність	Рішення про обмеження або спростування можна перевірити й оскаржити	Фіксація правової підстави, строку, автора та процедури перегляду	Публічний або службовий реєстр рішень
Адаптивність	Сценарії та повідомлення змінюються на основі даних і уроків	Післядієвий аналіз кожного значного інциденту	План коригувальних заходів і контроль виконання

Джерело: запропоновано автором з урахуванням [45; 48; 84; 119; 150; 151; 159; 160].

Операціоналізація принципів створює єдиний стандарт поведінки для різних органів влади. Вона також дозволяє оцінювати не лише кінцевий

інформаційний продукт, а й якість процесу його підготовки: чи була перевірена інформація, чи залучено предметного експерта, чи проведено оцінку правових ризиків, чи зафіксовано причини зміни позиції.

Наратив у системі стратегічних комунікацій доцільно розуміти не як гасло, а як стійку причинно-наслідкову рамку, яка пояснює, хто є суб'єктом дії, яку проблему він вирішує, на яких цінностях ґрунтується рішення, які зміни очікуються та за якими фактами можна перевірити прогрес. Наратив не повинен замінювати факти; навпаки, він упорядковує факти та робить політику зрозумілою для різних аудиторій [78; 137; 138; 144].

Важливо розмежовувати стратегічний наратив, повідомлення і комунікаційний продукт. Наратив задає довгострокову логіку; повідомлення конкретизує її для певної теми й аудиторії; продукт є матеріальною формою – виступом, інфографікою, відео, відповіддю на запит або роз'ясненням. Таке розмежування знижує ризик механічного тиражування однакових фраз і дозволяє адаптувати форму без зміни суті.

Пропонується запровадити «паспорт стратегічного наративу», який містить правову основу, ціннісну тезу, перевірювані факти, цільові аудиторії, потенційні хибні інтерпретації, чутливі питання, набір доказів, допустимі межі розкриття інформації та індикатори сприйняття. Паспорт не є інструментом цензури; це внутрішній документ якості, що забезпечує послідовність і дає змогу швидко оновлювати повідомлення при зміні обставин.

Каскад формування й реалізації стратегічного наративу показано на рис. 3.6. Він забезпечує зв'язок між цілями політики та конкретними продуктами, а також повертає реакцію аудиторій до управлінського циклу.

На етапі матриці аудиторій необхідно відмовитися від спрощеного поділу лише за віком або територією. Для державної політики значення мають рівень попереднього знання, доступ до каналів, довіра до інституцій, досвід взаємодії з державою, ризик уразливості, мовні та сенсорні потреби. Комунікація, яка ігнорує ці характеристики, може бути формально правильною, але практично недоступною.

1. ДЕРЖАВНА ЦІЛЬ І ПУБЛІЧНА ПРОБЛЕМА	Що має змінитися та чому це важливо
↓ 2. ЦІННІСНА РАМКА	Конституційні принципи, суспільні інтереси, права людини
↓ 3. СТРАТЕГІЧНИЙ НАРАТИВ	Причинно-наслідкове пояснення та довгострокова логіка
↓ 4. МАТРИЦЯ АУДИТОРІЙ	Потреби, бар'єри, ризики, канали, рівень знань
↓ 5. ПОВІДОМЛЕННЯ І ДОКАЗИ	Тези, факти, джерела, відповіді на складні питання
↓ 6. ПРОДУКТИ І КАНАЛИ	Брифінги, сайти, медіа, соцмережі, прямі консультації
↻ 7. ЗВОРОТНИЙ ЗВ'ЯЗОК І КОРИГУВАННЯ	Розуміння, довіра, помилки, запити, зміна поведінки

Рис. 3.6. Каскад наративного планування стратегічних комунікацій

Джерело: розроблено автором

Узгодженість повідомлень не означає абсолютну ідентичність текстів. Центральний орган формулює незмінне смислове ядро, предметні органи уточнюють факти, а регіональні й місцеві суб'єкти адаптують пояснення до контексту. Обов'язковими залишаються правдива основа, відсутність суперечностей, чітке розмежування підтверджених фактів і прогнозів, а також єдині правила повідомлення про зміну позиції.

Оперативна протидія дезінформації залежить не від максимально широкого моніторингу, а від здатності перетворювати сигнали на перевірене управлінське знання. Для цього пропонується багатоджерельна система ситуаційної обізнаності, що поєднує звернення громадян, повідомлення регіональних органів, моніторинг відкритих джерел, аналітику медіа, дані партнерських організацій, сигнали цифрових платформ і предметну експертизу [22; 37; 45; 145; 150].

Кожний сигнал має отримувати структуровану картку: зміст твердження; первинне джерело; час і географія поширення; ознаки координованості; потенційно вразливі аудиторії; можливий зв'язок із реальною подією; правовий режим інформації; попередній рівень достовірності; очікувана шкода. Така стандартизація запобігає прийняттю рішень на підставі емоційної реакції або популярності окремого допису.

Для відокремлення суспільно небезпечної кампанії від звичайної критики пропонується оцінювати щонайменше п'ять критеріїв: навмисність, недостовірність або маніпулятивність, координованість, масштаб потенційної

шкоди та зв'язок із захищеним суспільним інтересом. Негативна оцінка діяльності органу влади сама по собі не є дезінформацією. Такий підхід відповідає вимогам пропорційності та зменшує ризик використання безпекової риторики для обмеження демократичної дискусії [35; 48; 84; 117; 119; 160].

Система раннього попередження повинна працювати з прогнозованими ризиками. Календар ризиків формується на основі майбутніх рішень, річниць, кризових сезонів, виборчих і міжнародних подій, змін у наданні послуг та тем, щодо яких уже існує дефіцит довіри. Для кожної теми готуються перевірені довідки, спікери, шаблони запитань і відповідей, резервні канали та критерії ескалації.

Пропонується чотирирівнева класифікація інформаційних інцидентів, наведена в таблиці 3.9. Часові параметри мають характер авторських цільових стандартів і можуть уточнюватися після пілотування.

Таблиця 3.9.

Запропоновані рівні інформаційних інцидентів і стандарти реагування

Рівень	Критерії	Провідний суб'єкт	Перша дія	Цільовий час	Форма реагування
I — локальний	Обмежене охоплення; низька ймовірність шкоди; відсутність скоординованості	Комунікаційний підрозділ предметного органу або громади	Перевірка факту, уточнення першоджерела	до 2 годин	Точкова відповідь, оновлення сторінки, робота з автором запиту
II — міжрегіональний	Швидке поширення; кілька каналів; ризик для окремої політики або групи	Провідний центральний орган із регіональною мережею	Міжвідомча верифікація та узгодження позиції	до 60 хвилин	Консолідоване роз'яснення, брифінг, партнерське поширення
III — національний	Високий суспільний резонанс; скоординована кампанія; ризик паніки або недовіри	Міжвідомча кризова група	Активація кризового протоколу та єдиного ситуаційного звіту	до 30 хвилин	Перше підтверджене повідомлення, регулярні оновлення, робота з платформами
IV — стратегічний	Загроза національній безпеці, критичній інфраструктурі, міжнародній підтримці або життю	Стратегічний рівень координації з уповноваженими безпековими органами	Безперервний режим, правова й безпекова оцінка	до 15 хвилин для активації	Національна та міжнародна комунікація, спеціальні правові й технічні заходи

Джерело: розроблено автором

Перевагою рівневої моделі є економія ресурсів і передбачуваність. Не кожне неправдиве твердження потребує загальнонаціонального спростування, яке іноді лише збільшує його видимість. Водночас відсутність швидкої реакції на критичну загрозу створює інформаційний вакуум. Формальні пороги допомагають збалансувати ці ризики.

Для значних інцидентів пропонується стандартна операційна процедура, що складається з послідовних етапів: реєстрація сигналу; первинний скринінг; предметна верифікація; оцінка масштабу й шкоди; правова перевірка; вибір сценарію; підготовка першого повідомлення; розгортання доказової комунікації; моніторинг реакції; завершення та післядієвий аналіз. Відсутність хоча б одного етапу підвищує ймовірність помилкового спростування або запізненої відповіді.

Перший публічний коментар не завжди має містити повне спростування. За дефіциту підтверджених даних доцільно повідомити, що інформацію перевіряють, назвати джерело майбутнього оновлення та визначити орієнтовний час наступного повідомлення. Така практика знижує вакуум, але не створює ілюзії впевненості. Після завершення перевірки необхідно чітко відокремити підтверджені факти, невстановлені обставини й оцінки.

Верифікація має бути предметною: комунікаційний фахівець не може самостійно визначати істинність складних військових, медичних, енергетичних або фінансових тверджень. За кожною тематикою формується мережа чергових експертів і резервних контактів. Для критичних тверджень застосовується правило двох джерел, якщо інше не обумовлено режимом секретності чи невідкладністю.

Вибір форми відповіді залежить від співвідношення шкоди й ризику додаткового поширення. Можливі сценарії: не реагувати публічно, але вести моніторинг; надати точкове уточнення; оприлюднити коротке спростування; підготувати розгорнуте пояснення; організувати брифінг; залучити незалежних експертів; передати платформі обґрунтований сигнал; застосувати передбачені законом заходи. Рішення має бути зафіксованим і переглядатися при появі нових даних [18; 35; 59; 63; 66; 117].

Алгоритм реагування подано на рис. 3.7. Схема включає точки правової та аналітичної перевірки, що запобігають автоматичному ототожненню будь-якого небажаного контенту з дезінформацією.

СИГНАЛ	РЕЄСТРАЦІЯ	ПЕРВИННИЙ СКРИНІНГ
Чи стосується захищеного суспільного інтересу?	НІ → моніторинг / звичайна комунікація	ТАК → предметна верифікація
ОЦІНКА ДОСТОВІРНОСТІ	ОЦІНКА КООРДИНОВАНOSTІ	ОЦІНКА ШКОДИ
ПРАВОВИЙ ТЕСТ	законність • мета • необхідність	пропорційність • строк • оскарження
ВИБІР СЦЕНАРІЮ	мовчазний моніторинг • уточнення • спростування	роз'яснення • брифінг • платформа • правовий захід
ПЕРШЕ ПОВІДОМЛЕННЯ	що відомо / що перевіряється	коли і де буде оновлення
ДОКАЗОВА ВІДПОВІДЬ	первинні дані • експерт • доступний формат	адаптація до аудиторій • партнерське поширення
МОНІТОРИНГ → КОРИГУВАННЯ → ПІСЛЯДІЄВИЙ АНАЛІЗ	охоплення • розуміння • довіра	уроки • відповідальність • оновлення сценаріїв

Рис. 3.7. Алгоритм виявлення, верифікації та реагування на дезінформаційний інцидент

Джерело: розроблено автором

Важливою процедурою є виправлення власних помилок державного органу. Видалення некоректного повідомлення без пояснення погіршує довіру. Пропонується стандарт корекції: зберегти посилання або архів первинної версії, чітко назвати помилку, подати правильні дані, пояснити причину виправлення та вказати час оновлення. Культура відкритого виправлення демонструє пріоритет точності над репутаційним самозахистом.

Післядієвий аналіз повинен проводитися не лише після невдалих інцидентів. Для успішних кейсів також необхідно встановити, які фактори забезпечили результат: готовність даних, авторитет спікера, вибір каналу, партнерське поширення або попереднє тестування. Висновки перетворюються на конкретні зміни сценаріїв, контактних списків, навчальних програм і нормативних документів.

Превентивна складова має включати не лише загальну медіаграмотність, а й тематичне попередження про ймовірні маніпуляції. Перед прогнозованою кризою громадянам доцільно пояснювати, які ознаки матимуть фальшиві

повідомлення, де перевіряти інформацію, які дані офіційні органи не запитують через неформальні канали та як діяти за відсутності зв'язку. Такий підхід знижує ефективність майбутньої атаки без повторення її конкретного неправдивого змісту [147; 149; 150; 159; 161].

Спростування має бути побудоване так, щоб не закріплювати неправдиву тезу в пам'яті. Доцільною є структура «факт – коротке попередження про маніпуляцію – пояснення – повторення факту – практична дія». Заголовок і перші речення повинні містити правильну інформацію, а не емоційне відтворення фейку. Для складних тем додається доступне первинне джерело й пояснення методики.

Особливе значення має створення постійної бази перевірених фактів, що містить не лише спростування, а й відповіді на повторювані питання, набори відкритих даних, експертні контакти, візуалізації та історію оновлень. Публічний модуль такої бази полегшує роботу журналістів і громадських фактчекерів; службовий модуль забезпечує швидке повторне використання доказів у кризі.

Склад інструментарію за етапами комунікаційного циклу систематизовано в таблиці 3.10.

Таблиця 3.10.

Інструменти стратегічних комунікацій і протидії дезінформації за етапами управлінського циклу

Етап	Основні інструменти	Управлінська мета	Типовий результат
Передбачення	Календар ризиків, сценарний аналіз, соціальне слухання, експертні мережі	Виявити теми, де можливий вакуум або маніпуляція	Карта ризиків і готові сценарії
Проектування політики	Комунікаційна експертиза, карта аудиторій, паспорт нарративу, правовий тест	Узгодити зміст рішення з його поясненням	Матриця повідомлень і доказів
Підготовка	Претестування, FAQ, навчання спікерів, доступні формати, резервні канали	Зменшити ймовірність неоднозначного сприйняття	Пакет готовності до запуску
Реалізація	Брифінги, сайти, медіа, соцмережі, прямі консультації, партнерські кампанії	Донести факти й забезпечити діалог	Своєчасне та сегментоване інформування
Реагування	Верифікація, спростування, розгорнуте пояснення, координація з платформами	Обмежити шкоду й відновити фактичну картину	Підтверджена позиція та коригувальні дії
Оцінювання	Опитування, контент-аналіз, вимірювання розуміння, аудит прав, after-action review	Встановити реальний внесок комунікації	Звіт результативності й план удосконалення

Джерело: систематизовано автором за [23; 45; 55; 137; 144; 150; 151; 159].

Таблиця демонструє, що протидія дезінформації починається задовго до появи фейку. Якість політики, доступність даних, готовність спікерів та передбачуваність процедур є такими ж важливими інструментами стійкості, як фактчекінг або взаємодія з цифровими платформами.

Цифрове середовище змінило швидкість і масштаб поширення інформації, а генеративний штучний інтелект знизив вартість створення переконливого синтетичного контенту. Deepfake-відео, імітація голосу, автоматизовані мережі та масове персоналізоване поширення потребують не лише технічного виявлення, а й організаційної готовності: наявності еталонних записів, перевірених каналів, процедури підтвердження автентичності й заздалегідь визначеного спікера [36; 66; 145; 157].

Пропонується запровадити протокол цифрової автентичності офіційних повідомлень. Він передбачає публікацію критично важливого контенту через перелік підтверджених каналів; використання кваліфікованих електронних засобів там, де це доцільно; збереження оригіналів і метаданих; швидку перевірку підозрілих копій; резервний канал підтвердження; видиме повідомлення про виправлення або компрометацію. Протокол має бути зрозумілим громадянам і журналістам.

Алгоритмічні інструменти моніторингу можуть допомагати групувати схожі повідомлення, виявляти аномальне поширення та визначати теми для експертної перевірки. Однак вони не повинні автоматично встановлювати неправдивість або санкціонувати обмеження. Висновок системи є сигналом, а не доказом; рішення приймає уповноважена особа, яка бачить джерела, методику й рівень помилки. Необхідні журналювання, тестування упереджень і періодичний аудит.

Взаємодія з платформами має бути формалізована через контактні точки, стандартизовану форму повідомлення, вимоги до збереження доказів, строки відповіді та можливість перегляду. Передання сигналу про контент повинно містити конкретну правову або політичну підставу, опис шкоди й підтверджені дані. Масове надсилання необґрунтованих запитів послаблює довіру й створює ризик надмірного блокування [64; 66; 141; 154].

Ефективна стратегічна комунікація не може бути виключно вертикальною. Незалежні медіа забезпечують перевірку і переклад складних рішень мовою суспільної дискусії; громадські організації мають доступ до локальних аудиторій і досвід фактчекінгу; наукові установи розробляють методики та оцінюють результати; цифрові платформи володіють інструментами поширення і даними про координовану поведінку. Партнерство підвищує охоплення і легітимність, якщо не перетворюється на залежність або приховане управління редакційною політикою.

Для медіа пропонується система рівного доступу до перевірених фактів: регулярні технічні брифінги, відкриті набори даних, контактні списки предметних експертів, можливість уточнювати методику, публічний календар оновлень і зрозумілі правила роботи з чутливою інформацією. Орган влади не повинен вимагати некритичного відтворення своєї позиції; його завдання – забезпечити якість і своєчасність джерел [82; 84; 95; 101; 109; 156].

Громадські фактчекери та дослідницькі центри можуть залучатися до спільних навчань, незалежного тестування сценаріїв, оцінювання інформаційних кампаній і розроблення методик. Водночас державне фінансування таких проєктів має бути прозорим, конкурсним і не впливати на незалежність висновків. Результати досліджень, що не містять чутливих даних, доцільно оприлюднювати.

На регіональному рівні доцільно створити мережу контактних вузлів, що поєднує органи влади, громади, місцеві медіа, заклади освіти й громадські організації. Їх функція полягає в передачі ранніх сигналів, адаптації загальнонаціональних пояснень, підтриманні резервних каналів та роботі з групами, які мають обмежений доступ до цифрової інформації [25; 55; 158].

Модель партнерської взаємодії представлено на рис. 3.8. В її центрі перебуває не державний контроль над усіма учасниками, а спільний стандарт фактів, прозорості та захисту прав.

ОРГАНИ ПУБЛІЧНОЇ ВЛАДИ		МЕДІА		ЦИФРОВІ ПЛАТФОРМИ
ГРОМАДИ Й ОСВІТА		СПІЛЬНЕ ЯДРО верифіковані факти правила координації правові гарантії відкриті методики		ГРОМАДСЬКІ ОРГАНІЗАЦІЇ
НАУКОВІ УСТАНОВИ		МІЖНАРОДНІ ПАРТНЕРИ		ПРОФЕСІЙНІ СПІЛЬНОТИ

Рис. 3.8. Партнерська екосистема стратегічних комунікацій і протидії дезінформації

Джерело: розроблено автором

Партнерська модель створює множинність незалежних каналів підтвердження. Саме така множинність, а не монополія на трактування подій, підвищує стійкість демократичного інформаційного середовища. Держава зберігає відповідальність за офіційні дані й безпекові рішення, але визнає право партнерів на критичну оцінку та власні висновки.

Вдосконалення протидії дезінформації має супроводжуватися посиленням гарантій свободи слова, доступу до інформації, захисту приватності та незалежності медіа. Без таких запобіжників короткострокова ефективність може обернутися довгостроковою втратою довіри. Конституційні гарантії та спеціальне законодавство вимагають чіткого розмежування між спростуванням, модерацією, обмеженням доступу й юридичною відповідальністю [48; 84; 91; 93; 95; 119].

Пропонується обов'язковий правовий тест для будь-якого рішення, що може обмежити поширення інформації або вплинути на права особи. Тест включає: наявність закону; визначену легітимну мету; доведену необхідність; найменш обмежувальний засіб; пропорційність очікуваній шкоді; часові межі; документування; повідомлення особи, якщо це не створює додаткового ризику; можливість адміністративного або судового оскарження; подальший перегляд.

Окремо слід розмежувати державну комунікацію і психологічні операції. Комунікація з власними громадянами повинна бути правдивою, відкритою щодо джерела та спрямованою на усвідомлене розуміння. Приховане маніпулювання,

фабрикація фактів або використання персональних даних для експлуатації вразливостей несумісні з демократичним публічним управлінням. Безпеківі операції мають здійснюватися уповноваженими суб'єктами в межах спеціального правового режиму [13; 17; 42; 75; 130].

Система правових та етичних запобіжників зведена в таблиці 3.11.

Таблиця 3.11.

Правові та етичні запобіжники в механізмі протидії дезінформації

Ризик	Запобіжник	Процедурне забезпечення	Форма підзвітності
Помилкове визнання критики дезінформацією	Чіткі критерії навмисності, недостовірності, координованості та шкоди	Подвійна експертна оцінка для рішень із правовими наслідками	Мотивоване рішення і можливість перегляду
Надмірне обмеження свободи вираження	Тест законності, необхідності й пропорційності	Вибір найменш обмежувального заходу та строк дії	Публічна статистика, парламентський і судовий контроль
Порушення приватності під час моніторингу	Мінімізація даних, цільове призначення, рольовий доступ	Оцінка впливу на захист даних, журнал доступу, строки видалення	Аудит і повідомлення про порушення
Алгоритмічне упередження	Людський контроль, тестування точності й групових помилок	Валідація моделей, документування даних і меж застосування	Незалежний технічний аудит
Прихована державна пропаганда	Ідентифікація офіційного джерела й заборона фабрикації фактів	Редакційний стандарт і внутрішній контроль якості	Оприлюднення політик та виправлення помилок
Тиск на незалежні медіа або партнерів	Прозорі правила доступу та фінансування, відсутність вимоги лояльності	Конкурсні процедури, рівні умови, конфлікт інтересів	Громадський нагляд і публічні звіти

Джерело: розроблено автором

Запобіжники не є перешкодою для оперативності. Навпаки, завчасно погоджені тести й шаблони дозволяють приймати швидкі рішення без імпровізації та зменшують ризик їх подальшого скасування. Найбільш чутливі рішення доцільно піддавати прискореному незалежному перегляду після завершення гострої фази інциденту.

Механізм залишатиметься формальним без професійної команди. Потрібен міждисциплінарний профіль, що поєднує знання публічного управління, права, аналізу даних, соціальних досліджень, журналістики, кризової комунікації, кібербезпеки та поведінкових наук. Неможливо вимагати

всіх компетентностей від однієї особи; тому доцільні командні ролі й спільні сервіси.

Пропонується запровадити базовий професійний стандарт для фахівців державних стратегічних комунікацій. Він має містити компетентності з планування, сегментації аудиторій, верифікації, роботи з відкритими даними, прав людини, цифрової безпеки, використання штучного інтелекту, комунікації невизначеності, оцінювання та післядієвого аналізу. Для керівників потрібні модулі з управління ризиком і міжвідомчої координації.

Навчання доцільно будувати на сценаріях, а не лише на лекціях. Команди мають відпрацьовувати випадки *deepfake*, витоку даних, інформаційного вакууму після технічної аварії, суперечливих заяв різних органів, масового поширення неправдивих порад і міжнародної дезінформаційної кампанії. Оцінюються не риторичні навички, а здатність отримати факти, визначити межі розкриття, узгодити ролі, діяти в часі та документувати рішення.

Для регіонів і громад доцільно створити спільний навчально-методичний центр, дистанційні модулі, бібліотеку шаблонів і мобільні команди підтримки. Мінімальна спроможність кожної громади повинна включати призначену контактну особу, перелік резервних каналів, доступ до верифікованої бази фактів, порядок ескалації та зв'язок із регіональним вузлом.

Впровадження доцільно здійснювати поетапно, щоб уникнути одночасного запровадження великої кількості формальних процедур без реальної зміни практики. На підготовчому етапі необхідні інвентаризація чинних протоколів, визначення пілотних тем, базове вимірювання спроможності та формування міжвідомчої групи. Далі апробуються двоконтурна модель, класифікація інцидентів, паспорти наративів і показники.

Пілотування доцільно проводити на темах, які мають високий суспільний інтерес, але дозволяють безпечно відпрацьовувати процедури: комунікація державних послуг, європейської інтеграції, енергетичної стійкості, цивільного захисту або реінтеграції. Після оцінювання модель масштабується на регіони й критичні напрями, а успішні процедури закріплюються в нормативних та організаційних документах [27; 45; 112].

Фінансування має передбачати не лише інформаційні кампанії, а й аналітику, підготовку персоналу, доступність, резервні канали, аудит та оцінювання. Без цих витрат видимий контент створюватиметься без інфраструктури якості. Доцільно окремо планувати кошти на незалежні дослідження і тестування, що підвищують доказовість управлінських рішень.

Таблиця 3.13.

Дорожня карта впровадження механізмів стратегічних комунікацій та протидії дезінформації

Етап	Строк	Ключові заходи	Результат	Критерій переходу
I. Підготовка	0–4 місяці	Інвентаризація; базове вимірювання; визначення ролей; проекти стандартів; вибір пілотів	Карта процесів, перелік прогалин, пакет проєктів документів	Затверджені відповідальні та ресурси
II. Пілотування	5–12 місяців	Паспорти наративів; рівні інцидентів; база фактів; навчання; дві міжвідомчі симуляції	Перевірені процедури та перша база показників	Не менше 80 % пілотних процесів виконано за стандартом
III. Масштабування	13–24 місяці	Підключення регіонів; партнерські протоколи; цифрова платформа; аудит доступності й прав	Єдина мережа та уніфікована звітність	Досягнення мінімальних значень готовності й доказовості
IV. Інституціоналізація	25–36 місяців	Нормативне закріплення; стабільне бюджетування; професійний стандарт; зовнішнє оцінювання	Сталий механізм із регулярним навчанням	Виконання не менше 85 % рекомендацій аудиту
V. Оновлення	Після 36 місяців	Перегляд сценаріїв; тестування нових технологій; міжнародна взаємодія; повторне вимірювання	Адаптивна модель, сумісна з європейськими підходами	Позитивна динаміка результативних індикаторів

Джерело: розроблено автором

Реалізація дорожньої карти потребує визначення власника кожного процесу. Стратегічний рівень затверджує цілі й стандарти; координаційний рівень підтримує спільні процедури; предметні органи відповідають за достовірність фактів; регіональні вузли забезпечують адаптацію; незалежні партнери беруть участь у тестуванні та оцінюванні. Такий розподіл виключає ситуацію, коли «всі відповідають» за комунікацію, але ніхто не несе відповідальності за конкретний результат.

Отже, запропонована двоконтурна модель поєднує проактивне пояснення політики, раннє попередження, доказову верифікацію, пропорційне реагування,

партнерство, правові гарантії та оцінювання. Це перетворює розрізнені заходи на підзвітний і адаптивний механізм реалізації державної інформаційної політики.

3.3. Система моніторингу й оцінювання ефективності реалізації державної інформаційної політики

Розроблення дієвих механізмів державної інформаційної політики потребує переходу від фіксації кількості проведених заходів до системного встановлення того, які зміни вони спричиняють у доступності інформації, якості публічної комунікації, довірі до інституцій, інформаційній стійкості та здатності держави своєчасно реагувати на загрози. За відсутності узгодженої системи моніторингу органи публічної влади формують розрізнені звіти, використовують несумісні показники та переважно оцінюють власну активність, а не суспільний результат. Це ускладнює порівняння, не дає змоги виявляти причинно-наслідкові зв'язки та послаблює підзвітність державної інформаційної політики.

У межах запропонованого інтегрованого організаційно-управлінського механізму система моніторингу й оцінювання має виконувати не контрольну функцію у вузькому розумінні, а функцію управлінського навчання. Її призначення полягає у регулярному збиранні перевірених даних, порівнянні фактичних результатів із базовими та цільовими значеннями, поясненні причин відхилень, визначенні внеску окремих інструментів, виявленні непередбачених наслідків і перетворенні висновків на коригувальні рішення. Такий підхід відповідає сучасному розумінню публічної комунікації як невід'ємної частини політичного циклу, а не допоміжної діяльності пресслужб.

Наукове й прикладне значення має чітке розмежування моніторингу, оцінювання, контролю, аудиту та публічної звітності. Моніторинг є безперервним або періодичним спостереженням за перебігом реалізації політики на підставі заздалегідь визначених показників. Оцінювання здійснюється у певний момент і спрямоване на пояснення доцільності, результативності, ефективності, впливу та стійкості політики. Контроль перевіряє дотримання рішень і процедур, аудит – достовірність, законність або належність

використання ресурсів, а звітність забезпечує представлення результатів уповноваженим суб'єктам і громадськості. Змішування цих процесів призводить до переважання формальної перевірки над аналітичним навчанням.

Специфіка державної інформаційної політики ускладнює оцінювання. Її результати залежать від дій багатьох суб'єктів, динаміки медіасередовища, зовнішніх інформаційних операцій, кризових подій, технологічних змін і початкового рівня довіри. Один і той самий комунікаційний продукт може бути по-різному сприйнятий аудиторіями, а позитивна зміна не завжди безпосередньо пов'язана з діями конкретного органу влади. Тому система має оцінювати не лише прямий причинний вплив, який часто неможливо ізолювати, а й обґрунтований внесок державних заходів у спостережуваний результат [136; 137; 138; 151].

Ефективність у досліджуваній сфері не може бути зведена до економності витрат. Вона охоплює щонайменше п'ять взаємопов'язаних характеристик: відповідність заходів визначеним суспільним потребам; досягнення запланованих результатів; співвідношення результату та використаних ресурсів; справедливість розподілу інформаційних можливостей між групами населення; стійкість до криз і маніпулятивних впливів. Додатковою умовою є правомірність, оскільки навіть результативний захід не може вважатися ефективним, якщо він непропорційно обмежує свободу вираження поглядів, право на доступ до інформації або захист персональних даних.

У дисертації пропонується таке авторське визначення: система моніторингу й оцінювання ефективності реалізації державної інформаційної політики – це інституційно, методично та технологічно впорядкована сукупність суб'єктів, показників, джерел даних, процедур аналізу, правил верифікації, форм звітності й механізмів зворотного зв'язку, що забезпечує безперервне спостереження за реалізацією політики, періодичне визначення її релевантності, результативності, ефективності, впливу, правомірності та стійкості, а також використання доказів для коригування управлінських рішень і публічної підзвітності.

Запропоноване визначення принципово поєднує технічний і управлінський виміри. Наявність цифрової панелі або набору статистичних показників ще не утворює систему, якщо не встановлено відповідальних суб'єктів, правила перевірки даних, порядок розгляду відхилень і обов'язок приймати рішення за результатами аналізу. Водночас управлінські процедури без належної інформаційної інфраструктури залишаються залежними від ручного збирання даних, вибіркового звітування та суб'єктивних оцінок.

Таблиця 3.14.

Розмежування складових доказового супроводу державної інформаційної політики

Складова	Основне питання	Час здійснення	Типові методи	Управлінський продукт
Моніторинг	Що відбувається і чи відповідає перебіг плану?	Постійно або з установленою періодичністю	Адміністративні дані, вебаналітика, реєстр заходів, спостереження	Оперативна панель, попередження, квартальний звіт
Оцінювання	Чому отримано такий результат і який внесок політики?	До, під час або після циклу політики	Опитування, інтерв'ю, порівняння, кейс-стаді, внесковий аналіз	Оціночний звіт, рекомендації, рішення про продовження або зміну
Контроль	Чи виконано рішення, строки та обов'язкові процедури?	За графіком або при виявленні порушення	Перевірка документів, контрольні листи, службовий розгляд	Припис, коригувальний план, дисциплінарне рішення
Аудит	Чи є дані, витрати й процеси достовірними, законними та належними?	Періодично незалежно від операційного управління	Фінансовий, відповідності, ефективності, інформаційний аудит	Аудиторський висновок і план усунення недоліків
Публічна звітність	Що зроблено, чого досягнуто і як використано ресурси?	Регулярно та після завершення програм	Відкриті дані, річні звіти, публічні обговорення	Звіт для громадськості, набір даних, протокол консультацій

Джерело: систематизовано автором за [69; 115; 124; 150; 151; 159].

Розмежування, наведене в таблиці 3.14, не передбачає ізоляції окремих функцій. Дані моніторингу є основою оцінювання; результати аудиту впливають на довіру до показників; контроль забезпечує виконання коригувальних рішень; публічна звітність повертає громадянам інформацію про досягнення та обмеження політики. Система має будуватися так, щоб одна й та сама інформація повторно не запитувалася різними органами, а первинні дані могли використовуватися для кількох аналітичних завдань із дотриманням правових режимів.

Система моніторингу й оцінювання повинна ґрунтуватися на принципах законності, цільової релевантності, методичної обґрунтованості, незалежності оцінки, пропорційності збору даних, своєчасності, інтегрованості, захисту персональних даних, відкритості результатів, участі заінтересованих сторін та обов'язковості управлінського реагування. Кожен принцип має бути закріплений у методичному стандарті та переведений у конкретну вимогу: наприклад, своєчасність – у граничний строк оновлення показника, незалежність – у правила залучення зовнішніх оцінювачів, а відкритість – у перелік даних, що публікуються у машинозчитуваному форматі [84; 88; 91; 98; 150; 159].

Інституційна архітектура має поєднувати централізоване встановлення стандартів із децентралізованим формуванням первинних даних. Надмірна централізація створює вузьке місце, зменшує розуміння галузевої специфіки й підвищує ризик політичного контролю над оцінками. Повна децентралізація, навпаки, призводить до несумісності показників. Оптимальним є розподіл, за якого координаційний рівень затверджує методологію, словник даних і базові індикатори, а власники політик доповнюють їх галузевими показниками та відповідають за якість первинної інформації.

Доцільно сформувати постійний міжвідомчий методичний осередок, який не дублює повноваження органів, а забезпечує ведення реєстру показників, методичну підтримку, перевірку сумісності даних, підготовку консолідованого звіту й організацію незалежних оцінювань. У межах кожного центрального органу визначається власник результату, аналітичний координатор і розпорядники наборів даних. На регіональному та місцевому рівнях функції можуть виконуватися наявними підрозділами стратегічного планування, цифровізації та комунікацій за умови чіткого розмежування ролей.

Інституційну архітектуру системи відображено на рис. 3.9. Вона складається з чотирьох рівнів і трьох наскрізних контурів: даних, аналітики та управлінського реагування.

СТРАТЕГІЧНИЙ РІВЕНЬ	Єдині цілі, методичний стандарт, національні індикатори	Рішення щодо пріоритетів і ресурсів
ГАЛУЗЕВИЙ РІВЕНЬ	Власники політик, галузеві показники, верифікація	Коригування програм та комунікацій
РЕГІОНАЛЬНИЙ І МІСЦЕВИЙ РІВЕНЬ	Первинні дані, контекст, зворотний зв'язок громад	Адаптація інструментів до потреб аудиторій
НЕЗАЛЕЖНИЙ КОНТУР	Наука, медіа, громадськість, зовнішні оцінювачі	Перевірка, альтернативні дані, рекомендації
КОНТУР ДАНИХ	Збір → стандартизація → контроль якості → сховище	Захист, доступ, відкриті набори
КОНТУР НАВЧАННЯ	Моніторинг → оцінювання → обговорення	Рішення → виконання → повторне вимірювання

Рис. 3.9. Інституційна архітектура системи моніторингу й оцінювання державної інформаційної політики

Джерело: розроблено автором

Таблиця 3.15.

Розподіл основних ролей у системі моніторингу й оцінювання

Суб'єкт	Основні повноваження	Ключовий продукт	Запобіжник конфлікту інтересів
Координаційний рівень	Затвердження методології, національного набору показників, календаря оцінювань	Консолідована панель і щорічна доповідь	Колегіальне погодження та публікація методики
Власник державної політики	Визначення логіки результатів, цілей, цільових значень і коригувальних дій	Паспорт політики та план поліпшення	Відокремлення відповідальності за дані від самооцінки впливу
Аналітичний підрозділ	Збір, очищення, аналіз, візуалізація, підготовка пояснень відхилень	Оперативні й тематичні аналітичні записки	Протокол якості даних і відтворюваність розрахунків
Регіональні та місцеві органи	Формування первинних даних, контекстуалізація, фіксація потреб громад	Територіальний профіль і реєстр зворотного зв'язку	Єдині визначення показників та вибіркові перевірки
Незалежні оцінювачі	Періодичне оцінювання результатів, впливу, правомірності й стійкості	Публічний оціночний звіт	Відбір за прозорою процедурою, декларування інтересів
Громадяни, медіа, громадські організації	Надання зворотного зв'язку, участь у формуванні критеріїв, громадський контроль	Альтернативні дані, консультаційний висновок	Відкритий доступ до несекретної методології та агрегованих даних

Джерело: запропоновано автором

Розподіл ролей має закріплювати не лише право формувати звіт, а й персональну відповідальність за конкретні елементи ланцюга даних. Для кожного показника в електронному паспорті зазначаються власник змісту, постачальник первинних даних, верифікатор, дата оновлення, формула розрахунку, допустимий рівень похибки й порядок виправлення. Це зменшує ризик ситуації, коли розбіжності пояснюються невизначеністю повноважень.

Передумовою змістовного оцінювання є формування логічної моделі, яка пояснює, яким чином ресурси й діяльність органів влади мають привести до очікуваних суспільних змін. Без такої моделі показники перетворюються на

довільний набір чисел. Для державної інформаційної політики доцільно використовувати послідовність «ресурси – процеси – продукти – безпосередні результати – середньострокові наслідки – суспільний вплив». Між ланками фіксуються припущення та зовнішні чинники, від яких залежить перехід до наступного рівня.

Ресурси охоплюють правову основу, фінансування, персонал, цифрову інфраструктуру, дані та партнерські мережі. Процеси характеризують планування, координацію, створення й поширення контенту, консультації, верифікацію та реагування. Продуктами є доступні набори даних, роз'яснення, брифінги, інформаційні кампанії, відповіді на запити, протоколи реагування. Безпосередні результати відображають охоплення, доступність, розуміння й якість взаємодії; середньострокові – довіру, участь, зменшення інформаційної вразливості; вплив – спроможність демократичної держави реалізовувати політику в стійкому та правомірному інформаційному середовищі [120; 121; 124; 136; 137].

Ланцюг результатів запропонованої системи подано на рис. 3.10. Стрілки зворотного зв'язку підкреслюють, що виявлені відхилення повинні змінювати не лише комунікаційний продукт, а за потреби й саму державну політику.

1. РЕСУРСИ	Право, фінанси, персонал, інфраструктура, дані, партнерства
↓ 2. ПРОЦЕСИ	Планування, координація, вироблення інформації, консультації, реагування
↓ 3. ПРОДУКТИ	Відкриті дані, повідомлення, послуги, кампанії, відповіді, протоколи
↓ 4. БЕЗПОСЕРЕДНІ РЕЗУЛЬТАТИ	Доступність, своєчасність, охоплення, зрозумілість, взаємодія
↓ 5. СЕРЕДНЬОСТРОКОВІ НАСЛІДКИ	Довіра, участь, інформаційна компетентність, зниження вразливості
↓ 6. СУСПІЛЬНИЙ ВПЛИВ	Стійке демократичне врядування та захищене інформаційне середовище
↺ ЗВОРОТНИЙ ЗВ'ЯЗОК	Коригування інструментів, ресурсів, цілей і нормативних рішень

Рис. 3.10. Логічна модель результатів реалізації державної інформаційної політики

Джерело: розроблено автором

Таблиця 3.16.

Фрагмент теорії змін для державної інформаційної політики

Проблема	Інструмент	Очікуваний результат	Ключове припущення	Індикатор перевірки
Фрагментарність повідомлень органів влади	Єдиний цикл планування та міжвідомча координація	Зменшення суперечностей і швидше надання пояснень	Органи використовують погоджені дані та дотримуються протоколів	Частка узгоджених повідомлень; середній час погодження
Низька доступність публічної інформації	Відкриті дані, доступні формати, проактивне оприлюднення	Зростання фактичного доступу різних груп	Користувачі знають про ресурс і можуть ним скористатися	Повнота наборів; доступність; частка успішних пошуків
Інформаційний вакуум під час криз	Протокол першого повідомлення та резервні канали	Скорочення часу невизначеності й поширення чуток	Дані надходять від предметних служб без критичної затримки	Час першого підтвердженого повідомлення; охоплення цільових груп
Вразливість до дезінформації	Пребанкінг, медіаграмотність, партнерський фактчекінг	Підвищення розпізнавання маніпуляцій і зниження вторинного поширення	Навчальні формати відповідають потребам аудиторій	Зміна знань; готовність перевіряти; коефіцієнт повторного поширення
Слабкий зворотний зв'язок	Єдиний реєстр звернень, консультації, аналіз запитів	Урахування потреб громадян у рішеннях і комунікації	Висновки зворотного зв'язку розглядаються власниками політик	Частка пропозицій із формальною відповіддю; кількість змінених рішень
Недовіра до державної комунікації	Доказовість, пояснення невизначеності, публікація методології	Зростання передбачуваності та обґрунтованої довіри	Дії органів відповідають публічним повідомленням	Індекс довіри; частка громадян, які вважають пояснення зрозумілими

Джерело: розроблено автором

Теорія змін має переглядатися щонайменше один раз на рік і після значної зміни контексту. Перегляд не повинен автоматично означати зниження цілей під фактичні результати. Необхідно документувати, які припущення не справилися, які зовнішні чинники виникли та чому запропоновано новий причинний зв'язок. Це забезпечує накопичення інституційної пам'яті.

Для кожного очікуваного результату доцільно визначати також можливі негативні наслідки. Збільшення швидкості повідомлень може знижувати точність; автоматизація – створювати алгоритмічні упередження; інтенсивне поширення офіційного контенту – витіснити незалежні джерела; надмірна централізація – послаблювати локальну адаптацію. Моніторинг небажаних ефектів є обов'язковою ознакою зрілої системи.

Система показників повинна відповідати логічній моделі та поєднувати кількісні й якісні вимірювання. Кількісні індикатори забезпечують регулярність і порівнянність, а якісні пояснюють причини та контекст. Для кожної мети доцільно використовувати обмежену кількість ключових показників, доповнених діагностичними індикаторами. Надмірний набір збільшує звітне навантаження й ускладнює визначення пріоритетів.

Запропонована система містить три рівні. Перший – стратегічні індикатори суспільного результату, які характеризують довіру, доступ, участь та інформаційну стійкість. Другий – індикатори результатів окремих напрямів: відкритих даних, стратегічних комунікацій, взаємодії з медіа, протидії дезінформації, цифрової інклюзії. Третій – операційні показники строків, якості процесів і використання ресурсів. Звітність має рухатися знизу вгору, а управлінські рішення – узгоджувати всі рівні.

Якісний показник повинен мати однозначну назву, управлінське призначення, формулу, одиницю вимірювання, базове й цільове значення, джерело даних, періодичність, відповідального, правила дезагрегації та обмеження інтерпретації. Паспорт показника має бути доступним користувачам системи; для публічних індикаторів його доцільно оприлюднювати разом із даними.

Ієрархію показників відображено на рис. 3.11. Вона запобігає підміні суспільного результату операційною активністю та забезпечує зв'язок між щоденними діями й стратегічними цілями.

СТРАТЕГІЧНИЙ ВПЛИВ	Стійкість демократичного інформаційного середовища	1–3 роки
СУСПІЛЬНІ НАСЛІДКИ	Довіра, доступ, участь, стійкість до маніпуляцій	6–24 місяці
БЕЗПОСЕРЕДНІ РЕЗУЛЬТАТИ	Зрозумілість, своєчасність, охоплення, задоволеність	1–12 місяців
ПРОДУКТИ	Дані, повідомлення, консультації, кампанії, відповіді	Щотижня / щомісяця
ПРОЦЕСИ ТА РЕСУРСИ	Строки, витрати, компетентності, координація, якість даних	Оперативно

Рис. 3.11. Ієрархія показників ефективності реалізації державної інформаційної політики

Джерело: розроблено автором

Запропонований каталог ключових показників системи моніторингу

Вимір	Ключовий показник	Спосіб визначення	Бажаний напрям	Періодичність
Інституційна узгодженість	Частка пріоритетів, забезпечених міжвідомчим планом і власником результату	Кількість забезпечених пріоритетів / загальна кількість $\times 100 \%$	Зростання	Щокварталу
Правова якість	Частка інструментів із документованою оцінкою прав і ризиків	Кількість перевірених інструментів / загальна кількість $\times 100 \%$	Зростання	Щокварталу
Відкритість	Індекс повноти обов'язкових наборів даних	Зважена частка оприлюднених, актуальних і машиночитаних наборів	Зростання	Щокварталу
Доступ до інформації	Частка запитів, опрацьованих у встановлений строк	Своєчасні відповіді / усі завершені запити $\times 100 \%$	Зростання	Щомісяця
Якість інформації	Частка матеріалів із посиланням на перевірюване джерело	Матеріали з джерелом / вибірка матеріалів $\times 100 \%$	Зростання	Щомісяця
Своєчасність	Медіанний час першого підтвердженого повідомлення під час інциденту	Медіана часу від реєстрації до першого повідомлення	Скорочення	За інцидентами
Доступність	Частка ключових матеріалів у доступних і альтернативних форматах	Доступні матеріали / визначений перелік $\times 100 \%$	Зростання	Щокварталу
Охоплення	Частка цільової аудиторії, що фактично отримала повідомлення	Опитування, панельні дані, агрегована аналітика каналів	Зростання в цільових групах	За кампаніями
Розуміння	Частка представників аудиторії, які правильно відтворюють основний зміст	Післяконтактне опитування або тестування	Зростання	За кампаніями
Взаємодія	Частка змістовних звернень із завершеним циклом відповіді	Звернення з відповіддю й зафіксованим результатом / усі звернення	Зростання	Щомісяця
Участь	Частка консультацій, у яких оприлюднено звіт про врахування пропозицій	Консультації зі звітом / завершені консультації $\times 100 \%$	Зростання	Щокварталу
Довіра	Індекс обґрунтованої довіри до офіційної інформації	Репрезентативне опитування за стандартизованою шкалою	Зростання без вимоги некритичності	Півріччя
Протидія дезінформації	Частка значних інцидентів, опрацьованих за стандартною процедурою	Інциденти з повним протоколом / значні інциденти $\times 100 \%$	Зростання	Щокварталу
Стійкість	Коефіцієнт вторинного поширення спростованого твердження	Обсяг поширення після реакції / до реакції	Зменшення	За інцидентами
Якість даних	Інтегральний коефіцієнт якості моніторингових даних	Середньозважена повнота, своєчасність, валідність і узгодженість	Зростання	Щомісяця
Ефективність ресурсів	Вартість досягнення визначеного результату	Повні витрати / одиниця результату з поясненням контексту	Оптимізація, не мінімізація	Щороку
Організаційне навчання	Частка рекомендацій оцінювання, щодо яких прийнято рішення	Рекомендації з рішенням / усі рекомендації $\times 100 \%$	Зростання	Щопівроку

Джерело: розроблено автором

Каталог у таблиці 3.17 є базовим і може доповнюватися галузевими індикаторами. Водночас кожний додатковий показник має пройти тест управлінської корисності: яке рішення зміниться залежно від його значення; чи існує надійне джерело; чи виправдані витрати на збір; чи не створює індикатор стимулу до небажаної поведінки. Якщо на ці питання немає відповіді, показник не повинен включатися до обов'язкової звітності.

Для порівняння різновимірних показників пропонується їх нормування до шкали від 0 до 100. Для показників-стимуляторів, зростання яких є позитивним, застосовується відношення фактичного значення до встановленого діапазону. Для дестимуляторів, зокрема часу реагування або частки прострочень, шкала інвертується. Межі нормування мають визначатися на підставі базового періоду, правових нормативів, міжнародних орієнтирів або обґрунтованої експертної оцінки й не можуть змінюватися без документованого пояснення.

Для стимулятора нормований бал S_i може визначатися за формулою:

$$S_i = 100 \times (X_i - X_{min}) / (X_{max} - X_{min}).$$

Для дестимулятора, де менше значення є кращим, використовується зворотне нормування:

$$S_i = 100 \times (X_{max} - X_i) / (X_{max} - X_{min}).$$

Значення, що виходять за межі діапазону, обмежуються 0 або 100, але зберігаються в первинному наборі. Якщо показник має правовий поріг, наприклад строк відповіді на запит, доцільно застосовувати нелінійну шкалу: незначне відхилення та систематичне порушення не повинні отримувати майже однакову оцінку. Для якісних індикаторів створюється рубрика з описом рівнів, що зменшує розбіжності між експертами.

Показники об'єднуються у вісім вимірів: інституційна узгодженість; правомірність і відкритість; якість та своєчасність інформації; доступність і охоплення; взаємодія та участь; довіра й стратегічні результати; інформаційна стійкість; якість даних та організаційне навчання. Бал кожного виміру D_k розраховується як зважена сума нормованих індикаторів, а інтегральний індекс — як сума балів вимірів.

$$D_k = \sum(a_{ik} \times S_{ik}), \quad I_{DIP} = \sum(w_k \times D_k), \quad \text{де } \sum a_{ik} = 1 \text{ та } \sum w_k = 1.$$

Ваги не повинні визначатися виключно політичним рішенням або зручністю наявних даних. Пропонується комбінований підхід: початкове рівне зважування; експертне обговорення з представниками науки, громадськості й органів влади; аналіз чутливості, який показує, чи змінюється підсумкова оцінка при розумному варіюванні ваг. Якщо індекс нестійкий, пріоритет надається профілю окремих вимірів, а не єдиному числу.

Інтегральний індекс є інструментом навігації, а не самодостатнім рейтингом. Високий середній бал може приховувати критичне провалля в одному вимірі, тому запроваджується правило мінімального стандарту: за наявності показника нижче критичного порога загальна оцінка не може бути класифікована як висока. Так само порушення прав людини або маніпуляція даними не компенсуються високим охопленням.

Таблиця 3.18.

Авторська шкала інтерпретації результатів моніторингу

Діапазон	Рівень	Управлінське трактування	Обов'язкова дія
85–100	Стійкий	Результати досягаються, стандарти виконуються, система здатна адаптуватися	Підтримання, поширення практик, перевірка стійкості
70–84	Достатній	Основні результати досягнуто, але наявні окремі слабкі місця	Точковий план поліпшення та контроль у наступному циклі
50–69	Нестабільний	Результати нерівномірні, існують системні відхилення або розриви даних	Обов'язковий коригувальний план із відповідальними та строками
30–49	Низький	Механізми працюють частково, суттєві ризики для цілей політики	Поглиблене оцінювання, перегляд інструментів і ресурсів
0–29	Критичний	Цілі не досягаються або існує неприйнятний правовий/безпековий ризик	Невідкладне рішення, незалежна перевірка, припинення шкідливого інструменту
Критичний поріг незалежно від суми	Запобіжний статус	Грубе порушення прав, фальсифікація даних або незахищена критична вразливість	Автоматична ескалація та окреме розслідування

Джерело: розроблено автором.

Запропоновані діапазони мають характер методичних орієнтирів і потребують калібрування під час пілотного впровадження. Їх перевага полягає у зв'язку кожного рівня з обов'язковою управлінською дією. Без такого зв'язку кольорове позначення на панелі стає декоративним і не змінює практику.

Система повинна використовувати багатоджерельну модель. Адміністративні дані відображають виконання процедур і строків; цифрова

аналітика – поширення та взаємодію; репрезентативні опитування – розуміння, довіру й поведінкові зміни; моніторинг медіа – структуру інформаційного поля; консультації та звернення – потреби й проблемні точки; незалежні дослідження – зовнішню перевірку. Жодне джерело не є достатнім окремо, тому ключові висновки доцільно підтверджувати триангуляцією.

Адміністративні дані часто створюються для інших цілей і можуть не відповідати потребам оцінювання. Наприклад, реєстрація кількості відповідей не показує їх повноти, а загальна відвідуваність сайту не відокремлює громадян від автоматизованого трафіку. Перед включенням набору до системи необхідно описати походження, семантику полів, правила оновлення, пропуски, зміни методології та ризики викривлення.

Таблиця 3.19.

Матриця джерел даних для системи моніторингу й оцінювання

Джерело	Що вимірює	Періодичність	Відповідальний	Основний ризик	Спосіб верифікації
Адміністративні й інформаційні системи	Строки, обсяги, виконання процедур, ресурси	Оперативно / щомісяця	Розпорядник системи	Неповне або формальне внесення	Логічні перевірки, вибірковий аудит первинних записів
Офіційні сайти та відкриті дані	Повноту, актуальність, доступність, використання	Щомісяця / щокварталу	Власник вебресурсу й набору	Застарілі або несумісні метадані	Автоматизована перевірка та контрольна вибірка
Аналітика цифрових каналів	Охоплення, перегляди, взаємодію, переходи	Щоденно / за кампаніями	Комунікаційний підрозділ	Боти, зміна алгоритмів, «метрики марнославства»	Фільтрація, порівняння каналів, незалежні панельні дані
Репрезентативні опитування	Довіру, розуміння, доступ, поведінку	Півріччя / щороку	Незалежний виконавець	Помилка вибірки й соціально бажані відповіді	Публікація методики, повторні вимірювання
Фокус-групи та інтерв'ю	Причини сприйняття, бар'єри, досвід груп	За етапами оцінювання	Оцінювальна команда	Обмежена узагальнюваність	Триангуляція з кількісними даними
Моніторинг медіа й відкритих джерел	Теми, наративи, тональність, поширення інцидентів	Оперативно	Аналітичний центр	Помилки автоматичної класифікації	Ручна верифікація вибірки та прозорий словник
Звернення, консультації, петиції	Проблеми, очікування, якість відповіді, участь	Постійно / щокварталу	Підрозділ взаємодії з громадськістю	Самовідбір активних користувачів	Порівняння з репрезентативними даними
Незалежні дослідження та аудит	Зовнішню валідність, правомірність, ефективність	За календарем оцінювань	Зовнішній виконавець	Несумісність методик або конфлікт інтересів	Технічне завдання, рецензування, відкриті методи

Джерело: розроблено автором за [84; 88; 91; 98; 150; 151; 153; 154; 159].

Якість даних пропонується оцінювати за шістьма критеріями: повнота, своєчасність, валідність, внутрішня узгодженість, унікальність і

простежуваність. Для кожного критерію визначається бал від 0 до 100, після чого розраховується інтегральний коефіцієнт якості. Якщо показник має низьку якість даних, його значення відображається на панелі з попередженням і не використовується для санкційних або рейтингових рішень.

Коефіцієнт якості даних DQ доцільно визначати як середньозважене значення шести складових:

$$DQ = 0,20C + 0,20T + 0,20V + 0,15K + 0,10U + 0,15R,$$

де C – повнота; T – своєчасність; V – валідність; K – узгодженість; U – унікальність; R – простежуваність. Ваги є авторськими орієнтирами; для критичних систем частка валідності та простежуваності може бути збільшена.

Застосування систем штучного інтелекту до моніторингу повинно бути допоміжним. Автоматизований висновок не може самостійно визначати неправдивість матеріалу, правомірність обмеження або санкцію щодо особи. Потрібні людський нагляд, перевірка точності на українськомовних і регіональних даних, документування помилок, оцінка дискримінаційних ризиків та можливість оскарження [157].

Захист персональних даних реалізується за принципами мінімізації, цільового використання, обмеження строку зберігання, розмежування доступу та псевдонімізації. Публічний рівень системи містить агреговані дані, які не дозволяють ідентифікувати учасників звернень або вразливі малі групи. Збір даних «про всяк випадок» суперечить і правовим вимогам, і принципу пропорційності [91; 153].

Повний цикл роботи з даними та управлінськими рішеннями подано на рис. 3.12.

1. ФОРМУВАННЯ ПИТАННЯ	Яке рішення має підтримати інформація?
↓ 2. ЗБІР ДАНИХ	Адміністративні, цифрові, опитувальні, якісні джерела
↓ 3. КОНТРОЛЬ ЯКОСТІ	Повнота, валідність, своєчасність, простежуваність
↓ 4. АНАЛІЗ І ТРИАНГУЛЯЦІЯ	Порівняння джерел, пояснення причин, оцінка невизначеності
↓ 5. ВІЗУАЛІЗАЦІЯ	Панель, профіль ризику, відхилення від цілей
↓ 6. УПРАВЛІНСЬКИЙ РОЗГЛЯД	Рішення, відповідальний, строк, ресурс
↓ 7. ВИКОНАННЯ І ПУБЛІЧНА ВІДПОВІДЬ	Коригувальна дія та пояснення заінтересованим сторонам
↺ 8. ПОВТОРНЕ ВИМІРЮВАННЯ	Перевірка результату й оновлення теорії змін

Рис. 3.12. Цикл даних, аналізу та управлінського реагування

Джерело: розроблено автором

Моніторинг відповідає переважно на питання про перебіг і відхилення, тоді як оцінювання має пояснити причини. Для цього формується матриця оціночних питань: чи відповідає політика актуальним потребам; чи досягає вона запланованих результатів; які інструменти спрацювали для яких аудиторій; чи виправдані витрати; які наслідки не були передбачені; чи дотримано прав і принципів; чи збережеться результат після завершення заходу. Кожне питання пов'язується з критеріями, джерелами та методом.

Оцінювання до початку реалізації використовується для перевірки логіки, ризиків і реалістичності цілей. Формативне оцінювання під час реалізації дає змогу поліпшити інструменти, а підсумкове – визначити досягнуті результати. Швидке оцінювання застосовується під час криз, але його висновки мають містити рівень невизначеності. Оцінювання впливу є найбільш вимогливим, оскільки потребує встановлення того, що відбулося б без втручання.

Таблиця 3.20.

Рекомендовані методи оцінювання державної інформаційної політики

Метод	Завдання	Перевага	Обмеження	Доцільне застосування
Аналіз документів і процесів	Перевірка відповідності планам, стандартам і правовим вимогам	Відтворюваність і невисока вартість	Не показує фактичного сприйняття аудиторій	Оцінювання інституційної узгодженості та процедур
Репрезентативне опитування	Вимірювання доступу, розуміння, довіри, поведінки	Можливість узагальнення на населення	Вартість, похибки відповідей, часовий лаг	Базове, проміжне та підсумкове вимірювання
Фокус-групи й глибинні інтерв'ю	Пояснення бар'єрів, мотивів і неоднозначного сприйняття	Глибина та контекст	Обмежена репрезентативність	Розроблення інструментів і пояснення кількісних результатів
Аналіз цифрових слідів	Оперативне дослідження поширення та взаємодії	Швидкість і деталізація	Залежність від платформ, боти, нерепрезентативність	Моніторинг кампаній та інформаційних інцидентів
До/після з порівняльною групою	Оцінка зміни, пов'язаної з втручанням	Сильніша причинна аргументація	Складність добору порівнянної групи	Територіальні або поетапні пілоти
Перерваний часовий ряд	Виявлення зміни рівня або тренду після заходу	Використовує тривалі спостереження	Чутливість до одночасних подій	Зміни правил, платформ, протоколів реагування
Внесковий аналіз	Перевірка теорії змін і альтернативних пояснень	Придатність для складних систем	Не дає єдиного точного ефекту	Національні програми з багатьма учасниками
Кейс-стаді й післядівний огляд	Детальний аналіз інциденту, рішень і наслідків	Організаційне навчання	Ризик вибіркової кейсів	Кризи, дезінформаційні кампанії, значні помилки
Аналіз витрат і результатів	Порівняння ресурсів із досягнутими результатами	Підтримка бюджетних рішень	Складність монетизації довіри й стійкості	Вибір між альтернативними каналами та форматами

Джерело: систематизовано автором

Вибір методу визначається оціночним питанням, а не доступністю інструменту. Використання аналізу тональності для висновку про довіру або кількості переглядів для висновку про зміну поведінки є методично некоректним. План оцінювання має заздалегідь визначати, які твердження можна зробити на підставі кожного джерела та які альтернативні пояснення необхідно перевірити.

Базове вимірювання проводиться до суттєвого втручання або відновлюється за надійними історичними даними. Цільові значення мають бути амбітними, але реалістичними, і містити часовий горизонт. Зміна методики опитування, платформи або складу вибірки фіксується; за неможливості забезпечити порівнянність часовий ряд починається заново або перераховується за прозорим правилом.

До технічного завдання незалежного оцінювання включаються критерії, питання, мінімальні методи, вимоги до вибірки, доступ до даних, етичні правила, формат публічного звіту та порядок управлінської відповіді. Водночас замовник не повинен визначати бажаний висновок. Проект звіту може проходити фактологічну перевірку, але зміна оціночних суджень допускається лише за наявності нових доказів.

Цифрова панель має забезпечувати різні рівні доступу. Операційний рівень містить деталізовані дані для відповідальних працівників; управлінський – ключові відхилення, ризики та статус коригувальних дій; публічний – агреговані показники, методологію, часові ряди та пояснення. Розмежування необхідне для захисту персональних даних і чутливої безпекової інформації, але не повинно використовуватися для приховування незручних результатів [83; 84; 91; 105].

Візуалізація має показувати не лише поточний бал, а й тренд, ціль, якість даних, дату оновлення та пояснення значної зміни. Для кожного червоного індикатора відкривається картка відхилення: причина, масштаб, відповідальний, запланована дія, строк і статус. Якщо показник погіршується три періоди поспіль або перетинає критичний поріг, система автоматично ініціює управлінський розгляд.

Публічна звітність повинна бути багаторівневою. Коротке резюме пояснює основні результати доступною мовою; аналітична частина містить методи, часові ряди та обмеження; відкритий набір даних дозволяє повторний аналіз; управлінська відповідь показує, які рекомендації прийнято, відхилено або відкладено та з яких причин. Такий формат поєднує зрозумілість і професійну перевірюваність.

Управлінська відповідь є центральною ланкою системи. Звіт без формального розгляду й відстеження рекомендацій не створює зміни. Для кожної рекомендації встановлюється статус: прийнята, частково прийнята, відхилена або відкладена. Відхилення потребує письмового обґрунтування, а прийнята рекомендація – відповідального, ресурсу, строку та індикатора виконання.

Для критичних рішень зберігається протокол розгляду: які дані використано, які обмеження визнано, хто брав участь, які альтернативи оцінено та чому обрано конкретну дію. Це підвищує інституційну пам'ять і дає можливість перевірити, чи було рішення доказовим, навіть якщо очікуваний результат не досягнуто.

Запровадження системи доцільно здійснювати поетапно, оскільки одночасна вимога подавати великий набір даних може збільшити навантаження та знизити їх якість. На початковому етапі формується нормативно-методична основа, реєстр чинних показників і карта джерел. Після цього проводиться пілотування в кількох напрямках, де є різні типи даних: доступ до інформації, стратегічна комунікація та реагування на інформаційні інциденти. Результати пілоту використовуються для спрощення форм і калібрування порогів.

Технологічна платформа має будуватися модульно й використовувати наявні державні інформаційні ресурси, а не дублювати їх. Основними компонентами є каталог показників, модуль завантаження й обміну даними, сховище, правила якості, аналітичний модуль, панель і реєстр рекомендацій. Інтероперабельність забезпечується єдиними ідентифікаторами, форматами, метаданими та програмними інтерфейсами відповідно до розвитку національної інформатизації й публічних реєстрів [98; 102].

Дорожня карта впровадження системи моніторингу й оцінювання

Етап і строк	Основні дії	Результат	Показник готовності	Ключовий ризик
I. Підготовчий, 0–3 місяці	Інвентаризація цілей, показників, наборів даних і звітних вимог; створення методичної групи	Концепція системи, карта даних, перелік дублювань	Затверджено власників усіх базових показників	Формальне копіювання чинної звітності
II. Проектування, 4–6 місяців	Розроблення логічної моделі, паспортів, стандарту якості, правил доступу та захисту	Методичний стандарт і технічне завдання	Для кожного показника визначено формулу, джерело, строк і рішення	Надмірна кількість показників
III. Пілот, 7–12 місяців	Запуск у 2–3 напрямках, базове вимірювання, тест панелі, навчання команд	Пілотна панель і перший оцінювальний звіт	Не менше 80 % даних проходять встановлений контроль якості	Низька якість первинних даних
IV. Масштабування, 13–24 місяці	Підключення органів і територій, автоматизація обміну, відкриття публічного рівня	Національна система з територіальними профілями	Регулярне оновлення базових показників за календарем	Цифрова нерівність та несумісність систем
V. Інституціоналізація, 25–36 місяців	Незалежне оцінювання, аудит методики, перегляд ваг і порогів, закріплення бюджетного циклу	Стабільний цикл моніторингу, оцінювання та управлінської відповіді	Рекомендації мають відстежувати рішення і повторне вимірювання	Використання системи лише для звітності

Джерело: розроблено автором

Таблиця 3.23.

Ризики функціонування системи та заходи їх мінімізації

Ризик	Прояв	Наслідок	Запобіжний захід
Підміна мети показником	Установи оптимізують лише те, що легко виміряти	Формальне зростання балів без суспільного результату	Регулярний перегляд логіки, якісні методи, моніторинг небажаних наслідків
Маніпуляція даними	Вибір сприятливого періоду, приховування пропусків, зміна формули	Втрата довіри та хибні рішення	Версійність методики, аудит, відкриття первинних агрегованих даних
Надмірна звітність	Дублювання форм і ручне введення	Перевантаження персоналу та низька якість	Принцип одноразового збору, автоматизація, видалення некорисних показників
Хибна точність	Єдиний індекс подається без похибок і контексту	Неправильне ранжування та політизація	Інтервали невизначеності, профіль вимірів, пояснювальні записки
Порушення приватності	Надмірна деталізація або повторна ідентифікація	Шкода особам і правова відповідальність	Мінімізація, агрегування, оцінка впливу на захист даних, контроль доступу
Алгоритмічне упередження	Автоматична класифікація помиляється щодо мовних або регіональних груп	Дискримінаційні висновки та помилкові реакції	Людський нагляд, тестування, аудит моделей, механізм оскарження
Політичний тиск на оцінювання	Негативні висновки змінюються або не публікуються	Втрата незалежності та навчальної функції	Прозоре технічне завдання, зовнішнє рецензування, обов'язкова управлінська відповідь
Безпекове розкриття	Публікація методів або даних, корисних противнику	Посилення вразливості держави	Багаторівневий доступ, оцінка ризику розкриття, публікація агрегованих результатів

Джерело: розроблено автором

Людська спроможність є не менш важливою за програмне забезпечення. Потрібні компетентності у сфері політичного аналізу, статистики, соціології,

роботи з даними, візуалізації, комунікацій, прав людини, інформаційної безпеки та управління змінами. Навчання має відбуватися на реальних кейсах і завершуватися підготовкою паспортів показників, планів оцінювання та управлінських відповідей.

Особливо небезпечним є ризик підміни мети показником. Коли винагорода або репутація безпосередньо залежать від одного числа, учасники системи починають оптимізувати число, а не суспільний результат. Запобігання потребує поєднання індикаторів, зовнішньої перевірки, аналізу аномалій і можливості повідомляти про методичні проблеми без негативних наслідків.

Публічна участь у системі не обмежується наданням оцінки готовому звіту. Представників цільових груп доцільно залучати до визначення критеріїв доступності, тестування інструментів, інтерпретації неоднозначних результатів і формування рекомендацій. Таке залучення підвищує релевантність показників, але не замінює професійних вимог до вибірки й аналізу.

Запропонована система моніторингу й оцінювання створює завершальний контур інтегрованого механізму реалізації державної інформаційної політики. Її новизна полягає у поєднанні логічної моделі результатів, багаторівневої системи показників, коефіцієнта якості даних, інтегрального індексу з правилом мінімального стандарту, багатоджерельного аналізу, цифрової панелі та формалізованої управлінської відповіді. На відміну від традиційної звітності, система оцінює не лише виконані заходи, а й доступність, розуміння, довіру, участь, стійкість, правомірність і здатність інституцій навчатися.

Практичне значення має встановлення прямого зв'язку між значенням показника та рішенням. Виявлене відхилення реєструється, отримує відповідального, строк і ресурс; виконання перевіряється повторним вимірюванням. Критичні правові та безпекові пороги не можуть компенсуватися високим середнім балом. Це забезпечує пріоритет прав людини й національної стійкості над формальною результативністю.

Система підтримує баланс відкритості та безпеки через багаторівневий доступ. Методологія, агреговані результати, часові ряди та управлінські відповіді підлягають оприлюдненню, тоді як персональні й оперативно чутливі

дані захищаються. Такий підхід дає змогу забезпечити громадський контроль без створення додаткових вразливостей [83; 84; 91; 105; 153].

Впровадження запропонованої моделі сприятиме переходу від фрагментарної оцінки інформаційних заходів до доказового управління повним циклом державної інформаційної політики. Органи влади отримають інструмент раннього виявлення проблем, порівняння альтернатив, обґрунтування ресурсних рішень і накопичення інституційної пам'яті; громадяни та медіа – перевірювану інформацію про досягнення, обмеження й подальші дії; наукове середовище – стандартизовані дані для незалежного аналізу.

Отже, ефективність реалізації державної інформаційної політики доцільно визначати не кількістю створених повідомлень, а мірою досягнення суспільно значущих, правомірних і стійких результатів. Система моніторингу й оцінювання повинна стати постійним управлінським механізмом, який з'єднує дані, аналіз, публічну підзвітність і коригування політики. Її інституціоналізація є необхідною умовою адаптивності держави в динамічному інформаційному середовищі та завершення запропонованого в дисертації циклу формування, реалізації, оцінювання й удосконалення державної інформаційної політики.

Верифікацію запропонованої моделі доцільно здійснювати через пілотне застосування в органах із різним функціональним профілем. Пілот має перевірити не лише технічну можливість збору даних, а й зрозумілість паспортів показників, міжекспертну узгодженість якісного кодування, стійкість інтегральної оцінки до зміни ваг, реальну вартість вимірювання та здатність керівництва використовувати висновки. За результатами апробації уточнюються пороги, періодичність і перелік обов'язкових індикаторів; зміни документуються, щоб не порушувати порівнянність часових рядів.

Система має бути сумісною з європейськими та міжнародними підходами до публічної комунікації, кіберстійкості, врядування цифрових платформ, свободи медіа, використання штучного інтелекту та інформаційної доброчесності. Сумісність не означає механічного перенесення іноземних індексів. Вона передбачає відображення спільних принципів у національних показниках, можливість зіставлення окремих результатів і використання

міжнародних стандартів як зовнішніх орієнтирів із урахуванням українського безпекового й інституційного контексту.

Подальший розвиток системи повинен враховувати появу синтетичного контенту, зміну алгоритмів платформ, нові форми координованого впливу та розширення автоматизованої аналітики. Це потребує регулярного перегляду словника ризиків, тестування алгоритмічних моделей, збереження людського контролю й удосконалення показників інформаційної стійкості. Адаптивність методики не суперечить стабільності вимірювання, якщо кожна зміна має обґрунтування, номер версії, дату введення та правила зіставлення з попередніми даними.

Висновки до розділу 3

Обґрунтовано необхідність переходу від фрагментарної моделі реалізації державної інформаційної політики до інтегрованого організаційно-управлінського механізму. Його формування не зводиться до створення нового централізованого органу або адміністративного підпорядкування всіх учасників інформаційної сфери. Інтеграція полягає у функціональному поєднанні стратегічного планування, аналізу середовища, вироблення рішень, правової експертизи, комунікації, кризового реагування, цифрового обміну даними, участі стейкхолдерів та оцінювання результатів. Це дає змогу усунути розриви, за яких аналітичні матеріали не впливають на управлінські рішення, комунікаційні підрозділи долучаються після їх ухвалення, а отриманий досвід не використовується для перегляду політики.

Уточнено зміст інтегрованого організаційно-управлінського механізму та принципи його функціонування. Запропоновано розуміти його як інституційно закріплену, багаторівневу й технологічно підтриману систему узгоджених повноважень, процесів, стандартів, ресурсів і зворотних зв'язків, за допомогою якої публічні інституції у взаємодії з громадянами, медіа, громадянським суспільством, науковими установами, цифровими платформами та міжнародними партнерами здійснюють повний цикл інформаційної політики. До базових принципів віднесено верховенство права, людиноцентричність,

доказовість, стратегічну узгодженість, розподілену відповідальність, субсидіарність, оперативність, інтероперабельність, безпеку і приватність за проєктуванням, відкритість, інклюзивність, адаптивність та організаційне навчання.

Розроблено структурно-функціональну архітектуру інтегрованого механізму, що охоплює нормативно-стратегічну, інституційно-координаційну, аналітично-прогностичну, комунікаційно-партисипативну, цифрово-технологічну, безпеково-кризову, ресурсно-кадрову та моніторингово-оцінювальну підсистеми. Їх взаємодія забезпечує перетворення стратегічних пріоритетів на конкретні процеси, продукти та суспільні результати. Для міжвідомчої координації запропоновано поєднати стратегічний контур, який визначає цілі, стандарти й пріоритети, з операційним контуром, відповідальним за повсякденну реалізацію, швидке погодження фактів, роботу з аудиторіями та реагування на інциденти.

Удосконалено механізми стратегічних комунікацій шляхом обґрунтування двоконтурної моделі. Проактивний контур спрямований на довгострокове пояснення державної політики, формування суспільно значущих наративів, запобігання інформаційним вакуумам, розвиток медіаграмотності, міжнародну комунікацію та підтримання постійного діалогу. Захисний контур охоплює ситуаційний моніторинг, раннє попередження, виявлення координованих кампаній, предметну верифікацію, кризове реагування, взаємодію з медіа і цифровими платформами та післядієвий аналіз. Обидва контури спираються на спільні стандарти доказовості, аналітичну платформу та систему оцінювання, завдяки чому безпекове реагування не відривається від повсякденної комунікації.

Розроблено багаторівневу систему виявлення, верифікації та реагування на дезінформаційні інциденти. Її методичною основою є розмежування ненавмисно помилкової інформації, навмисної дезінформації та правдивих відомостей, використаних для завдання шкоди поза належним контекстом. Така диференціація унеможливорює однакове реагування на різні явища: помилка потребує уточнення, організована кампанія – встановлення координованості,

джерел і цілей, а поширення чутливої правдивої інформації – правової оцінки режиму доступу. Запропонована чотирирівнева класифікація інцидентів пов’язує масштаб загрози, очікувану шкоду, рівень упевненості, строки реагування, суб’єкта координації та набір допустимих інструментів.

Обґрунтовано систему моніторингу й оцінювання як завершальний контур інтегрованого механізму та інструмент управлінського навчання. Її призначенням є не лише контроль виконання заходів, а регулярне збирання і перевірка даних, зіставлення фактичних результатів із базовими та цільовими значеннями, пояснення причин відхилень, визначення внеску окремих інструментів, виявлення непередбачених наслідків і перетворення висновків на обов’язкові коригувальні рішення. Запропоноване авторське визначення поєднує інституційний, методичний і технологічний виміри та розглядає ефективність через релевантність, результативність, співвідношення результатів і ресурсів, правомірність, справедливість доступу, вплив та стійкість.

Сформовано інституційну та технологічну архітектуру моніторингу й оцінювання. На стратегічному рівні передбачено затвердження методології, національного набору показників і календаря оцінювань; на галузевому – визначення логіки результатів, цільових значень і коригувальних заходів; на регіональному й місцевому – збирання первинних даних та врахування контексту громад; у незалежному контурі – зовнішню перевірку, альтернативні дані й експертні рекомендації. Для кожного показника має складатися паспорт із формулою, джерелом, періодичністю, відповідальним, правилами верифікації, обмеженнями та управлінським рішенням, яке запускається при відхиленні.

Наукова новизна полягає у поєднанні в єдиній моделі принципу координованої поліцентричності, двоконтурного механізму стратегічних комунікацій і протидії дезінформації, замкненого управлінського циклу, федеративної цифрової інфраструктури та системи моніторингу й оцінювання з формалізованим переходом від показника до рішення. Це дає змогу розглядати реалізацію державної інформаційної політики не як сукупність розрізнених інформаційних заходів, а як повний цикл спільного вироблення, виконання, перевірки та вдосконалення публічних рішень.

ВИСНОВКИ

У дисертаційній роботі здійснено теоретичне узагальнення та запропоновано вирішення важливого науково-прикладного завдання, що полягає в теоретико-методологічному обґрунтуванні й розробленні науково-практичних засад удосконалення механізмів реалізації державної інформаційної політики України в умовах цифрової трансформації, гібридних загроз і європейської інтеграції. Досягнення поставленої мети забезпечено послідовним виконанням дев'яти завдань дослідження. Одержані результати відображають основні положення наукової новизни, розкривають сучасний стан досліджуваної сфери та утворюють взаємопов'язаний комплекс організаційних, комунікаційних, цифрових, безпекових і оціночних рішень. Проведене дослідження дало підстави сформулювати такі висновки.

1. Узагальнено еволюцію наукових поглядів на формування державної інформаційної політики та встановлено її кумулятивний характер. Виокремлено державоцентричну, організаційно-правову, демократично-комунікаційну, інформаційно-суспільну, безпекову та цифрово-платформну парадигми. На основі інтеграції наукових підходів сформульовано авторське визначення державної інформаційної політики як цілеспрямованої, нормативно впорядкованої, інституційно скоординованої та технологічно підтриманої діяльності публічної влади у партнерстві з громадянами, медіа, громадянським суспільством, бізнесом, науковим середовищем, органами місцевого самоврядування, цифровими платформами та міжнародними партнерами, спрямованої на гарантування інформаційних прав і свобод, формування якісної публічної комунікації, розвиток цифрового врядування, захист інформаційного простору, зміцнення суспільної стійкості та створення вимірюваної публічної цінності. На відміну від вузького трактування політики як сукупності інформаційних заходів або медійного регулювання, запропоноване визначення поєднує управлінський, правовий, комунікаційний, цифровий і безпековий виміри та поширює відповідальність держави на повний цикл від діагностики інформаційної потреби до оцінювання суспільного результату.

2. Систематизовано функції, цілі та пріоритети державної інформаційної політики й обґрунтовано їх функціонально-цільову взаємозалежність. До ключових функцій віднесено правозахисну, нормативно-регуляторну, інституційно-координаційну, аналітично-прогностичну, комунікаційно-діалогічну, сервісно-цифрову, інформаційно-просвітницьку, безпеково-захисну, міжнародно-репутаційну та моніторингово-оціночну. Запропоновано функціонально-цільову архітектуру за логікою «цінності – функції – цілі – пріоритети – механізми – результати – зворотний зв'язок». Генеральною метою визначено створення відкритого, безпечного, стійкого й людиноцентричного інформаційного середовища. Обґрунтовано п'ять взаємопов'язаних цільових напрямів: гарантування інформаційних прав і відкритості; зміцнення довіри, діалогу та громадянської участі; забезпечення інформаційної безпеки й стійкості; цифровий розвиток та інклюзія; європейська інтеграція і міжнародна присутність.

3. Розроблено методичні засади дослідження механізмів реалізації державної інформаційної політики. Методологічну конструкцію сформовано шляхом узгодженого застосування історико-генетичного, системного, інституційного, структурно-функціонального, процесного, мережевого, ризик-орієнтованого та результативно-оціночного підходів. Запропоновано алгоритм комплексного дослідження та оцінювання, який охоплює операціоналізацію понять, контент-аналіз нормативної бази, картування суб'єктів, опис процесів та інструментів, визначення ресурсів, формування критеріїв і показників, оцінювання результатів, аналіз ризиків, моделювання змін, апробацію та валідацію рекомендацій. Систему критеріїв сформовано за блоками правомірності, стратегічної узгодженості, інституційної спроможності, доступності, оперативності, двосторонності, достовірності, ресурсної ефективності, безпекової стійкості, довіри, впливу та адаптивності.

4. Охарактеризовано систему суб'єктів формування та реалізації державної інформаційної політики та розмежовано їх ролі у багаторівневому управлінському циклі. Встановлено, що система має поліцентричний і міжгалузевий характер. Доведено, що основною інституційною дисфункцією є

не дефіцит суб'єктів, а фрагментарність їх взаємодії: дублювання функцій, розрив між стратегічними документами й операційним виконанням, несумісність показників, затримки обміну даними, суперечливі повідомлення, нечіткість власника процесу та недостатнє використання зворотного зв'язку. Запропоновано принцип координованої поліцентричності, який поєднує єдині цілі, фактологічну основу, стандарти, кризові протоколи та показники з автономією уповноважених суб'єктів у межах їх компетенції. Розроблено функціонально-рольову матрицю з визначенням провідного суб'єкта, виконавців, погоджувальних і консультативних ролей, власників даних, незалежних оцінювачів, зон спільної відповідальності та процедур ескалації.

5. Проаналізовано сучасний стан інструментів інформаційної взаємодії органів публічної влади з громадянами та медіа. Інструменти систематизовано за групами офіційного інформування, доступу до публічної інформації й відкритих даних, сервісної комунікації, електронної демократії, взаємодії з медіа, соціальних мереж, кризових комунікацій, протидії дезінформації та аналітичного зворотного зв'язку. Уточнено, що їх зрілість визначається не фактом наявності сайту, сторінки чи сервісу, а правовою визначеністю процедури, якістю змісту, доступністю, двосторонністю, швидкістю, автентичністю, фіксацією звернення, можливістю оскарження й використання отриманих даних для зміни управлінського рішення.

6. Сформовано концептуальну архітектуру інтегрованого організаційно-управлінського механізму реалізації державної інформаційної політики та визначено засоби його впровадження. Механізм представлено як багаторівневу систему нормативно-стратегічного, інституційно-суб'єктного, функціонального, інструментально-комунікаційного, ресурсно-забезпечувального та моніторингово-оціночного контурів. Управлінською основою архітектури визначено координовану поліцентричність, інститут власника процесу, матрицю відповідальності та принцип «комунікація за задумом політики», за яким потреби аудиторій, бар'єри розуміння, ризики недовіри і канали зворотного зв'язку аналізуються до ухвалення рішення. Цифрову підтримку запропоновано будувати за федеративною моделлю: установи зберігають власні інформаційні

ресурси, але використовують спільні метадані, ідентифікатори, контроль доступу, журналювання та захищені інтерфейси обміну.

8. Удосконалено механізми стратегічних комунікацій і протидії дезінформації шляхом розроблення двоконтурної моделі. Проактивний контур спрямований на довгострокове пояснення державної політики, наративне планування, заповнення інформаційних вакуумів, розвиток медіаграмотності, міжнародну комунікацію та сталий суспільний діалог. Захисний контур охоплює ситуаційний моніторинг, раннє попередження, виявлення координованих кампаній, предметну верифікацію, рівневу ескалацію, кризове реагування, взаємодію з медіа й платформами та післядієвий аналіз. Для проактивного контуру розроблено каскад «цінності – стратегічні цілі – тематичні наративи – доказова база – адаптовані повідомлення – канали – показники сприйняття». Наратив визначено не як пропагандистське гасло, а як послідовну пояснювальну рамку, підтверджену рішеннями, даними й поведінкою інституцій. Запропоновано індекс якості стратегічної комунікації за критеріями доказовості, своєчасності, узгодженості, доступності та зворотного зв'язку.

9. Розроблено систему моніторингу й оцінювання ефективності реалізації державної інформаційної політики, що перетворює оцінювання з завершального звіту на постійний контур управління. Методичним ядром визначено теорію змін і логічну модель «ресурси – процеси – продукти – безпосередні результати – суспільні наслідки – стратегічний вплив». Сформовано стратегічний, результативний та операційний рівні показників. Запропоновано інтегральний індекс ефективності з правилом мінімального стандарту, відповідно до якого критичне порушення інформаційних прав, маніпуляція даними або небезпечна вразливість не можуть бути компенсовані високим середнім балом.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Абакумов В. М. Правове регулювання протидії інформаційним війнам в Україні: дис. ... канд. юрид. наук : 12.00.07. Запоріжжя, 2010. 213 с.
2. Акімов А. Сучасна інформаційна політика України. Взаємодія державних і правоохоронних органів у протидії дезінформації. Національні інтереси України. 2026. № 2(19). С. 1350–1364.
3. Арістова І. В. Державна інформаційна політика : організаційно-правові аспекти: монографія / за заг. ред. О. М. Бандурки. Харків : Вид-во Ун-ту внутрішніх справ, 2000. 368 с.
4. Арістова І. В. Розбудова правової держави в Україні: правовий механізм забезпечення права на доступ до інформації в суспільстві знань. Правова інформатика. 2010. № 1 (25). С. 3–13. URL: <https://ippi.org.ua/sites/default/files/10aivisz.pdf>
5. Баран М. В. Адміністративно-правове забезпечення інформаційної безпеки в Україні : дис. д-ра філософії : 081 Право. Львів, 2023. 244 с.
6. Баранов О. А. Правове забезпечення інформаційної сфери : теорія, методологія і практика : монографія. Київ : Едельвейс, 2014. 497 с.
7. Барнич К. І. Реалізація конституційного права на свободу думки і слова, на вільне вираження своїх поглядів і переконань: дис. ... канд. юрид. наук: 12.00.02. Ужгород, 2020. 207 с.
8. Беляков К. І., Онопрієнко С. Г., Шопіна І. М. Інформаційна культура в Україні : правовий вимір : монографія. Київ : КВІЦ, 2018. 168 с.
9. Босак І. Інформаційна безпека України: загрози та методи протидії. Київський економічний науковий журнал. 2025. № 9. С. 33–38. URL: <https://doi.org/10.32782/2786-765X/2025-9-4>
10. Брижко В. М., Швець М. Я., Цимбалюк В. С. Е-боротьба в інформаційних війнах та інформаційне право: монографія. Київ: ПанТОТ, 2007. 218 с.
11. Валюшко І. О. Кібербезпека України: наукові та практичні виміри сучасності. Вісник НТУУ «КПІ». Політологія. Соціологія. Право. 2016. № 3–4 (31–32). С. 117–124.

12. Вдовичин О. Формування державної інформаційної політики України в умовах наближення до Європейського Союзу. Вісник Прикарпатського університету. Серія: Політологія. 2025. Вип. 21. С. 67–78. URL: <https://doi.org/10.32782/2312-1815/2025-21-8>
13. Верголяс О. О. Правове забезпечення спеціальних інформаційних операцій : дис. ... канд. юрид. наук : 12.00.07. Київ, 2020. 287 с.
14. Галіпчак В. Д. Державно-правовий механізм інформаційної безпеки України в умовах російської агресії. Політикус. 2023. № 5. С. 19–24.
15. Галіпчак В. Д. Інституційні чинники інформаційної політики євроінтеграції України: безпековий вимір. Політикус. 2023. № 3. С. 97–102.
16. Глобенко С. В. Публічне управління захистом інформаційного простору в умовах надзвичайних ситуацій : дис. д-ра філософії : 281 Публічне управління та адміністрування. Київ, 2024. 177 с.
17. Головка О. М. Інформаційно-правова політика України у сфері безпеки людини у медіапросторі : дис. ... канд. юрид. наук : 12.00.07. Київ, 2018. 244 с.
18. Голосніченко Д. І. Запобігання поширенню недостовірної інформації. Юридичний науковий електронний журнал. 2025. № 1. С. 286–289. URL: <https://doi.org/10.32782/2524-0374/2025-1/62>
19. Голосніченко Д. І. Право на достовірну інформацію в сучасних умовах воєнного стану. Юридичний науковий електронний журнал. 2024. № 12. С. 233–236. URL: <https://doi.org/10.32782/2524-0374/2024-12/50>
20. Гончаров М. В., Гончаров А. В. До питання дослідження шляхів вдосконалення інформаційної безпеки в Україні. Аналітично-порівняльне правознавство. 2026. Т. 1, № 2. С. 18–22.
21. Горбань Ю. О. Інформаційна війна проти України та засоби її ведення. Вісник Національної академії державного управління при Президентові України. 2015. № 1. С. 136–141.
22. Горбулін В. П., Додонов О. Г., Ланде Д. В. Інформаційні операції та безпека суспільства : загрози, протидія, моделювання : монографія. Київ : Інтертехнологія, 2009. 164 с.

23. Грицяк Н. В. Інформаційні кампанії як механізм підвищення ефективності реалізації державної політики у сфері євроінтеграції. Стратегічні пріоритети. 2007. № 2. С. 37–44.
24. Губерський Л. В., Камінський Є. Є., Макаренко Є. А., Ожеван М. А., Шнирков О. І. Інформаційна політика України: європейський контекст : монографія. Київ : Либідь, 2007. 360 с.
25. Гуйда О. Г., Кучерявий В. М., Головченко М. М. Інформаційна безпека дітей та молоді як складова державної реінтеграційної політики України. Вчені записки ТНУ імені В. І. Вернадського. Серія: Публічне управління та адміністрування. 2026. Т. 37(76), № 2. С. 47–52.
26. Дабіжа В. Державне регулювання інформаційної безпеки: проблеми та перспективи розвитку. Вісник Хмельницького національного університету. Економічні науки. 2026. Т. 352, № 2. С. 84–91.
27. Деякі питання реалізації Стратегії комунікації з питань європейської інтеграції України на період до 2026 року : розпорядження Кабінету Міністрів України від 25.06.2025 № 622-р. URL: <https://zakon.rada.gov.ua/laws/show/622-2025-%D1%80#Text>
28. Дубов Д. В. Державна інформаційна політика України в умовах гібридного миру та війни. Стратегічні пріоритети. 2016. № 3 (40). С. 86–93. URL: http://nbuv.gov.ua/UJRN/spa_2016_3_12
29. Дубовик Д. Інформаційна політика як інструмент державного управління в умовах цифровізації. Вісник Хмельницького національного університету. 2026. № 1. С. 572-578.
30. Дубовик Д. Інституційний механізм реалізації державної інформаційної політики в умовах цифрової трансформації. Вісник Хмельницького національного університету. 2025. № 6. С. 496-502.
31. Дубовик Д.Є., Гривко С.Д. Вплив цифровізації на зайнятість та ринок праці в інформаційному суспільстві. Економічний простір. 2025. № 208. С. 203-209.
32. Дубовик Д.Є. Цифрові трансформації в інформаційному суспільстві. Публічне управління і адміністрування в Україні. 2024. Випуск 44. С. 231-235.

33. Дяковський О. С. Правові та інституційні механізми протидії дезінформації у розвинутих країнах світу. *Право і суспільство*. 2024. № 4. С. 210–216. URL: <https://doi.org/10.32842/2078-3736/2024.4.28>
34. Дяковський О. С., Чернецький С. С. Діяльність суб'єктів публічної влади в системі протидії дезінформації: вітчизняний та зарубіжний досвід. *Юридичний науковий електронний журнал*. 2023. № 11. С. 775–778. URL: <https://doi.org/10.32782/2524-0374/2023-11/188>
35. Дяковський О., Габрелян А. Основні засади та принципи протидії дезінформації. *Юридичний вісник*. 2024. № 4. С. 30–36. URL: <https://doi.org/10.32782/yuv.v4.2024.4>
36. Єфіменко І. Стратегічні комунікації як елемент забезпечення інформаційної безпеки в умовах воєнного стану: нормативно-правові аспекти України. *Наукові перспективи*. 2026. № 4(70). С. 939–947.
37. Животова К. В. Механізми вироблення державної політики у сфері протидії дезінформації : дис. д-ра філософії : 281 Публічне управління та адміністрування. Київ, 2024. 277 с.
38. Запорожець С. Інформаційна безпека України в умовах гібридної війни. Проблеми створення, випробування, застосування та експлуатації складних інформаційних систем. 2019. Вип. 17. С. 52–63.
39. Захаренко К. В. Особливості формування ефективної державної інформаційної політики. *Політичне життя*. 2019. № 3. С. 71–76. URL: http://nbuv.gov.ua/UJRN/pollife_2019_3_13
40. Звоздецька О. Дезінформація як загроза національній безпеці Європейського Союзу: проблеми та підходи. *Історико-політичні проблеми сучасного світу*. 2021. № 43. С. 30–39. URL: <https://doi.org/10.31861/mhpi2021.43.30-39>
41. Золотар О. О. Генеза суспільних відносин щодо інформаційної безпеки людини. *Інформація і право*. 2018. № 1 (24). С. 139–148. URL: http://ippi.org.ua/sites/default/files/17_4.pdf

42. Золотар О. О. Інформаційна безпека людини : теорія і практика : монографія. Київ: АртЕк, 2018. 446 с. URL: https://pdf.lib.vntu.edu.ua/books/2021/Zolotar_2018_446.pdf
43. Кашка В. В. Право на інформацію як фундаментальне право людини. Науковий вісник Ужгородського національного університету. Серія: Право. 2018. Вип. 49. Т. 1. С. 71–73.
44. Кириченко Г. Публічне управління у сфері інформаційної безпеки: теоретико-правовий аналіз сучасних викликів. Вісник Хмельницького національного університету. Економічні науки. 2026. Т. 352, № 2. С. 47–54.
45. Климчук О. В., Лазор О. Д. Стратегічні комунікації як інструмент забезпечення інформаційної стійкості держави в умовах цифровізації публічного простору. Національні інтереси України. 2026. № 2(19). С. 1480–1493.
46. Кобко Є. В. Інформаційна війна та дезінформація: вплив на національну безпеку України. Актуальні питання юридичної науки. 2023. № 20. С. 141–147. URL: <https://doi.org/10.32782/ln.2023.20.20>
47. Козьмініх А. В. Інформаційні механізми євроінтеграційної політики України. Актуальні проблеми політики. 2020. Вип. 65. С. 41–48. URL: <https://doi.org/10.32837/app.v0i65.304>
48. Конституція України: Закон України від 28.06.1996 № 254к/96-ВР. URL: <https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text>
49. Костенко А. М. Інформаційно-комунікативні стратегії євроінтеграції в Україні. Грані. 2018. Т. 21. № 11. С. 70–77. URL: <https://doi.org/10.15421/1718154>
50. Кочубей Л. О. Інформаційна безпека держави: інструменти захисту українського інформаційного поля (на прикладі особливостей інформаційно-комунікаційних технологій у сучасному Донбасі). Наукові записки Інституту політичних і етнонаціональних досліджень імені І. Ф. Кураса НАН України. 2015. Вип. 3. С. 220–237.

51. Крикун В., Бауліна Т. Дезінформація як засіб гібридної війни: сутність і наслідки. Вісник Київського національного університету імені Тараса Шевченка. Державне управління. 2022. № 2 (7). С. 30–33. URL: <https://doi.org/10.17721/2523-4064.2022/7-5/11>
52. Курбан О. В. Історія становлення та розвитку технологій інформаційних війн. Вісник Книжкової палати. 2016. № 4. С. 50–51. URL: https://elibrary.kubg.edu.ua/id/eprint/17002/1/Kurban_VisnykKP_04.2016.pdf
53. Курбан О. В. Сучасні інформаційні війни в мережевому онлайн-просторі : навч. посіб. Київ : ВІКНУ, 2016. 286 с. URL: <http://www.interinf.chnu.edu.ua/res//interinf/Inf%20vijny.pdf>
54. Ларіончева Н. А. Сучасні інформаційні війни: на прикладі російсько-українського протистояння. Політикус. 2024. № 1. С. 14–20. URL: http://politicus.od.ua/1_2024/4.pdf
55. Левченко А., Пойда С. Розвиток механізмів цифрової комунікації органів публічної влади в умовах цифрової трансформації. Наукові перспективи. 2026. № 4(70). С. 449–460.
56. Лешик С. В. Інституційно-правовий механізм інформаційної політики України в процесі євроінтеграції. Політичне життя. 2024. № 3. С. 53–60. URL: <https://doi.org/10.31558/2519-2949.2024.3.6>
57. Лешик С. В. Особливості інформаційної політики в процесі євроінтеграції України. Політологічний вісник. 2024. Вип. 92. С. 198–211. URL: <https://zpv.knu.ua/index.php/pb/article/view/232/214>
58. Лисенко О. О. Правовий захист суспільства від шкідливої інформації : дис. ... канд. юрид. наук : 12.00.07. Харків, 2011. 226 с.
59. Литвин Н. А., Ярош А. О. Вплив дезінформації на національну безпеку України в умовах воєнного стану. Юридичний науковий електронний журнал. 2024. № 2. С. 288–290. URL: <https://doi.org/10.32782/2524-0374/2024-2/69>
60. Максименко Ю. Є. Теоретико-правові засади забезпечення інформаційної безпеки України : дис. ... канд. юрид. наук : 12.00.01. Київ, 2007. 186 с.

61. Маляренко В. І. Кращі практики зарубіжного досвіду боротьби з фейками та дезінформацією. Інформація і право. 2021. № 3 (38). С. 21–27. URL: [https://doi.org/10.37750/2616-6798.2021.3\(38\).243793](https://doi.org/10.37750/2616-6798.2021.3(38).243793)
62. Марущак А. І. Інформаційне право України : підручник. Київ : Дакор, 2011. 456 с.
63. Марущак А. І. Міжнародно-правові підходи та національно-правове регулювання протидії дезінформації. Інформаційна безпека людини, суспільства, держави. 2021. № 1–3 (31–33). С. 64–71.
64. Марущак А. І. Передумови для формування правових механізмів протидії дезінформації в соціальних медіа у контексті національної безпеки: постановка проблеми. Інформація і право. 2022. № 1 (40). С. 82–88.
65. Марущак А. І., Кудрявцева Н. О. Доступ до інформації про діяльність Служби безпеки України в контексті протидії дезінформації. Вісник Харківського національного університету внутрішніх справ. 2022. № 2. С. 281–291. URL: <https://doi.org/10.32631/v.2022.2.25>
66. Марущак А. І., Петров С. Г. Правові механізми ЄС та США для виявлення і блокування російської дезінформації у соціальних мережах. Інформація і право. 2024. № 4 (51). С. 66–72.
67. Мирошніченко М. М. Правове забезпечення інформаційної безпеки держави : дис. ... канд. юрид. наук : 12.00.07. Київ, 2018. 214 с.
68. Негодченко В. О. Основні напрями державної інформаційної політики в Україні. Підприємництво, господарство і право. 2016. № 4. С. 77–81.
69. Нестеряк Ю. В. Державна інформаційна політика України: теоретико-методологічні засади : монографія. Київ : НАДУ, 2014.
70. Нестеряк Ю. В. Міжнародні критерії інформаційної безпеки держави: теоретико-методологічний аналіз. Вісник Національної академії державного управління при Президентові України. 2013. № 3. С. 40–45.
71. Ніколаєць Ю. О. Державна інформаційна політика України в умовах повномасштабного воєнного вторгнення Російської Федерації: суспільно-мобілізаційний потенціал і ефективність. Політичні дослідження. 2024. № 1 (7). С. 42–67. URL: <https://doi.org/10.53317/2786-4774-2024-1-3>

72. Ніщименко О. А. Інформаційна безпека України на сучасному етапі розвитку держави і суспільства. Наше право. 2016. № 1. С. 17–23.
73. Новицька Н. Б. Правові основи захисту суспільної моралі в інформаційній сфері України: теорія та практика : дис. ... д-ра юрид. наук : 12.00.02. Ірпінь, 2016. 454 с.
74. Новицька Н. Б., Петрик В. М., Кудико В. М. Дезінформування як засіб ведення інформаційної війни Російської Федерації проти України. Ірпінський юридичний часопис. 2022. № 1 (8). С. 118–130.
75. Олійник О. В. Інформаційна безпека України: доктрина адміністративно-правового регулювання : дис. ... д-ра юрид. наук : 12.00.07. Київ, 2013. 460 с.
76. Павленко Т. А. Дезінформація: поняття, ознаки, перспективи протидії. Юридичний науковий електронний журнал. 2022. № 7. С. 337–339.
77. Поступна О. В., Волікова М. М. Інституційна іміджелогія в системі національної безпеки: аналіз публічної політики протидії дезінформації та інформаційним загрозам. Дніпровський науковий часопис публічного управління, психології, права. 2026. № 1. С. 13–20.
78. Почепцов Г. Г. Сучасні інформаційні війни. Київ : Києво-Могилянська академія, 2015. 497 с.
79. Правдюк А. Л. Конституційні засади права на інформацію: актуальні проблеми. Юридичний науковий електронний журнал. 2021. № 11. С. 102–104.
80. Про авторське право і суміжні права: Закон України від 01.12.2022 № 2811-IX. URL: <https://zakon.rada.gov.ua/laws/show/2811-20#Text>
81. Про відкритість використання публічних коштів : Закон України від 11.02.2015 № 183-VIII. URL: <https://zakon.rada.gov.ua/laws/show/183-19#Text>
82. Про державну підтримку медіа, гарантії професійної діяльності та соціальний захист журналіста: Закон України від 23.09.1997 № 540/97-ВР. URL: <https://zakon.rada.gov.ua/laws/show/540/97-%D0%B2%D1%80#Text>
83. Про державну таємницю: Закон України від 21.01.1994 № 3855-XII. URL: <https://zakon.rada.gov.ua/laws/show/3855-12#Text>

84. Про доступ до публічної інформації: Закон України від 13.01.2011 № 2939-VI. URL: <https://zakon.rada.gov.ua/laws/show/2939-17#Text>
85. Про електронні документи та електронний документообіг : Закон України від 22.05.2003 № 851-IV. URL: <https://zakon.rada.gov.ua/laws/show/851-15#Text>
86. Про електронні комунікації: Закон України від 16.12.2020 № 1089-IX. URL: <https://zakon.rada.gov.ua/laws/show/1089-20#Text>
87. Про електронну ідентифікацію та електронні довірчі послуги: Закон України від 05.10.2017 № 2155-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2155-19#Text>
88. Про затвердження наборів даних, які підлягають оприлюдненню у формі відкритих даних : постанова Кабінету Міністрів України від 21.10.2015 № 835. URL: <https://zakon.rada.gov.ua/laws/show/835-2015-%D0%BF#Text>
89. Про затвердження плану заходів з реалізації Стратегії інформаційної безпеки на період до 2025 року : розпорядження Кабінету Міністрів України від 30.03.2023 № 272-р. URL: <https://zakon.rada.gov.ua/laws/show/272-2023-%D1%80#Text>
90. Про захист інформації в інформаційно-комунікаційних системах: Закон України від 05.07.1994 № 80/94-ВР. URL: <https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text>
91. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI. URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text>
92. Про інформаційні агентства: Закон України від 28.02.1995 № 74/95-ВР. URL: <https://zakon.rada.gov.ua/laws/show/74/95-%D0%B2%D1%80#Text>
93. Про інформацію: Закон України від 02.10.1992 № 2657-XII. URL: <https://zakon.rada.gov.ua/laws/show/2657-12#Text>
94. Про критичну інфраструктуру : Закон України від 16.11.2021 № 1882-IX. URL: <https://zakon.rada.gov.ua/laws/show/1882-20#Text>
95. Про медіа: Закон України від 13.12.2022 № 2849-IX. URL: <https://zakon.rada.gov.ua/laws/show/2849-20#Text>

96. Про науково-технічну інформацію: Закон України від 25.06.1993 № 3322-XII. URL: <https://zakon.rada.gov.ua/laws/show/3322-12#Text>
97. Про національну безпеку України: Закон України від 21.06.2018 № 2469-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2469-19#Text>
98. Про Національну програму інформатизації: Закон України від 01.12.2022 № 2807-IX. URL: <https://zakon.rada.gov.ua/laws/show/2807-20#Text>
99. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text>
100. Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки: Закон України від 09.01.2007 № 537-V. URL: <https://zakon.rada.gov.ua/laws/show/537-16#Text>
101. Про порядок висвітлення діяльності органів державної влади та органів місцевого самоврядування в Україні медіа : Закон України від 23.09.1997 № 539/97-ВР. URL: <https://zakon.rada.gov.ua/laws/show/539/97-%D0%B2%D1%80#Text>
102. Про публічні електронні реєстри: Закон України від 18.11.2021 № 1907-IX. URL: <https://zakon.rada.gov.ua/laws/show/1907-20#Text>
103. Про рекламу: Закон України від 03.07.1996 № 270/96-ВР. URL: <https://zakon.rada.gov.ua/laws/show/270/96-%D0%B2%D1%80#Text>
104. Про санкції: Закон України від 14.08.2014 № 1644-VII. URL: <https://zakon.rada.gov.ua/laws/show/1644-18#Text>
105. Про Стратегію інформаційної безпеки: Указ Президента України від 28.12.2021 № 685/2021. URL: <https://zakon.rada.gov.ua/laws/show/685/2021#Text>
106. Про Стратегію кібербезпеки України: Указ Президента України від 26.08.2021 № 447/2021. URL: <https://zakon.rada.gov.ua/laws/show/447/2021#Text>
107. Про Стратегію комунікації з питань євроатлантичної інтеграції України на період до 2025 року: Указ Президента України від 11.08.2021 № 348/2021. URL: <https://zakon.rada.gov.ua/laws/show/348/2021#Text>

108. Про Стратегію національної безпеки України: Указ Президента України від 14.09.2020 № 392/2020. URL: <https://zakon.rada.gov.ua/laws/show/392/2020#Text>

109. Про Суспільні медіа України: Закон України від 17.04.2014 № 1227-VII. URL: <https://zakon.rada.gov.ua/laws/show/1227-18#Text>

110. Про схвалення Концепції популяризації України у світі та просування інтересів України у світовому інформаційному просторі: розпорядження Кабінету Міністрів України від 11.10.2016 № 739-р. URL: <https://zakon.rada.gov.ua/laws/show/739-2016-%D1%80#Text>

111. Про схвалення Концепції розвитку електронного урядування в Україні: розпорядження Кабінету Міністрів України від 20.09.2017 № 649-р. URL: <https://zakon.rada.gov.ua/laws/show/649-2017-%D1%80#Text>

112. Про схвалення Стратегії комунікації з питань європейської інтеграції України на період до 2026 року : розпорядження Кабінету Міністрів України від 09.12.2022 № 1155-р. URL: <https://zakon.rada.gov.ua/laws/show/1155-2022-%D1%80#Text>

113. Про утворення Центру протидії дезінформації : рішення Ради національної безпеки і оборони України від 11.03.2021, уведене в дію Указом Президента України від 19.03.2021 № 106/2021. URL: <https://zakon.rada.gov.ua/laws/show/106/2021#Text>

114. Пунда О. О., Добрянська О. Д., Новицька Н. Б. Принципи інформаційної політики в умовах війни та їх нормативно-правове закріплення. Екологічне право. 2022. № 1–2. С. 60–65.

115. Пушкар О. А. Розвиток державної інформаційної політики України: практичні механізми, теоретичні та методологічні підходи: монографія. Київ: Юрінком Інтер, 2025. 460 с.

116. Ржевська Н. Ф. Сучасна інформаційна політика: досвід США для України. Політичні дослідження. 2024. № 1 (7). С. 68–85.

117. Рудник Л. І. Дезінформація як прояв порушення права на доступ до інформації. Вісник Національної академії правових наук України. 2024. № 3. С. 103–118. URL: <https://doi.org/10.31359/1993-0909-2024-31-3-103>

118. Рудник Л. І. Поширення недостовірної інформації як засіб ведення гібридних війн. *Інформація і право*. 2024. № 4 (51). С. 46–54. URL: [https://doi.org/10.37750/2616-6798.2024.4\(51\).317765](https://doi.org/10.37750/2616-6798.2024.4(51).317765)
119. Рудник Л. І. Правові засади обмеження права на доступ до інформації в умовах воєнного стану. *Вісник НТУУ «КПІ». Політологія. Соціологія. Право*. 2023. № 4 (60). С. 32–39. URL: [https://doi.org/10.20535/2308-5053.2023.4\(60\).296975](https://doi.org/10.20535/2308-5053.2023.4(60).296975)
120. Савосько Т. О. Зміст та функції поняття державної інформаційної політики. *Вчені записки ТНУ імені В. І. Вернадського. Серія: Публічне управління та адміністрування*. 2024. Т. 35 (74). № 1. С. 28–32. URL: <https://doi.org/10.32782/TNU-2663-6468/2024.1/06>
121. Савосько Т. О. Особливості формування державної інформаційної політики. *Аспекти публічного управління*. 2024. Т. 12. № 1. С. 22–28. URL: <https://doi.org/10.15421/152403>
122. Сірий С., Турченко Ю. Інформаційна політика України доби глобалізації: теоретичний аналіз. *Політичний менеджмент*. 2012. № 4–5. С. 237–247.
123. Сірко В. С. Дезінформація під час російсько-української війни. *Південноукраїнський правничий часопис*. 2022. № 4. Ч. 3. С. 235–237. URL: <https://doi.org/10.32850/sulj.2022.4.3.39>
124. Соловйов С. Г., Бухтатий О. Є., Нестеряк Ю. В. та ін. Інформаційна складова державної політики та управління: монографія. Київ : К.І.С., 2015.
125. Твердохліб О. С. Європейський підхід до розроблення інформаційної політики держави. *Актуальні проблеми економіки*. 2016. № 3 (177). С. 429–435.
126. Тихомирова О. Інформаційна політика незалежної України: періодизація та вплив на громадянське суспільство. *Грані*. 2020. Т. 23. № 10. С. 24–35. URL: <https://doi.org/10.15421/172090>
127. Турченко Ю. В. Сутність державної інформаційної політики в умовах демократичного державотворення. *Держава і право*. 2009. Вип. 46. С. 631–637. URL: <https://irbis-nbuv.gov.ua/publ/REF-0000468951>

128. Угода про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони. URL: https://zakon.rada.gov.ua/laws/show/984_011#Text

129. Уханова Н. С. Проблеми протидії негативним інформаційним впливам та захисту інформаційної безпеки людини і суспільства : монографія. Київ ; Одеса : Фенікс, 2022. 120 с.

130. Шемчук В. В. Конституційно-правове забезпечення інформаційної безпеки сучасних держав: порівняльно-правовий аналіз : дис. ... д-ра юрид. наук : 12.00.02. Ужгород, 2020. 410 с.

131. Шинкар Т. І. Адміністративно-правові засади регулювання обмеження права на інформацію в інтересах національної безпеки : дис. ... д-ра юрид. наук : 12.00.07. Львів, 2023. 510 с.

132. Шлапаченко В. М. Дезінформація як спосіб інформаційно-психологічного впливу. Інформаційна безпека людини, суспільства, держави. 2013. № 2 (12). С. 78–86. URL: http://nbuv.gov.ua/UJRN/iblsd_2013_2_15

133. Яценко В. А. Інформаційна свідомість як фактор війни Росії проти України. Інформація і право. 2022. № 2 (41). С. 9–17.

134. Benkler Y., Faris R., Roberts H. Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics. New York : Oxford University Press, 2018. 472 p. URL: <https://doi.org/10.1093/oso/9780190923624.001.0001>

135. Bennett W. L., Livingston S. The disinformation order: Disruptive communication and the decline of democratic institutions. European Journal of Communication. 2018. Vol. 33, No. 2. P. 122–139. URL: <https://doi.org/10.1177/0267323118760317>

136. Braman S. Change of State: Information, Policy, and Power. Cambridge, MA : MIT Press, 2006. 545 p.

137. Canel M. J., Sanders K. Government Communication: Cases and Challenges. London : Bloomsbury Academic, 2013. 288 p.

138. Chadwick A. *The Hybrid Media System: Politics and Power*. 2nd ed. New York : Oxford University Press, 2017. 368 p.
139. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS 2 Directive). URL: <https://eur-lex.europa.eu/eli/dir/2022/2555/oj>
140. European Commission. *European Democracy Action Plan*. COM(2020) 790 final. 2020. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020DC0790>
141. European Commission. *Strengthened Code of Practice on Disinformation*. 2022. URL: <https://digital-strategy.ec.europa.eu/en/library/2022-strengthened-code-practice-disinformation>
142. Freelon D., Wells C. Disinformation as political communication. *Political Communication*. 2020. Vol. 37, No. 2. P. 145–156. URL: <https://doi.org/10.1080/10584609.2020.1723755>
143. Giles K. *Handbook of Russian Information Warfare*. Rome: NATO Defense College, 2016. 77 p. URL: <https://www.ndc.nato.int/news/news.php?icode=995>
144. Hallahan K., Holtzhausen D., van Ruler B., Verčič D., Sriramesh K. Defining strategic communication. *International Journal of Strategic Communication*. 2007. Vol. 1, No. 1. P. 3–35. URL: <https://doi.org/10.1080/15531180701285244>
145. Helmus T. C., Bodine-Baron E., Radin A. et al. *Russian Social Media Influence: Understanding Russian Propaganda in Eastern Europe*. Santa Monica, CA : RAND Corporation, 2018. URL: https://www.rand.org/pubs/research_reports/RR2237.html
146. Humprecht E., Esser F., Van Aelst P. Resilience to online disinformation: A framework for cross-national comparative research. *The International Journal of Press/Politics*. 2020. Vol. 25, No. 3. P. 493–516. URL: <https://doi.org/10.1177/1940161219900126>
147. Ireton C., Posetti J. (eds.). *Journalism, “Fake News” & Disinformation: Handbook for Journalism Education and Training*. Paris : UNESCO, 2018. 128 p. URL: <https://unesdoc.unesco.org/ark:/48223/pf0000265552>

148. Kavanagh J., Rich M. D. Truth Decay: An Initial Exploration of the Diminishing Role of Facts and Analysis in American Public Life. Santa Monica, CA : RAND Corporation, 2018. URL: https://www.rand.org/pubs/research_reports/RR2314.html
149. Lazer D. M. J. et al. The science of fake news. Science. 2018. Vol. 359, No. 6380. P. 1094–1096. URL: <https://doi.org/10.1126/science.aao2998>
150. OECD. Good Practice Principles for Public Communication Responses to Mis- and Disinformation. OECD Public Governance Policy Papers. 2023. No. 30. Paris : OECD Publishing. URL: <https://doi.org/10.1787/6d141b44-en>
151. OECD. Public Communication: The Global Context and the Way Forward. Paris : OECD Publishing, 2021. URL: <https://doi.org/10.1787/22f8031c-en>
152. Persily N., Tucker J. A. (eds.). Social Media and Democracy: The State of the Field, Prospects for Reform. Cambridge : Cambridge University Press, 2020. URL: <https://doi.org/10.1017/9781108890960>
153. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (General Data Protection Regulation). URL: <https://eur-lex.europa.eu/eli/reg/2016/679/oj>
154. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services (Digital Services Act). URL: <https://eur-lex.europa.eu/eli/reg/2022/2065/oj>
155. Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance (Data Governance Act). URL: <https://eur-lex.europa.eu/eli/reg/2022/868/oj>
156. Regulation (EU) 2024/1083 of the European Parliament and of the Council of 11 April 2024 establishing a common framework for media services in the internal market (European Media Freedom Act). URL: <https://eur-lex.europa.eu/eli/reg/2024/1083/oj>
157. Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). URL: <https://eur-lex.europa.eu/eli/reg/2024/1689/oj>

158. Shestakovska T., Dubovyk D. Formation of a transparent information policy in the context of decentralization: challenges and prospects. RFI Scientific Papers. 2025. № 4. C. 89-100.

159. UNESCO. Guidelines for the Governance of Digital Platforms: Safeguarding Freedom of Expression and Access to Information through a Multistakeholder Approach. Paris, 2023. URL: <https://unesdoc.unesco.org/ark:/48223/pf0000387339>

160. United Nations. Global Principles for Information Integrity: Recommendations for Multi-stakeholder Action. New York, 2024. URL: <https://www.un.org/en/information-integrity/global-principles>

161. Wardle C., Derakhshan H. Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making. Strasbourg : Council of Europe, 2017. URL: <https://edoc.coe.int/en/media/7495-information-disorder-toward-an-interdisciplinary-framework-for-research-and-policy-making.html>



НАРОДНИЙ ДЕПУТАТ УКРАЇНИ

01008, м. Київ, вул. Грушевського, 5

№ 116Д7/11-2025/196124

23.09.2025 р.

ДОВІДКА

щодо науково-практичної значущості результатів дисертаційного дослідження

Цією довідкою підтверджується, що окремі наукові положення, методичні розробки та практичні рекомендації дисертаційного дослідження Дубовика Д. Є. на тему «Механізми реалізації державної інформаційної політики», поданого на здобуття ступеня доктора філософії за спеціальністю 281 «Публічне управління та адміністрування», використано в аналітичній та законотворчій роботі народного депутата України під час опрацювання законодавчих ініціатив і підготовки пропозицій щодо вдосконалення державної інформаційної політики.

У практичній діяльності використано такі результати дослідження:

- концептуальну архітектуру інтегрованого організаційно-управлінського механізму реалізації державної інформаційної політики для систематизації повноважень, функцій і відповідальності суб'єктів інформаційної сфери;
- пропозиції щодо нормативного закріплення міжвідомчої координації, обміну даними, планового та кризового режимів публічної комунікації;
- двоконтурний механізм стратегічних комунікацій і протидії дезінформації, що поєднує проактивне пояснення державної політики з моніторингом, верифікацією, рівневою ескалацією та пропорційним реагуванням;
- систему показників моніторингу й оцінювання ефективності державної інформаційної політики, орієнтовану на якість інформації, своєчасність реагування, довіру, охоплення, доступність і суспільний результат.

Застосування запропонованих положень сприяло комплексному врахуванню правозахисного, управлінського, цифрового, комунікаційного та безпекового вимірів під час експертного опрацювання відповідних законодавчих пропозицій, а також підвищенню обґрунтованості рекомендацій щодо розмежування повноважень і оцінювання результативності державних рішень в інформаційній сфері.

Використання зазначених наукових результатів підтверджує їх практичну значущість, прикладну придатність і можливість подальшого застосування в системі публічного управління.

Народний депутат України

ГРИВКО С.Д.
(посв. №110)



МЕНСЬКА МІСЬКА РАДА

вул. Героїв АТО, 6, м. Мена Чернігівської області, 515600,
тел. (04644) 2-15-41 e-mail: miskradamena@cg.gov.ua, Web: <https://mena.cg.gov.ua>, код ЄДРПОУ 04061777

№ 05-23/2116

07.11.2025 р.

ДОВІДКА

щодо науково-практичної значущості результатів дисертаційного дослідження

Цією довідкою підтверджується, що окремі наукові положення, методичні розробки та практичні рекомендації дисертаційного дослідження Дубовика Д. Є. на тему «Механізми реалізації державної інформаційної політики», поданого на здобуття ступеня доктора філософії за спеціальністю 281 «Публічне управління та адміністрування», використано у діяльності Менської міської ради під час удосконалення інформаційної взаємодії органу місцевого самоврядування з мешканцями, медіа, громадськими організаціями та іншими заінтересованими сторонами.

У практичній діяльності використано такі результати дослідження: класифікацію інструментів інформаційної взаємодії, що охоплює офіційний вебсайт, соціальні мережі, відкриті дані, електронні звернення, публічні консультації, медіазаходи та кризові комунікації; матрицю розподілу ролей між керівництвом, структурними підрозділами, відповідальними за комунікації, цифрові сервіси, правове забезпечення та реагування на інформаційні ризики; рекомендації щодо підготовки комунікаційних планів, оперативної верифікації повідомлень, заповнення інформаційних вакуумів і координації дій у кризових ситуаціях; систему індикаторів для оцінювання своєчасності, доступності, зрозумілості та охоплення офіційної інформації, якості зворотного зв'язку й рівня довіри до комунікацій органу місцевого самоврядування.

Урахування цих рекомендацій забезпечило більш послідовне планування інформаційної роботи, узгодження повідомлень між структурними підрозділами, підвищення оперативності інформування громадян та орієнтацію комунікаційної діяльності на вимірюваний суспільний результат.

Використання зазначених наукових результатів підтверджує їх практичну значущість, прикладну придатність і можливість подальшого застосування в системі публічного управління.

Секретар ради

Юрій СТАЛЬНИЧЕНКО



УНІВЕРСИТЕТ ТРАНСФОРМАЦІЇ МАЙБУТНЬОГО

Вул. Ремісничка, 28, м. Чернігів, 14000, e-mail: utmzvo@gmail.com, код ЄДРПОУ 45630188

№ 19/25 від 18.10.2025 р.

ДОВІДКА

щодо науково-практичної значущості результатів дисертаційного дослідження Дубовика Д. Є. на тему «Механізми реалізації державної інформаційної політики»

Цією довідкою підтверджується, що окремі наукові положення, методичні розробки та практичні рекомендації дисертаційного дослідження використано у навчальній, методичній і науковій діяльності Закладу вищої освіти «Університет трансформації майбутнього».

У практичній діяльності використано такі результати дослідження:

- теоретичні положення щодо еволюції, функцій, цілей і пріоритетів державної інформаційної політики під час оновлення змісту освітніх компонентів із публічного управління, цифрового врядування, інформаційної безпеки та стратегічних комунікацій;
- концептуальну архітектуру інтегрованого організаційно-управлінського механізму як навчальну модель для аналізу суб'єктів, функцій, ресурсів, інструментів і зворотного зв'язку в системі реалізації публічної політики;
- двоконтурний механізм стратегічних комунікацій і протидії дезінформації для розроблення практичних кейсів, ситуаційних завдань і алгоритмів кризового реагування;

Інтеграція зазначених результатів у навчально-методичні матеріали дала змогу посилити міждисциплінарний і практико-орієнтований характер підготовки здобувачів, розвинути компетентності з аналізу інформаційних ризиків, стратегічного планування комунікацій, міжвідомчої координації та доказового оцінювання публічної політики.

Президент



Тетяна ШЕСТАКОВСЬКА



**Громадська
організація
«Освітній компас»**

14000, м.Чернігів вул.Ремісничка, 28

ЄДРПОУ 45243912
Тел. +380634023737

Вих. № 08/25 від 24.12.2025 р.

ДОВІДКА
щодо науково-практичної значущості результатів дисертаційного
дослідження Дубовика Д. Є. на тему «Механізми реалізації державної
інформаційної політики»

Цією довідкою підтверджується, що окремі наукові положення, методичні розробки та практичні рекомендації дисертаційного дослідження використано у діяльності громадської організації «Освітній компас» під час розроблення та реалізації громадських, освітніх і комунікаційних ініціатив.

У практичній діяльності використано такі результати дослідження: методику визначення цільових аудиторій, інформаційних потреб, ризиків і каналів комунікації під час планування суспільно орієнтованих проєктів; елементи проактивного контуру стратегічних комунікацій для формування зрозумілих повідомлень, розвитку медіаграмотності та попередження інформаційних вакуумів; інструменти виявлення і первинної перевірки сумнівного контенту, алгоритм внутрішньої ескалації та підготовки коректної публічної відповіді без посилення шкідливого інформаційного впливу; систему індикаторів моніторингу інформаційних кампаній і освітніх заходів, що враховує охоплення, залученість, якість зворотного зв'язку, зміну обізнаності та практичне використання отриманих знань.

Використання результатів дослідження сприяло підвищенню якості планування комунікацій, обґрунтованому добору каналів і форматів взаємодії, посиленню профілактичної складової протидії дезінформації та запровадженню регулярного оцінювання результатів громадських і освітніх ініціатив.

З повагою,

Заступник голови
ГО «Освітній компас»



Інна МОСКАЛЕЦЬ



Метадані

ДОКУМЕНТ

Заголовок

МЕХАНІЗМИ РЕАЛІЗАЦІЇ ДЕРЖАВНОЇ ІНФОРМАЦІЙНОЇ ПОЛІТИКИ

Автор

Денис Євгенович ДУБОВИК

Науковий керівник / Експерт

Zhytomyr Polytechnic

ІД документу

334404055

ОРГАНІЗАЦІЯ

Назва організації

State University "Zhytomyr Polytechnic"

підрозділ

State University "Zhytomyr Polytechnic"

ЗВІТ

Дата звіту

2026-06-23

Дата редагування

Обсяг знайдених подібностей

Коефіцієнт подібності визначає, який відсоток тексту по відношенню до загального обсягу тексту було знайдено в різних джерелах. Зверніть увагу, що високі значення коефіцієнта не автоматично означають плагіат. Звіт має аналізувати компетентна / уповноважена особа.



КП 1



КП 2

25

Довжина фрази для коефіцієнта подібності 2

46560

Кількість слів

407104

Кількість символів

Тривога

У цьому розділі ви знайдете інформацію щодо текстових спотворень. Ці спотворення в тексті можуть говорити про МОЖЛИВІ маніпуляції в тексті. Спотворення в тексті можуть мати навмисний характер, але частіше характер технічних помилок при конвертації документа та його збереженні, тому ми рекомендуємо вам підходити до аналізу цього модуля відповідально. У разі виникнення запитань, просимо звертатися до нашої служби підтримки.

Заміна букв		2
Інтервали		0
Мікропробіли		1
Білі знаки		20
Парафрази (SmartMarks)		12

Джерела

Нижче наведений список джерел. В цьому списку є джерела із різних баз даних. Копір тексту означає в якому джерелі він був знайдений. Ці джерела і значення Коефіцієнту Подібності не відображають прямого плагіату. Необхідно відкрити кожне джерело і проаналізувати зміст і правильність оформлення джерела.

10 найдовших фраз

Копір тексту

#	НАЗВА ТА АДРЕСА ДЖЕРЕЛА URL (НАЗВА БАЗИ)	КІЛЬКІСТЬ ІДЕНТИЧНИХ СЛІВ (ФРАГМЕНТІВ)
1	Титаренко_Marістерська_3.docx 12/20/2023	20 0 (0.04 %)

Lesya Ukrainka Volyn National University (Кафедра політології та публічного управління)

2	https://npu.edu.ua/images/file/vidil_aspirant/avtoref/D26.053.01/aref_Yanisiv.pdf	17 0 (0.04 %)
3	Розвиток людського капіталу підприємства в умовах цифровізації економіки 12/5/2025 State Biotechnological University (Кафедра економіки та бізнесу)	17 0 (0.04 %)
4	https://ztu.edu.ua/site/files/1/docs/aref_%D0%9F%D0%B5%D1%80%D0%B5%D0%B2%D0%B5%D1%80%D0%B7%D1%94%D0%B2.pdf	14 0 (0.03 %)
5	https://www.uzhnu.edu.ua/uk/infocentre/get/19617	14 0 (0.03 %)
6	https://krs.chmnu.edu.ua/jspui/bitstream/123456789/4009/1/%D0%90%D0%BD%D0%BE%D1%82%D0%B0%D1%86%D1%96%D1%8F%20%D0%A0%D0%B0%D1%87%D0%B8%D0%BD%D1%81%D1%8C%D0%BA%D0%B0.pdf	14 0 (0.03 %)
7	https://www.uzhnu.edu.ua/uk/infocentre/get/19617	14 0 (0.03 %)
8	https://ztu.edu.ua/site/files/1/docs/aref_%D0%9F%D0%B5%D1%80%D0%B5%D0%B2%D0%B5%D1%80%D0%B7%D1%94%D0%B2.pdf	14 0 (0.03 %)
9	http://diser.ntu.edu.ua/Kompanez.pdf	13 0 (0.03 %)
10	https://krs.chmnu.edu.ua/jspui/bitstream/123456789/896/1/%D0%90%D0%B2%D1%82%D0%BE%D1%80%D0%B5%D1%84%D0%B5%D1%80%D0%B5%D0%B0%D1%82%20%D0%A3%D1%80%D1%81%D1%83%D0%BB%20%D0%93.%D0%92..pdf	12 0 (0.03 %)

Домашня база даних

#	ЗАГОЛОВОК	КІЛЬКІСТЬ ІДЕНТИЧНИХ СЛІВ (ФРАГМЕНТІВ)
---	-----------	--

Програма обміну базами даних (0.19 %)

#	ЗАГОЛОВОК	КІЛЬКІСТЬ ІДЕНТИЧНИХ СЛІВ (ФРАГМЕНТІВ)
1	Титаренко_Магістерська_3.docx 12/20/2023 Lesya Ukrainka Volyn National University (Кафедра політології та публічного управління)	20 (1) (0.04 %)
2	Розвиток людського капіталу підприємства в умовах цифровізації економіки 12/5/2025 State Biotechnological University (Кафедра економіки та бізнесу)	17 (1) (0.04 %)
3	Управління процесом стратегічного планування на підприємстві з метою забезпечення сталого розвитку 3/15/2025 National Technical University of Ukraine Igor Sikorskyi Kyiv Politech Institute (National Technical University of Ukraine Igor Sikorskyi Kyiv Politech Institute)	16 (2) (0.03 %)
4	ІНФОРМАЦІЙНИЙ МЕНЕДЖМЕНТ ЯК СКЛАДОВА ДЕРЖАВНОЇ ІНФОРМАЦІЙНОЇ ПОЛІТИКИ.doc 11/23/2020 Kherson national technical university (Херсонський національний технічний університет)	14 (2) (0.03 %)
5	Роль громадянського суспільства в реалізації державної інформаційної політики 12/3/2025 Kyiv National Economic University named after Vadym Hetman KNEU (кафедра національної економіки та публічного управління)	13 (2) (0.03 %)
6	Робота_на_конкурс_Публ_фінанси_Околициний_Кирило_109_ПУА_Д22 3/26/2025 Ukrainian State University of Railway Transport (Ukrainian State University of Railway Transport)	7 (1) (0.02 %)

ІНТЕРНЕТ (0.04 %)

інтернет (0.04 %)		
#	ДЖЕРЕЛО URL	КІЛЬКІСТЬ ІДЕНТИЧНИХ СЛІВ (ФРАГМЕНТІВ)
7	https://www.uzhnu.edu.ua/uk/infocentre/get/19617	42 (4) (0.09 %)
8	http://repository.maranatha.edu/4497/2/0223109_Appendices.pdf	40 (8) (0.09 %)
9	https://ztu.edu.ua/site/files/1/docs/aref_%D0%9F%D0%B5%D1%80%D0%B5%D0%B2%D0%B5%D1%80%D0%B7%D1%94%D0%B2.pdf	34 (3) (0.07 %)
10	https://krs.chmnu.edu.ua/jspui/bitstream/123456789/4009/1/%D0%90%D0%BD%D0%BE%D1%82%D0%B0%D1%86%D1%96%D1%8F%20%D0%A0%D0%B0%D1%87%D0%B8%D0%BD%D1%81%D1%8C%D0%BA%D0%B0.pdf	22 (2) (0.05 %)
11	https://www.frontiersin.org/journals/sustainable-food-systems/articles/10.3389/fsufs.2024.1514409/full	20 (2) (0.04 %)
12	https://docplayer.net/82045883-Naukovo-doslidnyy-institut-informatiki-i-prava-nacionalnoyi-akademiyi-pravovih-nauk-ukrayini-radzievka-oksana-grigorivna.html	19 (3) (0.04 %)
13	https://nuczu.edu.ua/images/topmenu/science/spetsializovani-vcheni-rady/disPanchenko.pdf	18 (3) (0.04 %)
14	https://npu.edu.ua/images/file/vidil_aspirant/avtoref/D26.053.01/aref_Yanisiv.pdf	17 (1) (0.04 %)
15	http://diser.ntu.edu.ua/KompaneZ.pdf	13 (1) (0.03 %)
16	https://krs.chmnu.edu.ua/jspui/bitstream/123456789/896/1/%D0%90%D0%B2%D1%82%D0%BE%D1%80%D0%B5%D1%84%D0%B5%D1%80%D0%B5%D0%B0%D1%82%20%D0%A3%D1%80%D1%81%D1%83%D0%BB%20%D0%93%D0%92_.pdf	12 (1) (0.03 %)
17	https://card-file.onaft.edu.ua/bitstream/123456789/17633/1/Sylenko.pdf	11 (2) (0.02 %)
18	https://uu.edu.ua/upload/universitet/Osobisti_zdobutki/Zahist_disertacij_A_Z/Dobrovolskiy_avtoref.pdf	11 (1) (0.02 %)
19	http://irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?C21COM=2&I21DBN=UJRN&P21DBN=UJRN&Z21ID=&IMAGE_FILE_DOWNLOAD=1&image_file_name=PDF%2FInfor_2017_1.pdf	10 (1) (0.02 %)
20	https://docplayer.net/78927369-Nacionalniy-universitet-vodnogo-gospodarstva-ta-prirodokoristuvannya-ministerstvo-osviti-i-nauki-ukrayini-kapral-olga-rostislavivna-disertaciya.html	10 (1) (0.02 %)
21	http://www.khnu.km.ua/root/res/2-21-50-10.pdf	10 (1) (0.02 %)
22	https://library.krok.edu.ua/media/library/category/disertatsiji-avtoreferati-vidguki/etrova-l-g_2016-disertatsija.pdf	9 (1) (0.02 %)

Список прийнятих фрагментів

#	ЗМІСТ	КІЛЬКІСТЬ ОДНАКОВИХ СЛІВ (ФРАГМЕНТІВ)
---	-------	---------------------------------------