

УДК 351:004:332.1(477)

[https://doi.org/10.52058/3041-1254-2026-1\(23\)-1034-1047](https://doi.org/10.52058/3041-1254-2026-1(23)-1034-1047)

Сас Антон Ігорович аспірант кафедри менеджменту і публічного адміністрування, Харківський національний університет міського господарства імені О. М. Бекетова, м. Харків, <https://orcid.org/0009-0007-2582-8954>

ОСОБЛИВОСТІ ПУБЛІЧНОГО УПРАВЛІННЯ ІНФОРМАЦІЙНО-КОМУНІКАЦІЙНИМ ЗАБЕЗПЕЧЕННЯМ СОЦІАЛЬНО-ЕКОНОМІЧНОГО РОЗВИТКУ РЕГІОНІВ УКРАЇНИ

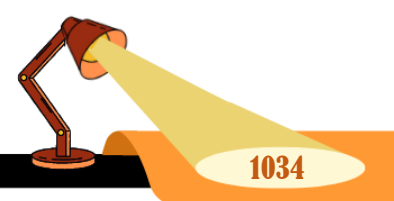
Анотація. У статті досліджено особливості публічного управління інформаційно-комунікаційним забезпеченням соціально-економічного розвитку регіонів України в умовах цифрової трансформації та посилення сучасних безпекових викликів. Обґрунтовано, що інформаційно-комунікаційне забезпечення є ключовою складовою ефективного функціонування механізмів державного регулювання та відіграє визначальну роль у підвищенні якості управлінських рішень на регіональному рівні.

Акцентовано увагу на значенні інтеграції сучасних інформаційних технологій та інноваційних організаційних рішень у діяльність органів публічної влади як чинника підвищення прозорості, відкритості та результативності публічного управління. Визначено, що формування ефективних інформаційних каналів взаємодії між органами влади, населенням, бізнесом, інвесторами та іншими заінтересованими сторонами сприяє зміцненню довіри до державних інституцій, активізації інноваційних процесів і забезпеченню сталого розвитку регіонів.

У межах дослідження інформаційно-комунікаційне забезпечення публічного управління розглянуто з урахуванням специфіки функціонування в умовах воєнного стану, зокрема обмежень доступу до окремих категорій публічної інформації, необхідності захисту інформаційних ресурсів та забезпечення стійкості критичної інформаційної інфраструктури. Підкреслено, що ефективність публічного управління значною мірою залежить від узгодженості інформаційних систем і якості комунікаційних процесів між різними рівнями влади.

Зроблено висновок, що розвиток інформаційно-комунікаційного забезпечення публічного управління є важливою передумовою мінімізації корупційних ризиків, підвищення інституційної спроможності органів влади та формування адаптивної системи державного управління, здатної ефективно реагувати на сучасні соціально-економічні виклики в регіональному вимірі.

Ключові слова: публічне управління, регіональний розвиток, інформаційне забезпечення, державне регулювання, соціально-економічний розвиток регіонів





України, персональні дані, кіберзахист, захист інформації, інформаційно-комунікаційне забезпечення, цифрова трансформація, захист даних, бази даних, інформаційно-комунікаційні системи, регіональне управління, електроні комунікації.

Sas Anton Igorovich Phd.student at the Department of Management and Public Administration, O. M. Beketov National University of Urban Economy in Kharkiv, <https://orcid.org/0009-0007-2582-8954>

FEATURES OF PUBLIC ADMINISTRATION OF INFORMATION AND COMMUNICATION SUPPORT FOR THE SOCIO-ECONOMIC DEVELOPMENT OF THE REGIONS OF UKRAINE

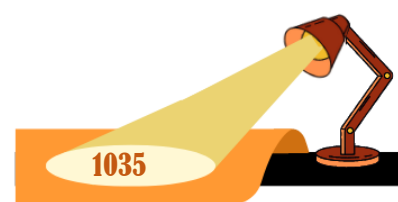
Abstract. The article investigates the features of public administration of information and communication support for the socio-economic development of the regions of Ukraine in the context of digital transformation and increasing contemporary security challenges. It is substantiated that information and communication support constitutes a key component of the effective functioning of state regulatory mechanisms and plays a decisive role in improving the quality of administrative decisions at the regional level.

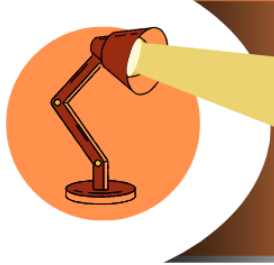
The study emphasizes the importance of integrating modern information technologies and innovative organizational solutions into the activities of public authorities as a factor enhancing transparency, openness, and the overall effectiveness of public administration. It is highlighted that establishing efficient communication channels among public authorities, citizens, businesses, investors, and other stakeholders strengthens trust in state institutions, stimulates innovative processes, and ensures sustainable regional development.

Within the framework of the research, information and communication support is considered in light of the specific challenges of functioning under martial law, including restrictions on access to certain categories of public information, the need to protect information resources, and ensuring the resilience of critical information infrastructure. The effectiveness of public administration is shown to largely depend on the coherence of information systems and the quality of communication processes across different levels of government.

The article concludes that the development of information and communication support in public administration is an essential prerequisite for minimizing corruption risks, enhancing the institutional capacity of authorities, and creating an adaptive public governance system capable of responding effectively to contemporary socio-economic challenges at the regional level.

Keywords: public administration, regional development, information support, state regulation, socio-economic development of Ukraine's regions, personal data,





cybersecurity, information protection, information and communication support, digital transformation, data protection, databases, information and communication systems, regional governance, electronic communications.

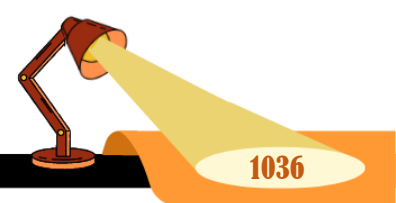
Постановка проблеми. У сучасних умовах глобальної цифрової трансформації, посилення безпекових викликів в Україні та зростання ролі інформації як стратегічного національного ресурсу публічне управління інформаційно-комунікаційним забезпеченням набуває концептуально важливого значення для забезпечення ефективного функціонування держави та регіонів. Інформаційні потоки, цифрові платформи та електронні сервіси стають невід'ємними елементами реалізації державної політики та регіонального розвитку, визначаючи якість управлінських рішень і рівень довіри суспільства до органів влади.

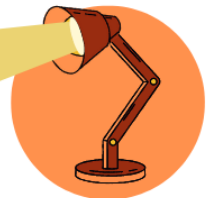
Водночас практика публічного управління в Україні засвідчує наявність низки системних проблем, пов'язаних із фрагментарністю нормативно-правового регулювання у сфері інформаційного забезпечення, недостатньою узгодженістю управлінських рішень між різними рівнями публічної влади, а також нерівномірністю розвитку інформаційно-комунікаційної інфраструктури регіонів. Додатковим ускладнюючим чинником є необхідність поєднання вимог прозорості та відкритості публічної інформації з потребами її захисту, забезпечення кібербезпеки та стійкості критичної інформаційної інфраструктури.

Особливої актуальності зазначені проблеми набувають в умовах воєнного стану, коли безперервність функціонування інформаційних систем, електронних реєстрів і цифрових сервісів органів публічної влади безпосередньо впливає на соціально-економічну стабільність регіонів, рівень безпеки населення та спроможність держави виконувати свої базові функції.

Аналіз останніх досліджень і публікацій. Питання публічного управління інформаційно-комунікаційним забезпеченням органів публічної влади є предметом дослідження як вітчизняних, так і зарубіжних науковців. Так, В. М. Бабаєв [1] у своїх працях наголошує на важливості інформаційного забезпечення як складової частини системи державного управління, розглядаючи його вплив на прийняття управлінських рішень та ефективність функціонування адміністративних механізмів. М. М. Бенько [2] зосереджує увагу на теоретичних засадах інформаційної політики, підкреслюючи роль інформаційних потоків у формуванні прозорості та підзвітності органів влади. І. М. Білан [3] аналізує практичні аспекти забезпечення інформаційної взаємодії між рівнями влади, акцентуючи увагу на проблемах узгодженості комунікаційних процесів.

Особливий внесок у дослідження механізмів інформаційно-комунікаційного забезпечення внесли П. В. Макушев [16] та Н. І. Олійченко [19], які розглядають інформаційні ресурси як інструмент реалізації стратегічних завдань розвитку регіонів, зокрема в контексті цифровізації управлінських процесів. У





публікації Плєскача В. Л. [20] підкреслено значення інтегрованих інформаційних систем для забезпечення оперативного обміну даними між суб'єктами публічного управління, що є критично важливим для підвищення адаптивності адміністративних механізмів до зміни зовнішніх умов.

Серед зарубіжних досліджень вагомий внесок у розуміння проблематики зробили David C. G. Brown та Sandra Toze [25], які аналізують сучасні підходи до інформаційно-комунікаційного забезпечення у публічному секторі, зокрема в аспектах відкритих даних, цифрової взаємодії з громадськістю та інтеграції інформаційних технологій у процеси державного управління. Вони підкреслюють, що ефективність інформаційних комунікацій значною мірою визначається не лише технічними можливостями, але й організаційними, правовими та культурними факторами.

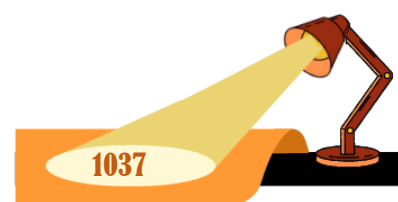
Незважаючи на значний внесок окремих дослідників у розкриття окремих аспектів проблеми, залишається нагальна потреба в системному, міждисциплінарному підході до вивчення особливостей публічного управління інформаційно-комунікаційним забезпеченням як критично важливої складової державного регулювання соціально-економічного розвитку регіонів.

Мета статті полягає у виявленні та науковому обґрунтуванні особливостей публічного управління інформаційно-комунікаційним забезпеченням соціально-економічного розвитку регіонів України, а також у визначенні напрямів підвищення ефективності відповідних управлінських механізмів в умовах цифрової трансформації та сучасних безпекових викликів.

Виклад основного матеріалу. У сучасних умовах цифрової трансформації визначальною характеристикою інформації є її мультиформатність, мережевий характер та здатність до обробки й поширення в режимі реального часу через інтегровані цифрові платформи та електронні комунікаційні мережі. Розвиток інформаційно-комунікаційних технологій і цифрових каналів передачі даних істотно впливає на масштаб, структуру та методи здійснення публічного управління, формуючи нові можливості для органів державної влади та місцевого самоврядування.

Сучасне публічне управління функціонує у середовищі цифрових систем, мобільних мереж, хмарних обчислень, великих даних та аналітичних платформ, що дозволяють ухвалювати управлінські рішення на основі даних. Це проявляється у впровадженні електронних адміністративних послуг, цифрових реєстрів, платформ міжвідомчої взаємодії, електронних петицій та інших інструментів електронної демократії й е-врядування.

Використання таких інструментів трансформує взаємодію між державою, бізнесом і громадянами, підвищує доступність публічних послуг, а також сприяє прозорості та оперативності управлінських процедур. Водночас складність сучасного інформаційного середовища зумовлює потребу в системному та





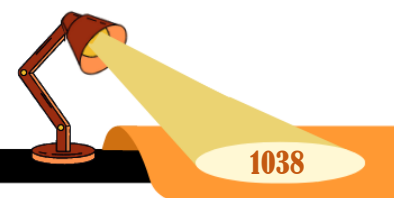
комплексному підході до інформаційно-комунікаційного забезпечення публічного управління, включно з ефективним нормативно-правовим регулюванням процесів формування, використання, захисту та розвитку інформаційних ресурсів. Це сприяє розвитку наукових концепцій та методологій, спрямованих на поглиблене розуміння складної, багатокомпонентної природи інформаційного забезпечення публічної влади.

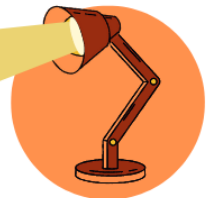
Зокрема, І. М. Олійченко підкреслює, що одним із ключових атрибутів держави, який визначає її вплив на соціально-економічний розвиток суспільства, є рівень сформованості системи інформаційного забезпечення в державних органах. За його оцінкою, належне інформаційне забезпечення сприяє обґрунтованому ухваленню публічних управлінських рішень і підвищує ефективність адміністрування [19]. Теоретичні узагальнення та практичний досвід розвитку публічного управління демонструють, що інформаційне забезпечення слід розглядати як стратегічну складову підвищення ефективності діяльності публічної влади, що безпосередньо впливає на результативність ухвалення рішень і реалізації політик на державному, галузевому, регіональному та міжнародному рівнях [19].

П. В. Макушев зазначає, що інформаційне забезпечення є важливим елементом функціонування кожної державної служби, оскільки воно визначає ефективність роботи та координації всіх структур [16].

У більшості наукових джерел інформаційні технології, а також ширший термін інформаційно-комунікаційні технології (information and communication technologies), визначають як систему методів, процесів та способів використання обчислювальної техніки і засобів зв'язку для створення, збирання, передавання, пошуку, оброблення та поширення інформації. Їх застосування спрямоване на забезпечення ефективної організації діяльності людей та підвищення результативності управлінських процесів [20].

Нормативно-правові засади публічного управління інформаційно-комунікаційним забезпеченням в Україні формуються на основі комплексної дії законодавства у сфері електронних комунікацій, інформаційних відносин і кібербезпеки, що відображає міждисциплінарний характер цієї сфери та її стратегічне значення для держави і регіонального розвитку. Закон України «Про електронні комунікації» [11] визначає організаційно-економічні та регуляторні засади функціонування електронних комунікаційних мереж і послуг, закріплюючи принципи технологічної нейтральності, конкуренції, доступності та безперервності надання послуг, що зумовлює необхідність активної ролі публічної влади у формуванні та координації інформаційно-комунікаційної інфраструктури. Закон України «Про інформацію» [8] встановлює базові правові засади обігу інформації, визначає принципи відкритості, достовірності, повноти та доступності інформації, а також обов'язки органів публічної влади щодо





формування й оприлюднення інформаційних ресурсів, що трансформує інформаційне забезпечення у ключовий інструмент публічного управління та підзвітності. Закон України «Про доступ до публічної інформації» [6] встановлює правові засади реалізації та гарантування права кожної особи на отримання інформації, що має суспільну значущість. Водночас Закон України «Про основні засади забезпечення кібербезпеки України» [10] інтегрує безпековий вимір у систему інформаційно-комунікаційного забезпечення, покладаючи на органи державної влади відповідальність за захист інформаційних ресурсів, електронних комунікаційних мереж і об'єктів критичної інфраструктури від кіберзагроз.

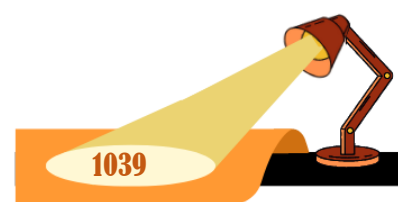
Сучасне публічне управління інформаційним забезпеченням неможливе без інтеграції ефективних механізмів кібербезпеки та захисту інформації, що ґрунтуються на світових стандартах і адаптовані до українського правового та інституційного контексту. У цій системі публічного управління Державна служба спеціального зв'язку та захисту інформації України відіграє ключову роль у впровадженні міжнародних підходів до управління кіберінцидентами інформаційної безпеки відповідно до ДСТУ ISO/IEC 27035-1:2018 [4], який визначає принципи організації та координації реагування на кіберінциденти протягом усього життєвого циклу інформаційних активів.

Нормативне підґрунтя практичної реалізації зазначених підходів формують національні ТЗІ – НД ТЗІ 3.6-006-21 [17] та НД ТЗІ 3.6-007-21 [18].

Системний аналіз нормативно-правових актів дозволяє виокремити особливості публічного управління інформаційно-комунікаційним забезпеченням, які полягають у поєднанні регуляторної, координаційної та безпекової функцій публічної влади та формує специфічну модель публічного управління інформаційно-комунікаційним забезпеченням, у межах якої інформація та електронні комунікації розглядаються не лише як технічний ресурс, а як стратегічний чинник соціально-економічного розвитку, інституційної стійкості та безпеки держави і регіонів.

У 2025 році Україна розпочала впровадження NIST Cybersecurity Framework 2.0 (CSF 2.0) [31] як однієї з провідних міжнародних практик управління кіберризиками, що дає змогу посилити захист державних і регіональних інформаційних систем, зокрема публічних реєстрів та об'єктів критичної інформаційної інфраструктури, шляхом інтеграції стратегічних функцій ідентифікації, захисту, моніторингу, виявлення, реагування, відновлення та постійної адаптації до нових загроз у кіберпросторі.

Це сприяло підвищенню стійкості цифрової державної та місцевої інформаційної інфраструктури, формуванню єдиної системи моніторингу й реагування на кіберзагрози, а також зміцненню довіри суспільства та міжнародних партнерів до державних інституцій, що є критично важливим компонентом інформаційного забезпечення публічного управління.



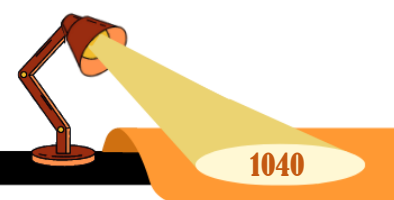


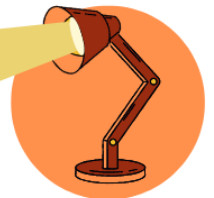
Подальший розвиток теоретичних підходів до осмислення інформаційно-комунікаційного забезпечення публічного управління представлений у працях David C. G. Brown та Sandra Toze, які розглядають інформаційне врядування як інтегрований стратегічний механізм управління життєвим циклом інформації в умовах цифровізації публічного сектору, де інформація виступає ключовим чинником ухвалення управлінських рішень, забезпечення публічної підзвітності та прозорості діяльності органів влади. Автори наголошують на необхідності поєднання управління даними, захисту інформації, забезпечення доступу, архівування, оцінювання ризиків і дотримання нормативно-правових вимог у межах єдиного інституційного підходу, що узгоджується з комплексною природою публічного управління інформаційно-комунікаційним забезпеченням та обґрунтовує доцільність застосування циклічної моделі управління інформаційними ресурсами в публічних адміністраціях [25].

Специфічна модель публічного управління інформаційно-комунікаційним забезпеченням в Україні формується як інтегрована багатовимірна система, що поєднує регуляторні, організаційні, інформаційні та безпекові механізми. Її ключовою ознакою є поєднання публічно-владного регулювання з мережевою взаємодією органів державної влади, місцевого самоврядування, суб'єктів електронних комунікацій, інститутів громадянського суспільства та міжнародних партнерів. Така модель орієнтована не лише на нормотворчу й контрольну діяльність, а й на координацію розвитку інформаційно-комунікаційної інфраструктури, забезпечення відкритості та доступності інформації, впровадження цифрових управлінських інструментів і захист інформаційних ресурсів з урахуванням соціально-економічних особливостей регіонів.

Зазначена модель реалізується як динамічна система взаємопов'язаних управлінських процесів циклічного характеру, що охоплюють формування стратегічних цілей, планування та реалізацію інформаційно-комунікаційних рішень, їх моніторинг і оцінювання з подальшим коригуванням управлінських впливів. Застосування циклічного підходу забезпечує адаптивність і результативність публічного управління, сприяє інтеграції безпекового виміру та формуванню балансу між відкритістю, захистом інформації й соціально-економічними інтересами розвитку регіонів України.

Цикл публічного управління інформаційним забезпеченням формується як багаторівнева, динамічна система, у межах якої взаємодіють державний і регіональний рівні управління, суб'єкти ринку електронних комунікацій та громадянське суспільство з урахуванням впливу зовнішніх факторів, що наочно відображено на поданій схемі циклу публічного управління інформаційним забезпеченням. На державному рівні здійснюється формування політики у сфері інформаційного забезпечення, що включає розроблення та впровадження національних стратегій і програм інформатизації, координацію цифрового





розвитку між органами публічної влади, визначення стандартів, вимог і пріоритетів розвитку інформаційно-комунікаційних систем, а також забезпечення захисту, цілісності та стійкості об'єктів критичної інформаційної інфраструктури.

Сформована політика реалізується на регіональному рівні, де відбувається управління процесами цифрового розвитку, впровадження інформаційних систем і електронних сервісів, розвиток регіональних цифрових платформ, підтримка інноваційних проєктів та забезпечення практичного використання інформаційних ресурсів для вирішення соціально-економічних завдань територій. Важливою складовою циклу є вплив підприємств зв'язку, які забезпечують доступність послуг електронних комунікацій, розвиток і модернізацію ІКТ-інфраструктури, впровадження нових технологій і взаємодію з органами влади в умовах регуляторного середовища.

Паралельно здійснюється залучення громади, що проявляється в підвищенні цифрової грамотності населення, розвитку механізмів електронної участі, використанні електронних сервісів, а також формуванні зворотного зв'язку між громадянами та органами публічної влади. Увесь цикл функціонує з урахуванням зовнішніх факторів, зокрема глобальних цифрових тенденцій, міжнародних рейтингів і стандартів, воєнних і безпекових викликів, економічних і демографічних умов, які безпосередньо впливають на пріоритети та темпи розвитку інформаційного забезпечення.

Оцінювання рівня розвитку інформаційного забезпечення та його впливу на соціально-економічний розвиток регіонів України доцільно здійснювати на основі поєднання міжнародних і національних індексів цифрового розвитку, прозорості та якості електронних сервісів, що дозволяє комплексно охарактеризувати інституційну, технологічну та управлінську спроможність територій. До ключових міжнародних індикаторів, у яких Україна офіційно представлена, належить Індекс розвитку інформаційно-комунікаційних технологій (ICT Development Index) [27], який відображає рівень доступу до ІКТ-інфраструктури, інтенсивність використання цифрових технологій і розвиток цифрових навичок населення. Важливе місце посідають Індекс розвитку електронного урядування (E-Government Development Index) [28] та Індекс електронної участі (E-Participation Index) [29], що формуються Організацією Об'єднаних Націй і характеризують рівень цифровізації публічного управління, доступності публічної інформації та залучення громадян до управлінських процесів.

Безпековий вимір оцінювання забезпечує Глобальний індекс кібербезпеки (Global Cybersecurity Index) [30], який розраховується Міжнародним союзом електрозв'язку та відображає спроможність держави гарантувати захист інформаційних ресурсів і стійкість цифрової інфраструктури. Доповнює комплексну оцінку Індекс мережевої готовності (Network Readiness Index) [32], а також Глобальний індекс інноваційності та Індекс людського розвитку, які дозволяють врахувати інноваційний і соціальний виміри використання інформації та





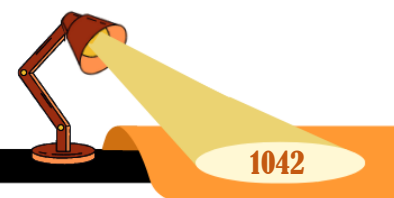
цифрових технологій. Сукупне застосування зазначених індикаторів створює методологічне підґрунтя для багатовимірного аналізу інформаційно-комунікаційного забезпечення та його ролі у формуванні цифрової рівності й соціально-економічної стійкості з метою забезпечення конкурентоспроможності регіонів України.

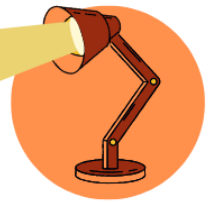
Водночас на регіональному та муніципальному рівнях особливого значення набувають національні індикатори цифрового розвитку, зокрема індекси цифрової трансформації регіонів і територіальних громад, що впроваджуються Міністерством цифрової трансформації України [23], а також індекси прозорості та електронних сервісів міст, розроблені в межах ініціатив, таких як «Transparent Cities» за участі Transparency International Ukraine [5]. Застосування цих інструментів дозволяє виявити не лише формальні показники цифровізації, а й реальний стан інформаційного забезпечення місцевого самоврядування, доступність електронних сервісів і сталість цифрових екосистем громад.

Таким чином, використання міжнародних і національних індексів розвитку інформаційно-комунікаційного забезпечення дозволяє здійснювати порівняльне оцінювання рівня цифровізації, відкритості, безпеки та управлінської спроможності публічної влади на різних рівнях. Водночас індекси фіксують лише результативний зріз стану інформаційного розвитку, не розкриваючи безпосередньо причинно-наслідкових зв'язків і механізмів формування відповідних показників. З цієї точки зору аналітичний потенціал індексного підходу потребує доповнення дослідженням чинників, які зумовлюють досягнення певного рівня інформаційно-комунікаційного забезпечення. Перехід від індексів до аналізу чинників дозволяє виявити інституційні, правові, технологічні, кадрові, економічні та безпекові передумови, що визначають ефективність публічного управління інформаційно-комунікаційною сферою, а також пояснити відмінності у динаміці розвитку між державами, регіонами та територіальними громадами.

Публічне управління інформаційним забезпеченням формується під впливом сукупності взаємопов'язаних чинників, які визначають його зміст, інструменти та ефективність у сучасних умовах цифрової трансформації. Визначальним чинником є нормативно-правове середовище, що задає правила формування, використання, поширення та захисту інформації й електронних комунікацій, а також розмежовує повноваження між суб'єктами публічної влади. Інституційний чинник проявляється у структурі та спроможності органів державної влади та місцевого самоврядування здійснювати координацію інформаційно-комунікаційних процесів на різних рівнях управління.

Вагомий вплив має технологічний чинник, пов'язаний із рівнем розвитку інформаційно-комунікаційної інфраструктури, цифрових платформ, реєстрів, систем електронних послуг і аналітики даних, що безпосередньо визначає можливості реалізації управлінських рішень. Не менш значущим є кадровий і компетентнісний чинник, який охоплює рівень цифрової грамотності, інфор-





маційної культури та управлінських навичок персоналу публічного сектору. Соціальний чинник пов'язаний із запитами суспільства на відкритість, доступність інформації, електронні послуги та участь у прийнятті рішень, тоді як економічний чинник визначається наявністю фінансових ресурсів і інвестиційних можливостей для розвитку інформаційно-комунікаційних систем.

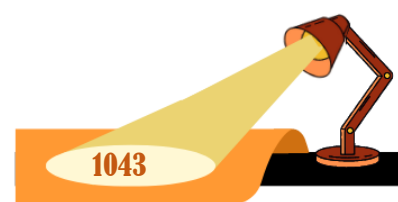
Окреме місце посідає безпековий чинник, що зумовлює інтеграцію вимог кібербезпеки, захисту персональних даних і стійкості критичної інформаційної інфраструктури в управлінські процеси. Сукупна дія зазначених чинників формує складне, динамічне середовище публічного управління інформаційно-комунікаційним забезпеченням, у межах якого ефективність управлінських рішень залежить від здатності публічної влади забезпечувати баланс між технологічним розвитком, правовим регулюванням, безпекою та соціально-економічними потребами суспільства.

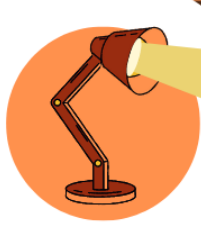
У період воєнних викликів інформаційно-комунікаційні технології відіграють важливу роль у забезпеченні соціально-економічної стійкості регіонів, зокрема через впровадження систем моніторингу та відеоспостереження як складової інформаційного забезпечення публічного управління. Реалізація таких проектів здійснюється на засадах міжсекторальної взаємодії органів державної влади, органів місцевого самоврядування та меценатів і поєднує фінансування з державного бюджету із благодійною підтримкою міжнародних партнерів, зокрема Фонду Говарда Баффетта.

Безпосереднє створення та технічне розгортання єдиної системи відеоспостереження в регіоні з можливими бойовими діями було здійснено Фондом Говарда Баффетта у співпраці з Національною поліцією України, що забезпечило інтеграцію сучасних ІКТ-рішень у діяльність правоохоронних органів [24]. Такий фінансово-організаційний підхід дозволяє забезпечити безперервність розвитку інформаційної інфраструктури навіть в умовах обмежених ресурсів, характерних для воєнного часу.

Впровадження єдиних систем відеоспостереження на базі ситуаційних центрів сприяє централізованому збору, обробці та аналізу інформації, підвищує ефективність координації дій служб реагування та рівень громадської безпеки. З позицій теорії регіонального розвитку наявність таких інформаційних систем зменшує рівень соціально-економічних ризиків, підвищує передбачуваність господарських процесів, сприяє збереженню людського капіталу та формує сприятливіші умови для економічної діяльності. Отже, спільне фінансування та реалізація ІКТ-базованих систем моніторингу за рахунок бюджетних і меценатських ресурсів слід розглядати як важливий елемент інформаційного забезпечення соціально-економічного розвитку регіонів України та їх адаптивності в кризових умовах.

Висновки. Резюмуючи зазначимо, публічне управління інформаційно-комунікаційним забезпеченням в Україні формується як складна, багаторівнева



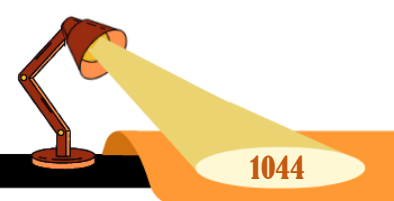


та динамічна система, у межах якої інформація та електронні комунікації виступають стратегічним ресурсом соціально-економічного розвитку регіонів України. Сформована специфічна модель публічного управління в цій сфері поєднує регуляторні, координаційні, управлінські та безпекові функції публічної влади і реалізується через циклічну логіку управлінських процесів, що забезпечує тяглість, адаптивність та зворотний зв'язок.

Аналіз чинників впливу засвідчує, що ефективність інформаційно-комунікаційного забезпечення визначається взаємодією правових, інституційних, технологічних, кадрових, економічних і безпекових передумов, які формують рамки управлінських рішень на державному, регіональному та місцевому рівнях. Оцінювання розвитку цієї сфери за допомогою міжнародних індексів цифровізації, електронного урядування, розвитку інформаційно-комунікаційних технологій і кібербезпеки дозволяє зафіксувати результати управлінських впливів, однак потребує доповнення аналізом причинно-наслідкових механізмів їх формування.

Література:

9. Бабаєв В. М. Управління великим містом: теоретичні і прикладні аспекти: монографія. Харків : ХНАМГ, 2010. 307 с.
10. Бенько М. М. Інформаційні системи і технології в обліку: навч. посіб. Київ: Нац. торг.-екон. ун-т, 2010. 336 с.
11. Білан Н. І. Соціальні комунікації в інформаційному суспільстві: теорія, еволюція, моделі та прикладні аспекти : дис. ... д-р. наук із соц. ком. : 27.00.01 теорія та історія соціальних комунікацій. Київ, 2016. 427 с.
12. Інформаційні технології. Методи захисту. Керування інцидентами інформаційної безпеки. ДСТУ ISO/IEC 27035-1:2018. Київ : ДП «УкрНДНЦ», 2018.
13. Електронні сервіси: як міста проходять «євротест» на прозорість. Transparency International Ukraine. URL:<https://transparentcities.in.ua/articles/elektronni-servisy-yak-mista-prokhodiat-yevrotest-na-prozorist> (дата звернення: 04.01.2026).
14. Про доступ до публічної інформації: Закон України від 13.01.2011 № 2939-VI URL: <https://zakon.rada.gov.ua/laws/show/2939-17#Text> (дата звернення: 12.10.2025).
15. Про захист персональних даних: Закон України від 01.06.2010 № 2297-VI. URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text> (дата звернення: 20.11.2025).
16. Про інформацію: Закон України від 02.10.1992 № 2657-XII. URL: <https://zakon.rada.gov.ua/laws/show/2657-12#Text> (дата звернення: 10.01.2026).
17. Про Національну програму інформатизації: Закон України від 01.12.2022 № 2807-IX. URL: <https://zakon.rada.gov.ua/laws/show/2807-20#Text> (дата звернення: 26.12.2025).
18. 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> (дата звернення: 10.11.2025).
19. Про електронні комунікації : Закон України від 16.12.2020 № 1089-IX. URL: <https://zakon.rada.gov.ua/laws/show/1089-20#n191> (дата звернення: 09.01.2026).
20. Інформаційна безпека: підручник / за ред. В. В. Остроухова. Київ: Ліра-К, 2021. 412 с.
21. Про затвердження Правил надання та отримання електронних комунікаційних послуг: Постанова Кабінету Міністрів України від 25 червня 2025 р. № 761. URL: <https://www.kmu.gov.ua/npas/pro-zatverdzhennia-pravyl-nadannia-ta-otrymannia-elektronnykh-komunikatsiinykh-posluh-761-250625> (дата звернення: 05.01.2026).



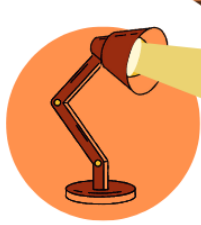


22. Про затвердження Порядку формування та ведення відкритого переліку забороненого до використання програмного забезпечення та комунікаційного (мережевого) обладнання: Постанова Кабінету Міністрів України від 22 жовтня 2025 р. № 1335. URL: <https://www.kmu.gov.ua/npas/pro-zatverdzhennia-poriadku-formuvannia-ta-vedennia-vidkrytoho-pereliku-zaboronenooho-do-vukorystannia-prohramnoho-zabezpechennia-k1335> (дата звернення: 04.01.2026).
23. Куйбіда В. С., Карпенко О. В., Риженко О. В. Інформаційно-комунікативна діяльність органів публічної влади : монографія. Київ: ЦП «Компринт», 2019. 358 с.
24. Макушев П. В. Система інформаційного забезпечення державної виконавчої служби України та персональні дані як їх складові. *Право і суспільство*. 2013. № 4. С. 70–77.
25. Порядок вибору заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем: НД ТЗІ 3.6-006-21. Київ, 2021.
26. Порядок впровадження заходів захисту інформації, вимога щодо захисту якої встановлена законом та не становить державної таємниці, для інформаційних систем: НД ТЗІ 3.6-007-21. Київ, 2021.
27. Олійченко І. М. Розвиток інформаційного забезпечення органів державної влади на регіональному рівні. управління обласною державною адміністрацією : дис. ... д-р. наук з держ. управл.: 25.00.02 механізми державного управління. теорія та історія соціальних комунікацій. Київ, 2010. 452 с.
28. Плєскач В. Л., Затонацька Т. Г. Інформаційні системи і технології на підприємствах: підручник. Київ: Знання, 2011. 718 с.
29. Портал Харків'янина. URL: <https://portal.city.kharkov.ua/> (дата звернення: 05.01.2026).
30. Роз'яснення щодо виконання Національної програми інформатизації URL: <https://pri.gov.ua/ua/newslit> (дата звернення: 04.01.2026).
31. Digital State UA. URL: <https://digitalstate.gov.ua/uk> (дата звернення: 20.11.2025).
32. У Харківській області впроваджуються сучасні цифрові та безпекові рішення. *Харківська обласна військова адміністрація. Офіційний сайт*. URL: <https://kharkivoda.gov.ua/news/129423> (дата звернення: 04.01.2026).
33. Brown D. C. G., Toze S. Information governance in digitized public administration. *Canadian Public Administration*. 2017. Vol. 60. pp. 581–604.
34. E-Government Survey 2024: Accelerating Digital Transformation for Sustainable Development. United Nations. URL: <https://publicadministration.un.org/egovkb/en-us/>.
35. ICT Development Index. URL: <https://www.itu.int/en/ITU-D/Statistics/Pages/IDI/default.aspx>
36. E-Government Development Index (EGDI). United Nations Department of Economic and Social Affairs. URL: <https://publicadministration.un.org/egovkb/en-us/Data-Center>
37. E-Participation Index. United Nations Department of Economic and Social Affairs. URL: <https://publicadministration.un.org/egovkb/en-us/Data-Center>
38. Global Cybersecurity Index (GCI). International Telecommunication Union. URL: <https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx>
39. National Institute of Standards and Technology (NIST). Cybersecurity Framework URL: <https://www.nist.gov/cyberframework>
40. Network Readiness Index. Portulans Institute. URL: <https://networkreadinessindex.org/>

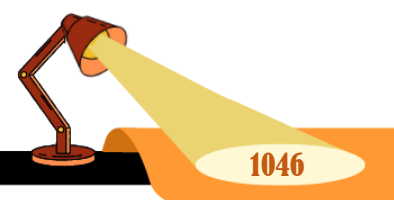
References:

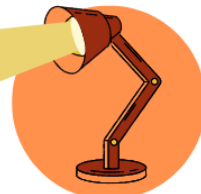
1. Babaiev V.M. (2010) *Upravlinnia velykym mistom: teoretychni i prykladni aspekty* [Management of a Large City: Theoretical and Applied Aspects]. Kharkiv: KhNAMH. 307 p. [in Ukrainian].





2. Benko M.M. (2010) *Informatsiini systemy i tekhnolohii v obliku* [Information Systems and Technologies in Accounting]. Kyiv: National University of Trade and Economics. 336 p. [in Ukrainian].
3. Bilan N.I. (2016) *Sotsialni komunikatsii v informatsiinomu suspilstvi: teoriia, evoliutsiia, modeli ta prykladni aspekty* [Social Communications in the Information Society: Theory, Evolution, Models and Applied Aspects]. Doctoral dissertation. Kyiv. 427 p. [in Ukrainian].
4. DSTU ISO/IEC 27035-1:2018 (2018) *Information Technology. Security Techniques. Information Security Incident Management*. Kyiv: UkrNDNC. [in Ukrainian].
5. Transparency International Ukraine (2026) *Elektronni servisy: yak mista prokhodiat «ievrotest» na prozorist* [Electronic Services: How Cities Pass the “Eurotest” for Transparency]. URL: <https://transparentcities.in.ua/articles/elektronni-servisy-yak-mista-prokhodiat-yevrotest-na-prozorist> (accessed: 04.01.2026) [in Ukrainian].
6. Pro dostup do publichnoi informatsii: *Zakon Ukrainy vid 13 sich. 2011 roku № 2939-VI* [On Access to Public Information: Law of Ukraine of January 13, 2011 No. 2939-VI]. URL: <https://zakon.rada.gov.ua/laws/show/2939-17#Text> [in Ukrainian].
7. Pro zakhyst personalnykh danykh: *Zakon Ukrainy vid 01 cherv. 2010 roku № 2297-VI* [On Personal Data Protection: Law of Ukraine of June 1, 2010 No. 2297-VI]. URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text> [in Ukrainian].
8. Pro informatsiiu: *Zakon Ukrainy vid 02 zhovt. 1992 roku № 2657-XII* [On Information: Law of Ukraine of October 2, 1992 No. 2657-XII]. URL: <https://zakon.rada.gov.ua/laws/show/2657-12#Text> [in Ukrainian].
9. Pro Natsionalnu prohramu informatyzatsii: *Zakon Ukrainy vid 01 hrud. 2022 roku № 2807-IX* [On the National Informatization Program: Law of Ukraine of December 1, 2022 No. 2807-IX]. URL: <https://zakon.rada.gov.ua/laws/show/2807-20#Text> [in Ukrainian].
10. Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy: *Zakon Ukrainy vid 05 zhovt. 2017 roku № 2163-VIII* [On the Basic Principles of Cybersecurity of Ukraine: Law of Ukraine of October 5, 2017 No. 2163-VIII]. URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text> [in Ukrainian].
11. Pro elektronni komunikatsii: *Zakon Ukrainy vid 16 hrud. 2020 roku № 1089-IX* [On Electronic Communications: Law of Ukraine of December 16, 2020 No. 1089-IX]. URL: <https://zakon.rada.gov.ua/laws/show/1089-20#n191> [in Ukrainian].
12. Ostroukhov V.V. (2021) *Informatsiina bezpeka* [Information Security]. Kyiv: Lira-K. 412 p. [in Ukrainian].
13. Pro zatverdzhennia Pravyl nadannia ta otrymannia elektronnykh komunikatsiinykh posluh: *Postanova Kabinetu Ministriv Ukrainy vid 25 cherv. 2025 roku № 761* [On Approval of the Rules for the Provision and Receipt of Electronic Communications Services: Resolution of the Cabinet of Ministers of Ukraine of June 25, 2025 No. 761]. URL: <https://www.kmu.gov.ua/npas/pro-zatverdzhennia-pravyl-nadannia-ta-otrymannia-elektronnykh-komunikatsiinykh-posluh-761-250625> [in Ukrainian].
14. Pro zatverdzhennia Poriadku formuvannia ta vedennia vidkrytoho pereliku zaboroneno do vykorystannia prohramnoho zabezpechennia ta komunikatsiinoho (merezhovoho) obladnannia: *Postanova Kabinetu Ministriv Ukrainy vid 22 zhovt. 2025 roku № 1335* [On Approval of the Procedure for the Formation and Maintenance of an Open List of Software and Communication (Network) Equipment Prohibited for Use: Resolution of the Cabinet of Ministers of Ukraine of October 22, 2025 No. 1335]. URL: <https://www.kmu.gov.ua/npas/pro-zatverdzhennia-poriadku-formuvannia-ta-vedennia-vidkrytoho-pereliku-zaboroneno-do-vykorystannia-prohramnoho-zabezpechennia-k1335> [in Ukrainian].
15. Kuibida V.S., Karpenko O.V., Ryzhenko O.V. (2019) *Informatsiino-komunikatyvna diialnist orhaniv publichnoi vlady* [Information and Communication Activity of Public Authorities]. Kyiv: Komprint. 358 p. [in Ukrainian].





16. Makushev P.V. (2013) Systema informatsiinoho zabezpechennia derzhavnoi vykonavchoi sluzhby Ukrainy ta personalni dani yak yii skladovi. *Pravo i suspilstvo* [Law and Society]. 4. pp. 70–77 [in Ukrainian].
17. ND TZI 3.6-006-21 (2021) *Procedure for Selecting Information Security Measures for Information Systems*. Kyiv. [in Ukrainian].
18. ND TZI 3.6-007-21 (2021) *Procedure for Implementing Information Security Measures for Information Systems*. Kyiv. [in Ukrainian].
19. Oliichenko I.M. (2010) *Rozvytok informatsiinoho zabezpechennia orhaniv derzhavnoi vlady na rehionalnomu rivni* [Development of Information Support of Public Authorities at the Regional Level]. Doctoral dissertation. Kyiv. 452 p. [in Ukrainian].
20. Pleskach V.L., Zatonatska T.H. (2011) *Informatsiini systemy i tekhnolohii na pidpriemstvakh* [Information Systems and Technologies at Enterprises]. Kyiv: Znannia. 718 p. [in Ukrainian].
21. Portal Kharkivianyna (2026) Official website. URL: <https://portal.city.kharkov.ua/> (accessed: 05.01.2026) [in Ukrainian].
22. National Informatization Program (2026) Clarifications on implementation. URL: <https://npi.gov.ua/ua/newslst> (accessed: 04.01.2026) [in Ukrainian].
23. Digital State UA (2025) Official website. URL: <https://digitalstate.gov.ua/uk> (accessed: 20.11.2025) [in Ukrainian].
24. Kharkiv Regional Military Administration (2026) Implementation of modern digital and security solutions in Kharkiv region. Official website. URL: <https://kharkivoda.gov.ua/news/129423> (accessed: 04.01.2026) [in Ukrainian].
25. Brown D.C.G., Toze S. (2017) Information governance in digitized public administration. *Canadian Public Administration*. Vol. 60. pp. 581–604 [in English].
26. United Nations (2024) *E-Government Survey 2024: Accelerating Digital Transformation for Sustainable Development*. URL: <https://publicadministration.un.org/egovkb/en-us/> [in English].
27. International Telecommunication Union ICT Development Index. URL: <https://www.itu.int/en/ITU-D/Statistics/Pages/IDI/default.aspx> [in English].
28. United Nations DESA E-Government Development Index (EGDI). URL: <https://publicadministration.un.org/egovkb/en-us/Data-Center> [in English].
29. United Nations DESA E-Participation Index. URL: <https://publicadministration.un.org/egovkb/en-us/Data-Center> [in English].
30. International Telecommunication Union Global Cybersecurity Index (GCI). URL: <https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx> [in English].
31. National Institute of Standards and Technology (NIST) Cybersecurity Framework. URL: <https://www.nist.gov/cyberframework> [in English].
32. Portulans Institute Network Readiness Index. URL: <https://networkreadinessindex.org/> [in English].

