

Цифровізація системи публічно-правового контролю як інструмент забезпечення національної безпеки України

Digitalization of the Public Law Control System as an Instrument for Ensuring Ukraine's National Security

Наталя Атаманова

кандидат юридичних наук, доцент кафедри державно-правових дисциплін, e-mail: 2025_2026@ukr.net, ORCID ID: <https://orcid.org/0000-0003-4940-5810>

Natalya Atamanova

PhD in Law, Associate Professor of the Department of Public Law Disciplines, e-mail: 2025_2026@ukr.net, ORCID ID: <https://orcid.org/0000-0003-4940-5810>

НВНЗ Міжнародний університет, м. Одеса, Україна

Private Higher Educational Institution "International Humanitarian University", Odesa, Ukraine

Received: June 1, 2026 | Revised: June 23, 2026 | Accepted: June 30, 2026

УДК 351.86:004

DOI: <https://doi.org/10.33445/sds.2026.16.3.3>

Мета роботи. Наукове обґрунтування цифровізації системи публічно-правового контролю як інструменту забезпечення національної безпеки України, визначення її правової природи, основних напрямів впливу на контрольну функцію держави та меж допустимого використання цифрових інструментів у сфері публічно-владного контролю.

Метод дослідження. У дослідженні використано діалектичний, системно-структурний, формально-юридичний, порівняльно-правовий та герменевтичний методи, а також методи правового моделювання й наукового узагальнення. Методологічний підхід дозволив комплексно проаналізувати нормативно-правові засади цифровізації публічно-правового контролю, європейські стандарти електронної ідентифікації та захисту даних, а також визначити місце цифрових технологій у системі забезпечення національної безпеки.

Результати дослідження. Встановлено, що цифровізація публічно-правового контролю виходить за межі технічної модернізації адміністративних процедур і трансформує зміст контрольної діяльності держави. Обґрунтовано багаторівневу структуру цифровізованого контролю, що охоплює нормативно-безпековий, адміністративно-організаційний, інформаційно-технологічний та правозахисний компоненти. Визначено роль електронної ідентифікації, цифрових реєстрів, інформаційно-аналітичних платформ і механізмів кіберзахисту у підвищенні ефективності контрольних процедур.

Теоретична цінність дослідження. Розвинено наукові підходи до розуміння цифровізованого публічно-правового контролю як самостійного правового феномену, що поєднує елементи публічного управління, інформаційного права, кібербезпеки та права національної безпеки.

Практична цінність дослідження. Сформульовано рекомендації щодо вдосконалення правового регулювання цифрового публічно-правового контролю, зокрема у частині міжвідомчого обміну даними, захисту персональних даних, забезпечення кіберстійкості державних інформаційних систем, регулювання автоматизованого моніторингу та процедур оскарження цифрових рішень.

Тип статті. Науково-дослідна стаття.

Purpose. The purpose of the study is to provide a scientific substantiation of the digitalization of the public-law control system as an instrument for ensuring Ukraine's national security, to determine its legal nature, the main directions of its influence on the state's control function, and the limits of the permissible use of digital tools in the sphere of public authority oversight.

Method. The study employs dialectical, systemic-structural, formal-legal, comparative-legal, and hermeneutic methods, as well as methods of legal modelling and scientific generalization. This methodological framework enabled a comprehensive analysis of the legal foundations of public-law control digitalization, European standards of electronic identification and data protection, and the role of digital technologies within the national security system.

Findings. The findings demonstrate that the digitalization of public-law control extends beyond the technical modernization of administrative procedures and fundamentally transforms the nature of state control activities. A multi-level structure of digitalized control is substantiated, encompassing normative-security, administrative-organizational, information-technological, and human-rights dimensions. The study identifies the role of electronic identification, digital registries, information-analytical platforms, and cybersecurity mechanisms in enhancing the effectiveness of control procedures.

Theoretical Implications. The research advances scientific approaches to understanding digitalized public-law control as an independent legal phenomenon that integrates elements of public administration, information law, cybersecurity, and national security law.

Practical Implications. The study formulates recommendations for improving the legal regulation of digital public-law control, particularly in the areas of interagency data exchange, personal data protection, cybersecurity resilience of state information systems, regulation of automated monitoring, and procedures for appealing digital decisions.

Paper Type. Research article.

Ключові слова: цифровізація; публічно-правовий контроль; національна безпека; публічне управління; кібербезпека; персональні дані; цифрове середовище

Key words: Digitalization; Public-Law Control; National Security; Public Administration; Cybersecurity; Personal Data; Digital Environment.

Вступ

Цифровізація системи публічно-правового контролю в умовах сучасних викликів безпеки потребує ґрунтовного науково-правового осмислення, зумовленого складністю, багатовимірністю та динамічністю трансформацій, що відбуваються у сфері публічного управління, національної безпеки та інформаційно-комунікаційної взаємодії. Так, розвиток цифрових технологій істотно змінює не лише форми адміністративної діяльності, але й саму логіку реалізації контрольної функції держави, яка дедалі більше пов'язується із використанням електронних реєстрів, автоматизованих інформаційних систем, цифрової ідентифікації, міжвідомчого обміну даними, аналітичного моніторингу та кіберзахисту. У цьому контексті публічно-правовий контроль постає як особливий різновид владно-організаційної діяльності, що має забезпечувати не тільки дотримання законності у сфері публічного управління, а й своєчасне виявлення загроз, захист критичної інфраструктури, стабільність цифрових державних сервісів і належний баланс між безпековими інтересами держави та правами людини.

Особливого значення досліджувана проблематика набуває в умовах воєнного стану, гібридних загроз, інформаційних впливів і кібератак, оскільки цифрова трансформація публічного сектору безпосередньо пов'язана з підвищенням стійкості державних інституцій. Закон України “Про національну безпеку України” від 21 червня 2018 року № 2469-VIII визначає національну безпеку через захищеність державного суверенітету, територіальної цілісності, демократичного конституційного ладу та інших національних інтересів від реальних і потенційних загроз. Водночас Закон України “Про основні засади забезпечення кібербезпеки України” від 5 жовтня 2017 року № 2163-VIII формує правову основу захисту кіберпростору, без якого цифровізований публічно-правовий контроль не може бути ефективним. Не менш важливим є Закон України “Про захист персональних даних” від 1 червня 2010 року № 2297-VI, оскільки цифровий контроль передбачає обробку значних масивів інформації, що потребує належних правових гарантій приватності, безпеки та пропорційності державного втручання (Verkhovna Rada Ukrainy, 2010; Verkhovna Rada Ukrainy, 2017; Verkhovna Rada Ukrainy, 2018).

З огляду на це, метою статті є наукове обґрунтування цифровізації системи публічно-правового контролю як інструменту забезпечення національної безпеки України, а також визначення її правової природи, основних напрямів впливу на контрольну функцію держави та меж допустимого використання цифрових інструментів у сфері публічно-владного контролю.

Для досягнення поставленої мети поставлено такі завдання:

розкрити сучасний стан наукового осмислення цифровізації публічного управління, публічно-правового контролю та національної безпеки;

визначити нормативно-правові засади цифровізації контрольної функції держави у сфері національної безпеки;

охарактеризувати цифровізований публічно-правовий контроль як багаторівневе правове явище;

проаналізувати співвідношення цифрового контролю, кібербезпеки, захисту персональних даних і прав людини;

з'ясувати значення електронної ідентифікації, довірчих послуг, автоматизованої обробки даних та інформаційно-аналітичних систем для публічно-правового контролю;

обґрунтувати напрями вдосконалення правового регулювання цифрового публічно-правового контролю з урахуванням потреб національної безпеки України.

Наукова новизна дослідження полягає в обґрунтуванні цифровізації публічно-правового контролю як особливого правового феномену, який виходить за межі електронного урядування та безпосередньо впливає на організацію контрольної діяльності держави у сфері забезпечення національної безпеки. У статті обґрунтовується підхід, за яким цифровізований публічно-правовий

контроль має розглядатися як багаторівневе явище, що поєднує нормативно-безпековий, адміністративно-організаційний, інформаційно-технологічний і правозахисний компоненти. Такий підхід дозволяє поглибити розуміння ролі цифрових технологій у забезпеченні національної безпеки, не відриваючи їх від принципів законності, пропорційності, правової визначеності, захисту персональних даних і підзвітності публічної влади.

Таким чином, дослідження спрямоване на формування цілісного уявлення про цифровізацію системи публічно-правового контролю як про складний правовий феномен, що водночас відображає модернізацію публічного управління, розвиток цифрового середовища, посилення безпекової функції держави та необхідність збереження фундаментальних гарантій прав людини. Саме поєднання технологічної спроможності держави з належною юридичною визначеністю дозволяє розглядати цифровізацію публічно-правового контролю як один із перспективних інструментів забезпечення національної безпеки України.

Огляд літератури

Сучасний стан наукової розробленості проблеми свідчить про активне формування міждисциплінарного підходу до цифровізації правової та управлінської сфер. У працях, присвячених цифровій трансформації права, обґрунтовується необхідність переосмислення традиційних правових категорій з урахуванням цифрового середовища, нових форм правореалізації та технологічного опосередкування юридично значущих дій (Anatiichuk, 2024; Bezklubyi, 2024; Tsvietkova, 2026). Зокрема, цифрове середовище дедалі частіше розглядається не як допоміжний простір комунікації, а як самостійна сфера правового впливу, у якій виникають нові об'єкти, суб'єкти, способи взаємодії та ризики порушення прав. Це має безпосереднє значення для дослідження публічно-правового контролю, оскільки контрольна діяльність у цифровій державі здійснюється не лише через рішення посадових осіб, а й через функціонування інформаційних систем, алгоритмів, реєстрів і цифрових платформ.

Окремий напрям сучасних досліджень стосується модернізації публічного управління та адміністративного моніторингу. Науковці обґрунтовують, що ефективність державних інституцій у сучасних умовах залежить від здатності органів публічної влади використовувати цифрові інструменти для аналізу інформації, координації управлінських рішень і підвищення результативності адміністративних процедур (Grytsyshen et al., 2025; Shkilniak et al., 2026). Водночас у зазначених підходах цифровізація здебільшого розглядається як засіб оптимізації публічного управління, тоді як її значення саме для системи публічно-правового контролю у сфері національної безпеки потребує подальшого поглиблення. Вбачається, що контрольна функція держави в цифровому середовищі має не тільки організаційно-управлінський, але й безпековий, правозахисний і доктринально-правовий вимір.

Важливе значення для обраної проблематики мають дослідження, присвячені інформаційній безпеці, кібербезпеці та захисту критичної інфраструктури. Інформаційні війни, кібератаки та вразливість інформаційних мереж критичної інфраструктури розглядаються як чинники, що безпосередньо впливають на стабільність держави, суспільну безпеку та спроможність органів влади виконувати свої функції (Sopilko et al., 2022; Holovko et al., 2025). З огляду на це, цифровізація публічно-правового контролю має розглядатися не лише як інструмент спрощення адміністративних процедур, але й як засіб підвищення стійкості держави до сучасних загроз. Водночас розширення цифрових контрольних можливостей держави актуалізує питання правових меж такого контролю, запобігання надмірному втручанню у приватну сферу, прозорості цифрових рішень та ефективності механізмів оскарження.

Особливого значення у цьому контексті набуває проблема захисту прав людини у цифрову епоху. Сучасні дослідження засвідчують, що цифровізація публічного управління не повинна послаблювати гарантії приватності, захисту персональних даних, рівності доступу до правових процедур і можливості особи впливати на виправлення помилкових або

неправомірно використаних даних (Kluban, 2026; Mykolalets et al., 2025). Регламент Європейського Парламенту і Ради Європейського Союзу 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з обробкою персональних даних і про вільний рух таких даних та скасування Директиви 95/46/ЄС закріплює принципи законності, прозорості, мінімізації даних, цільового обмеження та відповідальності суб'єктів обробки. Зазначені положення мають важливе методологічне значення для України, оскільки цифровізований публічно-правовий контроль у сфері національної безпеки неминуче пов'язаний із використанням великих масивів інформації, у тому числі критичної або службово значущої (European Parliament and Council of the European Union, 2016).

Водночас цифровізація публічно-правового контролю не може бути достатньо обґрунтована без звернення до європейських стандартів електронної ідентифікації та довірчих послуг. Регламент Європейського Парламенту і Ради Європейського Союзу № 910/2014 від 23 липня 2014 року про електронну ідентифікацію та довірчі послуги для електронних транзакцій на внутрішньому ринку та скасування Директиви 1999/93/ЄС створює правову норму, у межах якої електронна ідентифікація, електронні підписи, електронні печатки та інші довірчі послуги забезпечують юридичну визначеність цифрової взаємодії. Для сфери публічно-правового контролю це має принципове значення, оскільки легітимність цифрових контрольних процедур залежить від достовірності суб'єктів цифрової взаємодії, цілісності електронних документів, захищеності даних і довіри до електронних управлінських дій (European Parliament and Council of the European Union, 2014).

Попри наявність значної кількості сучасних досліджень, присвячених цифровізації права, публічного управління, кібербезпеки та прав людини, проблема цифровізації саме системи публічно-правового контролю як інструменту забезпечення національної безпеки України залишається недостатньо цілісно розкритою. У науковому дискурсі переважають підходи, в яких цифровізація аналізується або як засіб електронного урядування, або як напрям модернізації адміністративних процедур, або як чинник розвитку цифрового середовища. Водночас потребує додаткового обґрунтування питання про те, яким чином цифрові інструменти змінюють природу контрольної діяльності держави, які правові межі має мати автоматизований моніторинг, як забезпечити співвідношення безпекового інтересу та приватності, а також якою має бути відповідальність суб'єктів, залучених до функціонування цифрової контрольної інфраструктури.

Методологія дослідження

Дослідження цифровізації системи публічно-правового контролю як інструменту забезпечення національної безпеки України ґрунтувалося на комплексному науково-юридичному підході, зумовленому багаторівневим характером відповідного правового явища. Матеріальну основу дослідження становили нормативно-правові акти України та Європейського Союзу, а також сучасні наукові праці, присвячені цифровізації права, публічного управління, інформаційній безпеці, кібербезпеці, захисту персональних даних і трансформації механізмів правореалізації. Нормативну базу сформували Закон України "Про національну безпеку України" від 21 червня 2018 року № 2469-VIII (Verkhovna Rada Ukrainy, 2018), Закон України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року № 2163-VIII (Verkhovna Rada Ukrainy, 2017), Закон України "Про захист персональних даних" від 1 червня 2010 року № 2297-VI (Verkhovna Rada Ukrainy, 2010), розпорядження Кабінету Міністрів України "Про схвалення Концепції розвитку електронного урядування в Україні" від 20 вересня 2017 року № 649-р (Kabinet Ministriv Ukrainy, 2017) та розпорядження Кабінету Міністрів України "Про схвалення Концепції розвитку цифрових компетентностей" від 3 березня 2021 року № 167-р (Kabinet Ministriv Ukrainy, 2021). Для порівняльно-правового аналізу використано Регламент Європейського Парламенту і Ради Європейського Союзу №

910/2014 від 23 липня 2014 року про електронну ідентифікацію та довірчі послуги для електронних транзакцій на внутрішньому ринку та скасування Директиви 1999/93/ЄС (European Parliament and Council of the European Union, 2014), Регламент Європейського Парламенту і Ради Європейського Союзу 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з обробкою персональних даних і про вільний рух таких даних та скасування Директиви 95/46/ЄС (European Parliament and Council of the European Union, 2016), а також Директиву Європейського Парламенту і Ради Європейського Союзу 2019/770 від 20 травня 2019 року про деякі аспекти договорів постачання цифрового контенту та цифрових послуг (European Parliament and Council of the European Union, 2019).

Дослідження здійснювалося у кілька послідовних етапів, що дозволило забезпечити логічну цілісність аналізу та відтворюваність отриманих результатів. На першому етапі було визначено понятійно-категоріальну основу дослідження, зокрема зміст понять “цифровізація”, “публічно-правовий контроль”, “цифрове середовище”, “національна безпека”, “кібербезпека”, “електронне урядування”, “персональні дані” та “цифрові контрольні механізми”. На другому етапі проаналізовано нормативно-правову базу України та Європейського Союзу, що дозволило виявити правові передумови цифровізації контрольної діяльності, її безпекове значення та межі допустимого втручання держави у сферу приватності. На третьому етапі систематизовано сучасні наукові підходи до цифровізації правового середовища, публічного управління, адміністративного моніторингу, інформаційної безпеки та захисту прав людини. Зокрема, враховано положення про правову природу цифрового середовища, трансформацію правореалізації в умовах цифрової держави, використання штучного інтелекту публічними адміністраціями та модернізацію системи публічного управління (Anatiichuk, 2024; Bezklubiy, 2024; Tsvietkova, 2026). На завершальному етапі сформульовано узагальнення щодо правової природи цифровізованого публічно-правового контролю та визначено напрями його вдосконалення у контексті забезпечення національної безпеки України.

Методологічну основу дослідження становили діалектичний, системно-структурний, формально-юридичний, порівняльно-правовий, герменевтичний методи, а також метод правового моделювання та наукового узагальнення. Діалектичний метод дав змогу розглянути цифровізацію публічно-правового контролю як процес, що розвивається під впливом технологічних, правових, організаційних і безпекових чинників. Системно-структурний метод застосовувався для виокремлення нормативно-безпекового, адміністративно-організаційного, інформаційно-технологічного та правозахисного рівнів цифрового контролю. Формально-юридичний метод забезпечив аналіз змісту нормативно-правових актів, що регламентують національну безпеку, кібербезпеку, захист персональних даних, електронне урядування та цифрові компетентності. Порівняльно-правовий метод дозволив співвіднести українське правове регулювання з європейськими стандартами електронної ідентифікації, довірчих послуг, захисту персональних даних і цифрових сервісів. Герменевтичний метод використовувався для тлумачення правових категорій, які набувають нового змісту в умовах цифрового середовища, а метод правового моделювання – для обґрунтування цифровізованого публічно-правового контролю як системи взаємодії органів публічної влади, електронних реєстрів, інформаційно-аналітичних платформ, алгоритмічних інструментів, суб'єктів кіберзахисту та осіб, щодо яких здійснюється контрольна діяльність.

Результати дослідження

Дослідження цифровізації системи публічно-правового контролю як інструменту забезпечення національної безпеки України потребує застосування цілісного науково-юридичного підходу, зумовленого складністю, багатовимірністю та динамічністю сучасних безпекових процесів. Йдеться не лише про впровадження електронних сервісів,

автоматизованих реєстрів чи інформаційно-аналітичних платформ у діяльність органів публічної влади, а про глибшу трансформацію самої природи контрольної функції держави. У цьому контексті публічно-правовий контроль поступово постає як особливий різновид владно-організаційної діяльності, що функціонує на перетині адміністративного права, інформаційного права, права національної безпеки, кібербезпеки та прав людини.

У цьому контексті цифровізація публічно-правового контролю характеризує не лише зміну форми контрольних процедур, а й переорієнтацію логіки державного контролю, коли ключового значення набувають інтегровані цифрові системи, своєчасне виявлення ризиків, захищений обмін інформацією та належне адміністративне реагування. Такий підхід набуває особливої значущості в умовах воєнного стану, гібридних загроз, інформаційних впливів, кібератак і підвищеної вразливості критичної інфраструктури. Саме тому цифровізація у сфері публічно-правового контролю не може оцінюватися виключно як технічне оновлення управлінських процедур, оскільки вона безпосередньо впливає на спроможність держави забезпечувати національну безпеку, підтримувати стійкість публічного управління та гарантувати належний рівень правового захисту особи (Verkhovna Rada Ukrainy, 2018; Sopilko et al., 2022; Zakharchenko et al., 2026).

Нормативною основою такого розуміння є Закон України “Про національну безпеку України” від 21 червня 2018 року № 2469-VIII, у межах якого національна безпека пов’язується із захищеністю державного суверенітету, територіальної цілісності, демократичного конституційного ладу та інших національних інтересів від реальних і потенційних загроз. Водночас Закон України “Про основні засади забезпечення кібербезпеки України” від 5 жовтня 2017 року № 2163-VIII формує спеціальну правову основу для захисту кіберпростору, що є необхідною умовою функціонування цифрових контрольних механізмів. Не менш важливе значення має Закон України “Про захист персональних даних” від 1 червня 2010 року № 2297-VI, оскільки цифровізований контроль неминує передбачає збирання, накопичення, обробку, передачу та використання значних масивів інформації, частина якої безпосередньо стосується приватної сфери особи (Verkhovna Rada Ukrainy, 2010; Verkhovna Rada Ukrainy, 2017; Verkhovna Rada Ukrainy, 2018).

У цьому аспекті слід зазначити, що цифровізація системи публічно-правового контролю виявляє подвійний правовий зміст. З одного боку, вона забезпечує підвищення оперативності, точності та доказовості контрольної діяльності, сприяє зменшенню дублювання адміністративних процедур, посиленню міжвідомчої координації та швидшому виявленню ризиків. З іншого боку, цифровізація створює нові загрози, пов’язані з непрозорістю алгоритмічної обробки даних, можливістю надмірного адміністративного спостереження, помилками в інформаційних системах, несанкціонованим доступом до реєстрів, порушенням приватності та виникненням цифрової нерівності. Відтак правова оцінка цифрового контролю має спиратися не лише на критерій ефективності, але й на критерії законності, пропорційності, підзвітності, правової визначеності, кіберстійкості та захисту прав людини.

Результати аналізу дозволяють стверджувати, що цифровізований публічно-правовий контроль формується як багаторівневе правове явище. Його нормативно-безпековий рівень пов’язаний із визначенням меж державного втручання, правових підстав моніторингу, обробки даних і реагування на загрози. Адміністративно-організаційний рівень охоплює діяльність органів публічної адміністрації, суб’єктів сектору безпеки і оборони, органів місцевого самоврядування, адміністраторів державних реєстрів та інших суб’єктів, залучених до цифрової контрольної інфраструктури. Інформаційно-технологічний рівень характеризується використанням електронних реєстрів, цифрових платформ, інформаційно-аналітичних систем, засобів електронної ідентифікації та автоматизованої обробки даних. Правозахисний рівень визначає межі допустимого впливу держави на особу, гарантії приватності, захист персональних даних, доступ до правового захисту та можливість

оскарження цифрових або автоматизовано підготовлених рішень (Havrylenko, 2023; Kluban, 2026; Mykolaiets et al., 2025).

Важливою характеристикою цифровізації публічно-правового контролю є зміна його функціонального призначення. Традиційна модель контролю значною мірою орієнтована на встановлення факту порушення та застосування відповідних заходів реагування. Натомість цифрова модель орієнтується на завчасне виявлення ризиків, прогнозування можливих загроз і узгодження дій суб'єктів публічної влади. Це означає, що контрольна діяльність може бути спрямована не лише на фіксацію вже вчиненого правопорушення, а й на виявлення ризикових відхилень, прогнозування потенційних загроз, автоматизоване інформування компетентних органів і створення підстав для своєчасного управлінського рішення. Така трансформація є особливо важливою для сфери національної безпеки, де несвоєчасність реагування може призводити до істотних втрат, а загрози часто мають прихований, мережевий або міжсекторальний характер (Grytsyshen et al., 2025; Shkilniak et al., 2026).

Разом із тим превентивний потенціал цифрового контролю не повинен ототожнюватися з необмеженим розширенням контрольних можливостей держави. Цілком слушною вбачається позиція, відповідно до якої цифрові інструменти мають підпорядковуватися правовій логіці, а не замінювати її. Так, автоматизований моніторинг, алгоритмічна обробка інформації та використання штучного інтелекту в публічному адмініструванні можуть бути виправданими лише за наявності законної мети, визначених процедур, можливості людського контролю, можливості перевірки результатів і відповідальності за помилки цифрової системи. У протилежному випадку цифровізація здатна трансформувати публічно-правовий контроль із механізму забезпечення законності на інструмент непрозорого адміністративного впливу (Chiti, Marchetti, & Rangone, 2022; Tsvietkova, 2026).

Особливого значення набуває питання цифрового середовища як простору реалізації публічно-владних повноважень. У сучасній правовій науці цифрове середовище розглядається не лише як технічна інфраструктура, а як особлива сфера суспільних відносин, у якій виникають нові форми комунікації, об'єкти прав, способи ідентифікації, моделі поведінки та юридично значущі наслідки (Bezklubyi, 2024). Для системи публічно-правового контролю це означає, що об'єктом правового регулювання є не тільки діяльність підконтрольних суб'єктів, але й саме цифрове середовище, у якому така діяльність фіксується, аналізується, зіставляється з іншими даними та використовується для прийняття владних рішень. Відповідно, правовий режим цифрового контролю має охоплювати не лише питання повноважень органів влади, але й питання достовірності даних, цілісності реєстрів, доступу до інформації, захисту каналів комунікації та юридичної сили електронних дій.

У цьому контексті важливим є також значення електронної ідентифікації та довірчих послуг. Регламент Європейського Парламенту і Ради Європейського Союзу № 910/2014 від 23 липня 2014 року про електронну ідентифікацію та довірчі послуги для електронних транзакцій на внутрішньому ринку та скасування Директиви 1999/93/ЄС сформував правову норму, у межах якої електронна ідентифікація, електронні підписи, електронні печатки та інші довірчі послуги набувають значення інструментів забезпечення юридичної визначеності в цифровому середовищі (European Parliament and Council of the European Union, 2014). Для публічно-правового контролю це має принципове значення, оскільки без належної ідентифікації суб'єктів, автентичності електронних документів і цілісності інформації неможливо забезпечити легітимність цифрових контрольних процедур.

Наряду із цим Регламент Європейського Парламенту і Ради Європейського Союзу 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з обробкою персональних даних і про вільний рух таких даних та скасування Директиви 95/46/ЄС закріплює принципи законності, прозорості, цільового обмеження, мінімізації даних і відповідальності суб'єктів

обробки. Зазначені принципи є важливими не лише для приватного сектору, але й для цифрового публічно-правового контролю, оскільки діяльність держави у сфері безпеки часто пов'язана з обробкою великих обсягів інформації про фізичних осіб. Відтак, навіть за умов підвищеної безпекової необхідності держава не звільняється від обов'язку забезпечувати правомірність, пропорційність і контрольованість обробки персональних даних (European Parliament and Council of the European Union, 2016; Kluban, 2026).

Значення має і Директива Європейського Парламенту і Ради Європейського Союзу 2019/770 від 20 травня 2019 року про деякі аспекти договорів постачання цифрового контенту та цифрових послуг. Попри те, що вона безпосередньо спрямована на регулювання відносин щодо цифрового контенту та цифрових послуг, її положення дозволяють глибше осмислити якість цифрових сервісів як юридично значущу характеристику (European Parliament and Council of the European Union, 2019). У свою чергу, для публічно-правової сфери це означає, що цифровий сервіс держави не може сприйматися лише як технічний канал комунікації. Він стає елементом адміністративної процедури, від якого залежить можливість особи реалізувати право, виконати обов'язок, отримати інформацію або оскаржити владне рішення.

Зазначене підкреслює, що цифровізація публічно-правового контролю потребує не тільки розвитку технологічної інфраструктури, але й формування належної системи цифрових компетентностей. Розпорядження Кабінету Міністрів України "Про схвалення Концепції розвитку цифрових компетентностей" від 3 березня 2021 року № 167-р засвідчує, що цифрова трансформація публічного сектору неможлива без відповідного рівня цифрової грамотності посадових осіб, адміністраторів інформаційних систем і користувачів електронних сервісів (Kabinet Ministriv Ukrainy, 2021). У сфері публічно-правового контролю недостатній рівень таких компетентностей може призводити до помилкового внесення даних, некоректної інтерпретації результатів автоматизованого аналізу, порушення процедур доступу до інформації та зниження довіри до цифрової держави.

Погоджуючись із підходом, за яким цифровізація змінює механізми реалізації права, слід зазначити, що у сфері публічно-правового контролю ця зміна має особливо виразний характер. У цифровій державі, юридично значущий результат дедалі частіше формується не лише через безпосередню дію посадової особи, а й через взаємодію правової норми, електронної платформи, алгоритму, бази даних і технологічного посередника. Саме тому виникає потреба у переосмисленні класичних категорій контрольної діяльності, зокрема адміністративного рішення, контрольної процедури, доказовості, підконтрольності та відповідальності. У цьому аспекті цифровізація не заперечує традиційні форми правореалізації, але доповнює їх новими способами техніко-юридичного опосередкування (Tsvietkova, 2026; Yevdokimenko et al., 2024).

Окремо слід звернути увагу на проблему юридичної відповідальності в умовах цифровізованого контролю. У традиційній моделі публічно-правового контролю відповідальність здебільшого пов'язується з посадовою особою, органом влади або підконтрольним суб'єктом. У цифровому середовищі ця конструкція ускладнюється, оскільки фактичне функціонування контрольної системи залежить від адміністраторів реєстрів, операторів інформаційних систем, розробників програмного забезпечення, надавачів електронних довірчих послуг, фахівців із кіберзахисту та інших технологічних посередників. Відтак, доцільним є нормативне розмежування їхніх обов'язків, меж доступу до даних, відповідальності за технічні збої, порушення кібербезпеки, неправомірну обробку інформації та недотримання вимог до якості цифрових контрольних процедур (Kaganovska et al., 2025).

З огляду на це, практична цінність отриманих результатів полягає у визначенні правових орієнтирів удосконалення цифрового публічно-правового контролю у сфері національної безпеки. До таких орієнтирів слід віднести:

нормативне закріплення прозорих правил міжвідомчого обміну даними у сфері безпеки; визначення допустимих меж автоматизованого моніторингу; посилення гарантій захисту персональних даних; запровадження стандартів кіберстійкості державних інформаційних систем; створення процедур оскарження цифрових або автоматизовано підготовлених контрольних рішень; уточнення правового статусу технологічних посередників; узгодження національного регулювання з європейськими стандартами електронної ідентифікації, довірчих послуг, цифрових сервісів і захисту даних.

Обговорення

Результати проведеного аналізу доцільно розглядати у співвідношенні з сучасними науковими підходами до цифровізації публічного управління, адміністративного моніторингу, правореалізації та забезпечення національної безпеки. У сучасних наукових розвідках, присвячених модернізації публічного управління, цифровізація здебільшого подається як засіб підвищення ефективності державних інституцій, оптимізації адміністративних процедур, підвищення прозорості та результативності управлінських рішень (Grytsyshen et al., 2025; Shkilniak et al., 2026). Така позиція є обґрунтованою, однак у межах дослідження публічно-правового контролю вона потребує подальшого поглиблення. Ефективність цифрового контролю у сфері національної безпеки не може визначатися лише швидкістю обробки інформації або кількістю електронних сервісів. Вона повинна оцінюватися також через здатність контрольних процедур залишатися законними, перевірюваними, пропорційними, підзвітними та стійкими до зовнішнього впливу.

Порівняння отриманих результатів із дослідженнями інформаційної безпеки дозволяє зробити висновок, що цифровізація публічно-правового контролю перебуває у прямому зв'язку з проблемою інформаційних війн, гібридних загроз і захисту критичної інфраструктури. У науковій літературі інформаційні війни справедливо розглядаються як чинник, що впливає на стабільність суспільства, державну політику та безпекове середовище України (Sorilko et al., 2022). Водночас захист інформаційних мереж критичної інфраструктури потребує не лише технічних, але й правових механізмів, здатних забезпечити аудит, моніторинг, реагування та відповідальність за порушення встановлених вимог (Holovko et al., 2025). У цьому контексті цифровий контроль набуває значення не стільки допоміжного інструменту адміністрування, скільки засобу підтримання стійкості держави в умовах безпекової нестабільності.

Водночас саме в цій площині виникає найбільш складна наукова дискусія щодо співвідношення безпеки та свободи. З одного боку, національна безпека об'єктивно потребує своєчасного доступу до достовірної інформації, ефективного міжвідомчого обміну даними та здатності держави швидко реагувати на загрози. З іншого боку, надмірне розширення цифрового контролю може призводити до порушення приватності, непропорційного втручання у сферу автономії особи, цифрового профілювання та обмеження прав без достатньої процедурної основи. Саме тому цілком слушною вбачається необхідність формування такої моделі цифрового контролю, у якій безпекова доцільність не підміняє правову визначеність, а технологічна ефективність не послаблює вимоги верховенства права.

У цьому аспекті важливо зіставити отримані результати з дослідженнями права на приватність у цифрову епоху. Сучасні підходи до приватності виходять із того, що в умовах цифрової трансформації особа стає більш вразливою до неконтрольованого збирання, обробки та поширення даних (Kluban, 2026). У сфері публічно-правового контролю ця проблема загострюється, оскільки обробка даних може здійснюватися не лише для сервісних, але й для контрольних, безпекових або превентивних цілей. Відтак, доцільним є перехід від формального розуміння захисту персональних даних до ризик-орієнтованої моделі, у межах

якої оцінюються мета обробки, обсяг даних, строки їх зберігання, коло суб'єктів доступу, рівень технічного захисту, можливість виправлення помилок і доступність правового захисту.

Погоджуючись із науковими позиціями щодо трансформації механізму правореалізації в умовах цифрової держави, слід зазначити, що цифровізація публічно-правового контролю виявляє одну з найбільш складних форм такої трансформації. Якщо в класичній моделі застосування права передбачає відносно чіткий зв'язок між нормою, суб'єктом владних повноважень і прийнятим рішенням, то в цифровій моделі цей зв'язок опосередковується інформаційною системою, алгоритмом, реєстром, електронною ідентифікацією та технічними налаштуваннями платформи. Зазначене не усуває юридичної відповідальності органу влади, однак вимагає її нового доктринального осмислення, оскільки помилка може виникати не лише на рівні людського рішення, але й на рівні даних, програмної логіки або технологічного посередництва (Tsvietkova, 2026).

Не менш важливим є співвідношення отриманих результатів із дослідженнями цифрового середовища та цифрової трансформації цивільного права. У працях, присвячених цим питанням, наголошується на необхідності адаптації традиційних правових категорій до нових цифрових явищ, зокрема електронних договорів, цифрових послуг, персональних даних, віртуальних об'єктів і штучного інтелекту (Anatiichuk, 2024; Bezklubyi, 2024). Хоча публічно-правовий контроль має іншу галузеву природу, сама логіка адаптації є подібною. Так само, як приватне право переосмислює договір, зобов'язання та відповідальність у цифровому середовищі, публічне право має переосмислити контроль, адміністративну процедуру, владне рішення, доказовість і межі втручання держави.

Окремого обговорення потребує використання штучного інтелекту у публічному адмініструванні. Зарубіжні дослідження засвідчують, що застосування штучного інтелекту публічними адміністраціями може підвищувати управлінську ефективність, однак одночасно породжує питання прозорості, відповідальності, якості даних і контролю за автоматизованими рішеннями (Chiti, Marchetti, & Rangone, 2022). Для України ця проблематика має додатковий безпековий вимір, оскільки алгоритмічні інструменти можуть використовуватися не лише для сервісного адміністрування, але й для виявлення ризиків, обробки безпекової інформації та підготовки контрольних рішень. Відтак, впровадження штучного інтелекту в систему публічно-правового контролю потребує не лише технічної апробації, але й нормативного визначення меж його використання.

Проблема адміністративної відповідальності також набуває нового бачення. Сучасні дослідження адміністративної відповідальності акцентують увагу на її адаптації до нових викликів публічного управління, зростання складності правопорушень і потреби в оновленні правових механізмів реагування (Kaganovska et al., 2025). У цифровому контрольному середовищі це означає необхідність визначення відповідальності за недостовірність даних, порушення режиму доступу, неналежне адміністрування реєстрів, невжиття заходів кіберзахисту, неправомірне використання алгоритмічних інструментів або відсутність належного людського контролю за автоматизованими рішеннями. Зазначене підкреслює, що цифровізація не скасовує відповідальність, а ускладнює її структуру.

У контексті публічної безпеки в умовах воєнного стану важливо враховувати, що кризові обставини можуть об'єктивно зумовлювати розширення контрольних можливостей держави. Водночас міжнародно-правові механізми забезпечення публічної безпеки та захисту громадського порядку вказують на необхідність збереження правових меж навіть у надзвичайних умовах (Zakharchenko et al., 2026). Для цифрового контролю це означає, що безпекова необхідність не повинна перетворюватися на постійну модель непрозорого спостереження. Будь-яке цифрове втручання має мати законну мету, визначений обсяг, часові межі, процедуру перевірки та можливість оскарження.

Дискусійною, однак перспективною, є також проблема використання цифрових технологій у превентивній діяльності. Дослідження цифрової епохи у сфері запобігання окремим ризикам свідчать, що цифрові інструменти можуть використовуватися для раннього виявлення проблем, прогнозування небезпечних тенденцій і підвищення ефективності превентивних заходів (Zijadova, Malikova, & Kosov, 2026). Для системи публічно-правового контролю це відкриває можливість переходу від карально-реактивної моделі до превентивної. Однак така модель потребує особливої обережності, оскільки прогнозування ризиків не повинно перетворюватися на необґрунтоване профілювання осіб, груп чи організацій.

Загалом отримані результати дають підстави стверджувати, що цифровізація публічно-правового контролю виходить за межі звичайного оновлення адміністративних процедур і набуває значення одного з інструментів забезпечення стійкості держави перед сучасними загрозами безпеки. Її ефективність залежить не від самого факту впровадження цифрових технологій, а від якості правового режиму їх використання. Найбільш обґрунтованою вбачається така модель, у якій цифрові інструменти забезпечують швидкість, точність, координацію та превентивність контролю, а право встановлює межі, гарантії, процедури, відповідальність і механізми захисту від зловживань. Саме поєднання технологічної спроможності з юридичною визначеністю дозволяє розглядати цифровізацію публічно-правового контролю як реальний інструмент зміцнення національної безпеки, а не лише як зовнішній прояв цифрової трансформації держави.

Висновки

Проведене дослідження дозволяє стверджувати, що цифровізація системи публічно-правового контролю постає як складний правовий процес, зумовлений трансформацією публічного управління, посиленням безпекових викликів та необхідністю оперативного реагування держави на загрози національній безпеці. Вона не обмежується технічним оновленням адміністративних процедур, а змінює саму логіку контрольної діяльності, у межах якої ключового значення набувають завчасне виявлення ризиків, аналітичне опрацювання даних, міжвідомча електронна взаємодія та захищений інформаційний обмін.

Зазначене підкреслює, що цифровізований публічно-правовий контроль має багаторівневу природу. Його зміст охоплює нормативно-безпековий, адміністративно-організаційний, інформаційно-технологічний і правозахисний виміри, які у сукупності визначають межі державного втручання, порядок використання цифрових даних, функціонування електронних реєстрів і гарантії захисту прав людини. Саме тому ефективність цифрового контролю має оцінюватися не лише за критеріями швидкості та технологічної зручності, а й з позицій законності, пропорційності, правової визначеності, кіберстійкості та підзвітності публічної влади.

Вбачається, що цифровізація публічно-правового контролю може бути дієвим інструментом забезпечення національної безпеки України лише за умови належного правового врегулювання. Особливого значення набувають прозорі правила міжвідомчого обміну даними, визначення меж автоматизованого моніторингу, захист персональних даних, можливість перегляду й оскарження цифрових рішень, а також встановлення відповідальності суб'єктів, залучених до функціонування цифрової контрольної інфраструктури. Без таких гарантій цифрові інструменти можуть створювати ризики надмірного адміністративного впливу та порушення приватності.

Перспективи подальших досліджень доцільно пов'язати з аналізом правового режиму автоматизованого прийняття рішень, використанням штучного інтелекту у публічно-правовому контролі, визначенням статусу технологічних посередників та розробленням критеріїв алгоритмічної прозорості. Подальше опрацювання цих питань дозволить

сформувати більш цілісну правову доктрину цифрового публічно-правового контролю як інструменту забезпечення національної безпеки України.

Фінансування

Це дослідження не отримало конкретної фінансової підтримки.

Конкуруючі інтереси

Автори заявляють, що у них немає конкуруючих інтересів.

Використання штучного інтелекту

Автори заявляють, що використовували ШІ для перевірки правопису та пошуку ресурсів.

Список використаних джерел

- Анатійчук В. Правове регулювання цифрової трансформації й цифровізації у цивільному праві України [Електронний ресурс]. 2024. URL: <https://law.chnu.edu.ua/pravove-rehuliuвання-tsyfrovoi-transformatsii-y-tsyfrovizatsii-u-tsyvilnomu-pravi/> (дата звернення: 23.03.2026).
- Безклубий І. Правова семантика поняття «цифрове середовище». *Вісник Київського національного університету імені Тараса Шевченка. Юридичні науки*. 2024. Т. 127, № 1. С. 18–22. DOI: <https://doi.org/10.17721/1728-2195/2024/1.127-2>.
- Chiti E., Marchetti B., Rangone N. (2022) The use of artificial intelligence by Italian public administrations: dress rehearsal. *BioLaw Journal*, vol. 2022, no. 2, pp. 489–507. DOI: <https://doi.org/10.15168/2284-4503-2351>
- Регламент (ЄС) № 910/2014 Європейського Парламенту і Ради від 23 липня 2014 року щодо електронної ідентифікації та довірчих послуг для електронних транзакцій на внутрішньому ринку та про скасування Директиви 1999/93/ЄС (eIDAS). URL: <http://data.europa.eu/eli/reg/2014/910/oj> (дата звернення: 26.03.2026).
- Регламент (ЄС) 2016/679 Європейського Парламенту і Ради від 27 квітня 2016 року про захист фізичних осіб у зв'язку з обробкою персональних даних і про вільний рух таких даних та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних, GDPR). URL: https://zakon.rada.gov.ua/laws/show/984_008-16#Text (дата звернення: 17.03.2026).
- Директива (ЄС) 2019/770 Європейського Парламенту і Ради від 20 травня 2019 року щодо окремих аспектів договорів про постачання цифрового контенту та цифрових послуг. URL: <https://eur-lex.europa.eu/eli/dir/2019/770/oj> (дата звернення: 17.03.2025).
- Grytsyshen D., Somak O., Zelenskyi V., Bondarchuk O., Yuzyuk A. Measures for monitoring the functioning of public administration institutions, taking into account the legislative framework and level of efficiency. *Revista de Cercetare si Interventie Sociala*. 2025. Vol. 91. P. 221–238. DOI: <https://doi.org/10.33788/rcis.91.13>
- Гавриленко, Н. (2023). Офісні витрати в контексті сучасних підходів до обліку витрат. *Економічний простір*, (184), 153-157. <https://doi.org/10.32782/2224-6282/184-27>
- Holovko O., Kravchenko O., Pogrebytskyi M., Romaniuk I. Ways to improve legal regulation of critical infrastructure information networks protection. *Social and Legal Studios*. 2025. Vol. 8, No. 1. P. 70–81. DOI: <https://doi.org/10.32518/sals1.2025.70>.
- Kaganovska T., Koveino Y., Kamardina Y., Shestak L., Riabchenko M. Administrative liability in Ukraine: contemporary challenges and development prospects. *Relações Internacionais no Mundo Atual*. 2025. Vol. 3, No. 49. P. 123–136. DOI: <https://doi.org/10.21902/Revrima.v3i49.7692>.

- Клубан М. В. Право на приватність у цифрову епоху: міжнародні стандарти та практика їх реалізації в Україні. *Прикарпатський юридичний вісник*. 2026. № 1. С. 208–214. DOI: <https://doi.org/10.32782/pyuv.v1.2026.35>
- Mykolalets A., Hlushchenko S., Melnychuk N., Sereda V., Mykytiuk M. Human Rights Theory Development: From Natural Law to Constitutional Reflection Within Digital Transformation Context. *OIDA International Journal of Sustainable Development*. 2025. Vol. 18, No. 10. P. 155–166. URL: <https://ssrn.com/abstract=5289641> (date of access: 23.06.2026).
- Shkilniak M., Monastyrskiy G., Melnyk A., Vasina A., Dudkina O. (2026) Modernisation of the public management system in Ukraine. *P.A. Persona e Amministrazione*. 2026. Vol. 1, No. 1. P. 151–174.
- Sopilko I., Svintsytskyi A., Krasovska Y., Padalka A., Lyseiuk A. Information wars as a threat to the information security of Ukraine. *Conflict Resolution Quarterly*. 2022. Vol. 39, No. 3. P. 333–347. DOI: <https://doi.org/10.1002/crq.21331>
- Цветкова Ю. В. Трансформація механізму правореалізації в умовах цифрової держави: додаткові форми, зміна суб'єктів чи поява нової доктрини. *Альманах права*. 2026. С. 233–238. URL: <https://almanahprava.org/assets/images/issues/17/almanac-17-2026-04-30-2026.pdf> (дата звернення: 26.03.2026).
- Про національну безпеку України : Закон України від 21 червня 2018 р. № 2469-VIII. *Відомості Верховної Ради України*. 2018. № 31. Ст. 241. URL: <https://zakon.rada.gov.ua/laws/show/2469-19> (дата звернення: 01.06.2026).
- Про схвалення Концепції розвитку електронного урядування в Україні : розпорядження Кабінету Міністрів України від 20 вересня 2017 р. № 649-р. *Офіційний вісник України*. 2017. № 78. Ст. 2395. URL: <https://zakon.rada.gov.ua/laws/show/649-2017-%D1%80> (дата звернення: 01.06.2026).
- Про схвалення Концепції розвитку цифрових компетентностей : розпорядження Кабінету Міністрів України від 3 березня 2021 р. № 167-р. *Офіційний вісник України*. 2021. № 22. Ст. 1015. URL: <https://zakon.rada.gov.ua/laws/show/167-2021-%D1%80> (дата звернення: 01.06.2026).
- Про основні засади забезпечення кібербезпеки України : Закон України від 5 жовтня 2017 р. № 2163-VIII. *Відомості Верховної Ради України*. 2017. № 45. Ст. 403. URL: <https://zakon.rada.gov.ua/laws/show/2163-19> (дата звернення: 01.06.2026).
- Verkhovna Rada Ukrainy (2010) Pro zakhyst personalnykh danykh: Zakon Ukrainy vid 1 chervnia 2010 r. № 2297-VI [On Personal Data Protection: Law of Ukraine of June 1, 2010 No. 2297-VI]. *Vidomosti Verkhovnoi Rady Ukrainy*, no. 34, art. 481. Available at: <https://zakon.rada.gov.ua/laws/show/2297-17> (accessed 01 June 2026).
- Євдокименко С. А., Гіда Є. О., Лощикін О. М., Стерліков О. С. Перспективи розвитку теорії держави і конституційного права в умовах цифровізації суспільства. *Академічні візії*. 2024. № 30. URL: <https://academy-vision.org/index.php/av/article/view/2365> (дата звернення: 26.03.2026).
- Zakharchenko A., Varenyk O., Pidbereznykh I., Vykhrystiuk A., Verbytsky V. International legal mechanisms for ensuring public security and protecting public order under martial law. *Cadernos de Dereito Actual*. 2026. Vol. 2026, No. 31. P. 373–390.
- Zijadova D. Z., Malikova M. G., Kosov R. V. Peculiarities of environmental prevention in the digital age. *South of Russia: Ecology, Development*. 2026. Vol. 21, No. 1. P. 161–169. DOI: <https://doi.org/10.18470/1992-1098-2026-1-14>

References

- Anatiichuk V. (2024) Pravove rehuliuвання tsyfrovoy transformatsii y tsyfrovizatsii u tsyvilnomu pravi Ukrainy [Legal regulation of digital transformation and digitalization in civil law of

- Ukraine]. Available at: <https://law.chnu.edu.ua/pravove-rehuliuivannia-tsyfrovoi-transformatsii-y-tsyfrovizatsii-u-tsyvilnomu-pravi> (accessed 20 March 2026).
- Bezklubyi I. (2024) Pravova semantyka poniattia "tsyfrove seredovyshe" [Legal semantics of the concept of "digital environment"]. Visnyk Kyivskoho natsionalnoho universytetu imeni Tarasa Shevchenka. Yurydychni nauky [Bulletin of Taras Shevchenko National University of Kyiv. Legal Studies], vol. 127, no. 1, pp. 18–22.
- Chiti E., Marchetti B., Rangone N. (2022) The use of artificial intelligence by Italian public administrations: dress rehearsal. BioLaw Journal, vol. 2022, no. 2, pp. 489–507. DOI: <https://doi.org/10.15168/2284-4503-2351>
- European Parliament and Council of the European Union (2014) Regulation (EU) No 910/2014 of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC. Available at: <http://data.europa.eu/eli/reg/2014/910/oj> (accessed 26 March 2026).
- European Parliament and Council of the European Union (2016) Regulation (EU) 2016/679 of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC. Available at: https://zakon.rada.gov.ua/laws/show/984_008-16#Text (accessed 17 March 2026).
- European Parliament and Council of the European Union (2019) Directive (EU) 2019/770 of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services. Available at: <https://eur-lex.europa.eu/eli/dir/2019/770/oj> (accessed 17 March 2025).
- Grytsyshen D., Somak O., Zelenskyi V., Bondarchuk O., Yuzyuk A. (2025) Measures for monitoring the functioning of public administration institutions, taking into account the legislative framework and level of efficiency. Revista de Cercetare si Interventie Sociala, vol. 91, pp. 221–238. DOI: <https://doi.org/10.33788/rcis.91.13>
- Havrylenko N. (2023) Informatsiia v umovakh tsyvrovizatsii publichno-pravovoho upravlinnia [Information in the conditions of digitalization of public-legal management]. Ekonomichnyi prostir [Economic Space], no. 187, pp. 39–43. DOI: <https://doi.org/10.32782/2224-6282/187-6>
- Holovko O., Kravchenko O., Pogrebytskyi M., Romaniuk I. (2025) Ways to improve legal regulation of critical infrastructure information networks protection. Social and Legal Studios, vol. 8, no. 1, pp. 70–81. DOI: <https://doi.org/10.32518/sals1.2025.70>
- Kaganovska T., Koveino Y., Kamardina Y., Shestak L., Riabchenko M. (2025) Administrative liability in Ukraine: contemporary challenges and development prospects. Relacoes Internacionais no Mundo Atual, vol. 3, no. 49, pp. 123–136. DOI: <https://doi.org/10.21902/Revrima.v3i49.7692>
- Kluban M. V. (2026) Pravo na pryvatnist v tsyfrovi epokhu: mizhnarodni standarty ta praktyka yikh realizatsii v Ukraini [The right to privacy in the digital age: international standards and practice of their implementation in Ukraine]. Prykarpatskyi yurydychnyi visnyk [Subcarpathian Law Herald], no. 1, pp. 208–214. DOI: <https://doi.org/10.32782/pyuv.v1.2026.35>
- Mykolalets A., Hlushchenko S., Melnychuk N., Sereda V., Mykytiuk M. (2025) Human rights theory development: from natural law to constitutional reflection within digital transformation context. OIDA International Journal of Sustainable Development, vol. 18, no. 10, pp. 155–166.
- Shkilniak M., Monastyrskyi G., Melnyk A., Vasina A., Dudkina O. (2026) Modernisation of the public management system in Ukraine. P.A. Persona e Amministrazione, vol. 1, no. 1, pp. 151–174.

- Sopilko I., Svintsytskyi A., Krasovska Y., Padalka A., Lyseiuk A. (2022) Information wars as a threat to the information security of Ukraine. *Conflict Resolution Quarterly*, vol. 39, no. 3, pp. 333–347. DOI: <https://doi.org/10.1002/crq.21331>
- Tsvietkova Yu. V. (2026) Transformatsiia mekhanizmu pravorealizatsii v umovakh tsyfrovoy derzhavy: dodatkovy formy, zmina subiektiv chy poiava novoi doktryny [Transformation of the mechanism of legal realization in the conditions of the digital state: additional forms, change of subjects or emergence of a new doctrine]. *Almanakh prava [Almanac of Law]*, pp. 233–238. Available at: <https://almanahprava.org/assets/images/issues/17/almanac-17-2026-04-30-2026.pdf> (accessed 26 March 2026).
- Verkhovna Rada Ukrainy (2018) Pro natsionalnu bezpeku Ukrainy: Zakon Ukrainy vid 21 chervnia 2018 r. № 2469-VIII [On National Security of Ukraine: Law of Ukraine of June 21, 2018 No. 2469-VIII]. *Vidomosti Verkhovnoi Rady Ukrainy*, no. 31, art. 241. Available at: <https://zakon.rada.gov.ua/laws/show/2469-19> (accessed 01 June 2026).
- Kabinet Ministriv Ukrainy (2017) Pro skhvalennia Kontseptsii rozvytku elektronnoho uriaduvannia v Ukraini: rozporiadzhennia vid 20 veresnia 2017 r. № 649-r [On Approval of the Concept for the Development of E-Governance in Ukraine: Order of September 20, 2017 No. 649-r]. *Ofitsiinyi visnyk Ukrainy*, no. 78, art. 2395. Available at: <https://zakon.rada.gov.ua/laws/show/649-2017-%D1%80> (accessed 01 June 2026).
- Kabinet Ministriv Ukrainy (2021) Pro skhvalennia Kontseptsii rozvytku tsyfrovyykh kompetentnostei: rozporiadzhennia vid 3 bereznia 2021 r. № 167-r [On Approval of the Concept for the Development of Digital Competences: Order of March 3, 2021 No. 167-r]. *Ofitsiinyi visnyk Ukrainy*, no. 22, art. 1015. Available at: <https://zakon.rada.gov.ua/laws/show/167-2021-%D1%80> (accessed 01 June 2026).
- Verkhovna Rada Ukrainy (2017) Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy: Zakon Ukrainy vid 5 zhovtnia 2017 r. № 2163-VIII [On the Basic Principles of Cybersecurity of Ukraine: Law of Ukraine of October 5, 2017 No. 2163-VIII]. *Vidomosti Verkhovnoi Rady Ukrainy*, no. 45, art. 403. Available at: <https://zakon.rada.gov.ua/laws/show/2163-19> (accessed 01 June 2026).
- Verkhovna Rada Ukrainy (2010) Pro zakhyst personalnykh danykh: Zakon Ukrainy vid 1 chervnia 2010 r. № 2297-VI [On Personal Data Protection: Law of Ukraine of June 1, 2010 No. 2297-VI]. *Vidomosti Verkhovnoi Rady Ukrainy*, no. 34, art. 481. Available at: <https://zakon.rada.gov.ua/laws/show/2297-17> (accessed 01 June 2026).
- Yevdokimenko S. A., Hida Ye. O., Loshchykhin O. M., Sterlikov O. S. (2024) Perspektyvy rozvytku teorii derzhavy i konstytutsiinoho prava v umovakh tsyfrovizatsii suspilstva [Prospects for the development of the theory of state and constitutional law in the conditions of digitalization of society]. *Akademichni vizii [Academic Visions]* (electronic journal), no. 30. Available at: <https://academy-vision.org/index.php/av/article/view/2365> (accessed 26 March 2026).
- Zakharchenko A., Varenuk O., Pidbereznykh I., Vykhrystiuk A., Verbytsky V. (2026) International legal mechanisms for ensuring public security and protecting public order under martial law. *Cadernos de Dereito Actual*, vol. 2026, no. 31, pp. 373–390.
- Zijadova D. Z., Malikova M. G., Kosov R. V. (2026) Peculiarities of environmental prevention in the digital age. *South of Russia: Ecology, Development*, vol. 21, no. 1, pp. 161–169. DOI: <https://doi.org/10.18470/1992-1098-2026-1-14>

