УДК 351.86:004.7(477)
JEL H11, H56, O33, D73, L86
DOI https://doi.org/10.32782/2786-765X/2026-14-11

Загоруйко В.С.
здобувач третього рівня вищої освіти,
Національний університет цивільного захисту України
ORCID: https://orcid.org/0009-0009-1348-4503

БЕЗПЕКА ЦИФРОВОГО ПРОСТОРУ УКРАЇНИ ЯК ОБ'ЄКТ ДЕРЖАВНОГО УПРАВЛІННЯ: ДОКТРИНАЛЬНІ ТА КАТЕГОРІАЛЬНІ ЗАСАДИ

У статті обґрунтовано доцільність розгляду безпеки цифрового простору України як самостійного об'єкта державного управління, що не зводиться до технічного кіберзахисту інформаційних систем. Показано, що цифровий простір утворюється взаємодією електронних комунікацій, державних реєстрів, хмарних сервісів, цифрових платформ, критичної інформаційної інфраструктури, алгоритмічних систем, даних, органів публічної влади, бізнесу та громадянського суспільства. Його мережевість, трансграничність, висока швидкість змін і залежність від приватної технологічної інфраструктури унеможливлюють результативне управління виключно через централізовані адміністративні приписи. Розмежовано поняття кібербезпеки, інформаційної безпеки, цифрової стійкості, технологічного суверенітету та безпеки цифрового простору. Запропоновано авторське визначення останньої як підтримуваного системою публічного управління стану захищеності, стійкості, керованості та ціннісно узгодженої впорядкованості цифрового середовища, за якого забезпечуються безперервність життєво важливих послуг, суверенність критичних даних і технологічних рішень, права людини, довіра до електронної держави та спроможність учасників спільно запобігати, виявляти, стримувати, локалізувати й долати наслідки цифрових загроз. Систематизовано доктринальні принципи державного управління у досліджуваній сфері: законність, людиноцентричність, ризик-орієнтованість, пропорційність, стійкість за проєктуванням, субсидіарність, інтероперабельність, підзвітність, технологічна нейтральність, державно-приватна взаємодія, міжнародна сумісність та адаптивне навчання. Визначено рівні управління безпекою цифрового простору: загальнодержавний, секторальний, територіальний, організаційний і платформний. Обґрунтовано управлінський цикл, який поєднує доктринальне цілепокладання, стратегування, нормативне закріплення, формування спроможностей, моніторинг, реагування, відновлення та перегляд політики. Наукова новизна полягає у перенесенні акценту з охорони окремих інформаційних ресурсів на забезпечення цілісної безпеки соціотехнічного цифрового середовища та публічних інтересів у ньому. Практичне значення мають запропоновані критерії віднесення цифрових процесів до об'єктів державного управління і рамка для узгодження стратегій кібербезпеки, цифрової трансформації, захисту критичної інфраструктури та прав людини.

Ключові слова: безпека цифрового простору, державне управління, кібербезпека, цифрова стійкість, критична інфраструктура, цифрові платформи, публічні інтереси, технологічний суверенітет.

Постановка проблеми. Повномасштабна агресія проти України перетворила цифрове середовище на повноцінний простір здійснення державних функцій, ведення економічної діяльності, надання послуг, комунікації та протиборства. У 2025 р. CERT-UA опрацювала 5927 кіберінцидентів, що на 37,4 % більше, ніж у 2024 р., а у березні-квітні 2026 р. було зафіксовано інтенсифікацію атак на органи місцевого самоврядування і комунальні установи [10; 11]. Це свідчить, що об'єктом захисту є вже не окремий сервер або відомча мережа, а взаємопов'язана цифрова екосистема держави, порушення якої здатне спричинити одночасні управлінські, економічні, соціальні та безпекові наслідки.

Аналіз останніх досліджень і публікацій. У сучасних дослідженнях цифровий простір розглядається як мережеве середовище, в якому поряд із державою нормотворчі й організаційні функції фактично виконують власники платформ, оператори інфраструктури та професійні спільноти. Українські автори наголошують на необхідності системного поєднання організаційних, правових, технологічних та комунікативних компонентів цифровізації публічного управління [12; 13]. Міжнародні документи доповнюють цей підхід вимогами управління ризиками, безперервності, відповідальності керівних органів і транскордонної взаємодії [5; 6]. Водночас категорія «безпека цифрового простору» у науці державного управління залишається недостатньо відмежованою від суміжних понять.

Метою статті є обґрунтування безпеки цифрового простору України як комплексного об'єкта державного управління, уточнення її категоріального змісту, визначення доктринальних принципів, рівнів та управлінського

циклу забезпечення такої безпеки відповідно до сучасних викликів і євроінтеграційних орієнтирів України.

Виклад основного матеріалу дослідження. Цифровий простір доцільно розуміти не як географічно відокремлену територію та не як просту сукупність мереж. Це створене цифровими технологіями середовище суспільної взаємодії, в якому інформація перетворюється на управлінський ресурс, сервіс, економічний актив, доказ, засіб впливу й об'єкт посягання. До його інфраструктурного ядра належать електронні комунікаційні мережі, центри обробки даних, хмарні платформи, державні інформаційні ресурси, реєстри, системи електронної ідентифікації, платіжні та технологічні системи. Однак без суб'єктів, правил, довіри і практик використання ця інфраструктура не утворює самостійного управлінського простору.

Управлінська специфіка цифрового простору визначається п'ятьма взаємопов'язаними ознаками. По-перше, він має трансграничний характер: дані, обчислювальні ресурси, постачальники програмного забезпечення та власники платформ можуть перебувати в різних юрисдикціях. По-друге, цифрові взаємодії є мережевими, тому локальний інцидент здатний поширюватися через ланцюги довіри, спільні бібліотеки, облікові записи або постачальників. По-третє, технологічні й поведінкові зміни відбуваються швидше, ніж традиційний нормативний цикл. По-четверте, значна частина критичних спроможностей належить приватним суб'єктам. По-п'яте, цифрове середовище поєднує фізичні та віртуальні наслідки: порушення даних або алгоритмів може зупинити енергетичний, медичний, транспортний чи адміністративний процес.

Саме тому кібербезпека є необхідною, але не вичерпною складовою досліджуваного поняття. Закон України «Про основні засади забезпечення кібербезпеки України» пов'язує кібербезпеку із захищеністю життєво важливих інтересів людини, суспільства і держави під час використання кіберпростору [1]. Інформаційна безпека зосереджується на змісті, достовірності, конфіденційності, цілісності й доступності інформації, а також на протидії маніпулятивним впливам. Цифрова стійкість описує здатність систем і організацій продовжувати критичні функції, адаптуватися, відновлюватися й навчатися після порушення. Технологічний суверенітет стосується спроможності держави уникати критичної некерованої залежності від зовнішніх технологій, постачальників, даних і стандартів.

Безпека цифрового простору інтегрує ці компоненти, але не ототожнюється з жодним із них. Її об'єктом є не лише технічна система, а сукупність цифрових відносин, процесів, послуг, цінностей та інституційних зв'язків. Наприклад, безвідмовна робота платформи не означає безпеки, якщо алгоритм дискримінаційно обмежує доступ громадян до послуги. Високий рівень криптографічного захисту не компенсує відсутності законної мети обробки даних. Так само формальне виконання приписів не гарантує стійкості, коли організація не має резервних каналів, навченого персоналу й відпрацьованого плану відновлення.

З урахуванням цього пропонується визначати безпеку цифрового простору України як підтримуваний системою публічного управління стан захищеності, стійкості, керованості та ціннісно узгодженої впорядкованості цифрового середовища, за якого забезпечуються: безперервність життєво важливих функцій і публічних послуг; суверенність критичних даних та технологічних рішень; реалізація прав і свобод людини; достовірність та підзвітність цифрових управлінських процесів; спроможність державних і недержавних суб'єктів спільно запобігати, виявляти, стримувати, локалізувати й долати наслідки загроз.

Запропоноване визначення містить чотири взаємодоповнювальні виміри. Захищеність означає зменшення ймовірності та наслідків несанкціонованого доступу, руйнування, підміни, блокування чи неправомірного використання цифрових ресурсів. Стійкість характеризує здатність зберігати пріоритетні функції за умов атаки, відмови або дефіциту ресурсів. Керованість передбачає наявність визначених повноважень, інформації, процедур координації та засобів впливу. Ціннісна узгодженість вимагає, щоб заходи безпеки захищали конституційні права, демократію і публічний інтерес, а не створювали необмежений адміністративний контроль.

Доктринальний підхід є необхідним тому, що цифрова політика не може складатися з непов'язаних реакцій на окремі інциденти. Правова та управлінська доктрина формує понятійні межі, цілі, допустимі способи втручання і критерії належного результату. У цифровій сфері вона повинна відповідати щонайменше на чотири питання: які публічні цінності є пріоритетними; які ризики держава вважає неприйнятними; як розподіляються відповідальність і ресурси; які гарантії запобігають надмірному обмеженню прав. Без такої основи стратегічні документи перетворюються на перелік заходів, а нормативні акти – на фрагментарні технічні приписи.

Першим принципом державного управління безпекою цифрового простору є законність. Будь-яке спостереження, обмеження доступу, обмін даними, вимога до платформ або втручання в роботу інформаційної системи повинні мати чітку правову підставу, визначену мету та процедуру контролю. Другим є людиноцентричність: безпека оцінюється не тільки через стан мережі, а й через вплив на права, доступність послуг, недискримінацію, приватність та довіру. Третім є пропорційність, яка вимагає обирати найменш обмежувальний захід, достатній для нейтралізації конкретного ризику.

Ризик-орієнтованість означає диференціацію вимог залежно від критичності функції, масштабу потенційної шкоди, залежностей і реальної загрози. Однакові заходи для невеликого інформаційного ресурсу та системи, від якої залежить енергопостачання області, створюють або надмірні витрати, або неприйнятну вразливість. Закон № 4336-IX 2025 р. посилив системність української моделі, передбачивши національну систему обміну інформацією про кіберінциденти й оновлені підходи до захисту державних ресурсів та критичної інформаційної інфраструктури [4]. Цей напрям відповідає вимогам NIS2 щодо управління ризиками, звітності та відповідальності керівництва [6].

Принцип «стійкість за проєктуванням» вимагає закладати безпеку, резервування, відновлюваність і мінімізацію даних до архітектури сервісу, а не додавати їх після запуску. Технологічна нейтральність означає закріплення функціональних вимог замість прив'язки до конкретного продукту, якщо така прив'язка не обґрунтована безпекою. Інтероперабельність забезпечує сумісність процедур, даних, ідентифікаторів та протоколів обміну. Субсидіарність передбачає реагування на найближчому спроможному рівні, але з можливістю швидкого залучення секторальних і національних ресурсів.

Підзвітність у цифровій сфері має охоплювати не лише посадових осіб, а й автоматизовані рішення. Для кожної критичної цифрової функції повинні бути визначені власник процесу, відповідальний за ризик, джерело даних, критерії якості, журнал дій, порядок аудиту та відновлення. Відкритість не означає розкриття технічних уразливостей; вона передбачає зрозуміле пояснення громадянам мети обробки даних, логіки суттєвих автоматизованих рішень, порядку оскарження і результатів державної політики. Регламент ЄС про цифрові послуги закріплює ризик-орієнтовану відповідальність платформ, що має враховуватися під час наближення українського законодавства до acquis ЄС [7; 9].

Окремим принципом є співрегулювання. Держава зберігає владний мандат і відповідальність за захист публічного інтересу, але не володіє всіма даними, експертизою та інфраструктурою, потрібними для забезпечення безпеки. Власники платформ бачать поведінкові аномалії, оператори зв'язку – мережеві індикатори, постачальники кіберзахисту – технічні ознаки атак, громадянське суспільство – наслідки для прав людини. Завдання державного управління полягає у створенні довірчого правового режиму обміну інформацією, захисті добросовісних повідомлень, визначенні мінімальних стандартів та уникненні приватної монополізації регуляторних функцій.

Міжнародна сумісність має подвійний зміст. По-перше, трансграничні загрози потребують оперативного обміну технічною інформацією, взаємної допомоги, спільних навчань та узгоджених санкційних і правоохоронних механізмів. По-друге, сумісність правил і стандартів з ЄС є умовою інтеграції України до єдиного цифрового ринку. Четвертий кібердіалог Україна-ЄС у жовтні 2025 р. зосереджувався на NIS2, захисті критичної інфраструктури, безпеці 5G, резерві кібербезпеки ЄС, протидії кіберзлочинності та державно-приватному партнерстві [14].

Адаптивне навчання завершує систему принципів. У цифровому середовищі політика, що не змінюється після інцидентів, навчань і технологічних зрушень, швидко втрачає результативність. Аналітичні огляди Національного координаційного центру кібербезпеки та CERT-UA мають перетворюватися не лише на інформаційні матеріали, а на зміни вимог, бюджетних пріоритетів, програм підготовки та архітектури сервісів [10; 11]. Важливо фіксувати не тільки факт атаки, а й першопричину, організаційні передумови, час виявлення, повноту комунікації і здатність відновити функції.

Безпека цифрового простору забезпечується на кількох рівнях. Загальнодержавний рівень визначає доктрину, стратегічні цілі, правовий режим, національні спроможності й міжнародні зобов'язання. Секторальний рівень адаптує загальні вимоги до енергетики, фінансів, охорони здоров'я, транспорту, оборони та інших сфер. Територіальний рівень забезпечує стійкість місцевих сервісів, комунальних підприємств і регіональних систем оповіщення. Організаційний рівень відповідає за управління активами, доступом, персоналом і безперервністю. Платформний

рівень охоплює правила, алгоритми, модерацію, рекламу, ідентифікацію та обробку даних приватними цифровими посередниками.

Рівні не повинні утворювати ізольовану ієрархію. Їх поєднують залежності: громада може використовувати державний реєстр і приватну хмару; лікарня залежить від електронної системи охорони здоров'я, енергопостачання та телекомунікацій; центральний орган використовує програмні компоненти міжнародних постачальників. Тому об'єктом управління має бути не лише окрема установа, а критичний ланцюг створення публічної цінності. Для кожного такого ланцюга необхідно встановити функцію, дані, постачальників, точки відмови, мінімально допустимий рівень послуги і порядок переходу на резервний режим.

Запропонований управлінський цикл починається з доктринального цілепокладання. На цьому етапі визначаються захищувані цінності, допустимий ризик і модель взаємодії держави з недержавними суб'єктами. Стратегування перетворює ці положення на вимірювані цілі й пріоритети. Нормативний етап закріплює повноваження, стандарти, обов'язки, гарантії та відповідальність. Формування спроможностей охоплює фінансування, кадри, технології, резерви, навчання і партнерства. Моніторинг забезпечує дані про загрози, вразливості, виконання вимог та стан послуг.

Реагування у цьому циклі не повинно обмежуватися технічним усуненням інциденту. Воно включає управлінське рішення про пріоритети, координацію, правовий режим, комунікацію, залучення приватних і міжнародних ресурсів. Відновлення має повертати не лише працездатність системи, а й цілісність даних, довіру користувачів і законність процесів. Завершальним етапом є перегляд політики: аналіз причин, оцінка результативності, коригування стандартів, бюджетів та навчальних програм. NIST CSF 2.0 акцентує функцію governance поряд з ідентифікацією, захистом, виявленням, реагуванням і відновленням, що підтверджує управлінський характер сучасної кіберстійкості [5].

Для віднесення цифрового процесу до об'єктів пріоритетного державного управління доцільно використовувати п'ять критеріїв. Перший – суспільна критичність: масштаб порушення життєво важливих послуг або прав. Другий – системна залежність: можливість каскадного поширення через спільні дані, постачальників чи інфраструктуру. Третій – інформаційна асиметрія: нездатність громадян або окремих установ самостійно оцінити й мінімізувати ризик. Четвертий – трансграничність та юрисдикційна складність. П'ятий – дефіцит ринкових стимулів до інвестування в безпеку, коли витрати несе оператор, а значну частину шкоди – суспільство.

Застосування цих критеріїв дозволяє уникнути двох крайнощів. Надмірне регулювання створює бюрократичні витрати, гальмує інновації та може перетворити безпекову аргументацію на засіб непропорційного контролю. Недостатнє втручання залишає публічні інтереси залежними від комерційних рішень, які не враховують системні наслідки. Оптимальна модель поєднує обов'язкові мінімальні вимоги для критичних функцій, ризик-орієнтований нагляд, добровільні стандарти для некритичних суб'єктів, стимули до обміну інформацією та прозорі гарантії прав.

Станом на липень 2026 р. Україна має сформоване стратегічне ядро політики кібербезпеки, оновлену законодавчу основу та значний практичний досвід протидії державним кібератакам. Водночас звіт Європейської Комісії за 2025 р. вказує на необхідність подальшого узгодження з NIS2, правилами цифрових послуг, захистом персональних даних і безпекою 5G [9]. Отже, наступний етап має полягати не в механічному збільшенні кількості актів, а в доктринальному узгодженні цифрової, кібербезпекової, інформаційної, інфраструктурної та правозахисної політик.

Практична реалізація запропонованого підходу потребує запровадження паспорта безпеки критичної цифрової функції. У ньому мають фіксуватися публічна цінність функції, відповідальний орган, користувачі, ключові дані, залежності, допустимий час переривання, резервний спосіб надання послуги, вимоги до постачальників, порядок повідомлення про інцидент і критерії відновлення. Такий паспорт не замінює технічну документацію, а створює спільну управлінську мову для керівників, кіберфахівців, юристів, фінансистів і комунікаторів.

Не менш важливо пов'язати оцінювання безпеки з бюджетним процесом. Витрати на захист часто розглядаються як допоміжні ІТ-видатки, хоча фактично вони забезпечують безперервність публічної функції. Бюджетні запити мають містити оцінку ризику, критичності, залишкової вразливості та очікуваного зниження шкоди. Для типових сервісів доцільно створити базові профілі спроможностей, а для критичних – незалежне оцінювання і регулярні міжвідомчі навчання. Це дозволить перейти від фінансування

обладнання до фінансування вимірюваної стійкості.

Таким чином, безпека цифрового простору є результатом не одного механізму, а узгодженої діяльності, що поєднує цінності, право, інституції, дані, технології, кадри, фінанси, комунікацію та міжнародну взаємодію. Визнання її самостійним об'єктом державного управління дає змогу подолати відомчу фрагментарність і оцінювати політику за здатністю держави та суспільства зберігати критичні функції, права і довіру в умовах постійних цифрових змін.

Висновки.

1. Цифровий простір України є соціотехнічним, мережевим і трансграничним середовищем, у якому технічні системи, дані, платформи, публічні інституції та поведінка користувачів утворюють єдиний об'єкт управлінського впливу.

2. Безпеку цифрового простору доцільно визначати через поєднання захищеності, стійкості, керованості та ціннісної узгодженості. Вона охоплює кібербезпеку, інформаційну безпеку, безперервність послуг, технологічний суверенітет, права людини і суспільну довіру, але не зводиться до жодного з цих компонентів.

3. Доктринальними принципами державного управління у цій сфері є законність, людиноцентричність, пропорційність, ризикорієнтованість, стійкість за проєктуванням, субсидіарність, інтероперабельність, підзвітність, співрегулювання, міжнародна сумісність та адаптивне навчання.

4. Управління має здійснюватися на загальнодержавному, секторальному, територіальному, організаційному й платформному рівнях і будуватися навколо критичних ланцюгів створення публічної цінності, а не лише навколо меж окремих установ.

5. Запропонований цикл «доктрина – стратегія – норма – спроможність – моніторинг – реагування – відновлення – перегляд» створює основу для узгодження кібербезпекової, цифрової, інфраструктурної та правозахисної політик України відповідно до сучасних вимог ЄС.

Бібліографічний список

1. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19
2. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України»: Указ Президента України від 26.08.2021 № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021
3. Про критичну інфраструктуру: Закон України від 16.11.2021 № 1882-IX. URL: https://zakon.rada.gov.ua/laws/show/1882-20
4. Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури: Закон України від 27.03.2025 № 4336-IX. URL: https://zakon.rada.gov.ua/go/4336-20
5. NIST Cybersecurity Framework (CSF) 2.0. Gaithersburg: National Institute of Standards and Technology, 2024. DOI: https://doi.org/10.6028/NIST.CSWP.29
6. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 (NIS2 Directive). URL: https://eur-lex.europa.eu/eli/dir/2022/2555/oj
7. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services. URL: https://eur-lex.europa.eu/eli/reg/2022/2065/oj
8. Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law. Vilnius, 2024. URL: https://www.coe.int/en/web/artificial-intelligence/the-framework-convention-on-artificial-intelligence
9. European Commission. Ukraine Report 2025. Brussels, 2025. URL: https://enlargement.ec.europa.eu/ukraine-report-2025_en
10. Державна служба спеціального зв'язку та захисту інформації України. CERT-UA у 2025 році опрацювала майже 6000 кіберінцидентів: кількість ворожих атак зросла на 37%. 2026. URL: https://cip.gov.ua/ua/news/cert-ua-u-2025-roci-opracyuvala-maizhe-6000-kiberincidentiv-kilkist-vorozhikh-atak-zrosla-na-37
11. CERT-UA. Органи місцевого самоврядування та комунальні установи у фокусі кібератак у березні-квітні 2026 року. URL: https://cert.gov.ua/article/6288271
12. Галушко С.П. Модель функціонування механізмів публічного управління у сфері національної безпеки в умовах цифровізації та впливу її технологій. *Вісник Національного університету цивільного захисту України (Серія «Державне управління»)*. 2024. Випуск 2 (21). С. 102–109. DOI: https://doi.org/10.52363/2414-5866-2024-2-11
13. Сурай А. Цифровізація публічного управління в Україні: організаційний аспект. *Публічне управління: концепції, парадигма, розвиток, удосконалення*. 2024. № 7. С. 116–124. DOI: https://doi.org/10.31470/2786-6246-2024-7-116-124

14. European Commission. EU and Ukraine deepen cooperation on cyber security at 4th Cyber Dialogue. 20 October 2025. URL: https://enlargement.ec.europa.eu/news/eu-and-ukraine-deepen-cooperation-cyber-security-4th-cyber-dialogue-2025-10-20_en

References

1. Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy [On the main principles of ensuring cyber security of Ukraine]: Zakon Ukrainy vid 05.10.2017 № 2163-VIII. Available at: https://zakon.rada.gov.ua/laws/show/2163-19
2. Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 14 travnia 2021 roku "Pro Stratehiiu kiberbezpeky Ukrainy" [On the decision of the National Security and Defense Council of Ukraine dated May 14, 2021 "On the Cybersecurity Strategy of Ukraine"]: Ukaz Prezydenta Ukrainy vid 26.08.2021 № 447/2021. Available at: https://zakon.rada.gov.ua/laws/show/447/2021
3. Pro krytychnu infrastrukturu [On critical infrastructure]: Zakon Ukrainy vid 16.11.2021 № 1882-IX. Available at: https://zakon.rada.gov.ua/laws/show/1882-20
4. Pro vnesennia zmin do deiakykh zakoniv Ukrainy shchodo zakhystu informatsii ta kiberzakhystu derzhavnykh informatsiinykh resursiv, obiektiv krytychnoi informatsiinoi infrastruktury [On making changes to some laws of Ukraine regarding information protection and cyber protection of state information resources, objects of critical information infrastructure]: Zakon Ukrainy vid 27.03.2025 № 4336-IX. Available at: https://zakon.rada.gov.ua/go/4336-20
5. NIST Cybersecurity Framework (CSF) 2.0. Gaithersburg: National Institute of Standards and Technology, 2024. DOI: https://doi.org/10.6028/NIST.CSWP.29
6. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 (NIS2 Directive). Available at: https://eur-lex.europa.eu/eli/dir/2022/2555/oj
7. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services. Available at: https://eur-lex.europa.eu/eli/reg/2022/2065/oj
8. Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law. Vilnius, 2024. Available at: https://www.coe.int/en/web/artificial-intelligence/the-framework-convention-on-artificial-intelligence
9. European Commission. Ukraine Report 2025. Brussels, 2025. Available at: https://enlargement.ec.europa.eu/ukraine-report-2025_en
10. Derzhavna sluzhba spetsialnoho zviazku ta zakhystu informatsii Ukrainy. CERT-UA u 2025 rotsi opratsiuvala maizhe 6000 kiberintsydentiv: kilkist vorozhykh atak zrosla na 37%. 2026. URL: https://cip.gov.ua/ua/news/cert-ua-u-2025-roci-opracyuvala-maizhe-6000-kiberincidentiv-kilkist-vorozhikh-atak-zrosla-na-37
11. CERT-UA. Orhany mistsevoho samovriaduvannia ta komunalni ustanovy u fokusi kiberatak u berezni-kvitni 2026 roku. Available at: https://cert.gov.ua/article/6288271
12. Galushko S. (2024) Model funktsionuvannia mekhanizmiv publichnoho upravlinnia u sferi natsionalnoi bezpeky v umovakh tsyfrovizatsii ta vplyvu yii tekhnolohii [The functional model of public administration mechanisms in the sphere of national security in the conditions of digitalization and the influence of its technologies]. *Visnyk Natsionalnoho universytetu tsyvilnoho zakhystu Ukrainy (Seriia "Derzhavne upravlinnia") – Bulletin of National University of Civil Protection of Ukraine (State Management series)*, vol. 2 (21), pp. 102–109. DOI: https://doi.org/10.52363/2414-5866-2024-2-11
13. Surai A. (2024) Tsyfrovizatsiia publichnoho upravlinnia v Ukraini: orhanizatsiinyi aspekt [Digitalization of Public Administration in Ukraine: Organizational Aspect]. *Publichne upravlinnia: kontseptsii, paradyhma, rozvytok, udoskonalennia – Public Administration: Concepts, Paradigm, Development, Improvement*, no. 7, pp. 116–124. DOI: https://doi.org/10.31470/2786-6246-2024-7-116-124
14. European Commission. EU and Ukraine deepen cooperation on cyber security at 4th Cyber Dialogue. 20 October 2025. Available at: https://enlargement.ec.europa.eu/news/eu-and-ukraine-deepen-cooperation-cyber-security-4th-cyber-dialogue-2025-10-20_en

Valerii Zahoruiko
Postgraduate Student,
National University of Civil Protection of Ukraine
ORCID: https://orcid.org/0009-0009-1348-4503

SECURITY OF UKRAINE'S DIGITAL SPACE AS AN OBJECT OF PUBLIC ADMINISTRATION: DOCTRINAL AND CATEGORICAL FOUNDATIONS

The article substantiates the need to treat the security of Ukraine's digital space as an autonomous object of public administration rather than reducing it to the technical cyber protection of information systems. Digital space is interpreted as a socio-technical environment formed by electronic communications, public registers, cloud services,

digital platforms, critical information infrastructure, algorithmic systems, data, public authorities, businesses and civil society. Its networked, cross-border and rapidly changing nature, together with dependence on privately owned technological infrastructure, makes purely centralised administrative control insufficient. The study distinguishes cybersecurity, information security, digital resilience, technological sovereignty and digital-space security. The latter is defined as a condition of protection, resilience, governability and value-consistent ordering of the digital environment maintained by the public administration system. Such a condition ensures the continuity of vital services, sovereignty over critical data and technological decisions, protection of human rights, trust in the digital state, and the collective capacity of stakeholders to prevent, detect, deter, contain and overcome digital threats. The doctrinal principles of public administration in this field are systematised: legality, human-centredness, risk-based governance, proportionality, resilience by design, subsidiarity, interoperability, accountability, technological neutrality, public-private cooperation, international compatibility and adaptive learning. National, sectoral, territorial, organisational and platform levels of governance are identified. A policy cycle linking doctrine, strategy, regulation, capacity building, monitoring, response, recovery and policy review is proposed. The scientific novelty lies in shifting the focus from protecting isolated information resources to safeguarding the integrity of the socio-technical digital environment and public interests within it. The proposed criteria and conceptual framework may be used to align Ukraine's cybersecurity, digital transformation, critical infrastructure protection and human-rights policies as of July 2026.

Keywords: digital-space security, public administration, cybersecurity, digital resilience, critical infrastructure, digital platforms, public interests, technological sovereignty.

Дата надходження статті: 09.07.2026
Дата прийняття статті до публікації: 10.08.2026
Дата публікації статті: 02.09.2026