DOI: https://doi.org/10.32782/city-development.2026.3-6
УДК 351.746.1:004.056(477)

НОРМАТИВНО-ПРАВОВИЙ ТА ІНСТИТУЦІЙНИЙ МЕХАНІЗМИ ДЕРЖАВНОГО УПРАВЛІННЯ БЕЗПЕКОЮ ЦИФРОВОГО ПРОСТОРУ УКРАЇНИ

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

Анотація. У статті здійснено комплексний аналіз нормативно-правового та інституційного механізмів державного управління безпекою цифрового простору України станом на 26 липня 2026 р. Нормативно-правовий механізм розглянуто не як сукупність законів і підзаконних актів, а як систему визначення цілей, повноважень, процедур, стандартів, гарантій, відповідальності та підзвітності. Інституційний механізм охарактеризовано через взаємодію Верховної Ради України, Президента України, Ради національної безпеки і оборони України, Національного координаційного центру кібербезпеки, Кабінету Міністрів України, Держспецзв'язку, CERT-UA, Служби безпеки України, кіберполіції, Міністерства цифрової трансформації, секторних регуляторів, органів місцевого самоврядування, операторів критичної інфраструктури, цифрових платформ і громадянського суспільства. Встановлено, що законодавчі зміни 2025 р. створили передумови для переходу від відомчо фрагментованого захисту до єдиної національної системи реагування, обміну інформацією про кіберінциденти та ризик-орієнтованого управління. Водночас зберігаються проблеми термінологічної неузгодженості, перетинів компетенції, нерівномірної секторальної й територіальної спроможності, недостатньої інтеграції даних, залежності від зовнішніх постачальників, неповного наближення до NIS2, правил цифрових послуг і сучасних стандартів захисту персональних даних. Запропоновано авторську модель узгодження механізмів, яка включає: національну матрицю компетенцій; паспорт державного механізму; ієрархію базових та секторальних профілів безпеки; обов'язкове оцінювання регуляторного, правозахисного й технологічного впливу; єдиний реєстр інцидентів з диференційованим доступом; регулярний перегляд стратегій на основі даних; механізми відповідальності керівників та незалежного контролю. Обґрунтовано, що інституційна результативність визначається не кількістю органів, а чіткістю ролей, швидкістю координації, сумісністю процедур та здатністю перетворювати інформацію про ризики на своєчасні рішення.

Ключові слова: нормативно-правовий механізм, інституційний механізм, державне управління, безпека цифрового простору, кібербезпека, критична інфраструктура, NIS2, міжвідомча координація.

Актуальність проблеми. Безпека цифрового простору залежить не лише від технічної оснащеності, а від того, чи сформовано узгоджені правила, визначено відповідальних суб'єктів, забезпечено обмін інформацією та контроль за рішеннями. Українська система розвивалася під тиском повномасштабної війни, коли швидкість реагування часто випереджала нормативне оформлення. Закон № 4336-IX від 27 березня 2025 р. суттєво оновив базові акти у сфері захисту інформації та кібербезпеки, зокрема заклав правові основи національної системи обміну інформацією про кіберінциденти [3]. Проте результативність реформи визначатиметься якістю інституційної реалізації.

Аналіз останніх досліджень і публікацій. Наукові праці з публічного управління акцентують на системності механізмів, розподілі повноважень, інституційній спроможності та міжсекторальній взаємодії [14; 15]. Європейський підхід, втілений у NIS2, пов'язує кібербезпеку з управлінням ризиками, відповідальністю керівних органів, обов'язковим повідомленням про інциденти та наглядом [11]. Звіт Європейської Комісії за 2025 р. визнав прогрес України, але наголосив на потребі подальшого наближення до acquis ЄС у сфері кібербезпеки, цифрових послуг і захисту даних [12].

Метою статті є визначення сучасного стану нормативно-правового та інституційного механізмів державного управління безпекою цифрового простору України, виявлення їх системних розривів та обґрунтування інструментів узгодження компетенцій, процедур, стандартів і відповідальності.

© Загоруйко В. С., 2026
Стаття поширюється на умовах ліцензії відкритого доступу (CC BY 4.0)

Результати дослідження. Нормативно-правовий механізм у сфері цифрової безпеки доцільно тлумачити як організовану систему правових засобів, за допомогою яких держава визначає захищувані публічні інтереси, суб'єктів і межі їх компетенції, обов'язкові вимоги до управління ризиками, процедури обміну інформацією та реагування, гарантії прав, види контролю й відповідальності. Такий механізм має вертикальний вимір – від Конституції та законів до технічних вимог – і горизонтальний вимір, який забезпечує узгодженість кібербезпекової, інформаційної, цифрової, інфраструктурної, оборонної та правоохоронної політик.

Конституційною основою механізму є обов'язок держави захищати суверенітет, територіальну цілісність, права і свободи людини, а також забезпечувати інформаційну безпеку. Ці положення визначають подвійний стандарт державного втручання: воно має бути достатнім для захисту суспільства і водночас обмеженим законом, необхідністю та пропорційністю. У цифровому середовищі цей баланс особливо важливий, оскільки технічні заходи моніторингу, блокування, ідентифікації або обміну даними можуть одночасно підвищувати безпеку й створювати ризики для приватності, свободи вираження поглядів та рівного доступу до послуг.

Базовим галузевим актом є Закон України «Про основні засади забезпечення кібербезпеки України» [2]. Він визначає національну систему кібербезпеки, основних суб'єктів, напрями державно-приватної взаємодії та принципи захисту життєво важливих інтересів. Закон «Про критичну інфраструктуру» переводить захист із площини окремих інформаційних систем до площини безперервності критичних функцій [4]. Організаційно-технічна модель кіберзахисту, затверджена постановою Кабінету Міністрів № 1426, створює рамку для взаємодії організаційних і технічних елементів [5]. Постанова № 299 визначає процедури реагування суб'єктів забезпечення кібербезпеки на події у кіберпросторі [6].

Закон № 4336-IX 2025 р. став найбільш суттєвим етапом останнього періоду. Він оновив підходи до захисту державних інформаційних ресурсів, критичної інформаційної інфраструктури, оцінювання захищеності, обміну інформацією та реагування [3]. Його управлінське значення полягає у переході від локальної відповідальності власника системи до взаємопов'язаної національної моделі, де інцидент розглядається як джерело спільної ситуаційної обізнаності. Однак законодавче закріплення є лише передумовою: потрібні сумісні класифікатори, цифрові канали, правила доступу, відповідальні чергові підрозділи, навчання і контроль якості повідомлень.

У 2025–2026 рр. нормативна база продовжила деталізуватися. План реалізації Стратегії кібербезпеки на 2025 р. визначив конкретні заходи й відповідальних виконавців [7]. Постанова Кабінету Міністрів № 367 встановила вимоги до управління ризиками безпеки на об'єктах критичної інфраструктури першої категорії критичності [8]. Для паливно-енергетичного сектору були затверджені спеціальні вимоги з кіберзахисту [9]. У квітні 2026 р. Держспецзв'язку оновила порядок оцінки стану захищеності державних інформаційних ресурсів [10]. Ці кроки формують секторальну глибину регулювання, але водночас підвищують вимоги до узгодження та уникнення дублювання.

Проблемою залишається різний зміст близьких термінів у законах, стратегіях і технічних актах. «Кіберінцидент», «подія кібербезпеки», «кібератака», «криза», «критична інформаційна інфраструктура», «державний інформаційний ресурс» і «цифрова послуга» можуть мати різні управлінські наслідки. Якщо класифікація не уніфікована, одна подія отримує різний рівень пріоритету, строки повідомлення і склад учасників. Тому термінологічна гармонізація має бути не редакційною вправою, а елементом оперативної сумісності.

Друга проблема – розрив між правовою нормою й ресурсною спроможністю. Встановлення обов'язку без фінансування, методичної підтримки, кадрів і доступних технічних рішень породжує формальне виконання. Особливо це стосується громад, комунальних установ, закладів охорони здоров'я та невеликих операторів, які мають критичні функції, але не можуть утримувати повноцінні команди кібербезпеки. Нормативний механізм повинен передбачати спільні сервіси, секторальні центри підтримки, типові рішення, державні рамкові закупівлі та можливість швидкого залучення зовнішньої експертизи.

Третя проблема пов'язана з ланцюгами постачання. Органи влади використовують хмарні сервіси, програмні бібліотеки, обладнання, системи ідентифікації та послуги адміністрування, безпека яких залежить від третіх сторін. Традиційні тендерні критерії ціни й формальної відповідності не відображають ризик прихованої залежності, припинення підтримки, компрометації оновлень або юрисдикційного доступу до даних. Отже, нормативний механізм має включати вимоги до походження компонентів, життєвого циклу підтримки, повідомлення про вразливості, програмної специфікації складових, резервного переходу й аудиту постачальника.

Інституційний механізм є системою суб'єктів, їх ролей, взаємозв'язків і фактичних спроможностей. Верховна Рада формує законодавчу основу та здійснює парламентський контроль. Президент і Рада національної безпеки і оборони визначають

стратегічні пріоритети, а Національний координаційний центр кібербезпеки забезпечує координацію й аналітичне супроводження на рівні національної безпеки. Кабінет Міністрів організовує реалізацію політики, затверджує процедури, розподіляє ресурси та координує центральні органи виконавчої влади.

Держспецзв'язку виконує ключові функції у формуванні та реалізації політики кіберзахисту, урядового зв'язку, захисту державних ресурсів і координації реагування. CERT-UA забезпечує практичну допомогу, обробку інцидентів, аналіз шкідливої активності, попередження та рекомендації. Служба безпеки України протидіє кібертероризму, кібершпигунству й загрозам державній безпеці. Національна поліція розслідує кіберзлочини, а Міністерство цифрової трансформації відповідає за цифрові послуги, реєстри, інтероперабельність та політику цифровізації. Ці ролі доповнюють одна одну, але потребують чітких критеріїв передачі випадку, спільної ситуаційної картини і єдиного процесу ескалації.

Міністерство оборони, розвідувальні органи, Національний банк, енергетичний і телекомунікаційний регулятори, інші секторальні органи формують спеціальні контури безпеки. Їх перевагою є знання технологічних і операційних особливостей сектору. Ризик полягає у появі несумісних вимог, паралельних каналів звітності та різних стандартів оцінювання. Загальнодержавна політика має встановлювати мінімальне ядро, спільну шкалу критичності й формат обміну, а секторальне регулювання – деталізувати вимоги без руйнування сумісності.

Органи місцевого самоврядування є не периферійними користувачами, а повноцінними суб'єктами безпеки цифрового простору. Вони управляють реєстрами, соціальними, комунальними, освітніми та адміністративними сервісами, а також взаємодіють із населенням під час криз. Атаки 2026 р. на місцеві й комунальні установи показали, що слабка територіальна ланка може стати точкою входу до ширших мереж. Тому інституційна модель повинна передбачати регіональних координаторів, міжмуніципальні центри компетенцій, типові плани безперервності та обов'язкові навчання.

Оператори критичної інфраструктури несуть первинну відповідальність за управління власними ризиками, але держава має визначати мінімальні вимоги, здійснювати нагляд, підтримувати обмін інформацією й забезпечувати допомогу під час масштабних інцидентів. Власники цифрових платформ контролюють значні масиви даних, алгоритмічну видимість контенту, ідентифікацію користувачів і правила доступу. Їх рішення можуть впливати на інформаційну безпеку та права мільйонів осіб. Інституційне включення платформ має здійснюватися через прозорі обов'язки, ризик-орієнтовані процедури і механізми оскарження, а не через неформальні домовленості.

Громадянське суспільство й академічна спільнота виконують функції незалежної експертизи, моніторингу прав людини, виявлення вразливостей, підвищення цифрової грамотності та суспільної комунікації. Їх участь важлива для легітимності політики, однак повинна бути інституціоналізована: публічні консультації, експертні ради, прозорі критерії відбору, захист добросовісних дослідників безпеки, грантові програми й доступ до деперсоналізованих даних. За відсутності таких каналів держава втрачає частину знань, а суспільство – можливість впливати на заходи, що обмежують цифрові права.

Міжнародні партнери, ENISA, структури ЄС, НАТО, Tallinn Mechanism та двосторонні формати надають Україні технічну, фінансову й експертну підтримку. Водночас міжнародна допомога повинна інтегруватися в національну архітектуру, а не створювати паралельні проєкти. Для кожної програми потрібно визначати власника результату, стандарт сумісності, план підтримки після завершення фінансування й порядок використання отриманих даних. Четвертий кібердіалог Україна-ЄС у 2025 р. підтвердив пріоритет NIS2, критичної інфраструктури, 5G, резерву кібербезпеки та державно-приватного партнерства [13].

Для усунення компетенційної невизначеності пропонується національна матриця компетенцій. Її рядками мають бути типи функцій: стратегування, нормотворення, оцінювання ризиків, попередження, моніторинг, технічне реагування, розслідування, кризова координація, публічна комунікація, відновлення, нагляд і аудит. Стовпцями – органи та інші суб'єкти. Для кожного перетину встановлюється роль за моделлю «відповідальний – виконавець – консультант – поінформований», правова підстава, строк дії, канал взаємодії та резервний суб'єкт. Матриця має бути затверджена урядом і регулярно переглядатися.

Другим інструментом є паспорт механізму державного управління. Він повинен містити: проблему і захищувану публічну цінність; мету; правові підстави; власника механізму; учасників; цільові групи; ресурси; процедуру; дані; показники результату; ризики для прав; порядок контролю; умови перегляду. Наприклад, механізм обов'язкового повідомлення про інциденти не може оцінюватися кількістю повідомлень. Потрібно визначати повноту, своєчасність, якість класифікації, подальше використання інформації й зниження повторюваних уразливостей.

Третім інструментом є ієрархія профілів безпеки. Базовий профіль встановлює мінімальні вимоги для всіх суб'єктів: інвентаризацію активів, управління доступом, резервне копіювання,

оновлення, журналювання, реагування, навчання персоналу і повідомлення. Секторальний профіль додає вимоги, зумовлені конкретними технологічними процесами. Профіль критичної функції визначає допустимий час переривання, резервні сценарії та посилений нагляд. Така ієрархія дозволяє гармонізувати регулювання з NIS2 і водночас врахувати українські воєнні ризики.

Четвертим інструментом має стати обов'язкове комплексне оцінювання впливу проєктів нормативних актів і цифрових систем. Окрім фінансового та регуляторного аналізу, необхідно оцінювати кіберризики, залежності від постачальників, вплив на персональні дані, права людини, доступність, конкуренцію та операційну стійкість. Для високоризикових алгоритмічних систем потрібні людський нагляд, тестування упередженості, журналювання та механізм оскарження. Така процедура запобігатиме ситуації, коли безпекове рішення створює більшу системну або правозахисну шкоду, ніж ризик, на який воно спрямоване.

П'ятим інструментом є єдиний реєстр кіберінцидентів і значущих подій з багаторівневим доступом. Він не повинен бути відкритою базою технічних уразливостей. Його завдання – забезпечити спільну статистику, уніфіковану таксономію, аналіз тенденцій, виявлення повторюваних векторів, контроль строків та оцінювання результативності. Доступ має залежати від ролі й чутливості даних, а деперсоналізовані аналітичні зрізи – надаватися дослідникам і суспільству. Закон 2025 р. створив правові передумови для такого обміну, але управлінський дизайн має забезпечити якість і довіру [3].

Шостим інструментом є регулярний стратегічний перегляд. Стратегія не повинна чекати завершення формального строку, якщо змінилися загрози, технології або міжнародні зобов'язання. Доцільно проводити щорічну оцінку реалізації цілей, а кожні два роки – незалежний огляд архітектури управління. Звіт Держспецзв'язку про виконання плану Стратегії кібербезпеки у 2025 р. засвідчив загальний рівень реалізації заходів 86%, що є позитивним сигналом, але відсоток виконаних заходів має доповнюватися оцінкою реального зниження ризику й стійкості послуг.

Сьомим інструментом є персональна управлінська відповідальність керівників. NIS2 прямо посилює роль керівних органів в ухваленні й контролі заходів кібербезпеки [11]. В українській системі доцільно встановити обов'язок затверджувати профіль ризику, план безперервності, результати навчань і звіт про істотні інциденти на рівні керівника установи або оператора. Водночас відповідальність має бути справедливою: керівник не може відповідати за невиконання вимог, якщо держава не встановила зрозумілий стандарт або не забезпечила необхідний ресурс.

Восьмим інструментом є незалежний контроль і судовий захист. Безпекові повноваження, пов'язані з доступом до даних, обмеженням сервісів чи контенту, мають супроводжуватися документуванням підстав, строками, аудитом і можливістю оскарження. Участь парламентського контролю, омбудсмана, органу із захисту персональних даних, судів і громадських експертів створює систему стримувань. Такий контроль не послаблює кібербезпеку, а підвищує легітимність, якість рішень і готовність приватних суб'єктів до співпраці.

Загалом інституційна результативність визначається не кількістю органів та актів, а чіткістю ролей, швидкістю обміну, сумісністю процедур, наявністю ресурсів і здатністю навчатися. Європейська Комісія у звіті 2025 р. відзначила прогрес української цифрової трансформації й кібербезпеки, але наголосила на необхідності подальшої імплементації NIS2 та суміжного acquis [12]. Це означає, що нормативна гармонізація повинна супроводжуватися інституційною конвергенцією: спільними стандартами, незалежним наглядом, управлінською відповідальністю і доказовою оцінкою результатів.

Висновки.

1. Нормативно-правовий механізм безпеки цифрового простору є системою цілей, повноважень, процедур, стандартів, гарантій і відповідальності; його якість визначається горизонтальною узгодженістю різних політик, а не лише повнотою законодавчого переліку.

2. Реформа 2025 р. створила правові передумови для єдиної національної системи обміну інформацією про кіберінциденти та ризик-орієнтованого захисту, однак потребує сумісних класифікаторів, процедур, цифрових каналів і належної ресурсної підтримки.

3. Інституційна архітектура України охоплює державних, місцевих, приватних, громадських і міжнародних суб'єктів. Її слабкими місцями є перетини компетенцій, нерівномірність секторальної й територіальної спроможності, фрагментація звітності та недостатнє врахування ризиків ланцюгів постачання.

4. Для узгодження механізмів запропоновано національну матрицю компетенцій, паспорти механізмів, ієрархію базових і секторальних профілів, комплексне оцінювання впливу, єдиний реєстр інцидентів, регулярний стратегічний перегляд і персональну відповідальність керівників.

5. Наближення до NIS2 та інших актів ЄС має здійснюватися не як формальне перенесення норм, а як інституційна конвергенція, що поєднує управління ризиками, нагляд, захист прав, державно-приватну взаємодію та доказову оцінку результативності.

Бібліографічний список:

1. Закон України «Конституція України» від 28.06.1996 № 254к/96-ВР (Відомості Верховної Ради України (ВВР), 1996, № 30, ст. 141). Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text
2. Закон України «Про основні засади забезпечення кібербезпеки України» від 05.10.2017 № 2163-VIII (Відомості Верховної Ради (ВВР), 2017, № 45, ст. 403). Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text
3. Закон України «Про внесення змін до деяких законів України щодо захисту інформації та кіберзахисту державних інформаційних ресурсів, об'єктів критичної інформаційної інфраструктури» від 27.03.2025 № 4336-IX (Відомості Верховної Ради (ВВР), 2025, № 35, ст. 134). Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/4336-20#Text
4. Закон України «Про критичну інфраструктуру» від 16.11.2021 № 1882-IX (Відомості Верховної Ради (ВВР), 2023, № 5, ст. 13). Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text
5. Постанова Кабінету Міністрів України «Про затвердження Положення про організаційно-технічну модель кіберзахисту» від 29.12.2021 № 1426. Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/1426-2021-%D0%BF#Text
6. Постанова Кабінету Міністрів України «Деякі питання реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі» від 04.04.2023 № 299. Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/299-2023-%D0%BF#Text
7. Розпорядження Кабінету Міністрів України «Про затвердження плану заходів на 2025 рік з реалізації Стратегії кібербезпеки України» від 07.03.2025 № 204-р. Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/204-2025-%D1%80#Text
8. Постанова Кабінету Міністрів України «Про затвердження вимог щодо управління ризиками безпеки на об'єктах критичної інфраструктури I категорії критичності» від 01.04.2025 № 367. Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/367-2025-%D0%BF#Text
9. Наказ Міністерства енергетики України «Про затвердження Вимог з кіберзахисту паливно-енергетичного сектору критичної інфраструктури» від 07.10.2025 № 403. Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/z1599-25#Text
10. Наказ Адміністрації державної служби спеціального зв'язку та захисту інформації України «Про затвердження Змін до Порядку оцінки стану захищеності державних інформаційних ресурсів в інформаційних, електронних комунікаційних та інформаційно-комунікаційних системах» від 06.04.2026 № 257. Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/z0544-26#Text
11. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) № 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance): Document 32022L2555. European Union. URL: https://eur-lex.europa.eu/eli/dir/2022/2555/oj
12. Ukraine Report 2025. Brussels, 4.11.2025. 111 p. European Commission. URL: https://enlargement.ec.europa.eu/ukraine-report-2025_en
13. EU and Ukraine deepen cooperation on cyber security at 4th Cyber Dialogue. 20 October 2025. European Commission. URL: https://enlargement.ec.europa.eu/news/eu-and-ukraine-deepen-cooperation-cyber-security-4th-cyber-dialogue-2025-10-20_en
14. Крушеніцький В.С. Органи публічної влади як суб'єкти формування та реалізації політики національної безпеки в інформаційному просторі. *Наукові записки. Серія: Право.* 2024. № 17. С. 252–256. DOI: https://doi.org/10.36550/2522-9230-2024-17-252-256
15. Галушко С.П. Модель функціонування механізмів публічного управління у сфері національної безпеки в умовах цифровізації. *Вісник Національного університету цивільного захисту України (Серія «Державне управління»).* 2024. Випуск 2 (21). DOI: https://doi.org/10.52363/2414-5866-2024-2-11

References:

1. Zakon Ukrainy "Konstytutsiia Ukrainy" vid 28.06.1996 № 254k/96-VR (Vidomosti Verkhovnoi Rady Ukrainy (VVR), 1996, № 30, st. 141). Verkhovna Rada Ukrainy. Available at: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text
2. Zakon Ukrainy "Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy" vid 05.10.2017 № 2163-VIII (Vidomosti Verkhovnoi Rady (VVR), 2017, № 45, st. 403). Verkhovna Rada Ukrainy. Available at: https://zakon.rada.gov.ua/laws/show/2163-19#Text
3. Zakon Ukrainy "Pro vnesennia zmin do deiakykh zakoniv Ukrainy shchodo zakhystu informatsii ta kiberzakhystu derzhavnykh informatsiinykh resursiv, obiektiv krytychnoi informatsiinoi infrastruktury" vid 27.03.2025 № 4336-IX (Vidomosti Verkhovnoi Rady (VVR), 2025, № 35, st. 134). Verkhovna Rada Ukrainy. Available at: https://zakon.rada.gov.ua/laws/show/4336-20#Text
4. Zakon Ukrainy "Pro krytychnu infrastrukturu" vid 16.11.2021 № 1882-IX (Vidomosti Verkhovnoi Rady (VVR), 2023, № 5, st. 13). Verkhovna Rada Ukrainy. Available at: https://zakon.rada.gov.ua/laws/show/1882-20#Text

5. Postanova Kabinetu Ministriv Ukrainy "Pro zatverdzhennia Polozhennia pro orhanizatsiino-tekhnichnu model kiberzakhystu" vid 29.12.2021 № 1426. Verkhovna Rada Ukrainy. Available at: https://zakon.rada.gov.ua/laws/show/1426-2021-%D0%BF#Text
6. Postanova Kabinetu Ministriv Ukrainy "Deiaki pytannia reahuvannia subiektamy zabezpechennia kiberbezpeky na rizni vydy podii u kiberprostori" vid 04.04.2023 № 299. Verkhovna Rada Ukrainy. Available at: https://zakon.rada.gov.ua/laws/show/299-2023-%D0%BF#Text
7. Rozporiadzhennia Kabinetu Ministriv Ukrainy "Pro zatverdzhennia planu zakhodiv na 2025 rik z realizatsii Stratehii kiberbezpeky Ukrainy" vid 07.03.2025 № 204-r. Verkhovna Rada Ukrainy. Available at: https://zakon.rada.gov.ua/laws/show/204-2025-%D1%80#Text
8. Postanova Kabinetu Ministriv Ukrainy "Pro zatverdzhennia vymoh shchodo upravlinnia ryzykamy bezpeky na obiektakh krytychnoi infrastruktury I katehorii krytychnosti" vid 01.04.2025 № 367. Verkhovna Rada Ukrainy. Available at: https://zakon.rada.gov.ua/laws/show/367-2025-%D0%BF#Text
9. Nakaz Ministerstva enerhetyky Ukrainy "Pro zatverdzhennia Vymoh z kiberzakhystu palyvno-enerhetychnoho sektoru krytychnoi infrastruktury" vid 07.10.2025 № 403. Verkhovna Rada Ukrainy. Available at: https://zakon.rada.gov.ua/laws/show/z1599-25#Text
10. Nakaz Administratsii derzhavnoi sluzhby spetsialnoho zviazku ta zakhystu informatsii Ukrainy "Pro zatverdzhennia Zmin do Poriadku otsinky stanu zakhyshchenosti derzhavnykh informatsiinykh resursiv v informatsiinykh, elektronnykh komunikatsiinykh ta informatsiino-komunikatsiinykh systemakh" vid 06.04.2026 № 257. Verkhovna Rada Ukrainy. Available at: https://zakon.rada.gov.ua/laws/show/z0544-26#Text
11. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) № 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance): Document 32022L2555. European Union. Available at: https://eur-lex.europa.eu/eli/dir/2022/2555/oj
12. Ukraine Report 2025. Brussels, 4.11.2025. 111 p. European Commission. Available at: https://enlargement.ec.europa.eu/ukraine-report-2025_en
13. EU and Ukraine deepen cooperation on cyber security at 4th Cyber Dialogue. 20 October 2025. European Commission. Available at: https://enlargement.ec.europa.eu/news/eu-and-ukraine-deepen-cooperation-cyber-security-4th-cyber-dialogue-2025-10-20_en
14. Krushenitskyi V. (2024). Orhany publichnoi vlady yak subiekty formuvannia ta realizatsii polityky natsionalnoi bezpeky v informatsiinomu prostori [Public authority bodies as entities of forming and implementing national security policy in the information space]. *Naukovi zapysky. Seriia: Pravo – Scientific notes. Series: Law.* № 17. S. 252–256. DOI: https://doi.org/10.36550/2522-9230-2024-17-252-256
15. Halushko S.P. (2024). Model funktsionuvannia mekhanizmiv publichnoho upravlinnia u sferi natsionalnoi bezpeky v umovakh tsyfrovizatsii. *Visnyk Natsionalnoho universytetu tsyvilnoho zakhystu Ukrainy (Seriia "Derzhavne upravlinnia") – Bulletin of National University of Civil Protection of Ukraine (State Management series).* Vypusk 2 (21). DOI: https://doi.org/10.52363/2414-5866-2024-2-11

LEGAL AND INSTITUTIONAL MECHANISMS OF PUBLIC ADMINISTRATION OF UKRAINE'S DIGITAL-SPACE SECURITY

Valerii Zahoruiko
Postgraduate Student
National University of Civil Protection of Ukraine

Summary. The article provides a comprehensive analysis of the legal and institutional mechanisms of public administration of Ukraine's digital-space security as of 26 July 2026. The legal mechanism is viewed not merely as a body of legislation, but as a system for defining objectives, powers, procedures, standards, safeguards, responsibility and accountability. The institutional mechanism is examined through the interaction of Parliament, the President, the National Security and Defence Council, the National Cybersecurity Coordination Centre, the Cabinet of Ministers, the State Service of Special Communications and Information Protection, CERT-UA, the Security Service, Cyber Police, the Ministry of Digital Transformation, sectoral regulators, local authorities, critical-infrastructure operators, digital platforms and civil society. The 2025 legislative reform created preconditions for moving from fragmented departmental protection to a unified national incident-response and information-sharing system based on risk management. However, terminology remains inconsistent, mandates partly overlap, sectoral and territorial capacity is uneven, information systems are insufficiently integrated, supply-chain dependence remains high, and alignment with the NIS2 Directive, digital-services rules and modern personal-data protection standards is

incomplete. The author proposes an alignment model comprising a national competence matrix, a passport for each public-administration mechanism, a hierarchy of baseline and sector-specific security profiles, mandatory regulatory, human-rights and technological impact assessment, a unified incident register with differentiated access, regular data-driven strategic review, managerial accountability and independent oversight. Institutional effectiveness is shown to depend not on the number of public bodies, but on clarity of roles, speed of coordination, procedural interoperability and the ability to convert risk information into timely decisions.

Keywords: legal mechanism, institutional mechanism, public administration, digital-space security, cybersecurity, critical infrastructure, NIS2, inter-agency coordination.

Дата надходження статті: 20.08.2026
Дата прийняття статті до публікації: 23.09.2026
Дата публікації статті: 03.11.2026