УДК 351.862.4

О. І. Урсол

РОЗВИТОК ДЕМОКРАТИЧНОГО ЦИВІЛЬНОГО КОНТРОЛЮ У СФЕРІ ПУБЛІЧНОГО УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ КРИТИЧНО ВАЖЛИВОЇ ІНФРАСТРУКТУРИ УКРАЇНИ

Обґрунтовано актуальність забезпечення інформаційної безпеки критично важливої інфраструктури України в умовах повномасштабної збройної агресії та зростання кіберзагроз, з акцентом на необхідності поєднання ефективності безпекової політики з дотриманням демократичних принципів. Розкрито сутність і значення демократичного цивільного контролю як ключового механізму забезпечення прозорості, підзвітності та законності діяльності суб'єктів сектору безпеки і оборони. Визначено основні напрями розвитку системи цивільного контролю, зокрема вдосконалення нормативно-правової бази, формування інституційної спроможності, розбудова організаційного складника та посилення суспільних елементів. Висновлено, що формування ефективної системи демократичного цивільного контролю є важливою передумовою зміцнення національної безпеки, підвищення стійкості держави і забезпечення її європейської та євроатлантичної інтеграції. Окреслено перспективи подальших досліджень.

Ключові слова: *критична інфраструктура, публічне управління та адміністрування, демократичний цивільний контроль, сектор безпеки і оборони, кризові ситуації, державна безпека, захист об'єктів критичної інфраструктури.*

Постановка проблеми. Актуальність дослідження публічного управління у сфері інформаційної безпеки критично важливої інфраструктури України визначається посиленням значення інформаційного простору як ключового чинника національної безпеки в умовах гібридних загроз і цифровізації. Об'єкти критичної інфраструктури, зокрема енергетика, транспорт, зв'язок, фінансова та медична сфери, дедалі більше залежать від інформаційно-комунікаційних технологій. Водночас така залежність не лише підвищує ефективність їх функціонування, а й формує нові ризики, пов'язані з кіберзагрозами, інформаційними атаками та іншими деструктивними впливами.

В умовах повномасштабної збройної агресії проти України суттєво зросла кількість й інтенсивність кібератак на державні інформаційні ресурси, системи управління та об'єкти критичної інфраструктури, що зумовлює необхідність формування ефективної системи публічного управління інформаційною безпекою. У зв'язку із цим особливого значення набуває забезпечення безперервності функціонування критично важливих систем та належного захисту інформаційних ресурсів. Водночас пріоритетним є підвищення стійкості до кіберзагроз і забезпечення своєчасного реагування на інциденти.

У розрізі зазначеного не менш важливого значення набуває дослідження розвитку демократичного цивільного контролю у сфері публічного управління інформаційною безпекою критично важливої інфраструктури України, яка зумовлена необхідністю забезпечення балансу між ефективністю безпекових заходів і дотриманням демократичних принципів, прозорості та підзвітності влади. Критично важлива інфраструктура, яка функціонує на основі складних інформаційно-комунікаційних систем, потребує не лише технічного захисту, а й ефективних механізмів демократичного нагляду, що забезпечують законність, обґрунтованість та контрольованість управлінських рішень. У цьому контексті важливим є залучення інститутів громадянського суспільства, незалежних експертів та парламентського контролю до формування і реалізації державної політики у сфері інформаційної безпеки.

Додаткової актуальності дослідженню надає курс України на європейську та євроатлантичну інтеграцію, що передбачає запровадження принципів належного врядування, верховенства права та цивільного контролю над сектором безпеки. Це потребує вдосконалення нормативно-правової бази, розвитку інституційних механізмів підзвітності, прозорості та ефективної взаємодії між державою, приватним сектором і громадськістю. Отже, розвиток демократичного цивільного контролю є необхідною умовою підвищення стійкості системи інформаційної безпеки, зміцнення довіри суспільства та забезпечення національної безпеки України в умовах сучасних викликів.

Аналіз останніх досліджень і публікацій. Проблематика розвитку демократичного цивільного контролю у сфері публічного управління інформаційною безпекою критично важливої інфраструктури України є міждисциплінарною, тому її досліджували представники різних наукових напрямів – публічного управління, права, національної безпеки, кібербезпеки та економіки.

Стосовно різнопланової проблематики захисту критичної інфраструктури проведено достатню кількість досліджень. Зокрема, О. І. Яременко та Я. І. Страхніцький дослідили теоретичні підходи до визначення дефініції критичної інфраструктури як об'єкту державного управління [1]. Актуальні проблеми та шляхи їх вирішення з питань захисту національної критичної інформаційної інфраструктури вивчив Д. С. Мельник [2]. Дисертаційну роботу з адміністративно-правового регулювання державної системи захисту критичної інфраструктури України виконав С. С. Теленик [3]. Теоретико-правові основи забезпечення інформаційної безпеки України розробив О. Д. Довгань [4]. Науковці С. Г. Гордієнко та І. М. Доронін обґрунтували інформаційно-правові аспекти захисту критичної інфраструктури України [5]. Дослідники А. В. Ільєнко, В. А. Телющенко та О. В. Дубчак визначили сучасні кіберзагрози критичної інфраструктури України та світу [6]. На вдосконаленні політики безпеки інформаційних систем об'єктів критичної інфраструктури України на основі концепції ZERO TRUST закцентував увагу О. С. Трофімов [7]. Безпековий вимір критичної інфраструктури з погляду економіки вивчив О. І. Барановський [8].

Дослідженню проблемних питань демократичного цивільного контролю у сфері функціонування складових сектору безпеки і оборони приділено увагу численною науковою спільнотою. Поняття і процедури здійснення громадського контролю за діяльністю Національної поліції як суб'єкта сектору безпеки і оборони досліджено В. В. Безегою [9]. Науковиця М. В. Сіцінська вивчала елементи громадського контролю в системі демократичного цивільного контролю над сектором безпеки і оборони [10], а також питання раціональності громадського контролю за діяльністю органів державної влади у сфері безпеки і оборони [11]. Дослідники А. В. Чуб та Є. М. Найдьон обґрунтували питання розвитку демократичного цивільного контролю за діяльністю системи органів сектору безпеки і оборони України.

При цьому доречно зауважити, що вивченню саме проблемних питань демократичного цивільного контролю у сфері публічного управління інформаційною безпекою критично важливої інфраструктури України не було приділено достатньої уваги, що й актуалізувало напрям дослідження.

Метою статті є дослідження демократичного цивільного контролю у сфері публічного управління інформаційною безпекою критично важливої інфраструктури України, а також обґрунтування пропозицій подальшого розвитку цієї актуальної проблематики.

Виклад основного матеріалу. В умовах повномасштабної збройної агресії та зростання кіберзагроз держава змушена посилювати контроль і регулювання у сфері інформаційної безпеки, що водночас актуалізує ризики надмірної централізації, обмеження прав і свобод громадян та зниження рівня суспільної довіри.

Як підкреслює Д. С. Мельник, в Україні зберігаються суттєві проблеми у правовому регулюванні функціонування і захисту національної критичної інформаційної інфраструктури, а також недосконаліть державної політики у цій сфері, особливо в умовах підвищених ризиків диверсій, терористичних та кібератак на відповідні об'єкти. У зв'язку із цим для забезпечення належного рівня їх захисту необхідно завершити формування цілісної законодавчої бази, створити ефективну загальнодержавну систему захисту та запровадити уніфіковані підходи до забезпечення їхнього стабільного функціонування. Водночас важливим є запровадження міжнародних стандартів, розвиток державно-приватного партнерства та активізація міжнародного співробітництва у цій сфері [2, с. 13].

На думку С. Г. Гордієнка та І. М. Дороніна, інформаційно-правові аспекти захисту критичної інфраструктури свідчать про наявність низки проблем, які можна умовно поділити на дві групи. Перша група пов'язана зі складністю віднесення окремих елементів до об'єктів критичної інфраструктури, оскільки чинні законодавчі підходи переважно орієнтовані на фізичні об'єкти і недостатньо враховують специфіку інформаційної інфраструктури, інформаційних ресурсів та систем обробки даних. Друга група проблем стосується визначення організаційних заходів інформаційного захисту та обмеження доступу до інформації про такі об'єкти, адже забезпечення балансу між політикою відкритих даних і прозорістю публічного управління, доступу громадськості та потребами безпеки є складним завданням [5, с. 122].

Науковці О. І. Яременко та Я. І. Страхніцький підкреслюють, що критична інфраструктура є складовою національної інфраструктури, що зумовлює її ключове значення для забезпечення функціонування суспільства, економіки та сталого розвитку держави загалом. Проведений аналіз підходів різних країн до трактування терміна «критична інфраструктура» дає підстави стверджувати про існування пріоритетної тріади в структурі його змістовного наповнення – «людина – суспільство – держава», яка відображає об'єкти національної інфраструктури, що мають вирішальне значення для забезпечення громадянської, суспільної та державної безпеки [1, с. 80].

Як зазначають А. В. Ільєнко, В. А. Телющенко та О. В. Дубчак, одним із ключових аспектів є розвиток міжнародної співпраці й обміну інформацією між державними органами, приватним сектором та спеціалізованими організаціями, що забезпечує можливість своєчасного реагування на новітні виклики. Міждержавна взаємодія й обмін досвідом набувають важливого значення у протидії глобальним загрозам, а імплементація міжнародних стандартів, зокрема директиви NIS2, сприяє формуванню уніфікованих механізмів кіберзахисту. Окремо наголошується на необхідності підвищення рівня підготовки персоналу та впровадження чітких політик доступу до інформаційних систем, оскільки людський фактор і надалі залишається одним із найбільш вразливих елементів кібербезпеки [6, с. 162].

Отже, на основі аналізу наведених наукових досліджень можна дійти висновку, що у сфері захисту критично важливої інфраструктури на цей час для наукової спільноти становить інтерес питання взаємодії та співпраці органів влади із громадськістю. Додаткову актуальність зумовлює курс України на інтеграцію до європейського та євроатлантичного безпекового простору, що передбачає гармонізацію національного законодавства і впровадження міжнародних стандартів у сфері кібер- й інформаційної безпеки. Важливим є розвиток ефективної публічно-приватної взаємодії у зазначеній сфері. У цих умовах особливого значення набувають удосконалення координаційних механізмів публічного управління, чітке розмежування повноважень і розвиток систем моніторингу, аналізу та прогнозування загроз із залученням механізмів демократичного цивільного контролю.

Демократичний цивільний контроль у сфері безпеки і оборони є ключовою умовою функціонування правової, демократичної держави, оскільки забезпечує підзвітність, прозорість та законність діяльності силових структур. Його важливість полягає у запобіганні надмірній концентрації влади у секторі безпеки, недопущенні зловживань, порушень прав і свобод громадян, а також у формуванні довіри суспільства до державних інституцій. Через механізми парламентського, урядового, судового та громадського контролю забезпечується відповідність діяльності сил безпеки національному законодавству та демократичним принципам.

В умовах сучасних безпекових викликів, зокрема воєнної агресії та гібридних загроз, значення демократичного цивільного контролю не зменшується, а, навпаки, зростає, оскільки саме він дає змогу поєднати ефективність оборонної діяльності з дотриманням принципів верховенства права. Водночас він сприяє підвищенню якості управлінських рішень, забезпечує раціональне використання ресурсів та формує систему стримувань і противаг у секторі безпеки і оборони. Отже, демократичний цивільний контроль є не лише інструментом нагляду, а й важливим чинником зміцнення національної безпеки, стійкості держави та її євроатлантичної інтеграції.

Демократичний цивільний контроль набуває особливого значення у сфері публічного управління інформаційною безпекою критично важливої інфраструктури України. Стрімка цифровізація і зростання залежності ключових галузей, зокрема енергетики, транспорту, зв'язку та фінансової системи, від інформаційно-комунікаційних технологій посилюють вимоги до управління зазначеною сферою. У зв'язку із цим ефективне управління потребує не лише технічних і організаційних рішень, а й забезпечення належного рівня підзвітності, прозорості та контролю.

У цьому контексті демократичний цивільний контроль є важливим інструментом забезпечення законності управлінських рішень, недопущення зловживань та підвищення ефективності функціонування системи інформаційної безпеки. Він сприяє залученню громадянського суспільства, експертного середовища та приватного сектору до формування і реалізації державної політики, що дає змогу підвищити якість управління та адаптивність до сучасних загроз. Отже, розвиток публічного управління у сфері інформаційної безпеки критично важливої інфраструктури України має ґрунтуватися на поєднанні ефективних безпекових механізмів із принципами демократичного цивільного контролю, що забезпечує стійкість, відкритість та надійність державної системи безпеки.

Науковці А. В. Чуб та Є. М. Найдьон зауважують, що встановлення ефективного демократичного цивільного контролю розглядається як важливий крок до вдосконалення цивільно-військових відносин, забезпечення верховенства права та підзвітності силових структур суспільству. Це є не лише актуальною вимогою сучасності, а й необхідною умовою функціонування правової держави з розвиненим громадянським суспільством. Такий підхід відповідає стандартам держав із усталеною демократією і сприяє процесам євроатлантичної інтеграції України [12, с. 151, 152].

Згідно з чинним законодавством система цивільного контролю охоплює контроль, що здійснюється Президентом України, Верховною Радою України, Радою національної безпеки і оборони України, Кабінетом Міністрів України, іншими органами виконавчої влади та органами місцевого самоврядування, а також судовий контроль і громадський нагляд. Громадяни України реалізують право на участь у цивільному контролі через діяльність громадських об'єднань, депутатів

місцевих рад або безпосередньо шляхом звернень до Уповноваженого Верховної Ради України з прав людини чи інших державних органів відповідно до Конституції України та чинного законодавства [13].

Громадським об'єднанням, створеним і зареєстрованим у встановленому законом порядку, гарантується можливість у межах законодавства та їх статутної діяльності отримувати від державних органів інформацію щодо функціонування сектору безпеки і оборони (за винятком інформації з обмеженим доступом), проводити наукові дослідження у сфері національної безпеки і оборони та оприлюднювати їх результати, а також створювати відповідні аналітичні центри й експертні платформи. Вони мають право здійснювати громадську експертизу проєктів нормативно-правових актів, державних програм та рішень, подавати свої пропозиції до органів державної влади, а також брати участь у публічних обговореннях, парламентських слуханнях та інших формах відкритого діалогу з питань розвитку сектору безпеки і оборони, охоплюючи питання соціального і правового захисту військовослужбовців, працівників правоохоронних і розвідувальних органів, ветеранів та членів їхніх сімей [13].

Нагляд за додержанням законодавства під час реалізації заходів із захисту критичної інфраструктури здійснюється Верховною Радою України відповідно до порядку, визначеного Конституцією України. Профільні парламентські комітети, зокрема той, що опікується питаннями національної безпеки і оборони, а також комітет, до компетенції якого належать питання кібербезпеки об'єктів критичної інформаційної інфраструктури, на своїх засіданнях розглядають звіт уповноваженого органу про результати незалежного аудиту ефективності функціонування системи захисту критичної інфраструктури. За підсумками розгляду зазначеного звіту Комітет Верховної Ради України з питань національної безпеки і оборони має право ініціювати винесення відповідних питань на розгляд парламенту [14].

Право на здійснення громадського нагляду у сфері захисту критичної інфраструктури реалізується громадянами України через участь у громадських об'єднаннях, через депутатів місцевих рад, а також безпосередньо шляхом звернень до Уповноваженого Верховної Ради України з прав людини або до інших державних органів. Крім того, громадяни можуть брати участь у роботі громадських рад при органах, що формують і реалізують державну політику у цій сфері, ініціювати проведення незалежного аудиту їх діяльності, а також отримувати доступ до відкритої частини звітів щодо забезпечення захисту об'єктів критичної інфраструктури. Доступ до інформації у сфері захисту критичної інфраструктури з метою здійснення громадського нагляду може бути обмежений відповідно до рівня державної таємниці [14].

Науковець В. В. Безега визначає сутність контролю у загальному розумінні як діяльність уповноважених суб'єктів, що здійснюється на підставі законодавства і полягає у спостереженні, виявленні й фіксації недоліків у роботі підконтрольних об'єктів, а також у запобіганні та недопущенні порушень режиму законності [9, с. 98].

До елементів громадського контролю в системі демократичного цивільного контролю за діяльністю компетентних органів державної влади у сфері безпеки і оборони М. В. Сіцінська відносить вісім рівнів: терапію, маніпулювання, інформування, консультування, примирення, партнерство, делегування повноважень та безпосередньо громадський контроль. При цьому науковиця зазначає, що в українських умовах громадський контроль є найвищим рівнем суспільної участі, який реалізується переважно «знизу», на основі приватної ініціативи. Він виступає важливою формою демократичного врядування та способом залучення громадян до здійснення цивільного контролю за діяльністю сектору безпеки і оборони, а також до процесів управління суспільством і державою [10, с. 115]. Крім того, авторка зауважує, що наявний стан інститутів громадянського суспільства в Україні лише частково відповідає завданням ефективного демократичного контролю за процесами формування національної безпеки. Зареєстровані в державі громадські організації мають обмежений вплив на вироблення державної політики у сфері національної безпеки, а їхня практична діяльність нерідко використовується в інтересах окремих політичних або бізнесових проєктів [11, с. 110].

Отже, аналіз сучасної наукової думки і практичного стану функціонування механізмів демократичного цивільного контролю сферою національної безпеки України дає можливість виокремити перспективні складники розвитку демократичного цивільного контролю у сфері публічного управління інформаційною безпекою критично важливої інфраструктури України. Зазначені складники доцільно розглядати як багатовимірну систему, що поєднує нормативно-правові, інституційні, організаційні та суспільні елементи (рисунок 1). Надалі коротко розкриємо їхній зміст.

Рисунок 1 – Перспективні складники розвитку демократичного цивільного контролю у сфері публічного управління інформаційною безпекою критично важливої інфраструктури України

По-перше, ключовим напрямом є вдосконалення нормативно-правового забезпечення, яке має формувати цілісну й узгоджену основу функціонування демократичного цивільного контролю у сфері інформаційної безпеки критично важливої інфраструктури. У цьому контексті необхідним є не лише формальне оновлення законодавства, а і його системне переосмислення з огляду на сучасні виклики і загрози, що пов'язані із цифровізацією, кіберризиками та гібридними впливами. Особливої уваги потребує уточнення правових засад цивільного контролю, що передбачає деталізацію його принципів, форм та механізмів реалізації. Важливо забезпечити чітке визначення повноважень суб'єктів контролю, включно з органами державної влади, парламентськими структурами, спеціалізованими органами у сфері кібербезпеки, а також інститутами громадянського суспільства. Такий підхід сприятиме уникненню дублювання функцій, підвищенню рівня координації та забезпеченню ефективної взаємодії між усіма учасниками процесу контролю. Ключовим стратегічним напрямом є адаптація національного законодавства до європейських і євроатлантичних стандартів. Це передбачає імплементацію сучасних підходів до кіберзахисту, управління ризиками, реагування на інциденти та забезпечення стійкості критичної інфраструктури. Така гармонізація дасть змогу забезпечити узгодженість підходів до захисту критично важливих об'єктів, посилити міжнародну співпрацю та сприяти інтеграції України у спільний безпековий простір.

По-друге, важливим компонентом є розвиток інституційної спроможності, який є необхідною передумовою ефективного функціонування системи демократичного цивільного контролю у сфері інформаційної безпеки критично важливої інфраструктури. Йдеться не лише про формальне існування відповідних інституцій, а і про їхню реальну здатність здійснювати контрольні, координаційні та аналітичні функції на належному рівні. У цьому контексті особливого значення набуває посилення ролі парламентського контролю, який має забезпечувати системний нагляд за діяльністю органів сектору безпеки і оборони, формуванням та реалізацією державної політики у сфері інформаційної безпеки. Це передбачає активізацію діяльності профільних комітетів, удосконалення процедур парламентських слухань, запровадження регулярного звітування відповідних органів, а також підвищення рівня експертної підтримки народних депутатів. Важливим напрямом є створення і подальше вдосконалювання діяльності незалежних регуляторних і наглядових органів, які повинні мати достатній рівень автономії, ресурсного забезпечення та професійної компетентності. Такі інституції мають виконувати функції моніторингу, аудиту, оцінювання ризиків і реагування на порушення у сфері інформаційної безпеки, забезпечуючи при цьому баланс між державними інтересами та правами громадян.

По-третє, організаційний складник передбачає запровадження комплексного і системного підходу до здійснення контролю у сфері інформаційної безпеки критично важливої інфраструктури, який охоплює всі етапи управлінського циклу – від планування до оцінювання результатів. Такий підхід має базуватися на чітко визначених процедурах, стандартах та регламентах, що забезпечують узгодженість дій усіх суб'єктів контролю і підвищують ефективність управлінських рішень. Ключовими елементами цього складника є регулярний аудит, системний моніторинг, а також усебічне оцінювання ризиків і загроз. Оцінювання ризиків, зі свого боку, сприяє визначенню пріоритетних напрямів захисту та раціональному розподілу ресурсів. Окрему увагу варто приділити запровадженню процедур внутрішнього контролю та управління якістю, що дасть змогу підвищити дисципліну виконання рішень і забезпечити їхню відповідність визначеним цілям. Водночас важливо забезпечити прозорість процедур прийняття управлінських рішень, що сприятиме підвищенню довіри з боку суспільства і посиленню підзвітності органів влади. При цьому необхідно зберігати належний рівень конфіденційності інформації, особливо тієї, що стосується вразливостей системи безпеки чи має обмежений доступ. Баланс між відкритістю та захищеністю інформації є ключовою умовою ефективного функціонування системи контролю.

По-четверте, суспільні елементи розвитку демократичного цивільного контролю у сфері публічного управління інформаційною безпекою критично важливої інфраструктури України являють собою значущий складник забезпечення його ефективності, оскільки саме вони визначають рівень залучення громадян, довіри до державних інституцій та прозорості управлінських процесів. Передусім ідеться про активізацію участі інститутів громадянського суспільства, зокрема громадських організацій, аналітичних центрів, професійних об'єднань та незалежних експертів у формуванні й оцінюванні державної політики у сфері інформаційної безпеки. Їх залучення до публічних консультацій, експертних обговорень та розроблення нормативно-правових актів сприяє підвищенню якості управлінських рішень та врахуванню суспільних інтересів. Важливим напрямом є розвиток механізмів публічного діалогу та зворотного зв'язку між державою і суспільством. Це передбачає створення відкритих платформ для обговорення питань кібербезпеки, проведення громадських слухань, оприлюднення звітів органів влади, а також забезпечення доступу до публічної інформації в межах, що не шкодять національній безпеці. Така відкритість сприяє підзвітності органів влади та зміцненню демократичних інститутів.

Окремим аспектом є забезпечення громадського моніторингу діяльності суб'єктів сектору безпеки і оборони. Це може реалізовуватися через незалежні дослідження, аналітичні звіти, громадські експертизи та діяльність наглядових рад. Такий контроль підвищує прозорість, сприяє виявленню проблемних аспектів та стимулює вдосконалення державної політики. Не менш важливою є підтримка розвитку довіри між державою, бізнесом та суспільством. У сфері інформаційної безпеки це є особливо актуальним, оскільки значна частина критичної інфраструктури перебуває у приватній власності. Ефективна взаємодія між цими суб'єктами, що ґрунтується на принципах партнерства, відповідальності та обміну інформацією, є необхідною умовою стійкості всієї системи. Крім того, доцільно підкреслити роль засобів масової інформації та нових медіа, які виконують функцію інформування суспільства, формування громадської думки та здійснення громадського контролю. Водночас важливо забезпечити їхню відповідальність, дотримання стандартів журналістики та протидію дезінформації.

Узагальнюючи, можна стверджувати, що розвиток демократичного цивільного контролю у зазначеній сфері має базуватися на принципах прозорості, підзвітності, системності та партнерства між державою, бізнесом та громадянським суспільством, що в сукупності забезпечить належний рівень інформаційної безпеки критично важливої інфраструктури України. Комплексне вдосконалювання нормативно-правового забезпечення створює необхідні передумови для формування ефективної, прозорої та підзвітної системи демократичного цивільного контролю, яка здатна адекватно реагувати на сучасні виклики у сфері інформаційної безпеки критичної інфраструктури України. Розвиток інституційної спроможності передбачає комплексне зміцнення організаційних, функціональних та кадрових можливостей суб'єктів контролю, що загалом забезпечує ефективність демократичного цивільного контролю та підвищує рівень інформаційної безпеки держави. Організаційний складник є практичним механізмом реалізації демократичного цивільного контролю, забезпечуючи його системність, безперервність та результативність у сфері інформаційної безпеки критично важливої інфраструктури. Суспільні елементи розвитку демократичного цивільного контролю полягають у забезпеченні широкої участі громадян, відкритості та підзвітності влади, формуванні культури кібербезпеки та зміцненні партнерства між державою і суспільством, що в цілому сприяє підвищенню рівня інформаційної безпеки критично важливої інфраструктури України.

Висновки

На основі викладеного в статті можливо дійти таких висновків.

1. В умовах повномасштабної збройної агресії та зростання кіберзагроз питання забезпечення інформаційної безпеки критично важливої інфраструктури України набуває стратегічного значення, водночас актуалізуючи необхідність збереження балансу між безпекою та дотриманням демократичних принципів. Демократичний цивільний контроль є ключовим інструментом забезпечення прозорості, підзвітності та законності діяльності суб'єктів сектору безпеки і оборони, а також важливим чинником недопущення надмірної концентрації влади та порушення прав і свобод громадян. Його значення особливо зростає в умовах гібридних загроз, оскільки він забезпечує поєднання ефективності безпекової політики з принципами верховенства права.
2. Розвиток системи демократичного цивільного контролю у сфері інформаційної безпеки критично важливої інфраструктури має здійснюватися на основі комплексного підходу, який передбачає вдосконалення нормативно-правової бази, зміцнення інституційної спроможності, запровадження ефективних організаційних механізмів контролю та активізацію суспільної участі. Важливу роль при цьому відіграють гармонізація законодавства з європейськими та євроатлантичними стандартами, розвиток державно-приватного партнерства та міжнародного співробітництва, розширення участі інститутів громадянського суспільства, розвиток механізмів публічного діалогу та забезпечення належного рівня доступу до інформації за умови збереження вимог безпеки.
3. Формування ефективної системи демократичного цивільного контролю у сфері публічного управління інформаційною безпекою критично важливої інфраструктури України є необхідною передумовою зміцнення національної безпеки та підвищення стійкості держави. Така система має розвиватися на засадах системності, відкритості, підзвітності та партнерства між державою, суспільством та приватним сектором. Її запровадження сприятиме належному захисту національних інтересів і зміцненню довіри громадян до державних інституцій, а також підтримці європейського та євроатлантичного курсу України.

Подальші наукові дослідження будуть спрямовані на обґрунтування інноваційних підходів до формування державної політики інформаційної безпеки критично важливої інфраструктури України.

Перелік джерел посилання

1. Яременко О. І., Страхніцький Я. І. Теоретичні підходи до визначення дефініції критичної інфраструктури як об'єкту державного управління. *Публічне управління та митне адміністрування*. 2022. № 1. С. 76–82. DOI: https://doi.org/10.32836/2310-9653-2022-1.13.
2. Мельник Д. С. Захист національної критичної інформаційної інфраструктури: актуальні проблеми та шляхи їх вирішення. *Адміністративне право і процес*. 2022. № 3 (38). С. 5–16. DOI: https://doi.org/10.17721/2227-796X.2022.3.01.
3. Теленик С. С. Адміністративно-правове регулювання державної системи захисту критичної

інфраструктури України : дис. д-ра юрид. наук : 12.00.07. Запоріжжя, 2021. 467 с.

4. Довгань О. Д. Теоретико-правові основи забезпечення інформаційної безпеки України : автореф. дис. д-ра юрид. наук : 12.00.07. Київ, 2016. 46 с.

5. Гордієнко С. Г., Доронін І. М. Інформаційно-правові аспекти захисту критичної інфраструктури України. *Інформація і право*. 2024. № 3 (50). С. 115–123. DOI: https://doi.org/10.37750/2616-6798.2024.3(50).311678.

6. Ільєнко А. В., Телющенко В. А., Дубчак О. В. Сучасні кіберзагрози критичної інфраструктури України та світу. *Кібербезпека: освіта, наука, техніка*. 2025. № 3 (27). С. 150–164. DOI: https://doi.org/10.28925/2663-4023.2023.27.719.

7. Трофімов О. С. Вдосконалення політики безпеки інформаційних систем об'єктів критичної інфраструктури України на основі концепції ZERO TRUST. *Телекомунікаційні та інформаційні технології*. 2025. № 3 (88). С. 15–25. DOI: https://doi.org/10.31673/2412-4338.2025.038702.

8. Барановський О. І. Критична інфраструктура: безпековий вимір. *Acta Academiae Beregsasiensis. Economics*. 2025. № 1 (8). С. 13–37. DOI: https://doi.org/10.58423/2786-6742/2025-8-13-37.

9. Безега В. В. Поняття та процедури здійснення громадського контролю за діяльністю Національної поліції як суб'єкта сектору безпеки й оборони. *Науковий вісник публічного та приватного права*. 2020. Вип. 3. С. 96–101. DOI: https://doi.org/10.32844/2618-1258.2020.3.17.

10. Сіцінська М. В. Елементи громадського контролю в системі демократичного цивільного контролю над сектором безпеки і оборони. *Інвестиції: практика та досвід*. 2013. № 14. С. 112–115.

11. Сіцінська М. В. Актуальні питання раціональності громадського контролю за діяльністю органів державної влади у сфері безпеки і оборони. *Економіка та держава*. 2013. № 4. С. 108–110. URL: http://nbuv.gov.ua/UJRN/ecde_2013_4_31 (дата звернення: 15.03.2026).

12. Чуб А. В., Найдьон Є. М. Демократичний цивільний контроль за діяльністю системи органів сектору безпеки і оборони України. *Аналітично-порівняльне правознавство*. 2025. Том 1. № 4. С. 147–152. DOI: https://doi.org/10.24144/2788-6018.2025.04.1.23.

13. Про національну безпеку : Закон України від 21.06.2018 р. № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text (дата звернення: 15.03.2026).

14. Про критичну інфраструктуру : Закон України від 16.11.2021 р. № 1882-IX. URL: https://zakon.rada.gov.ua/laws/show/1882-20#Text (дата звернення: 15.03.2026).

Стаття надійшла до редакції 20.03.2026 р.
Прийнято до друку після рецензування 17.04.2026 р.
Дата публікації 29.05.2026 р.

UDC 351.862.4

O. I. Ursol

DEVELOPMENT OF DEMOCRATIC CIVILIAN CONTROL IN THE FIELD OF PUBLIC MANAGEMENT OF CRITICAL INFRASTRUCTURE INFORMATION SECURITY OF UKRAINE

The analysis shows that in the context of full-scale armed aggression and growing cyber threats, the issue of ensuring the information security of Ukraine's critical infrastructure is becoming strategically important, while at the same time actualizing the need to maintain a balance between security and compliance with democratic principles. It has been established that the existing problems of regulatory and legal regulation, institutional interaction and organizational support reduce the efficiency of the functioning of the critical infrastructure protection system, which requires their comprehensive improvement.

It has been found that democratic civilian control is a key tool for ensuring transparency, accountability and legality of the activities of security and defense sector entities, as well as an important factor in preventing excessive concentration of power and violation of the rights and freedoms of citizens. Its importance is especially important in the context of hybrid threats, as it ensures a combination of the effectiveness of security policy with the principles of the rule of law.

It is substantiated that the development of the system of democratic civilian control in the field of information security of critical infrastructure should be carried out on the basis of an integrated approach, which provides for the improvement of the regulatory framework, strengthening of institutional capacity, the

introduction of effective organizational control mechanisms and the intensification of public participation. An important role in this is played by the harmonization of legislation with European and Euro-Atlantic standards, as well as the development of public-private partnership and international cooperation.

A significant reserve for increasing the effectiveness of control is the expansion of the participation of civil society institutions, the development of mechanisms for public dialogue and ensuring an appropriate level of access to information, provided that security requirements are maintained. At the same time, the institutional structure of control needs to be further improved and its real capacity to influence the formation of state policy needs to be increased.

It is concluded that the formation of an effective system of democratic civilian control in the field of public management of information security of the critical infrastructure of Ukraine is a necessary prerequisite for strengthening national security, increasing the resilience of the state and ensuring its progress in the direction of European and Euro-Atlantic integration. Such a system should be based on the principles of consistency, openness, accountability and partnership, which together will ensure an appropriate level of protection of national interests and public trust in state institutions.

Keywords: *critical infrastructure, public administration and administration, democratic civilian control, security and defense sector, crisis situations, state security, protection of critical infrastructure facilities.*

Урсол Олексій Ігорович – аспірант кафедри публічного управління та адміністрування, Хмельницький університет управління та права імені Леоніда Юзькова

https://orcid.org/0009-0006-9847-4694