УДК 351.862.4

О. І. Урсол

ТЕОРЕТИЧНІ ОСНОВИ ФУНКЦІОНУВАННЯ І РОЗВИТКУ ПУБЛІЧНОГО УПРАВЛІННЯ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ КРИТИЧНО ВАЖЛИВОЇ ІНФРАСТРУКТУРИ УКРАЇНИ

Актуалізовано питання обґрунтування теоретичних основ функціонування і розвитку публічного управління у сфері інформаційної безпеки критично важливої інфраструктури України. Установлено, що інформаційна безпека має забезпечуватися з участю всіх внутрішніх суб'єктів інформаційних відносин і за умов ефективної взаємодії держави з громадянським суспільством, а також приватним сектором та окремими громадянами. Визначено, що на сьогодні нормативно-правова база стосовно захисту об'єктів критичної інфраструктури в Україні є слаборозвиненою. Зазначено, що актуальним залишається питання дослідження інформаційної безпеки критично важливої інфраструктури України. Доведено, що забезпечення інформаційної безпеки України є однією з найважливіших функцій держави щодо забезпечення національної безпеки.

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

Постановка проблеми. Сучасний розвиток українського суспільства дедалі частіше характеризується виникненням кризових ситуацій, що загрожують національній безпеці. Зближення світових цивілізацій та інші процеси глобалізації завжди супроводжуються збройними конфліктами. Свідченням цього є численні збройні конфлікти й терористичні акти останнього часу. На жаль, Україна не є винятком у цій серйозній проблемі. В умовах збройної агресії з боку росії об'єкти критичної інфраструктури постійно стають цілями ворожої держави.

Воєнні загрози, які спричинені агресією проти України, висувають до публічного управління нові вимоги. Це також стосується питань забезпечення безпеки критичної інфраструктури. Сьогодні головними причинами існування загроз є геополітичне положення України та відповідна слабо ефективна робота органів публічної влади щодо запобігання виникненню загроз на об'єктах критичної інфраструктури.

Отже, створення передумов для розбудови інформаційної безпеки України критично важливої інфраструктури України є ключовим завданням публічної влади держави. Інформаційна безпека має забезпечуватися з участю всіх внутрішніх суб'єктів інформаційних відносин і за умов ефективної взаємодії держави з громадянським суспільством, а також приватним сектором та окремими громадянами в інтересах ефективного розвитку інформаційної сфери і спільного захисту від загроз об'єктам критичної інфраструктури держави.

Аналіз останніх досліджень і публікацій. Проблеми функціонування і розвитку публічної політики у сфері захисту об'єктів критичної інфраструктури в Україні ґрунтовно досліджували у наукових працях відомі вітчизняні науковці і практики. Питанням криміналістичного забезпечення протидії злочинам на об'єктах критичної інфраструктури приділяли увагу О. В. Батюк, О. Ф. Кобзар, О. Г. Комісаров, Д. В. Павлов, І. Є. Євтушенко, С. А. Кузніченко, М. С. Пузирьов та інші вчені. Проблеми реагування складових сектору безпеки і оборони на загрози у сфері захисту об'єктів критичної інфраструктури вивчали у своїх працях С. В. Бєлай, В. В. Мацюк, І. М. Волков, С. М. Горєлишев, Д. В. Павлов, В. О. Євсєєв, В. Я. Покайчук, О. Д. Черкашин та інші науковці. Питання вдосконалення політики держави у сфері захисту критичної інфраструктури досліджували Д. С. Бірюков, О. П. Єрменчук, С. І. Кондратов, В. В. Бухарєв, С. О. Гнатюк, Н. А. Сєйлова, В. М. Сидоренко, М. Б. Домарацький, О. М. Суходоля, Я. О. Страхніцький та ін.

Отже, учені розглянули достатній обсяг проблематичних напрямів захисту об'єктів критичної інфраструктури. Однак питання публічного управління у сфері інформаційної безпеки критично важливої інфраструктури України на рівні держави майже не вивчалися, що й обумовило актуальність цієї статті.

Метою статті є дослідження теоретичних основ функціонування і розвитку публічного управління у сфері інформаційної безпеки критично важливої інфраструктури України, а також визначення відповідних напрямів подальшого вдосконалювання.

Виклад основного матеріалу. У попередніх дослідженнях [1, 2] автором установлено, що на сьогодні нормативно-правова база щодо захисту об'єктів критичної інфраструктури в Україні є слаборозвиненою. На цей час чинним є Закон України «Про національну безпеку України» [3], а також Закон України «Про критичну інфраструктуру» [4].

Відповідно до Закону України «Про національну безпеку» [3] національною безпекою України є захищеність державного суверенітету, територіальної цілісності, демократичного конституційного ладу та інших національних інтересів України від реальних та потенційних загроз, а національними інтересами є життєво важливі інтереси людини, суспільства і держави, реалізація яких забезпечує державний суверенітет України, її прогресивний демократичний розвиток, а також безпечні умови життєдіяльності і добробут її громадян. Цим Законом запроваджено поняття «національна система захисту критичної інфраструктури», якою є сукупність органів управління, сил та засобів центральних і місцевих органів виконавчої влади, органів місцевого самоврядування, операторів критичної інфраструктури, на які покладається формування та/або реалізація державної політики у сфері захисту критичної інфраструктури [3].

Як зазначає законодавець [4], безпекою критичної інфраструктури є стан захищеності критичної інфраструктури, за якого забезпечуються функціональність, безперервність роботи, відновлюваність, цілісність і стійкість критичної інфраструктури. Захистом критичної інфраструктури є всі види діяльності, що виконуються перед або під час створення, функціонування, відновлення і реорганізації об'єкта критичної інфраструктури, спрямовані на своєчасне виявлення, запобігання і нейтралізацію загроз безпеці об'єктів критичної інфраструктури, а також мінімізацію та ліквідацію наслідків у разі їх реалізації [4].

Розглянуті закони України є підґрунтям функціонування публічного управління у сфері інформаційної безпеки критично важливої інфраструктури. Для подальшого дослідження теоретичних основ розвитку публічного управління у сфері інформаційної безпеки критично важливої інфраструктури України доцільним є проведення більш глибокого аналізу наукових джерел за зазначеною проблематикою. Далі розглянемо деякі найбільш вдалі відповідні останні наукові напрацювання.

Науковці С. В. Бєлай та І. С. Лавров у дослідженні [5] актуалізували питання стосовно обґрунтування системи захисту об'єктів критичної інфраструктури на рівні держави. Вони проаналізували нормативно-правові акти з регулювання повноважень складових сектору безпеки і оборони України, на які покладаються формування і реалізація державної політики у сфері захисту критичної інфраструктури. Довели надзвичайно важливі роль і місце Національної гвардії України у захисті об'єктів критичної інфраструктури України. Авторами обґрунтовано напрями подальших наукових досліджень у сфері захисту інфраструктури України. Установлено, що організування безпеки критичної інфраструктури є складним процесом, який охоплює не тільки безпекові механізми, але й координаційні та управлінські аспекти. Для ефективного функціонування цієї системи потрібні висококваліфіковані фахівці з підготовки, перепідготовки та практичного досвіду [5].

Автори статті [6] визначили актуальність питання вивчення методологічних засад дослідження проблем захисту об'єктів критичної інфраструктури. Вони провели експертне опитування щодо сучасних проблемних питань у сфері захисту об'єктів критичної інфраструктури в Україні. Загалом результати експертного опитування вказують на те, що безпека об'єктів критичної інфраструктури є актуальною проблемою, потребує комплексного підходу та спільних зусиль різних структур і суб'єктів влади, зокрема постійного вдосконалювання законодавства та правової бази у сфері захисту об'єктів критичної інфраструктури. Відповіді респондентів свідчать про потребу в підвищенні кваліфікації персоналу, ефективному управлінні та координації дій між складовими сектору безпеки і оборони, активізують питання розвитку інноваційних технологій для підвищення рівня безпеки захисту об'єктів критичної інфраструктури та обґрунтовують важливість інвестицій у сучасні технології й системи безпеки, аби забезпечити відповідну захищеність об'єктів критичної інфраструктури. Крім того, авторами доведено необхідність розроблення моделей реагування на загрози об'єктам критичної інфраструктури в різних умовах: в особливий період, у мирний час. Такий підхід потребує системного і гнучкого планування та реагування на потенційні загрози незалежно від контексту. Зроблено припущення, що розроблення відповідних моделей дасть можливість підвищити ефективність заходів забезпечення безпеки об'єктів критичної інфраструктури і сприятиме готовності до різних сценаріїв кризових ситуацій [6].

Науковці О. В. Батюк та І. Є. Євтушенко проводили дослідження [7] щодо визначення значення науки криміналістики у забезпеченні протидії злочинам на об'єктах критичної інфраструктури. Вони

наголосили на теоретичному і практичному значенні науки криміналістики, а також дали визначення механізму вчинення злочинів на об'єктах критичної інфраструктури. На їхню думку, під механізмом учинення злочину на об'єкті критичної інфраструктури слід розуміти процес скоєння злочину, зокрема його спосіб і всі дії злочинця, що супроводжуються утворенням слідів матеріальних і нематеріальних, які можуть бути використані для розкриття та розслідування злочину [7].

У статті [8] викладено результати дослідження криміналістичного і службово-бойового забезпечення протидії терористичній та диверсійній загрозам на об'єктах критичної інфраструктури. Наголошено, що криміналістичне і службово-бойове забезпечення протидії терористичній та диверсійній загрозам на об'єктах критичної інфраструктури спрямоване на формування умов, що потрібні для створення оптимальної структури діяльності з протидії відповідним злочинам, її етапів, окремих дій виконавців. Зроблено висновок, що всі рівні криміналістичного і службово-бойового забезпечення протидії терористичній та диверсійній загрозам на об'єктах критичної інфраструктури за наявності принципових відмінностей за предметом здійснюваної на них діяльності й особливостями їхньої внутрішньої та зовнішньої взаємодії мають двоєдину мету: це формування правових, організаційних, науково-технічних, кадрових та інших умов постійної готовності правоохоронних органів до дій з розкриття й розслідування злочинів з використанням криміналістичних методів, засобів та рекомендацій; здійснення практичної діяльності, що має вираження у професійно грамотній, тактично вивіреній реалізації таких умов у повсякденній практиці розкриття й розслідування злочинів [8].

У своїй дисертаційній роботі [9] М. Б. Домарацький обґрунтував і розробив теоретичні засади та науково-практичні рекомендації щодо вдосконалення державного управління забезпеченням безпеки критичної інфраструктури в Україні. Він надав сутнісну характеристику критичної інфраструктури як об'єкта державного управління, описав механізми державного управління захистом об'єктів критичної інфраструктури, охарактеризував державну систему забезпечення безпеки і захисту критичної інфраструктури. У цій праці також проаналізовано досвід зарубіжних країн стосовно державного управління критичною інфраструктурою, виокремлено специфіку державного управління критичною інфраструктурою в Україні, здійснено оцінку вітчизняного нормативного й адміністративного забезпечення державного управління критичною інфраструктурою. Удосконалено державні механізми забезпечення безпеки і підвищення ефективності захисту критичної інфраструктури, виокремлено напрями розвитку системи державного управління захистом критичної інфраструктури, запропоновано підходи до вдосконалювання державної політики захисту критичної інфраструктури в Україні. Обґрунтовано, що для практичної реалізації заходів державного управління стосовно стратегічних ризиків для критичної інфраструктури мають застосовуватися системно-правовий, політичний, інформаційний, економічний та організаційно-адміністративний механізми у межах комплексного механізму державного управління критичною інфраструктурою. Крім того, запропоновано шляхи вдосконалювання державної політики захисту критичної інфраструктури в Україні. Розроблено комплекс заходів, що забезпечують реалізацію основних механізмів й етапів упровадження державної політики у сфері забезпечення безпеки автоматизованих систем управління критичної інфраструктури [9].

Дослідник Я. О. Страхніцький у дисертаційній роботі [10] запропонував вирішення наукового завдання щодо узагальнення теоретико-методологічних особливостей сучасної державної політики у сфері захисту критичної інфраструктури та теоретичного обґрунтування доктринальних поглядів у фокусі вдосконалення механізмів державного управління забезпеченням безпеки об'єктів критичної інфраструктури та генерування відповідних науково-практичних рекомендацій. Він уперше обґрунтував науково-методичний апарат комплексного застосування механізмів та процедур розроблення і здійснення стратегії забезпечення рівня захисту критичної інфраструктури в умовах сучасної геополітичної та воєнної обстановки на основі кластерного підходу, а також запровадив у науковий обіг дефінітивну експозицію «кластер резильєнтності критичної інфраструктури» та ін. [10].

У науковій статті [11] Д. С. Бірюков дослідив роль концепції захисту критичної інфраструктури в системі забезпечення національної безпеки країн ЄС. Автором надано короткий огляд етапів імплементації зазначеної концепції у нормативно-правових документах ЄС та охарактеризовано основні чинники і тенденції, що спричиняють загрози для об'єктів критичної інфраструктури у країнах ЄС. Зроблено висновок, що Україна за своїм географічним положенням є частиною енергетичного та транспортного пан-європейського простору, а отже, де-факто пов'язана з європейською критичною інфраструктурою, що відкриває можливості для діалогу з питань безпеки

критичної інфраструктури між уповноваженими органами влади України та країн європейських сусідок України [11].

Підсумовуючи проведений аналіз наукових джерел, де розглянуто проблематику питання функціонування публічного управління у сфері інформаційної безпеки критично важливої інфраструктури, можливо зазначити, що актуальним залишається питання дослідження інформаційної безпеки критично важливої інфраструктури України. Отже, доречним є подальший аналіз стану розвитку саме концептуальних і стратегічних засад функціонування і розвитку публічного управління у сфері інформаційної безпеки критично важливої інфраструктури України.

Забезпечення інформаційної безпеки України є однією з найважливіших функцій держави щодо забезпечення національної безпеки. Чинна Стратегія інформаційної безпеки України [12] визначає актуальні виклики і загрози національній безпеці України в інформаційній сфері, стратегічні цілі та завдання, спрямовані на протидію таким загрозам, захист прав осіб на інформацію та захист персональних даних. Її метою є посилення спроможностей щодо забезпечення інформаційної безпеки держави, її інформаційного простору, підтримки інформаційними засобами і заходами соціальної та політичної стабільності, оборони держави, захисту державного суверенітету, територіальної цілісності України, демократичного конституційного ладу, забезпечення прав та свобод кожного громадянина [12].

Відповідно до Стратегії інформаційної безпеки [12] інформаційними загрозами є потенційно або реально негативні явища, тенденції та чинники інформаційного впливу на людину, суспільство і державу, що застосовуються в інформаційній сфері з метою унеможливлення чи ускладнення реалізації національних інтересів та збереження національних цінностей України і можуть прямо чи опосередковано завдати шкоди інтересам держави, її національній безпеці та обороні. Основними напрямами забезпечення інформаційної безпеки України є стійкість та взаємодія, для досягнення яких необхідним є виконання таких стратегічних цілей та завдань.

Стратегічною ціллю 1 є протидія дезінформації та інформаційним операціям, насамперед держави-агресора, спрямованим, серед іншого, на ліквідацію незалежності України, повалення конституційного ладу, порушення суверенітету і територіальної цілісності держави, пропаганду війни, насильства, жорстокості, розпалювання національної, міжетнічної, расової, релігійної ворожнечі та ненависті, вчинення терористичних актів, посягання на права і свободи людини [12].

Це означає, що протидія дезінформації та інформаційним операціям, насамперед держави-агресора, які спрямовані на вчинення терористичних актів, є наразі вкрай актуальним напрямом дослідження. Крім того, поширення кіберзагроз на об'єкти критичної інфраструктури та вдосконалення інструментарію їх реалізації зумовлюють необхідність зміни стратегії і тактики протидії їм. Набувають значущості максимально швидке виявлення вразливостей і кібератак, реагування та поширення інформації про них для мінімізації можливої шкоди.

Кіберпростір разом з іншими фізичними просторами визнано одним із можливих театрів воєнних дій. Набирає сили тенденція зі створення кібервійськ, до завдань яких належить не лише забезпечення захисту критичної інфраструктури від кібератак, а й проведення превентивних наступальних операцій у кіберпросторі, що передбачає виведення з ладу критично важливих об'єктів інфраструктури противника шляхом руйнування інформаційних систем, які управляють такими об'єктами.

Наразі вдосконалено нормативне забезпечення з питань кіберзахисту об'єктів критичної інфраструктури, ухвалено порядок її визначення та загальні вимоги до її кіберзахисту. Утворено центри (підрозділи) забезпечення кібербезпеки або кіберзахисту в Державній службі спеціального зв'язку та захисту інформації України, Службі безпеки України, Національному банку України, Міністерстві інфраструктури України, Міністерстві оборони України, Збройних Силах України.

Стратегією кібербезпеки України [13] установлено, що для досягнення кіберстійкості Україна у співпраці із суб'єктами приватного сектору, академічною спільнотою та громадськістю забезпечить посилення національної кіберготовності та кіберзахисту шляхом: розроблення Національного плану реагування на кризові ситуації в кіберпросторі, який визначить механізми реагування на кібератаки загальнонаціонального масштабу щодо об'єктів критичної інфраструктури та заходи з подальшого відновлювання; упровадження ризик-орієнтованого підходу в частині заходів забезпечення кібербезпеки об'єктів критичної інфраструктури; запровадження на постійній основі оцінки стану захищеності об'єктів критичної інфраструктури та державних інформаційних ресурсів на вразливість; упровадження системи аудиту інформаційної безпеки, насамперед на об'єктах критичної інфраструктури та ін.

Відповідно до проєкту Концепції інформаційної безпеки України [14] під інформаційною

безпекою розуміється стан захищеності життєво важливих інтересів людини і громадянина, суспільства і держави, при якому запобігається завдання шкоди через неповноту, несвоєчасність і недостовірність поширюваної інформації, порушення цілісності та доступності інформації, несанкціонований обіг інформації з обмеженим доступом, а також через негативний інформаційно-психологічний вплив та умисне спричинення негативних наслідків застосування інформаційних технологій. Основною метою державної політики з питань інформаційної безпеки є захист інформаційного суверенітету, збереження духовних і культурних цінностей Українського народу, розвиток його національної самоідентичності та цивілізаційної єдності, створення в Україні розвиненого інформаційного суспільства, національного інформаційного простору, перетворення України в інформаційно розвинену державу і повноправного учасника життєдіяльності європейської та міжнародної спільноти [14].

Проаналізувавши чинні і перспективні концептуальні нормативно-правові акти [12, 13, 14], зазначимо, що у сфері забезпечення інформаційної безпеки важливо забезпечити захист людини і громадянина, суспільства та держави від інформаційних загроз, якими є потенційно або реально негативні явища, тенденції та чинники інформаційного впливу на людину, суспільство і державу, що застосовуються в інформаційній сфері з метою унеможливлення чи ускладнення реалізації національних інтересів та збереження національних цінностей України і можуть прямо або опосередковано завдати шкоди інтересам держави, її національній безпеці та обороні.

Проєктом Закону України «Про засади інформаційної безпеки України» [15] було пропоновано здійснити такий поділ загроз інформаційної сфери. Для людини і громадянина – забезпечення конституційних прав і свобод людини і громадянина на збирання, зберігання, використання та поширення інформації; право на спілкування мовою походження; недопущення несанкціонованого втручання у зміст, процеси оброблення, передачі та використання персональних даних; захищеність від негативного впливу інформаційних технологій та інформаційно-психологічного впливу. Для суспільства – збереження і примноження духовних, культурних і моральних цінностей Українського народу та громадян України усіх національностей; інформаційне забезпечення суспільно-політичної стабільності, міжетнічної і міжконфесійної злагоди та розвитку громадянського суспільства. Для держави – забезпечення інформаційного суверенітету, запобігання інформаційній агресії, експансії та інформаційній блокаді України з боку іноземних держав, організацій, груп та осіб; формування і реалізація органами державної влади та інститутами громадянського суспільства ефективної державної політики в інформаційній сфері; інформаційно-інфраструктурне забезпечення суспільно-економічного і науково-технічного розвитку та формування позитивного іміджу України; становлення і розвиток інформаційного суспільства в Україні; інтеграція України у європейський та світовий інформаційний простір [15].

Варто цілком погодитися з такою позицією і додати, що досі актуальними залишаються основні напрями державної політики з питань національної безпеки України в інформаційній сфері, які були визначені Законом України «Про основи національної безпеки» [16] (втратив чинність у 2018 р.), якими є: забезпечення інформаційного суверенітету України; удосконалення державного регулювання розвитку інформаційної сфери шляхом створення нормативно-правових та економічних передумов; активне залучення засобів масової інформації; забезпечення неухильного дотримання конституційних прав на свободу слова, доступ до інформації; вжиття комплексних заходів щодо захисту національного інформаційного простору та протидії монополізації інформаційної сфери України та ін.

Підбиваючи підсумок, зазначимо, що органи публічної влади держави у сфері забезпечення інформаційної безпеки повинні: гарантувати конституційні права і свободи людини і громадянина в інформаційній сфері; захищати інформаційний суверенітет, конституційний лад та територіальну цілісність України; здійснювати правове, науково-технічне забезпечення становлення і розвитку українського інформаційного суспільства; утверджувати загальнолюдські та національні цінності у національному інформаційному просторі, зберігати і розвивати духовні та культурні традиції українського народу; формувати вітчизняну індустрію високотехнологічних інформаційних продуктів, розробляти і впроваджувати новітні інформаційні технології та програмні продукти; на основі стимулювання вітчизняних товаровиробників формувати й оновлювати національну інформаційну інфраструктуру, національні інформаційні ресурси, продукти та послуги; забезпечувати захист персональних даних, обмежувати доступ до інформації та технічний захист інформації; розвивати міжнародне співробітництво з питань інформаційної безпеки [1, 2].

Отже, актуальність теми дослідження щодо становлення публічного управління у сфері інформаційної безпеки критично важливої інфраструктури України та напрями подальших

досліджень за цією проблематикою визначаються:

– перспективою виконання завдань органами публічної влади щодо забезпечення інформаційної безпеки об'єктів критичної інфраструктури;

– необхідністю вдосконалювання організаційно-правових засад публічного управління у сфері інформаційної безпеки критично важливої інфраструктури України;

– розбіжністю сучасних наукових підходів до формування системи захисту об'єктів критичної інфраструктури у країнах ЄС і НАТО й в Україні;

– нерозробленістю теоретико-методологічних засад функціонування органів публічного управління, а також складових сектору безпеки і оборони у сфері захисту об'єктів критичної інфраструктури України щодо забезпечення інформаційної безпеки;

– практичною значущістю державних механізмів забезпечення інформаційної безпеки критичної інфраструктури.

Висновки

На основі проведеного дослідження можливо дійти таких висновків.

1. В умовах збройної агресії росії об'єкти критичної інфраструктури постійно стають цілями ворожої держави. Воєнні загрози, які спричинені агресією проти України, висувають до публічного управління нові вимоги. Це також стосується питань забезпечення безпеки критичної інфраструктури. Створення передумов для розбудови інформаційної безпеки України критично важливої інфраструктури України є ключовим завданням публічної влади держави. Інформаційна безпека має забезпечуватися з участю всіх внутрішніх суб'єктів інформаційних відносин та за умов ефективної взаємодії держави із громадянським суспільством, а також приватним сектором та окремими громадянами в інтересах ефективного розвитку інформаційної сфери і спільного захисту від загроз об'єктам критичної інфраструктури держави.

2. На сьогодні нормативно-правова база щодо захисту об'єктів критичної інфраструктури в Україні є слаборозвиненою. Чинні закони України становлять підґрунтя для функціонування публічного управління у сфері інформаційної безпеки критично важливої інфраструктури. Для подальшого дослідження теоретичних основ розвитку публічного управління у сфері інформаційної безпеки критично важливої інфраструктури України було здійснено аналіз наукових джерел за наведеною проблематикою. Зазначено, що актуальним залишається питання дослідження інформаційної безпеки критично важливої інфраструктури України в частині концептуальних і стратегічних засад функціонування і розвитку публічного управління у сфері інформаційної безпеки критично важливої інфраструктури України.

3. Забезпечення інформаційної безпеки України є однією з найважливіших функцій держави щодо забезпечення національної безпеки. Протидія дезінформації та інформаційним операціям, насамперед держави-агресора, що спрямовані на вчинення терористичних актів, є на цей час вкрай актуальним напрямом дослідження. Крім того, поширення кіберзагроз на об'єкти критичної інфраструктури та вдосконалення інструментарію їхньої реалізації зумовлюють необхідність зміни стратегії і тактики протидії їм. Набувають значущості максимально швидке виявлення вразливостей і кібератак, реагування та поширення інформації про них для мінімізації можливої шкоди.

4. Проведений аналіз чинних і перспективних концептуальних нормативно-правових актів засвідчив, що у сфері забезпечення інформаційної безпеки важливо забезпечити захист людини і громадянина, суспільства та держави від інформаційних загроз, якими є потенційно або реально негативні явища, тенденції та чинники інформаційного впливу на людину, суспільство і державу, що застосовуються в інформаційній сфері з метою унеможливлення чи ускладнення реалізації національних інтересів та збереження національних цінностей України і можуть прямо чи опосередковано завдати шкоди інтересам держави, її національній безпеці та обороні.

Подальші наукові дослідження будуть спрямовані на вивчення методологічних засад функціонування і розвитку публічного управління у сфері інформаційної безпеки критично важливої інфраструктури України.

Перелік джерел посилання

1. Урсол О. І. Актуалізація дослідження становлення публічного управління у сфері інформаційної безпеки критично-важливої інфраструктури України. *Публічне управління в Україні: виклики сьогодення та глобальні імперативи :* зб. тез IV Міжнар. наук.-практ. конф., м. Хмельницький, 7 лют. 2025 р. Хмельницький : ХУУП імені Леоніда Юзькова, 2025. С. 138–140.

2. Урсол О. І. До питання розвитку концептуальних засад забезпечення інформаційної безпеки України. *Тези Всеукраїнської науково-практичної онлайн-конференції здобувачів вищої освіти і молодих учених, присвяченої Дню науки*, м. Житомир, 12–17 трав. 2025 р. Житомир : Житомирська політехніка, 2025. С. 748–749.

3. Про національну безпеку України : Закон України від 21.06.2018 р. № 31. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text (дата звернення: 7.05.2025).

4. 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: 7.05.2025).

5. Лавров І. С., Бєлай С. В. Теоретичні засади формування системи захисту об'єктів критичної інфраструктури України. *Честь і закон*. 2023. № 2 (85). С. 5–11.

6. Лавров І. С., Бєлай С. В. Методологічні засади вивчення проблем захисту об'єктів критичної інфрастуктури. *Безпека держави*. 2024. № 1 (3). С. 75–82.

7. Батюк О. В., Євтушенко І. Є. Значення науки криміналістики у забезпеченні протидії злочинам на об'єктах критичної інфраструктури. *Честь і закон*. 2022. № 2 (81). С. 42–47.

8. Комісаров О. Г., Батюк О. В., Павлов С. П. Криміналістичне та службово-бойове забезпечення протидії терористичній та диверсійній загрозам на об'єктах критичної інфраструктури. *Честь і закон.* 2021. № 4 (79). С. 33–39.

9. Домарацький М. Б. Державне управління забезпеченням безпеки критичної інфраструктури в Україні : дис. канд. наук з держ. упр. : 25.00.05 / Національний університет цивільного захисту України. Харків, 2022. 259 с.

10. Страхніцький Я. О. Особливості формування та реалізації державної політики у сфері захисту критичної інфраструктури : дис. д-ра філософії : 281 / Вінницький державний педагогічний університет імені Михайла Коцюбинського. Вінниця, 2024. 312 с.

11. Бірюков Д. Концепція захисту критичної інфраструктури як елемент загальноєвропейської безпекової політики. *Наукові записки*. 2019. № 6 (68). С. 106−115.

12. Про Стратегію інформаційної безпеки : Указ Президента України від 28.12.2021 р. № 685/2021. URL : https://surl.li/yefbkh (дата звернення: 7.05.2025).

13. Про Стратегію кібербезпеки України : Указ Президента України від 26.08.2021 р. № 447/2021. URL : https://surl.li/qnputy (дата звернення: 01.01.2025).

14. Концепція інформаційної безпеки України : проєкт [неофіц. текст] від 09.06.2015 р. (не набрав чинності). Офіц. сайт ОБСЄ. URL: https://surl.li/seqjoz (дата звернення: 7.05.2025).

15. Про засади інформаційної безпеки України : проєкт Закону України від 28.05.2014 р. № 4949. URL: https://surl.li/seqjoz (дата звернення: 7.05.2025).

16. Про основи національної безпеки : Закон України від 19.06.2003 р. № 964-IV (втратив чинність на підставі Закону № 2469-VIII від 21.06.2018 р.). URL: https://zakon.rada.gov.ua/laws/show/964-15#Text (дата звернення: 7.05.2025).

Стаття надійшла до редакції 10.05.2025 р.

UDC 351.862.4

O. Ursol

THEORETICAL FOUNDATIONS FOR THE FUNCTIONING AND DEVELOPMENT OF PUBLIC ADMINISTRATION IN THE FIELD OF INFORMATION SECURITY OF UKRAINE'S CRITICAL INFRASTRUCTURE

The author of the given article used it to highlight the issue of substantiating the theoretical foundations for the functioning and development of public administration in the field of information security for Ukraine's critical infrastructure. They have established that information security must be ensured through the involvement of all internal stakeholders in information relations and through effective cooperation between the state, civil society, the private sector, and individual citizens. Such collaboration is crucial for the efficient development of the information domain and the collective protection against threats to the country's critical infrastructure.

The study has determined that, at present, the regulatory and legal framework for the protection of critical infrastructure facilities in Ukraine remains underdeveloped. The researcher notes that investigating the conceptual and strategic principles of functioning and advancing public administration around They

demonstrated that safeguarding Ukraine's information security constitutes one of the most essential functions of the state in ensuring national security. Countering disinformation and information operations – primarily those orchestrated by the aggressor state and aimed at committing acts of terrorism – remains a particularly urgent research priority. Furthermore, the proliferation of cyber threats targeting critical infrastructure and the improvement of tools for their execution necessitate changes in the strategies and tactics used to counteract them. Rapid identification of cyberattacks vulnerabilities, as well as prompt response and dissemination of information about such incidents, have become increasingly significant in minimizing potential harm. Prospective directions for further research have also been identified.

Keywords: *critical infrastructure, public management and administration, 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