УДК [1:[351:004.056]](477)
DOI: https://doi.org/10.21564/2663-5704.62.310722

Прудникова Олена Вікторівна, докторка філософських наук, професорка, професорка кафедри культурології, Національний юридичний університет імені Ярослава Мудрого, м. Харків, Україна
e-mail: elenvikprud@ukr.net
ORCID ID: 0000-0003-4610-908X

ДІЯЛЬНІСТЬ ДЕРЖАВНИХ ТА НЕДЕРЖАВНИХ СУБ'ЄКТІВ У СИСТЕМІ ФУНКЦІОНУВАННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

Проаналізовано сутнісні характеристики інформаційної безпеки крізь призму діяльності державних та недержавних суб'єктів. Зазначено, що основним завданням держави є створення та підтримання інституційного механізму забезпечення інформаційної безпеки. Обґрунтовано провідну роль у функціонуванні системи інформаційної безпеки демократичних країн таких недержавних суб'єктів, як аналітичні центри та засоби масової інформації.

Ключові слова: *інформаційна безпека, державні суб'єкти інформаційної безпеки, недержавні суб'єкти інформаційної безпеки, система інформаційної безпеки, аналітичні центри, ЗМІ.*

Постановка проблеми. Інформаційна безпека в сучасних умовах є стрижневим сектором у системі забезпечення національної безпеки держав та суспільств. Її вплив на інші сегменти захисту держави становить критично важливий характер, детермінуючи їх зміцнення або, навпаки, ослаблення. У демократичних країнах, в Україні зокрема, інформаційна безпека залежить від низки інституційних та неінституційних суб'єктів аналіз діяльності яких може надати уявлення про недоліки та переваги функціонування безпекової системи в цілому. Недержавні структури у вітчизняних реаліях стали дієвими помічниками щодо захисту інформаційного простору країни, особливо в тих випадках, коли державні інституції виявляли недостатню спроможність у вирішенні актуальних завдань інформаційного спротиву. Критично важливою стала співпраця державних та недержавних суб'єктів інформаційної безпеки під час російсько-української війни.

Аналіз останніх досліджень і публікацій. Проблематика інформаційної безпеки як складної системи поєднання діяльності державних й недержавних суб'єктів знайшла відображення в низці наукових праць сучасної гуманітаристики. Зокрема, О. Олійник [1] визначив чотири базових рівні організаційно-функціональної системи забезпечення інформаційної безпеки, а К. Захаренко [2] обґрунтував методи комплексної інформаційно-безпекової діяльності держави в сучасних умовах. З точки зору В. Пашковського [3], основним призначенням держави є створення інституційного механізму інформаційної безпеки як особливого структурного складника державного механізму в царині національної безпеки. Натомість Н. Леоненко, О. Поступна [4] виокремили функції інституційного механізму забезпечення інформаційної безпеки, а О. Косиця [5] сформулював низку умов його ефективного функціонування. Такі дослідники, як А. Головка [6], П. Міненкова [7], О. Довгань [8], окреслили у своїх наукових працях переваги та недоліки діяльності аналітичних центрів як суб'єктів інформаційної безпеки. О. Панченко [9] та Д. Дубов [10] всебічно проаналізували роль ЗМІ як акторів інформаційного простору, визначаючи їх конструктивну та деструктивну роль у безпековому контексті.

Формулювання мети. У нашому дослідженні ми ставимо за мету визначити та проаналізувати основні характеристики діяльності державних та недержавних суб'єктів у сфері інформаційної безпеки.

Виклад основного матеріалу. У сучасних демократичних країнах інформаційна безпека забезпечується органічною взаємодією державних та недержавних суб'єктів, діяльність яких підпорядковано єдиній стратегічній меті – захисту національних інтересів у всіх вимірах інформаційного простору, від державного до глобального.

З точки зору О. Олійника, можна визначити такі рівні організаційно-функціональної системи забезпечення інформаційної безпеки:

І рівень – стратегічний, загальнодержавний, який включає Верховну Раду України, Президента України, Кабінет Міністрів України та полягає у прийнятті політичних рішень, законодавчого і нормативно-правового забезпечення, встановленні порядку міжнародного співробітництва та ін.;

ІІ рівень – організаційно-виконавчий, відомчо-територіальний, який включає центральні органи виконавчої влади, органи місцевого самоврядування, правоохоронні органи та органи судової влади. На вказаному рівні здійснюється організаційне і методичне забезпечення інформаційної безпеки у відповідних галузях та адміністративно-правових утвореннях, координація і контроль діяльності у сферах відповідальності державно-владних структур;

ІІІ рівень – критично важливі інфраструктури країни, до яких доцільне включення підприємств, установ, організацій, комунікацій національного

інформаційного простору та інших об'єктів, управління якими здійснюється з використанням електронно-комунікаційних засобів та інформаційних технологій;

IV рівень – рівень суб'єктів невладного характеру, до яких належать громадяни України, їх об'єднання, державні та приватні ЗМІ [1, с. 219–220].

Разом із тим системотворчим суб'єктом, що забезпечує якісні параметри інформаційної безпеки, є держава та дотичні до неї інституції. Вона формує правові та політичні рамки діяльності інших суб'єктів, що забезпечують необхідний для існування країни та суспільства рівень інформаційної безпеки.

К. Захаренко підкреслює, що комплексна інформаційно-безпекова діяльність держави повинна передбачити правові, організаційно-економічні, технологічні, політичні, а також ціннісно-культурні методи роботи, що доповнюють та увиразнюють зміст один одного. Держава через низку політичних інституцій здійснює заходи для забезпечення інформаційної безпеки та є головним агентом збереження стабільної рівноваги й упровадження прогресивних змін у перехідному суспільстві. Держава в цій сфері аналізується як така, що за різних обставин може як наближати, так і віддаляти перспективу інформаційного суспільства (перешкоджати громадській ініціативі, обмежувати творчий та інтелектуальний порив у цьому напрямку). Державні інститути визначають правові рамки інформаційного простору, але, як і будь-які інші, можуть і (не)свідомо порушувати відповідні норми в обличчі окремих державних службовців чи й цілих організацій [2, с. 16].

Можна погодитися з вищеозначеним науковцем у тому, що держава не завжди є ефективним та дієвим суб'єктом у царині інформаційної безпеки. Державні чиновники та інституції час від часу прагнуть під різними приводами контролювати, цензурувати, приховувати інформаційні потоки та повідомлення, зменшуючи рівень демократії в інформаційному просторі. Якщо така тенденція стає стійкою, то виникає пряма загроза демократичним правам та свободам громадян, створюються передумови для згортання демократії.

Для того, щоб зловживань із боку держави було якомога менше, має бути напрацьовано інституційний механізм забезпечення інформаційної безпеки, визначено чіткі правові рамки діяльності акторів інформаційного поля країни.

Як зазначає В. Пашковський, інституційний механізм інформаційної безпеки – це особливий структурний складник державного механізму, що забезпечує створення норм і правил, які регулюють взаємодію різних суб'єктів в інформаційній сфері щодо запобігання загрозам інформаційній безпеці. Оскільки інституційний механізм (від загального уявлення про інституціоналізацію як процесу визначення й закріплення в системі певних норм, правил, статусів, ролей, здатних діяти в напрямі реалізації окремих суспільних за-

вдань) є складним і багатоплановим явищем, у науковій літературі використовуються найрізноманітніші методологічні підходи до його дослідження [3, с. 70].

Загалом сутність інституційного механізму проявляється через його функції. На думку науковців, інституційний механізм виконує такі функції, які можна застосувати й до механізму забезпечення інформаційної безпеки: 1) інтеграція агентів в один інститут з метою здійснення спільної діяльності в рамках загальних статусів і норм; 2) диференціювання норм і статусів, а також суб'єктів і агентів різних інститутів, що розділяють та ігнорують їхні вимоги; регламентація взаємодії інституту і його агентів відповідно до встановлених вимог; 3) здійснення імплементації нових вимог у реальну практику; 4) забезпечення відтворення рутинних інновацій; 5) субординація і координація відносин між суб'єктами, які належать до різних інститутів; 6) інформування суб'єктів про нові норми і правила поведінки; 7) регулювання діяльності суб'єктів; 8) контроль за виконанням норм, правил і угод [4, с. 117–118].

Аналізуючи інституційний механізм у системі забезпечення інформаційної безпеки в сучасних умовах, О. Косиця доводить, що його ефективне функціонування можливе за таких умов: оновлення законодавства, а саме внесення змін до законів і положень, які регламентують діяльність суб'єктів забезпечення інформаційної безпеки, взаємоузгодження завдань і функцій із забезпечення інформаційної безпеки; встановлення механізму керівництва, контролю та нагляду у сфері забезпечення інформаційної безпеки з чітким розподілом ролей і повноважень; введення інституту відповідальності за неналежний рівень організації дотримання вимог внутрішньої інформаційної безпеки; запровадження системи загальної підготовки суб'єктів забезпечення інформаційної безпеки до виконання покладених на них завдань; активація взаємодії та інформаційного обміну між суб'єктами забезпечення інформаційної безпеки як ефективного інструменту вирішення покладених на них завдань. Дотримання вказаних умов сприятиме упровадженню та реалізації дієвої політики інформаційної безпеки як основоположного складника всіх елементів національної безпеки [5, с. 153].

Відповідно держава здійснює забезпечення інформаційної безпеки шляхом удосконалення функціонування інституційного механізму, розроблення та втілення інформаційної політики, яку спрямовано на захист національних інтересів у цій царині.

Фахівці зазначають, що ефективна реалізація стратегічних пріоритетів, основних принципів і завдань державної політики інформаційної безпеки потребує вдосконалення правових та організаційних механізмів управління

інформаційною безпекою, його відповідного інтелектуально-кадрового і ресурсного забезпечення, зокрема вдосконалення законодавства з питань національної безпеки, насамперед шляхом:

– розвитку правових засад управління національною безпекою через розроблення відповідних законів, концепцій, доктрин, стратегій і програм, зокрема антикорупційного законодавства, Національної програми протидії тероризму та екстремізму, Концепції розвитку Воєнної організації держави, Національної стратегії формування інформаційного суспільства, Доктрини інноваційного та науково-технологічного розвитку тощо;

– розроблення та упровадження національних стандартів та технічних регламентів застосування інформаційно-комунікаційних технологій, гармонізованих із відповідними європейськими стандартами, у тому числі з вимогами ратифікованої Верховною Радою України Конвенції про кіберзлочинність;

– приведення законодавства з питань охорони державної таємниці до європейських стандартів;

– розроблення та упровадження загальнодержавної системи визначення та моніторингу порогових значень показників (індикаторів), що характеризують рівень захищеності національних інтересів у різних сферах життєдіяльності та виникнення реальних загроз національній безпеці [11, с. 128].

На нашу думку, держава як основний актор у сфері інформаційної безпеки має в першу чергу дбати про інформаційний суверенітет країни, оскільки події, що передували повномасштабному вторгненню проти нашої країни, супроводжувались постійними інформаційними атаками, спрямованими на руйнування суспільної свідомості, історичної пам'яті та національних традицій Українського народу.

У цьому контексті Ю. Калиновський та Є. Мануйлов стверджують, що посягання на інформаційний суверенітет України знайшли свій прояв у потужних негативних впливах на духовну сферу вітчизняного соціуму, спробах викривити національну пам'ять, зменшити значущість національних цінностей, протиставити духовні цінності різних соціальних груп тощо [12, p. 25].

Разом із тим природно, що демократична держава залучає до вирішення проблем у сфері інформаційної безпеки інститути громадянського суспільства, що спроможні діяти ефективно, фахово на користь національних інтересів.

До недержавних суб'єктів інформаційної безпеки можна віднести: громадські організації, громадські рухи, недержавні аналітичні та наукові центри, об'єднання громадян − політичні, економічні, волонтерські, правозахисні, мережеві, культурно-просвітницькі тощо. Аналізуючи перебіг Помаранчевої революції, Революції гідності, російсько-української війни, можна дійти ви-

сновку, що в нашій країні існує нагальна необхідність інституціалізації та оновлення правового статусу діяльності громадського сектору, який став локомотивом суспільних змін і дієвим суб'єктом у сфері національної та інформаційної безпеки (діяльність «кіберармії», громадського центру «Інформаційний спротив», волонтерського інтернет-проєкту «StopFake» тощо.) [13, с. 22].

З точки зору А. Головка, особливу роль у забезпеченні інформаційної безпеки держави відіграють неурядові аналітичні центри, або так звані «мозкові центри», «фабрики думки». Так прийнято називати публічні науково-дослідні установи, що здійснюють консультування державних структур і, як правило, спеціалізуються на гуманітарній проблематиці – політиці, економіці, праві та ін. Продукція таких організацій включає в себе прикладну соціально-політичну експертизу, аналітичні дослідження, оцінку та прогнозування економічних та соціокультурних наслідків політичних рішень. Неурядовий аналітичний центр як елемент громадянського суспільства становить своєрідне ядро концентрації інтелектуального потенціалу експертів та науковців, які в змозі генерувати суспільно значущі ідеї і, за допомогою каналів зв'язку з державними інститутами, забезпечувати їх практичну реалізацію. Багато зарубіжних політологів вважають, що велика кількість цілей, які ставлять перед собою сучасні держави, зокрема в секторі безпеки, вимагають від політичного керівництва країни розширеного пошуку засобів розроблення конкурентоспроможних програм для ефективного захисту національних інтересів в інформаційній сфері [6, с. 15].

Значення недержавних аналітичних центрів полягає передусім у тому, що вони здатні надавати незаангажовану та висококваліфіковану експертну оцінку у сфері інформаційної безпеки, оскільки не фінансуються з державного бюджету та, як правило, прагнуть до залучення авторитетних фахівців у тій чи іншій сфері.

Як підкреслює П. Міненкова, недержавні аналітичні центри водночас виступають як у ролі посередників між інтелектуальним середовищем і державним апаратом, так і в ролі ефективного інструменту громадянського контролю та ініціатора публічного обговорення найбільш гострих політичних питань, що постають перед країною. «Мозкові центри» є генераторами нових ідей для владно-політичного керівництва, пропонуючи аналітичну продукцію, інноваційні рішення та механізми їх реалізації. При цьому для своїх розробок недержавні аналітичні центри використовують позабюджетні джерела фінансування, тобто держава має можливість залучити додатковий інтелектуальний ресурс без бюджетних витрат. За участі представників «мозкових центрів» виробляються найбільш важливі стратегічні документи. Експерти недержав-

них аналітичних центрів беруть участь у робочих групах із розроблення державних рішень найвищого національного рівня або входять до складу громадських експертних рад при державних органах [7, с. 52].

Водночас держава має помірковано та виважено послуговуватись результатами діяльності аналітичних центрів, не допускаючи їх надмірного впливу на систему прийняття стратегічних рішень, виключаючи безальтернативність надання окремими структурами аналітики з певних проблем.

На переконання О. Довгань, система інформаційно-аналітичних центрів в Україні в цілому заслуговує на увагу з точки зору організації інформаційної безпеки у зв'язку з тим, що продукти таких структур, створені на базі аналізу актуальних і достатньою мірою репрезентабельних масивів інформації, можуть бути впливовими, авторитетними; розробки таких центрів можуть суттєво впливати на політичну ситуацію, особливо – з використанням резонансних подій; такі матеріали за відсутності авторитетних альтернатив використовуються управлінськими структурами, таким чином впливаючи на державну політику [8, с. 118].

Також впливовими суб'єктами інформаційної безпеки є різноманітні ЗМІ, як державні, так і недержавні. Їх значущість зумовлена тим, що ЗМІ формують інформаційний порядок денний і відіграють найважливішу роль у створенні громадської думки. Цей факт визначає особливе значення ЗМІ як механізму реалізації державної інформаційної політики. Існує низка факторів, таких як, наприклад, форма фінансування, територія мовлення, політичні позиції власників ЗМІ, які визначають положення ЗМІ в медіасистемі країни і здатність їх формувати інформаційний порядок денний в інформаційному полі держави [9].

Вочевидь ЗМІ, як суб'єкти інформаційної безпеки, можуть відігравати як позитивну, так і негативну роль щодо захисту національних інтересів: з одного боку, вони можуть надавати об'єктивну, неупереджену інформацію, висвітлюючи подію як вона є, а з іншого – маніпулювати настроями громадян, свідомо змінюючи реальність на користь замовника.

З цього приводу Д. Дубов зауважує, що унікальна можливість, яку мають сучасні ЗМІ, – це конструювання реальності через контроль над порядком висвітлення подій. Головний редактор визначає, що слід висвітлювати, а що ні. Більше того, суспільство стикається з реальною можливістю глобальних маніпуляцій, коли ЗМІ «створюють» подію, якої не було. У свідомості ж людей вона стає реальною, тож може бути спонукальним мотивом подальших дій [10, с. 60].

У цьому контексті, французький філософ Ж. Бодріяр зауважував: «Про засоби інформації слід думати радше так, ніби вони перебувають на зовнішній орбіті та є різновидом генетичного коду, який керує мутацією реального в гіперреальне, точнісінько так, як інший код, мікромолекулярний, керує пере-

ходом від сфери смислу (репрезентативної) до сфери програмованого знаку (генетичної)» [14, с. 49–50].

Ураховуючи недоліки та переваги недержавних суб'єктів інформаційної безпеки, можна виокремити такі основні різновиди їх діяльності:

– участь у роботі консультативно-дорадчих органів при органах державного управління в інформаційній сфері;

– участь у публічних громадських обговореннях, що проводяться органами державного управління в інформаційній сфері;

– участь у вивченнях громадської думки, що проводяться органами державного управління в інформаційній сфері;

– направлення органам державного управління в інформаційній сфері інформаційних запитів та скарг у ході громадського контролю за їх діяльністю, а також скарг та заяв про інформаційні правопорушення у процесі громадського контролю за дотриманням законності в інформаційній сфері;

– направлення органам державного управління в інформаційній сфері заяв (клопотань) про задоволення прав та законних інтересів у цій сфері [15, с. 34].

З точки зору Л. Сіпайло та Н. Сіпайло, формами взаємодії неурядових і державних організацій щодо забезпечення інформаційної безпеки є:

– проведення загальних прес-конференцій, круглих столів, виступи в ЗМІ;

– подання один одному інформації про надання послуг для координації зусиль;

– проведення спільних акцій, нарад;

– навчання партнерів основам соціальної роботи, обмін досвідом;

– надання послуг, що доповнюють послуги, гарантовані законом;

– проведення спільних (або на замовлення) досліджень проблеми [16, с. 298].

Висновки. Інформаційна безпека як складний соціальний та інституційний феномен потребує перманентної уваги з боку як державних органів, так і структур громадянського суспільства. Основне завдання держави полягає в тому, щоб запропонувати всім суб'єктам у сфері інформаційної безпеки чіткий та прозорий інституційний механізм її забезпечення з правової, політичної, духовно-ціннісної точок зору. Саме у взаємодії державних та недержавних суб'єктів інформаційної безпеки можливе ефективне підтримання системи захисту національного інформаційного та духовно-культурного простору.

ЛІТЕРАТУРА

1. Олійник О. В. Теоретико-методологічні засади адміністративно-правового забезпечення інформаційної безпеки України : монографія. Київ : Укр. пріоритет, 2012. 400 с.

2. Захаренко К. В. Інституційний вимір інформаційної безпеки України: трансформаційні виклики, глобальні контексти, стратегічні орієнтири : автореф. дис. … д-ра політ. наук. Львів, 2021. 37 с.
3. Пашковський В. Ф. Інституційний механізм інформаційної безпеки України в умовах гібридної війни: характер та перспективи трансформацій. *Політикус :* наук. журн. 2021. Вип. 1. С. 69–78.
4. Леоненко Н. А., Поступна О. В. Інформаційна безпека України: механізми, сучасні виклики та загрози в умовах інформаційного глобалізму. *Вісник НУЦЗ України.* Серія: Державне управління. 2022. Вип. 2 (17). С. 113–120.
5. Косиця О. О. Інституціональний механізм системи інформаційної безпеки. *Порівняльно-аналітичне право*. 2016. №4. С. 150–153.
6. Головка А. А. Інститути громадянського суспільства в системі інформаційної безпеки України. *Вісник НТУУ «КПІ».* Політологія. Соціологія. Право. 2015. Вип. 3/4 (27/28). С. 13–16.
7. Міненкова П. В. Недержавні аналітичні центри в системі стратегічного політичного консультування: реалії постіндустріального суспільства. *Регіональні студії.* 2020. №20. С. 51–55.
8. Довгань О. Д. Сучасні інформаційні структури як компоненти інформаційної безпеки. *Інформація і право.* 2015. №2 (14). С. 111–120.
9. Панченко О. А. Засоби масової комунікації як платформа державної інформаційної політики. *Державне управління: удосконалення та розвиток*. 2020. №4. URL: http://www.dy.nayka.com.ua/?op=1&z=1632 (дата звернення: 28.06.2024).
10. Дубов Д. Засоби масової інформації як якісно нові суб'єкти політичних комунікацій. *Політичний менеджмент*. 2007. №1. С. 57–65.
11. Медвідь Ф. Інформаційна безпека України: виклики та загрози. *Наукові праці МАУП.* 2009. №2. С. 123–130. URL: https://nato.pu.if.ua/old/journal/2009-2/2009-2-28.pdf (дата звернення: 23.06.2024).
12. Manuilov E. M., Kalynovsky Y. Y. Information sovereignty of Ukraine: modern moral challenges and threats. *Вісник Національного юридичного університету імені Ярослава Мудрого.* Серія: Філософія. 2019. №3 (42). С. 22–34.
13. Прудникова О. В. Оптимізація діяльності недержавних суб'єктів у системі забезпечення інформаційної безпеки. *Сучасна війна: гуманітарний аспект :* зб. матеріалів VIII Міжнар. наук. конф. Харк. нац. ун-ту Повітряних Сил ім. Івана Кожедуба, 24–25 трав. 2024 р. Харків : ХНУПС ім. І. Кожедуба, 2024. С. 22–25.
14. Бодріяр Ж. Симулякри та симуляція. Київ : Вид-во Соломії Павличко «Основи», 2004. 230 с.
15. Бурило Ю. П. Участь недержавних суб'єктів у здійсненні державного управління інформаційною сферою. *Правова інформатика*. 2007. №4. С. 31–41.
16. Сіпайло Л. Г., Сіпайло Н. А. Діяльність неурядових організацій у системі забезпечення інформаційної безпеки країни. *Глобальні та національні проблеми економіки : електрон. наук. вид.* 2017. Вип. 18. С. 296–299.

REFERENCES

1. Oliinyk, O. V. (2012). Teoretyko-metodolohichni zasady administratyvno-pravovoho zabezpechennia informatsiinoi bezpeky Ukrainy: monohrafiia. Kyiv: Ukr. Priorytet [in Ukrainian].
2. Zakharenko, K. V. (2021). Instytutsiinyi vymir informatsiinoi bezpeky Ukrainy: transformatsiini vyklyky, hlobalni konteksty, stratehichni oriientyry. *Extended abstract of doctor's thesis*. Lviv [in Ukrainian].
3. Pashkovskyi, V. F. (2021). Instytutsiinyi mekhanizm informatsiinoi bezpeky Ukrainy v umovakh hibrydnoi viiny: kharakter ta perspektyvy transformatsii. *Naukovyi zhurnal «Politykus» – Scientific journal «Politicus», issue 1, 69–78* [in Ukrainian].
4. Leonenko, N. A., Postupna, O. V. (2022). Informatsiina bezpeka Ukrainy: mekhanizmy, suchasni vyklyky ta zahrozy v umovakh informatsiinoho hlobalizmu. *Visnyk NUTsZ Ukrainy. Seriia: Derzhavne upravlinnia – Bulletin of National University of Civil Defense of Ukraine: State Management series, issue 2*(17)*, 113–120* [in Ukrainian].
5. Kosytsia, O. O. (2016). Instytutsionalnyi mekhanizm systemy informatsiinoi bezpeky. *Porivnialno-analitychne pravo – Comparative and analytical law, 4, 150–153* [in Ukrainian].
6. Holovka, A. A. (2015). Instytuty hromadianskoho suspilstva v systemi informatsiinoi bezpeky Ukrainy. *Visnyk NTUU «KPI». Politolohiia. Sotsiolohiia. Pravo – Bulletin of the National Technical University of Ukraine «Kyiv Polytechnic Institute»: Political Science, Sociology, Law*, *issue 3/4* (27/28)*, 13–16* [in Ukrainian].
7. Minenkova, P. V. (2020). Nederzhavni analitychni tsentry v systemi stratehichnoho politychnoho konsultuvannia: realii postindustrialnoho suspilstva. *Rehionalni studii – Regional studios*, *20, 51–55* [in Ukrainian].
8. Dovhan, O. D. (2015). Suchasni informatsiini struktury yak komponenty informatsiinoi bezpeky. *Informatsiia i pravo – Information and law*, *2*(14)*, 111–120* [in Ukrainian].
9. Panchenko, O. A. (2020). Zasoby masovoi komunikatsii yak platforma derzhavnoi informatsiinoi polityky. *Derzhavne upravlinnia: udoskonalennia ta rozvytok – Public administration: improvement and development*, *4*. URL: http://www.dy.nayka.com.ua/?op=1&z=1632 [in Ukrainian].
10. Dubov, D. (2007). Zasoby masovoi informatsii yak yakisno novi sub'iekty politychnykh komunikatsii. *Politychnyi menedzhment – Political management*, *1, 57–65* [in Ukrainian].
11. Medvid, F. (2009). Informatsiina bezpeka Ukrainy: vyklyky ta zahrozy. *Naukovi pratsi MAUP – Scientific Works of Interregional Academy of Personnel Management*, *2, 123–130.* URL: https://nato.pu.if.ua/old/journal/2009–2/2009-2-28.pdf [in Ukrainian].
12. Manuilov, E. M., Kalynovsky, Y. Y. (2019). Information sovereignty of Ukraine: modern moral challenges and threats. *Visnyk Natsionalnoho yurydychnoho universytetu imeni Yaroslava Mudroho. Seriia: Filosofiia – The Bulletin of Yaroslav Mudryi National Law University. Series: Philosophy, 3*(42)*, 22–34.*
13. Prudnykova, O. V. (2024). Optymizatsiia diialnosti nederzhavnykh sub'iektiv u systemi zabezpechennia informatsiinoi bezpeky. *VIII Mizhnarodna naukova konferentsiia*

Kharkivskoho natsionalnoho universytetu Povitrianykh Syl imeni Ivana Kozheduba «Suchasna viina: humanitarnyi aspekt»: proceedings of Scientific and Practical Conference. Kharkiv: KhNUPS im. I. Kozheduba*. 22–25* [in Ukrainian].
14. Bodriiar, Zh. (2004). Symuliakry ta symuliatsiia. Kyiv: Vydavnytstvo Solomii Pavlychko «Osnovy» [in Ukrainian].
15. Burylo, Yu.P. (2007). Uchast nederzhavnykh sub'iektiv u zdiisnenni derzhavnoho upravlinnia informatsiinoiu sferoiu. *Pravova informatyka – Law informatics*, *4, 31–41* [in Ukrainian].
16. Sipailo, L. H., Sipailo, N. A. (2017). Diialnist neuriadovykh orhanizatsii u systemi zabezpechennia informatsiinoi bezpeky krainy. *Elektronne naukove vydannia «Hlobalni ta natsionalni problemy ekonomiky» – Electronic scientific publication «Global and National Problems of Economy», issue 18, 296–299* [in Ukrainian].

***Prudnykova Olena Victorivna**,* Doctor of Philosophy, Professor, Professor of the Department of Culturology, Yaroslav Mudryi National Law University, Kharkiv, Ukraine Asc. Prof. at Department of Philosophy, at Faculty of Humanities and Social Sciences, Ondokuz Mayıs University, Samsun, Turkey

ACTIVITIES OF STATE AND NON-STATE ENTITIES IN THE FUNCTIONING SYSTEM OF UKRAINE'S INFORMATION SECURITY

The essential characteristics of information security are analyzed through the activities of state and non-state entities. It is noted that the main task of the state is to create and maintain an institutional mechanism for ensuring information security. The leading role of non-state entities such as analytical centers and mass media in the functioning of the information security system of democratic countries is substantiated.

Keywords: information security, state entities of information security, non-state entities of information security, information security system, analytical centers, mass media.