МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЗАПОРІЗЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ

Недохлєбов Іван Іванович

УДК 342.9.351.4:746(477)(043)

ІНФОРМАЦІЙНА БЕЗПЕКА УКРАЇНИ В УМОВАХ СУЧАСНИХ ЗАГРОЗ: ОРГАНІЗАЦІЙНО-ПРАВОВІ АСПЕКТИ

12.00.07 – адміністративне право і процес;
фінансове право; інформаційне право

Автореферат
дисертації на здобуття наукового ступеня
кандидата юридичних наук

Запоріжжя – 2024

Дисертацією є рукопис.
Роботу виконано в Запорізькому національному університеті
Міністерства освіти і науки України.

Науковий керівник –
доктор юридичних наук, старший дослідник
Рувін Олександр Григорович,
Київський науково-дослідний інститут судових експертиз,
директор.

Офіційні опоненти:
доктор юридичних наук, професор
Тильчик Ольга Віталіївна,
Державний податковий університет,
професор кафедри кримінального судочинства
та аналітичної діяльності;

доктор юридичних наук, доцент
Бараненко Дмитро Володимирович,
Національний університет кораблебудування
імені адмірала Макарова,
завідувач кафедри теорії і історії держави і права.

Захист відбудеться «15» червня 2024 року о «13^{00}» годині на засіданні спеціалізованої вченої ради Д 17.051.07 Запорізького національного університету за адресою: 69600, м. Запоріжжя, пр. Соборний, 74, корп. 5, кім. 202-б.

З дисертацією можна ознайомитися в науковій бібліотеці Запорізького національного університету (м. Запоріжжя, вул. Жуковського, 66-а, корп. 2, кім. 101).

Автореферат розісланий «15» травня 2024 року.

Вчений секретар
спеціалізованої вченої ради Ш.Н. Гаджиєва

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми. Зростання ролі інформації в житті суспільства актуалізувало проблему забезпечення інформаційної безпеки, яка донедавна навіть не позиціонувалася як окремий складник національної безпеки. У 2014 році Україна зіткнулася із зовнішньою агресією та була змушена протистояти зовнішнім інформаційним загрозам, зокрема інформаційному тероризму й російській пропаганді, протидіяти мові ненависті, яку держава-агресор навмисно поширювала на тимчасово окупованих територіях. Ситуація ускладнилася після початку повномасштабного вторгнення в лютому 2022 року, що зумовлено появою новоокупованих територій та застосуванням окупантами більш радикальних способів формування ненависті до України в населення зазначених територій. Також стрімко зросла кількість кібератак із боку держави-агресора, що поставило під загрозу інформаційні ресурси, державні реєстри та бази персональних даних. Необхідно говорити також про активізацію внутрішніх загроз, зокрема окремі інформаційні кампанії проти влади, які фінансуються державою-агресором. В умовах воєнного стану це досить небезпечна тенденція, яка негативно позначається на всьому секторі безпеки та оборони. Інформаційна безпека України виявилася неготовою до таких загроз, що зумовлено декількома чинниками: відсутністю в органів влади досвіду забезпечення інформаційної безпеки в умовах збройного конфлікту; недосконалістю та неадаптованістю засобів правового регулювання питань протидії внутрішнім і зовнішнім загрозам в інформаційній сфері; нерозвиненістю державно-приватного партнерства в безпековій сфері, зокрема недостатністю залучення інститутів громадянського суспільства до реалізації державної інформаційної політики; недостатньою інтегрованістю України в європейський інформаційний простір. З огляду на зазначене дослідження організаційно-правових аспектів забезпечення інформаційної безпеки в умовах сучасних загроз є актуальним напрямом наукового пошуку.

Сутність категорії «інформаційна безпека» та адміністративно-правові аспекти її забезпечення в різні часи досліджували М.В. Баран, І.Р. Боднар, М.Т. Гаврильців, О.Д. Довгань, О.Ю. Дубинський, К.В. Захарченко, О.І. Зозуля, О.О. Золотар, Р.А. Калюжний, Б.А. Кормич, Н.А. Ліпкан, О.В. Логінов, С.І. Маркін, В.Я. Настюк, А.Ю. Нашинець-Наумова, І.В. Олефір, О.В. Олійник, Т.С. Перун, О.О. Тихомиров, Т.Ю. Ткачук, М.О. Шевчук, П.О. Яковлєв, О.Г. Ярема та інші вітчизняні науковці. Особливо варто виділити фундаментальні наукові праці Б.А. Кормича «Організаційно-правові засади політики інформаційної безпеки України» (2003 року), О.В. Логінова «Адміністративно-правове забезпечення інформаційної безпеки органів виконавчої влади» (2005 року), О.Д. Довганя «Забезпечення інформаційної безпеки в контексті глобалізації: теоретико-правові та організаційні аспекти» (2015 року), А.Ю. Нашинець-Наумової «Інформаційна безпека: питання правового регулювання» (2017 року), М.В. Баран «Адміністративно-правове забезпечення інформаційної безпеки в Україні» (2022 року). Зазначені

та інші вчені зробили вагомий внесок у розвиток науки інформаційного та адміністративного права. Однак вони розглядали категорію «інформаційна безпека» без урахування сучасних загроз і викликів, які постали перед Україною після початку повномасштабного вторгнення держави-агресора, що не дало змогу сформувати чітке бачення шляхів запобігання та протидії таким загрозам. До того ж правозастосовна практика виявила чимало прогалин, пов'язаних із відсутністю нормативно-правового визначення деяких категорій інформаційної безпеки та її окремих рівнів. Наведене не лише зумовило вибір теми дисертації, а й свідчить про актуальність її наукових положень як для теоретичного аналізу змісту поняття «інформаційна безпека», так і для визначення нових методологічних підходів до формування організаційно-правових засад її забезпечення в сучасних умовах.

Зв'язок роботи з науковими програмами, планами, темами. Дисертацію виконано відповідно до глави 1.9 «Правове забезпечення інформаційної сфери» Пріоритетних напрямів фундаментальних та прикладних наукових досліджень у галузі права Національної академії правових наук України на 2021–2025 роки та розділу III Стратегії національної безпеки, затвердженої Указом Президента України від 14 вересня 2020 року № 392/2020. Основні положення змісту дисертаційної роботи також узгоджуються зі Стратегією інформаційної безпеки України, затвердженою Указом Президента України від 21 грудня 2021 року № 685/2021 на підставі рішення Ради національної безпеки і оборони України. Дослідження здійснювалося в межах комплексної науково-дослідної роботи Запорізького національного університету «Дослідження проблем теорії адміністративного права в умовах глобалізаційних процесів» (номер державної реєстрації 0115U00710).

Мета та задачі дослідження. *Мета* роботи полягає в тому, щоб на підставі аналізу наукових поглядів, чинного законодавства України та практики його застосування дослідити організаційно-правові аспекти забезпечення інформаційної безпеки України в умовах сучасних загроз. Реалізація поставленої мети зумовлює необхідність вирішення таких *задач*:

– висвітлити поняття інформаційної безпеки та визначити її місце у структурі національної безпеки України;

– проаналізувати етапи еволюції, стан і проблеми законодавчого забезпечення інформаційної безпеки України;

– здійснити аналіз внутрішніх і зовнішніх загроз інформаційній безпеці України в сучасних умовах;

– розглянути структуру та рівні інформаційної безпеки України;

– охарактеризувати механізм забезпечення інформаційної безпеки України;

– описати правовий статус суб'єктів забезпечення інформаційної безпеки України;

– проаналізувати зарубіжний досвід організаційно-правового забезпечення інформаційної безпеки та можливості його імплементації в Україні;

– сформувати шляхи вдосконалення системи суб'єктів забезпечення інформаційної безпеки України;

– висвітлити проблеми та перспективи розвитку системи оцінювання ефективності рівня забезпечення інформаційної безпеки України.

Об'єктом дослідження є суспільні відносини, що виникають у сфері забезпечення інформаційної безпеки держави.

Предметом дослідження є організаційно-правові аспекти забезпечення інформаційної безпеки України в умовах сучасних загроз.

Методи дослідження. У процесі роботи над дисертацією відповідно до поставленої мети й завдань та з огляду на специфіку об'єкта й предмета дослідження використані загальнонаукові та спеціальні методи. Зокрема, формально-логічний метод застосований під час формулювання теоретичних положень дисертації, а саме для конструювання автором дефініцій понять. Статистичний і системно-структурний методи використані для побудови наукової класифікації основних загроз інформаційній безпеці, які постали на сучасному етапі. Метод моделювання дав змогу розробити низку пропозицій, спрямованих на вдосконалення наукових поглядів на структуру та рівні забезпечення інформаційної безпеки держави. Методи аналізу та синтезу дали можливість з'ясувати сутність механізму забезпечення інформаційної безпеки держави. Порівняльно-правовий метод використаний під час аналізу стану та проблем законодавчого забезпечення інформаційної безпеки України. Методи узагальнення та прогнозування були застосовані у процесі формулювання висновків до розділів і загальних висновків до роботи.

Нормативну основу роботи становлять Конституція України, закони України «Про інформацію», «Про національну безпеку України», «Про медіа», Стратегія інформаційної безпеки, затверджена Указом Президента України від 28 грудня 2021 року № 685/2021, інші закони, підзаконні нормативно-правові акти України, норми міжнародного права та зарубіжне законодавство окремих держав.

Емпіричну базу дослідження становлять політико-правова публіцистика, статистичні та аналітичні матеріали, довідкові видання.

Наукова новизна одержаних результатів полягає в тому, що дисертація є одним із перших системних досліджень теоретичних і практичних проблем забезпечення інформаційної безпеки України в умовах сучасних загроз. Унаслідок проведеного дослідження сформульовано низку наукових положень та висновків, основні з яких виносяться на захист, зокрема:

уперше:

– обґрунтовано необхідність запровадження моделі громадського інформаційного врядування, в основі якої лежить партнерство між владою та громадянським суспільством у сфері інформаційної діяльності та забезпечення інформаційної безпеки держави, суспільства й особистості;

– окреслено доцільність нормативно-правового визначення категорії «національний інформаційний простір», який являє собою індивідуалізований національний контекст розвитку окремих видів інформаційної діяльності, розглянутий крізь призму загроз і викликів, а також особливостей системи суб'єктів інформаційної безпеки;

– обґрунтовано необхідність процесу оцінювання рівня забезпечення інформаційної безпеки, яке охарактеризовано як вид діяльності уповноважених суб'єктів, що здійснюється на системній основі, є формалізованою та забезпечується системою кількісних і якісних критеріїв, запропонованих автором;

– аргументовано необхідність виділення рівня інформаційної безпеки територіальних громад, що зумовлено колом спільних інформаційних інтересів у межах територіальних громад, індивідуалізацією загроз, а також схожими проблемами доступу до публічної інформації;

удосконалено:

– наукові погляди щодо природи та змісту інформаційної безпеки, що дало змогу запропонувати ідеологоцентристський підхід, який заснований на розумінні інформаційної безпеки через інтереси держави, суспільства й особистості в інформаційній сфері, які є об'єктом правової охорони;

– організаційно-правову структуру інформаційної безпеки шляхом визначення таких її особливостей, як наявність взаємопов'язаних і взаємозалежних елементів, обмеженість зазначених елементів нормативно-правовими межами, автономність структурних елементів, відповідність елементів структури завданням держави на кожному рівні організаційно-правового забезпечення захисту інформації;

– наукові погляди щодо системи суб'єктів забезпечення інформаційної безпеки держави, завдяки чому вдалося обґрунтувати необхідність їх поділу на стратегічних (визначають ідеологічні засади політики держави), розпорядчих (відповідають за реалізацію державних стратегій) та контролюючих (забезпечують дотримання законодавства) суб'єктів;

– комплексне дефінітивне визначення окремих категорій інформаційної безпеки держави (зокрема, понять «інформаційна безпека», «внутрішні і зовнішні загрози», «адміністративно-правовий механізм забезпечення інформаційної безпеки»), що надалі сприяло систематизації перспективних шляхів удосконалення організаційно-правових засад її забезпечення;

набули подальшого розвитку:

– теоретичні підходи щодо класифікації загроз інформаційній безпеці держави шляхом їх поділу за такими критеріями: за походженням (зовнішні, внутрішні), за ймовірністю виникнення (реальні, потенційні), за характером (ситуативні, стратегічні), за змістом впливу (загальнодержавні, локальні), за підставами виникнення (природні, штучні), за рівнем (загрози безпеці держави, суспільства, особистості);

– наукові положення про принципи інформаційної безпеки, завдяки чому обґрунтовано їх універсальність і міжінституціональність, а також запропоновано перелік;

– наукові погляди на сферу нормативно-правового забезпечення інформаційної безпеки України за рахунок узагальнення та детального аналізу наявних проблем;

– теоретичні положення щодо визначення перспектив розвитку системи інформаційної безпеки України завдяки систематизації та аналізу суб'єктоцентричного, правоцентричного та об'єктоцентричного підходів.

Практичне значення одержаних результатів полягає в тому, що викладені в дисертації положення можуть бути використані в таких напрямах:

– *науково-дослідній сфері* – для подальшого розроблення теоретико-правових уявлень про структуру та рівні інформаційної безпеки держави, зокрема визначення механізмів взаємодії суб'єктів інформаційної безпеки різних рівнів з інститутами громадянського суспільства;

– *правотворчому процесі* – як концептуальна основа розроблення доктрин та стратегій інформаційної безпеки, а також для вдосконалення наявних законодавчих і підзаконних актів у сфері забезпечення інформаційної безпеки;

– *правозастосовній діяльності* – як методологічна основа вдосконалення діяльності суб'єктів забезпечення інформаційної безпеки та розбудови системи громадського інформаційного врядування в Україні;

– *освітньому процесі* – під час створення підручників і навчальних посібників із дисциплін «Інформаційне право», «Адміністративне право», проведення занять із відповідних дисциплін, а також для організації та проведення курсів підвищення кваліфікації державних службовців і посадових осіб органів місцевого самоврядування.

Апробація результатів дослідження. Основні теоретичні положення, висновки та практичні рекомендації, викладені в дослідженні, було оприлюднено на 5 науково-практичних конференціях, зокрема: «Development trends in legal science and education of Ukraine in the context of European integration» (м. Ченстохова, 2023 р.); «Гуманітарний і інноваційний ракурс професійної майстерності: пошуки молодих вчених» (м. Одеса, 2023 р.); «Восьмі Таврійські юридичні наукові читання» (м. Київ, 2023 р.); «Теоретичні та практичні проблеми реалізації норм права» (м. Кременчук, 2023 р.); «Юридичні науки: проблеми та перспективи» (м. Запоріжжя, 2023 р.).

Публікації. Основні положення дисертації викладено в 5 статтях, з яких 4 статті опубліковані в наукових фахових виданнях України та 1 стаття – у зарубіжному науковому періодичному виданні, а також у 5 тезах доповідей на науково-практичних конференціях.

Структура та обсяг дисертації. Дисертація складається з основної частини (вступ, три розділи, які містять вісім підрозділів, висновки), списку використаних джерел і додатків. Загальний обсяг дисертації становить 240 сторінок, з них основного тексту – 194 сторінки. Список використаних джерел налічує 284 найменування.

ОСНОВНИЙ ЗМІСТ ДИСЕРТАЦІЇ

У **вступі** обґрунтовано вибір теми дослідження, вказано на зв'язок роботи з науковими програмами, планами, темами, грантами; визначено мету й завдання дослідження відповідно до його предмета та об'єкта, перелічено використані

наукові методи дослідження; наведено аргументи щодо наукової новизни та практичного значення отриманих результатів, наведено відомості про апробацію результатів дисертаційного дослідження, його структуру та обсяг.

Розділ 1 «Теоретико-правовий аналіз інформаційної безпеки як складника національної безпеки України» складається з трьох підрозділів.

У *підрозділі 1.1 «Поняття інформаційної безпеки, її принципи, функції та місце у структурі національної безпеки України»* охарактеризовано підходи до розуміння природи інформаційної безпеки.

Встановлено, що правоцентристський підхід заснований на розумінні інформаційної безпеки через конституційне право на інформацію, тобто інформаційна безпека є гарантією та одночасно необхідною умовою реалізації цього права. З'ясовано, що безпекоцентристський підхід заснований на визначенні інформаційної безпеки через систему загроз в інформаційній сфері, тобто вона спрямована на запобігання та протидію наявним і потенційним загрозам.

Встановлено, що у структурі національної безпеки України інформаційна безпека має певний інтегруючий характер, адже питання інформаційного забезпечення інших напрямів державної політики частково вирішуються в процесі інформаційної діяльності (формування систем захисту інформації, інформаційно-аналітичне забезпечення органів виконавчої влади тощо).

Доведено, що методи інформаційної діяльності досить активно використовуються в політичній і зовнішньополітичній діяльності у вигляді чинників впливу, що вказує на пріоритетність сфери інформаційної діяльності у вирішенні окремих безпекових питань.

У *підрозділі 1.2 «Еволюція, стан та проблеми правового забезпечення інформаційної безпеки України»* обґрунтовано зв'язок розвитку засобів правового забезпечення з еволюцією відповідних правовідносин, який візуалізується в площині чинників, що вплинули на становлення законодавства у сфері інформаційної безпеки.

Систематизовано чинники процесу еволюції засобів правового забезпечення інформаційної безпеки, якими є: 1) зміни в політичному контексті розбудови інформаційного суспільства; 2) низький рівень міжнародної інформаційної співпраці; 3) недостатній рівень розвитку інформаційної інфраструктури; 4) деформування інформаційного суверенітету України; 5) зростання ролі окремих сфер інформаційної діяльності; 6) зростання залежності України від ефективності функціонування ключових інформаційних систем; 7) стрімка глобалізація інформаційного простору; 8) поява нових загроз, зумовлених збройним конфліктом та тимчасовою окупацією окремих українських територій; 9) євроінтеграційна політика держави.

У *підрозділі 1.3 «Аналіз внутрішніх і зовнішніх загроз інформаційній безпеці України в сучасних умовах»* узагальнено перелік ознак внутрішніх і зовнішніх загроз інформаційній безпеці, зокрема: а) здатність до негативного впливу на стан захищеності національних інтересів в інформаційній сфері; б) індивідуалізація на рівні окремих компонентів інформаційної діяльності

(одержання, використання, зберігання та поширення інформації); в) наявність опису алгоритму формування та характеру впливу; г) наявність реалістичного або потенційного характеру негативного впливу; ґ) наявність індивідуальних негативних наслідків впливу; д) унікальна природа виникнення та мета створення.

Визначено такі застереження щодо дослідження окремих внутрішніх і зовнішніх загроз інформаційній безпеці: 1) усі загрози повинні бути чітко розмежовані за інституціональною ознакою; 2) кожна окрема загроза повинна бути самостійною категорією, що наділена унікальними ознаками; 3) окремі загрози повинні мати специфічну сферу впливу на стан інформаційної безпеки; 4) у процесі дослідження необхідно звертати увагу на здатність окремих загроз до комбінованої дії, що може зумовити необхідність їх об'єднання; 5) негативний вплив кожної окремої загрози необхідно позиціонувати через конкретні наслідки, які є відображенням протиправної поведінки.

Розділ 2 «Організаційна структура та механізм забезпечення інформаційної безпеки України» складається з трьох підрозділів.

У *підрозділі 2.1 «Аналіз структури та рівнів інформаційної безпеки України»* встановлено, що інформаційна безпека має власну, унікальну структуру, яка складається із сукупності взаємопов'язаних і взаємозалежних елементів, що доповнюють один одного, утворюючи цілісне, багаторівневе правове явище.

Встановлено, що основною умовою існування структурних елементів інформаційної безпеки є комплексність, яка визначає сенс самої інформаційної безпеки, а також характеризує наділення елементів структури всією повнотою інформації про саму систему.

Доведено, що до структури інформаційної безпеки входять елементи, які визначають ціннісно-ідеологічні, організаційно-функціональні, процедурно-правові та змістово-методологічні аспекти її забезпечення.

У *підрозділі 2.2 «Характеристика адміністративно-правового механізму забезпечення інформаційної безпеки України»* доведено, що зазначений механізм характеризує напрями діяльності суб'єктів інформаційної безпеки, тобто він пов'язаний із методологією її забезпечення.

З'ясовано, що цей механізм через окремі методи та форми пов'язаний із системою загроз, тобто демонструє спрямованість системи інформаційної безпеки. Отже, наявні методи та форми є своєрідними засобами впливу на конкретні загрози, а отже, є чинниками, які окреслюють очікувані результати від діяльності уповноважених суб'єктів.

Встановлено, що в контексті специфіки інформаційної безпеки адміністративно-правовий механізм її забезпечення наділений певним ідеологічним змістом, у якому втілюється ціннісний вимір. Відповідно, методи та форми сприяють утвердженню базових цінностей, які надалі відображаються в напрямах державної політики та сферах діяльності суб'єктів інформаційної безпеки.

У *підрозділі 2.3 «Правовий статус суб'єктів забезпечення інформаційної безпеки України»* досліджено правове становище різних за рівнем суб'єктів забезпечення інформаційної безпеки, яких було індивідуалізовано на рівні трьох основних груп: стратегічні, розпорядчі та контрольні суб'єкти.

З'ясовано, що стратегічні суб'єкти характеризуються такими ознаками: а) специфікою конституційно-правового статусу; б) рівнем і характером актів, які ними приймаються; в) системою організаційних зв'язків; г) особливою компетенцією та повноваженнями; ґ) особливим правовим статусом в умовах воєнного стану.

Доведено, що розпорядчі суб'єкти мають такі особливості: а) їхній правовий статус дає змогу істотно впливати на стан захищеності інформаційних інтересів держави, суспільства та особистості; б) розпорядчий складник дає можливість забезпечити цілісність механізму забезпечення інформаційної безпеки; в) вони невід'ємно пов'язані з безпосередніми формами та методами забезпечення інформаційної безпеки; г) вони належать до числа суб'єктів адміністративно-правового захисту у сфері інформаційної безпеки; ґ) вони наділені певним ідеологічним складником, який проявляється у вигляді окреслених пріоритетів розвитку системи державного управління.

Встановлено, що контрольні суб'єкти характеризуються такими унікальними ознаками: а) вони мають специфічний характер впливу на інформаційну безпеку держави (запобігання правопорушенням, припинення правопорушень, усунення наслідків протиправної діяльності, відновлення прав); б) їхня діяльність позбавлена стратегічного або розпорядчого складника, оскільки сконцентрована виключно на необхідності забезпечення верховенства права; в) поєднання державного та недержавного статусу суб'єктів цієї групи дає можливість підвищити ефективність контролю за системою інформаційної безпеки шляхом розширення функціоналу їхньої діяльності.

Розділ 3 «Напрями вдосконалення організаційно-правових засад забезпечення інформаційної безпеки України» складається з двох підрозділів.

У *підрозділі 3.1 «Зарубіжний досвід організаційно-правового забезпечення інформаційної безпеки та можливість його імплементації в Україні»* акцентовано на позитивному закордонному досвіді у відповідній сфері, який цілком доречно імплементувати в Україні та який дасть змогу підвищити рівень інформаційної безпеки держави, суспільства й особистості.

Наголошено на тому, що позитивний досвід, по-перше, дає можливість покращити рівень захищеності національних інтересів в інформаційній сфері; по-друге, сприяє вдосконаленню законодавства в зазначеній сфері та практиці його застосування; по-третє, не пов'язаний із протиправними обмеженнями права на інформацію або надмірним втручанням держави в національну інформаційну систему; по-четверте, допомагає оперативно виявляти загрози та протидіяти їм; по-п'яте, покращує практику співпраці владних інституцій та громадськості у сфері інформаційної безпеки.

Систематизовано чинники, які визначають формування зарубіжного досвіду забезпечення інформаційної безпеки, а саме: рівень розбудови інформаційного суспільства, рівень інтеграції держави в наднаціональні структури, підхід до позиціонування інформаційної безпеки, підхід до формалізації основних засад інформаційної безпеки, спосіб позиціонування моделі інформаційної безпеки.

У *підрозділі 3.2 «Шляхи вдосконалення організаційно-правових засад забезпечення інформаційної безпеки України»* детально охарактеризовано підходи до визначення перспектив розвитку вітчизняної системи забезпечення інформаційної безпеки.

З'ясовано, що правоцентричний підхід є лише невід'ємним елементом цілісної моделі інформаційної безпеки України, оскільки правової регламентації не досить тому, що виключна імперативність не забезпечує розвиток національної інформаційної системи.

Доведено, що об'єктоцентричний підхід не вбачається перспективним, оскільки система інформаційної безпеки не може спиратися на розподіл інформації на відповідні категорії. Недоліком цього підходу є ризик виникнення певного конфлікту на різних рівнях інформаційної безпеки, які будуть реакцією на невідповідність національних інтересів потребам суспільства та особистості.

Аргументовано, що найбільш прийнятним є суб'єктоцентричний підхід, який спирається на поєднання зусиль різних за статусом учасників інформаційних правовідносин. Недоліком цього підходу є домінування владних інституцій, унаслідок чого громадянське суспільство є лише факультативним суб'єктом, завдання якого – дотримання встановлених державою вимог.

Варто зазначити, що оцінювання рівня забезпечення інформаційної безпеки має спиратися не на окремі сфери інформаційної діяльності, а на стан захищеності інтересів суб'єктів різного рівня. При цьому відмежованість від окремих сфер діяльності дає можливість уникнути фрагментарності, яка заважатиме об'єктивному оцінюванню. Обґрунтовано, що в основі процесу оцінювання має лежати національний інформаційний простір, який є своєрідним утіленням інформаційного суверенітету держави.

ВИСНОВКИ

У дисертації в результаті проведеного ґрунтовного теоретико-правового дослідження організаційно-правових аспектів забезпечення інформаційної безпеки в умовах сучасних загроз виявлено низку теоретичних і практичних задач, пов'язаних із питаннями визначення структури й рівнів інформаційної безпеки та розбудови системи державно-приватного партнерства у сфері її забезпечення, запропоновано шляхи вирішення зазначених задач та розроблено концептуальні положення, які спрямовані на вдосконалення процесу оцінювання рівня забезпечення інформаційної безпеки України. Ключові висновки цього дисертаційного дослідження, що розширюють і доповнюють винесені на захист положення наукової новизни, є такими:

1. Обґрунтовано ідеологоцентристський підхід, який заснований на розумінні інформаційної безпеки через інтереси держави, суспільства та особистості в інформаційній сфері, які є об'єктом правової охорони. Доведено, що в межах цього підходу інформаційна безпека є ідеологічною основою функціонування інформаційної системи держави, у якій окремі суб'єкти задовольняють свої інформаційні потреби, а держава забезпечує національні інтереси.

Запропоноване авторське визначення категорії «інформаційна безпека» як складника національної безпеки України, стану захищеності інтересів різних учасників в інформаційній сфері, який забезпечується шляхом індивідуалізованих засобів і способів, що реалізуються спеціально уповноваженими суб'єктами, а також фізичними та юридичними особами на окремих рівнях інформаційної діяльності.

2. Запропоновано під принципами інформаційної безпеки розуміти формалізовані вихідні засади формування та впровадження уповноваженими суб'єктами системи заходів щодо забезпечення належного стану захищеності інтересів держави, суспільства й особистості в інформаційній сфері. Встановлено, що принципи інформаційної безпеки наділені універсальністю та міжінституціональністю, оскільки дають змогу визначити засади діяльності щодо забезпечення інтересів різних суб'єктів (держави, суспільства, особистості).

Систематизовано принципи інформаційної безпеки, якими є: 1) принцип додержання прав і свобод людини та громадянина в процесі забезпечення інформаційної безпеки; 2) принцип гарантованості інформаційного суверенітету України; 3) принцип обґрунтованості захисту окремих видів інформації; 4) принцип своєчасності та прогнозування заходів інформаційної безпеки; 5) принцип обопільної відповідальності всіх суб'єктів за діяльність у межах забезпечення інформаційної безпеки; 6) єдність та взаємозв'язок напрямів забезпечення інформаційної безпеки; 7) інтегрованість вітчизняної системи інформаційної безпеки з міжнародними й регіональними безпековими системами; 8) превентивність та адекватність заходів інформаційної безпеки; 9) наукова обґрунтованість заходів забезпечення інформаційної безпеки; 10) організаційно-правова забезпеченість системи інформаційної безпеки.

3. Узагальнено проблеми правового забезпечення інформаційної безпеки, якими визначені такі явища: а) неналежний рівень формалізації загроз інформаційній безпеці в нормативно-правових актах; б) відсутність практики коригування загроз і викликів в інформаційній сфері; в) недосконалість механізмів реалізації права на інформацію; г) застарілість значної кількості законодавчих актів у сфері інформаційної безпеки; ґ) недостатня візуалізація інформаційного складника національної безпеки в чинному законодавстві; д) відсутність у законодавчих актах комплексного бачення стратегічних заходів протидії загрозам в інформаційній сфері; е) неналежна регламентація категорій інформаційної безпеки в регіональних програмах та стратегіях розвитку;

є) фрагментарність положень міжнародно-правових актів у сфері забезпечення інформаційної безпеки.

4. Розроблено класифікацію загроз інформаційній безпеці за такими критеріями: а) за походженням (зовнішні, внутрішні); б) за ймовірністю виникнення (реальні, потенційні); в) за характером (ситуативні, стратегічні); г) за змістом впливу (загальнодержавні, локальні); ґ) за підставами виникнення (природні, штучні); д) за рівнем впливу (загрози безпеці держави, суспільства та особистості).

Під внутрішніми загрозами інформаційній безпеці запропоновано розуміти сукупність явищ, чинників і подій, які виникають, формуються та реалізуються на внутрішньодержавному рівні, пов'язані з деструктивним впливом на інформаційну систему та загрожують інтересам держави, суспільства й особистості у сфері інформаційної діяльності. Досліджено такі внутрішні загрози інформаційній безпеці, як недосконаліть інформаційного законодавства, недосконаліть системи державного управління у сфері забезпечення інформаційної безпеки, низький рівень медіаграмотності суспільства та особистості, недосконаліть механізмів захисту інформації, неефективність системи стратегічних комунікацій, недосконаліть механізмів задоволення інформаційних потреб.

З'ясовано, що зовнішні загрози інформаційній безпеці являють собою сукупність явищ, чинників і подій, які виникають та формуються на міжнародному рівні, а реалізуються на внутрішньодержавному рівні, пов'язані з негативним зовнішнім впливом на інформаційну систему та загрожують національним інтересам у сфері інформаційної діяльності. До зовнішніх загроз віднесено інформаційний тероризм із боку держави-агресора, неконтрольованість змісту контенту в соціальних мережах, міжнародну кіберзлочинність, дезінформаційні кампанії проти України.

5. Запропоновано під структурою інформаційної безпеки розуміти сукупність загальних засад, методів, гарантій та умов забезпечення належного стану захищеності національних інтересів в інформаційній сфері від внутрішніх і зовнішніх загроз, комплексність та упорядкованість яких гарантує стабільність і контрольованість інформаційної системи України. Систематизовано та досліджено такі елементи цієї структури, як національні інтереси й загрози, принципи, гарантії, механізм, методи, юридична відповідальність. Узагальнено особливості структури інформаційної безпеки, якими є: а) наявність взаємопов'язаних і взаємозалежних елементів; б) обмеженість зазначених елементів нормативно-правовими межами; в) автономність структурних елементів; г) відповідність елементів структури завданням держави на кожному рівні організаційно-правового забезпечення захисту інформації.

6. З'ясовано, що рівні інформаційної безпеки визначають межі діяльності уповноважених суб'єктів, тобто характер їхнього виконавчо-розпорядчого впливу, що зумовлений специфікою інформаційних потреб, які задовольняються учасниками правовідносин. Запропоновано під рівнем

інформаційної безпеки розуміти законодавчо визначену сферу діяльності, яка характеризується специфікою інформаційних потреб та інтересів, унікальністю загроз і викликів, індивідуальністю суб'єктів, а також передбачає особливі засоби правового захисту інформації. Систематизовано й досліджено такі рівні: інформаційну безпеку держави, інформаційну безпеку суспільства, інформаційну безпеку особистості.

Аргументовано необхідність виділення рівня інформаційної безпеки територіальних громад, які є специфічними суб'єктами правовідносин і не можуть бути ототожнені з державою та суспільством. Доведено, що актуальність виокремлення такого рівня зумовлена колом спільних інформаційних інтересів у межах територіальних громад, які насамперед пов'язані з доступністю публічної інформації та створенням умов реалізації інформаційних потреб. Встановлено, що на рівні окремих територіальних громад наявні індивідуальні загрози, які можуть впливати на їхні безпекові стратегії.

7. Запропоновано під адміністративно-правовим механізмом інформаційної безпеки розуміти сукупність формалізованих методів і форм, які реалізуються уповноваженими суб'єктами на постійній основі з метою впливу на сферу інформаційної діяльності задля забезпечення належного рівня захисту національних інтересів та створення умов реалізації права на інформацію всіма учасниками інформаційних правовідносин. Доведено, що механізм забезпечення інформаційної безпеки характеризує напрями діяльності суб'єктів інформаційної безпеки, тобто пов'язаний із методологією її забезпечення. Зазначено, що через окремі методи та форми цей механізм пов'язаний із системою загроз, тобто демонструє спрямованість системи інформаційної безпеки.

Обґрунтовано необхідність поділу суб'єктів інформаційної безпеки залежно від їхнього правового статусу на такі групи: 1) стратегічні суб'єкти (визначають концептуальні питання, тобто ідеологічні засади політики держави у сфері інформаційної безпеки); 2) розпорядчі суб'єкти (безпосередньо відповідають за реалізацію державних стратегій інформаційної безпеки); 3) контролюючі суб'єкти (забезпечують дотримання законодавства у сфері інформаційної безпеки). Здійснено комплексний аналіз кожної з названих груп.

8. Доведено, що зарубіжний досвід забезпечення інформаційної безпеки може бути використаний в Україні щодо формування національного інформаційного простору, розбудови механізмів наукового обґрунтування загроз і запобігання їм, створення системи громадського інформаційного врядування, утвердження спеціальних владно-розпорядчих інституцій для захисту національних інтересів в інформаційній сфері, поєднання ліберальних методів та державного регулювання.

9. Встановлено, що процес удосконалення організаційно-правових аспектів забезпечення інформаційної безпеки має відбуватися з огляду на такі цілі: 1) максимальне залучення громадянського суспільства до процесів захисту інформації на всіх рівнях інформаційної безпеки; 2) встановлення балансу між

приватністю та національними інтересами в інформаційній сфері; 3) урахування контексту збройного конфлікту як вагомого чинника, що впливає на розвиток сучасної системи інформаційної безпеки; 4) урахування неможливості кодифікації інформаційного законодавства та різноплановості окремих сфер інформаційної діяльності; 5) недопущення випадків дублювання повноважень владно-розпорядчих суб'єктів у сфері інформаційної безпеки; 6) чітке позиціонування інтересів держави, суспільства та особистості у сфері інформаційної безпеки.

Систематизовано такі підходи до визначення пріоритетних напрямів розвитку системи забезпечення інформаційної безпеки, як суб'єктоцентричний (формування особливої моделі забезпечення інформаційної безпеки через взаємодію різних за статусом суб'єктів владних повноважень), правоцентричний (інформаційна безпека розглядається як правова конструкція, функціонування якої визначається законодавчими й підзаконними актами), об'єктоцентричний (формування системи інформаційної безпеки має відбуватися на основі поділу інформації на окремі категорії).

10. Обґрунтовано модель громадського інформаційного врядування, яка повинна формуватися на основі таких принципів: 1) залучення громадськості до питань розроблення й реалізації політики забезпечення інформаційної безпеки; 2) надання громадськості широкого кола повноважень (консультативно-дорадчих, правозастосовних, контрольних, інформаційно-методичних); 3) обопільної відповідальності влади та громадськості за забезпечення належного рівня інформаційної безпеки; 4) підзвітності всіх суб'єктів інформаційної безпеки (влади та громадянського суспільства); 5) пріоритетності прогнозування та запобігання загрозам інформаційній безпеці.

11. Систематизовано такі ознаки процесу оцінювання рівня забезпечення інформаційної безпеки України: а) формалізованість (наявність чіткої нормативно-правової регламентації методик оцінювання); б) системність (необмеженість процесу оцінювання відповідними строками або періодами розвитку суспільних відносин); в) цілеспрямованість (наявність чіткої мети, яка надалі забезпечить очікувані результати); г) комплексність (урахування специфіки різних рівнів інформаційної безпеки та відповідних інформаційних потреб учасників правовідносин); ґ) адаптивність (здатність системи пристосовуватися до зміни контексту загроз та змін у правовому регулюванні).

12. Запропоновано під процесом оцінювання рівня забезпечення інформаційної безпеки розуміти вид діяльності уповноважених суб'єктів, яка здійснюється на системній основі, є формалізованою та полягає в оцінюванні за допомогою системи кількісних і якісних критеріїв ефективності заходів, запроваджених державою з метою захисту інтересів держави, суспільства й особистості в інформаційній сфері. Аргументовано, що основою процесу оцінювання мають бути кількісні та якісні критерії, під якими пропонується розуміти відповідні показники ефективності рівня інформаційної безпеки, які

відображають реальний стан захищеності інтересів держави, суспільства та особистості в інформаційній сфері.

13. Надано перелік кількісних критеріїв оцінювання рівня забезпечення інформаційної безпеки, основними з яких є: 1) кількість попереджених кібератак, які були спрямовані на національні інформаційно-телекомунікаційні мережі; 2) кількість виявлених і знешкоджених джерел дезінформації та антиукраїнської пропаганди; 3) кількість звернень громадян до владних інституцій щодо порушення права на інформацію; 4) кількість цілей, які були досягнуті за період дії загальнодержавних стратегій інформаційної безпеки; 5) кількість обвинувальних вироків щодо осіб, які вчинили інформаційні правопорушення (проступки та злочини); 6) кількість прийнятих нормативно-правових актів, у яких регламентовані окремі питання інформаційної безпеки; 7) кількість створених владних інституцій та об'єднань громадян, предметом діяльності яких є забезпечення інформаційної безпеки.

14. Запропоновано до якісних критеріїв оцінювання рівня забезпечення інформаційної безпеки віднести такі умови: 1) рівень медіакультури, медіаграмотності та інформаційної гігієни суспільства й особистості; 2) стан імплементації позитивного зарубіжного досвіду забезпечення інформаційної безпеки; 3) рівень забезпечення однакових стандартів державного управління у сфері інформаційної безпеки; 4) стан координації і взаємодії влади та громадськості у сфері забезпечення інформаційної безпеки; 5) відповідність здобутків влади очікуваним результатам, зафіксованим у стратегії інформаційної безпеки; 6) якість задоволення інформаційних потреб суб'єктами відповідних правовідносин; 7) стан гарантованості інформаційного суверенітету України.

15. Зазначено, що успішне запровадження моделі громадського інформаційного врядування вимагає формування національного інформаційного простору, який являє собою індивідуалізований національний контекст розвитку окремих видів інформаційної діяльності, розглянутий крізь призму загроз і викликів, а також особливостей системи суб'єктів інформаційної безпеки. Доведено, що формалізація цієї категорії в законодавстві дасть змогу поєднати інтереси держави, суспільства та особистості в межах єдиної системи ціннісних орієнтирів.

СПИСОК ПРАЦЬ, ОПУБЛІКОВАНИХ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

1. Недохлєбов І.І. Теоретико-правовий аналіз зовнішніх загроз інформаційній безпеці України. *Науковий вісник Міжнародного гуманітарного університету. Серія «Юриспруденція»*. 2023. № 64. С. 18–21. DOI: https://doi.org/10.32841/2307-1745.2023.64.4.

2. Недохлєбов І.І. До питання природи та змісту рівнів інформаційної безпеки України. *Юридичний науковий електронний журнал*. 2023. № 11. С. 395–397. DOI: https://doi.org/10.32782/2524-0374/2023-11/95.

3. Недохлєбов І.І. Аналіз організаційно-правових форм забезпечення інформаційної безпеки України. *Правові новели*. 2023. № 21. С. 82–88. DOI: https://doi.org/10.32782/ln.2023.21.11.

4. Недохлєбов І.І. Проблеми визначення перспективних напрямів розвитку системи інформаційної безпеки України. *Юридичний вісник*. 2023. № 6. С. 264–269. DOI: https://doi.org/10.32782/yuv.v6.2023.32.

5. Недохлєбов І.І. Особливості правового статусу суб'єктів інформаційної безпеки. *KELM (Knowledge, Education, Law, Management)*. 2023. № 7(59). P. 155–159. DOI: https://doi.org/10.51647/kelm.2023.7.24.

6. Недохлєбов І.І. Інформаційна безпека в структурі національної безпеки України. *Development trends in legal science and education of Ukraine in the context of European integration* : proceeding of the international scientific conference, Częstochowa, November 1–2, 2023. Riga : Publishing House "Baltija Publishing", 2023. P. 148–152. DOI: https://doi.org/10.30525/978-9934-26-372-9-38.

7. Недохлєбов І.І. До питання еволюції засобів правового забезпечення інформаційної безпеки. *Гуманітарний і інноваційний ракурс професійної майстерності: пошуки молодих вчених* : матеріали IX Всеукраїнської науково-практичної конференції студентів, аспірантів та молодих учених, м. Одеса, 15 грудня 2023 р. Львів – Торунь : Liha-Pres, 2023. С. 95–99. DOI: https://doi.org/10.36059/978-966-397-357-9-26.

8. Недохлєбов І.І. Система інформаційної безпеки США: правові та організаційні аспекти. *Восьмі Таврійські юридичні наукові читання* : матеріали міжнародної науково-практичної конференції, м. Київ, 16–17 червня 2023 р. Львів – Торунь : Liha-Pres, 2023. С. 277–279. DOI: https://doi.org/10.36059/978-966-397-318-0-75.

9. Недохлєбов І.І. Забезпечення інформаційної безпеки на рівні ЄС та окремих держав-членів. *Теоретичні та практичні проблеми реалізації норм права* : матеріали IX Міжнародної науково-практичної конференції, м. Кременчук, 22–23 грудня 2023 р. Львів – Торунь : Liha-Pres, 2023. С. 378–381. DOI: https://doi.org/10.36059/978-966-397-351-7-101.

10. Недохлєбов І.І. Проблемні аспекти оцінювання рівня забезпечення інформаційної безпеки України. *Юридичні науки: проблеми та перспективи* : матеріали міжнародної науково-практичної конференції, м. Запоріжжя, 24–25 лютого 2023 р. Львів – Торунь : Liha-Pres, 2023. С. 380–383. DOI: https://doi.org/10.36059/978-966-397-292-3-107.

АНОТАЦІЇ

Недохлєбов І.І. Інформаційна безпека України в умовах сучасних загроз: організаційно-правові аспекти. – Рукопис.

Дисертація на здобуття наукового ступеня кандидата юридичних наук за спеціальністю 12.00.07 – адміністративне право і процес; фінансове право; інформаційне право. – Запорізький національний університет, Запоріжжя, 2024.

Дисертацію присвячено дослідженню організаційно-правових аспектів забезпечення інформаційної безпеки України в умовах сучасних загроз. На підставі комплексного аналізу теоретичних праць, національного й зарубіжного законодавства та практики його застосування сформульовано науково обґрунтовані висновки, пропозиції і рекомендації, спрямовані на вдосконалення законодавчого регулювання та адміністративно-правового механізму забезпечення інформаційної безпеки України. Здійснено теоретико-правовий аналіз інформаційної безпеки як складової частини національної безпеки України, охарактеризовано організаційну структуру та механізм забезпечення інформаційної безпеки України, а також запропоновано напрями вдосконалення організаційно-правових засад забезпечення інформаційної безпеки України.

Обґрунтовано модель громадського інформаційного врядування, яка повинна формуватися на основі таких принципів: залучення громадськості до питань розроблення й реалізації політики забезпечення інформаційної безпеки; надання громадськості широкого кола повноважень (консультативно-дорадчих, правозастосовних, контрольних, інформаційно-методичних); обопільної відповідальності влади та громадськості за забезпечення належного рівня інформаційної безпеки; підзвітності всіх суб'єктів інформаційної безпеки (влади та громадянського суспільства); пріоритетності прогнозування та запобігання загрозам інформаційній безпеці.

Зазначено, що успішне запровадження моделі громадського інформаційного врядування вимагає формування національного інформаційного простору, який являє собою індивідуалізований національний контекст розвитку окремих видів інформаційної діяльності, розглянутий крізь призму загроз і викликів, а також особливостей системи суб'єктів інформаційної безпеки. Доведено, що формалізація цієї категорії в законодавстві дасть змогу поєднати інтереси держави, суспільства та особистості в межах єдиної системи ціннісних орієнтирів.

Ключові слова: *гібридна війна, дезінформація, інформаційна безпека, інформаційний тероризм, інформаційні потреби, інформаційні правовідносини, національна безпека, право на інформацію, приватність, пропаганда.*

Nedokhlebov I.I. Information security of Ukraine in the conditions of modern threats: organizational and legal aspects. – Manuscript.

Dissertation for obtaining the scientific degree of candidate of legal sciences, specialty 12.00.07 – administrative law and process; finance law; information law. – Zaporizhzhia National University, Zaporizhzhia, 2024.

The dissertation is devoted to the study of organizational and legal aspects of ensuring information security of Ukraine in the conditions of modern threats and challenges. Based on a comprehensive analysis of theoretical works, national and foreign legislation, and the practice of its application, scientifically based conclusions, proposals and recommendations aimed at improving legislative regulation and administrative – the legal mechanism for ensuring information

security of Ukraine. A theoretical and legal analysis of information security as a component of the national security of Ukraine was carried out, the organizational structure and mechanism of ensuring information security of Ukraine were characterized, and directions for improving the organizational and legal foundations of ensuring information security of Ukraine were proposed.

The model of public information governance is substantiated, which should be formed on the basis of the following principles: public involvement in issues of development and implementation of information security policy; providing the public with a wide range of powers (consultative and advisory, law enforcement, control, informational and methodical); mutual responsibility of the authorities and the public for ensuring the appropriate level of information security; accountability of all information security subjects (government and civil society); the priority of forecasting and prevention of threats to information security.

It is noted that the successful implementation of the model of public information governance requires the formation of a national information space, which is an individualized national context of the development of certain types of information activities, considered through the prism of threats and challenges, as well as the peculiarities of the system of information security subjects. It has been proven that the formalization of this category in the legislation will allow combining the interests of the state, society and the individual within the framework of a single system of value guidelines.

Key words: *disinformation, hybrid warfare, information legal relations, information needs, information security, information terrorism, national security, privacy, propaganda, right to information.*

Підписано до друку 14.05.2024. Формат 60х90/16. Папір офсетний.
Друк цифровий. Умовн. друк. арк. 0,9. Тираж 100 прим. Зам. № 1105.
Видавництво і друкарня – Видавництво «Юридика»
65101, Україна, м. Одеса, вул. Інглезі, 6/1
Телефони: +38 (095) 934-48-28, +38 (097) 723-06-08
E-mail: mailbox@juridica.od.ua
Свідоцтво суб'єкта видавничої справи
ДК № 7653 від 18.08.2022 р.