**НАУКОВО-ДОСЛІДНИЙ ІНСТИТУТ ПУБЛІЧНОГО ПРАВА**

**ВДОВІН ІЛЛЯ ОЛЕКСАНДРОВИЧ**

УДК 342.9 (477)

# ОРГАНІЗАЦІЙНО-ПРАВОВІ ЗАСАДИ РЕАЛІЗАЦІЇ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ

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

**Автореферат дисертації на здобуття наукового ступеня кандидата юридичних наук**

**Київ – 2024**

Дисертацією є рукопис

Робота виконана в Науково-дослідному інституті публічного права

**Науковий керівник**
кандидат юридичних наук
**Червякова Оксана Вікторівна,**
Верховна Рада України,
представниця Уповноваженого з прав людини в Харківський області

**Офіційні опоненти:**
доктор юридичних наук, професор
**Моргунов Олександр Анатолійович,**
Дніпропетровський державний університет внутрішніх справ,
ректор

кандидат юридичних наук
**Іванов Антон Олександрович,**
Харківський національний університет внутрішніх справ,
доцент кафедри правоохоронної діяльності та поліцеїстики факультету № 6

Захист відбудеться «21» травня 2024 р. о $9^{00}$ на засіданні спеціалізованої вченої ради Д 26.503.01 у Науково-дослідному інституті публічного права за адресою: 03035, м. Київ, вул. Георгія Кірпи, 2А

З дисертацією можна ознайомитись у бібліотеці Науково-дослідного інституту публічного права за адресою: 03035, м. Київ, вул. Георгія Кірпи, 2А

Автореферат розісланий «19» квітня 2024 р.

Учений секретар
спеціалізованої вченої ради К. М. Куркова

# ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

**Обґрунтування вибору теми дослідження.** В цифрову епоху, в якій ми зараз живемо, одним із найцінніших ресурсів людства є інформація. Остання, в свою чергу, може використовуватись як для розвитку суспільства, так і з метою вчинення протиправних дій, які порушують права, свободи та інтереси інших людей. Саме тому ключовим завданням будь-якої сучасної та розвиненої держави є створення ефективної системи забезпечення інформаційної безпеки, яка в умовах сьогодення є надважливою та невід'ємною складовою національної безпеки. Втім постійний розвиток та вдосконалення інформаційної галузі значно ускладнює процес створення механізмів реалізації інформаційної безпеки.

Варто зауважити, що в останні роки в Україні було розроблено та прийнято низку стратегічних та концептуальних нормативно-правових актів, які були покликані якісно покращити правові та організаційні аспекти забезпечення реалізації інформаційної безпеки в нашій країні. Разом із тим, розробка і введення в дію вказаних нормативно-правових актів жодним чином не применшує актуальність проблематики забезпечення інформаційної безпеки, а також не вирішує всіх проблем її реалізації в Україні, а особливо сьогодні, в умовах повномасштабної війни на території нашої держави. Зазначене в тому числі пояснюється тим, що значна частина протистояння України та рф відбувається саме в інформаційному просторі. Саме тому, і українському законодавцю, і вітчизняним науковцям, слід вести активну роботу у напрямку покращення організаційно-правових засад реалізації інформаційної безпеки України.

*Зв'язок теми дисертації із сучасними дослідженнями.* Справедливим буде відзначити, що в останні декілька десятиліть проблема інформаційної безпеки ставала предметом дослідження багатьох науковців. Зокрема їй приділяли увагу: С.Є. Антонова, М.В. Баран, І.О. Валюшко, М.В. Грайворонський, Д.В. Дубов, А.О. Іванов, Р.А. Калюжний, М.О. Кириченко, Ю.О. Корнєєв, О.М. Косогов, О.В. Левченко, Л.С. Любохинець, А.І. Марущак, О.А. Моргунов , О.А. Панченко, О.М. Ситніченко, М.В. Сунгуровський, О.В. Червякова , Я.І. Чмир, П.О. Яковлєв та багато інших. Втім, незважаючи на значну кількість теоретичних здобутків, слід відзначити декілька важливих моментів: по-перше, більшість теоретичних розробок вже втратили свою актуальність, що обумовлено повномасштабною військовою агресією рф; по-друге, в роботах вказаних науковців питання організаційно-правових засад реалізації інформаційної безпеки розглядалось досить поверхнево, в межах більш широких проблематик.

Таким чином, наявність низки прогалин та недоліків у чинному законодавстві, норми якого спрямовані на закріплення реалізації інформаційної безпеки України, а також відсутність сучасних комплексних монографічних досліджень, присвячених вказаній проблематиці, обумовлюють актуальність та своєчасність представленого дисертаційного дослідження.

**Зв'язок роботи з науковими програмами, планами, темами, грантами.** Дисертаційне дослідження узгоджується з основними положеннями: «Стратегії інформаційної безпеки на період до 2025 року», затвердженої розпорядженням

Кабінету Міністрів України від 30 березня 2023 р. № 272-р.; «Стратегії національної безпеки України», схваленої Указом Президента України від 14 вересня 2020 р. № 392/2020; «Стратегії кібербезпеки України», що була введена в дію Указом Президента України від 26 серпня 2021 р. № 447/2021; «Стратегії воєнної безпеки України», затвердженої Указом Президента України від 25 березня 2021 р. № 121/2021; «Стратегії кібербезпеки України», схваленої Указом Президента України від 16 березня 2016 р. № 96/2016; «Стратегії забезпечення державної безпеки», затвердженої Указом Президента України від 16 лютого 2022 р. № 56/2022; «Стратегії комунікації з питань євроатлантичної інтеграції України на період до 2025 року» затвердженої Указом Президента України від 11 вересня 2021 р. № 348/2021. Дисертацію виконано відповідно до плану науково-дослідної роботи Науково-дослідного інституту публічного права «Правове забезпечення прав, свобод та законних інтересів суб'єктів публічно-правових відносин» (номер державної реєстрації 0120U105390).

**Мета і завдання дослідження.** *Мета* дисертаційного дослідження полягає у тому, щоб на основі аналізу наукових поглядів вчених, норм чинного законодавства, а також практики його реалізації, з'ясувати сутність та особливості організаційно-правових засад реалізації інформаційної безпеки України, а також, спираючись на позитивний вітчизняний та зарубіжний досвід, опрацювати напрями вдосконалення організаційно-правового забезпечення відповідної діяльності.

Для досягнення зазначеної мети у процесі дослідження необхідно вирішити такі *завдання:*

– охарактеризувати становлення та розвиток інформаційної безпеки України;

– розкрити напрямки розвитку державної політики у сфері забезпечення реалізації інформаційної безпеки України;

– оцінити сучасний стан правового регулювання забезпечення реалізації інформаційної безпеки України;

– здійснити розмежування галузей права у правовому регулюванні забезпечення реалізації інформаційної безпеки України;

– розкрити систему суб'єктів забезпечення реалізації інформаційної безпеки України та встановити місце серед них Служби безпеки України;

– визначити форми та методи реалізації інформаційної безпеки України;

– узагальнити міжнародний досвід правового регулювання забезпечення реалізації інформаційної безпеки та опрацювати можливості його використання в Україні;

– запропонувати напрямки вдосконалення організаційно-правового забезпечення реалізації інформаційної безпеки України.

*Об'єктом дослідження* є суспільні відносини, які виникають в процесі реалізації інформаційної безпеки України.

*Предметом дослідження* є організаційно-правові засади реалізації інформаційної безпеки України.

**Методи дослідження.** Методологічною основою роботи є сукупність загальнонаукових і спеціально-наукових методів та прийомів наукового пізнання,

застосування яких зумовлюється специфікою предмета дослідження. Так, використання *історико-правового* методу дозволило надати характеристику становленню та розвитку інформаційної безпеки України (підрозділ 1.1). Розкрити напрямки розвитку державної політики у сфері забезпечення реалізації інформаційної безпеки України (підрозділ 1.2); оцінити сучасний стан правового регулювання забезпечення реалізації інформаційної безпеки України (підрозділ 1.3), а також здійснити розмежування галузей права у правовому регулюванні забезпечення реалізації інформаційної безпеки України (підрозділ 2.1) вдалось за допомогою *аналітичного* методу та методу *документального аналізу*. *Структурно-логічний* та *системно-функціональний* методи використовувалися для того, щоб надати характеристику системі суб'єктів забезпечення реалізації інформаційної безпеки України та встановити місце серед них Служби безпеки України (підрозділ 2.2), а також встановити форми та методи реалізації інформаційної безпеки України (підрозділ 2.3). Для узагальнення міжнародного досвіду правового регулювання забезпечення реалізації інформаційної безпеки та опрацювання можливостей його використання в Україні (підрозділ 3.1) було використано *порівняльно-правовий* метод. З'ясувати напрямки вдосконалення організаційно-правового забезпечення реалізації інформаційної безпеки України (підрозділ 2.1) вдалось за допомогою використання методів *моделювання* та *прогнозування*.

*Науково-методологічну основу* дисертаційної роботи складає сукупність загальних та спеціальних методів наукового пізнання, застосування яких обумовлюється системним підходом, що надало можливість досліджувати проблеми в єдності їх соціального змісту і юридичної форми.

*Нормативно-правову основу* складають нормативно-правові акти різної юридичної сили, норми яких спрямовані на правове регулювання забезпечення реалізації інформаційної безпеки України.

*Науково-теоретичне підґрунтя* дисертації складають наукові праці фахівців в галузі адміністративного права, загальної теорії держави і права, конституційного права, а також інших галузевих наук, зокрема: соціології, політології, філософії тощо.

**Наукова новизна отриманих результатів** полягає у тому, що дисертаційне дослідження є однією із перших спроб комплексно, на монографічному рівні, з'ясувати сутність та особливості організаційно-правових засад реалізації інформаційної безпеки України, на основі чого розробити пропозиції та рекомендації щодо вдосконалення організаційно-правових засад здійснення відповідної діяльності. До основних наукових положень, що характеризують новизну отриманих результатів й виносяться на захист, належать такі:

*уперше:*

– на доктринальному рівні акцентовано увагу на тому, що тільки після початку агресії російської федерації проти України, яка в тому числі здійснюється в інформаційному просторі, українське суспільство та публічна влада почали по-справжньому уважно і відповідально ставитися до питання забезпечення інформаційної безпеки, зокрема, від визнання деяких окремих загроз і викликів, що стоять перед Україною в інформаційній сфері, а також від

визначення певних напрямків їх подолання, влада перейшла до: формулювання комплексу концептуальних засад, стратегічних пріоритетів, цілей і напрямків щодо забезпечення інформаційної безпеки України, як на глобальному, так і національному рівні; закріплення на законодавчому рівні основних засад організації та функціонування адміністративно-правового механізму забезпечення інформаційної безпеки із розподілом відповідних завдань і повноважень між суб'єктами публічної влади;

– комплексно виокремлено коло форм реалізації інформаційної безпеки України, які запропоновано поділити на три великі групи: 1) нормативно-правові (нормотворча, установча та правозастосовна форми); 2) організаційно-управлінські (проведення зборів (нарад); науково-практичних конференцій; розробка прогнозів, програм у сфері забезпечення інформаційної безпеки; матеріально-технічне забезпечення); та 3) спеціальні (інформаційний патронат; інформаційна кооперація; інформаційне протиборство);

– акцентовано увагу на тому, що в Україні на прикладі провідних держав Європи та світу варто розширити співпрацю не тільки між різними органами державної влади у сфері інформаційної безпеки, а й іншими недержавними суб'єктами, зокрема фахівцями ІТ-сфери, а також різними підприємствами, організаціями, які здійснюють свою діяльність у галузі використання інформаційних технологій;

*удосконалено:*

– теоретичний підхід щодо розуміння видів підзаконних нормативно-правових актів, які складають підґрунтя реалізації інформаційної безпеки України, які зокрема поділено на: 1) концептуальні, до яких належать ті акти, в яких викладені концептуальні та стратегічні засади державної політики у сфері забезпечення інформаційної безпеки, програмні цілі та завдання з її реалізації; 2) статусні – в яких закріплюється адміністративно-правовий статус (цілі, завдання, функції, права та обов'язки тощо) суб'єктів публічної влади, які у тій чи іншій мірі виконують коло завдань, спрямованих на забезпечення реалізації інформаційної безпеки; 3) функціональні – підзаконні нормативно-правові акти, положеннями яких закріплюються безпосередні заходи з реалізації інформаційної безпеки, врегульовуються і конкретизуються форми та процедури її здійснення;

– класифікацію суб'єктів забезпечення реалізації інформаційної безпеки, які поділено на дві групи: 1) суб'єкти загальної компетенції, до яких належать Верховна Рада України, Президент України, Кабінет Міністрів України, місцеві державні адміністрації, органи місцевого самоврядування; 2) суб'єкти забезпечення реалізації інформаційної безпеки України міжгалузевої компетенції (суди та органи прокуратури); 3) суб'єкти галузевої компетенції; 4) суб'єкти спеціальної компетенції (Державна служба спеціального зв'язку та захисту інформації України, Національна поліція України та Служба безпеки України);

– тезу про те, що правове регулювання забезпечення реалізації інформаційної безпеки є явищем комплексним і його не можна звести до засобів та (або) методів якоїсь окремої правової галузі, оскільки у механізмі цього забезпечення задіяна ціла низка суб'єктів різного рівня і статусу, а інструменти

реалізації інформаційної безпеки мають юридичний, управлінський, технічний, культурний та інший характер, використання яких опосередковується правовідносинами, що мають як управлінську, так й іншу природу;

*дістало подальшого розвитку:*

– обґрунтування наукової думки про те, що нормативно-правовий напрямок розвитку державної політики у сфері забезпечення реалізації інформаційної безпеки України включає: а) забезпечення своєчасного оновлення нормативно-правового підґрунтя механізму забезпечення інформаційної безпеки в Україні, приводячи його у відповідність до перспектив подальшого розвитку та актуальних викликів і загроз; б) гармонійне поєднання дотримання прав і свобод людини та громадянина в інформаційній сфері з національними інтересами держави; в) забезпечення нормативно-правових засад для ефективного просвітництва населення, підвищення їх медійної грамотності, правової культури та свідомості; г) створення сприятливих та нормативно-правових умов для розвитку економічної активності населення у інформаційній сфері; ґ) вдосконалення матеріально-правових та процедурних засад контролю в інформаційній сфері, своєчасне виявлення та оцінювання ризиків; д) створення сприятливого нормативно-правового середовища для взаємодії публічної влади всіх рівнів із громадськістю з питань інформації та інформаційної діяльності;

– обґрунтування необхідності розширення системи законодавчих актів у сфері забезпечення реалізації інформаційної безпеки шляхом прийняття таких Законів України: «Про захист інформації в сфері охорони здоров'я»; «Про електронний підпис»; «Про мережу та інформаційну безпеку»; «Про кіберзахист критичних інфраструктур»; «Про кіберзахист урядових систем». Прийняття цих документів, як вбачається: а) розширить сферу забезпечення інформаційної безпеки; б) створить сприятливі умови для захисту інформації в окремих важливих галузях, наприклад, діяльності уряду, а також критичних інфраструктур.

**Практичне значення отриманих результатів** полягає в тому, що сформульовані в дисертації пропозиції та висновки можуть бути використані у:

– *науково-дослідній сфері* – для подальшого наукового опрацювання теоретико-прикладних питань, пов'язаних із організаційно-правовими засадами реалізації інформаційної безпеки України;

– *правотворчості* – під час розробки нових та вдосконалення діючих нормативно-правових актів, норми яких спрямовані на регулювання суспільних відносин, які виникають в процесі реалізації інформаційної безпеки в Україні;

– *правозастосовній діяльності* – для покращення практичної діяльності суб'єктів, що уповноважені реалізовувати заходи у сфері забезпечення реалізації інформаційної безпеки України;

– *освітньому процесі* – під час підготовки лекційних, навчально- та науково-методичних матеріалів, підручників та навчальних посібників з дисципліни «Адміністративне право», а також інших дисциплін адміністративно-правового характеру.

**Апробація матеріалів дисертації.** Підсумки розробки проблеми у цілому, окремі її аспекти, одержані узагальнення і висновки були оприлюднені на

міжнародних конференціях: «Виклики сучасності та наукові підходи до їх вирішення» (м. Київ, 12–13 серпня 2020 року); «Актуальні проблеми імплементації наукових досягнень у практичну діяльність» (м. Київ, 19–20 січня 2022 року); «Науково-практичні засади розвитку наукової думки на сучасному етапі державотворення» (м. Київ, 22–23 вересня 2021 р.)

**Структура та обсяг дисертації.** Дисертація складається зі вступу, трьох розділів, які містять вісім підрозділів, висновків, списку використаних джерел і додатків. Загальний обсяг дисертації становить 223 сторінки. Список використаних джерел містить 165 найменувань на 18 сторінках.

## ОСНОВНИЙ ЗМІСТ РОБОТИ

У **вступі** обґрунтовуються вибір теми дисертаційного дослідження, її зв'язок з науковими програмами, темами, планами, грантами, визначаються об'єкт, предмет і методи дослідження, його мета та завдання, розкриваються наукова новизна отриманих результатів, теоретичне і практичне значення роботи, надаються відомості про апробацію результатів дослідження.

**Розділ 1 «Теоретико-методологічні забезпечення реалізації інформаційної безпеки України»** складається із трьох підрозділів, в яких: здійснено історико-правовий аналіз становлення та розвитку інформаційної безпеки України; розкрито напрямки розвитку державної політики у сфері забезпечення реалізації інформаційної безпеки України; проаналізовано сучасний стан правового регулювання забезпечення реалізації інформаційної безпеки України.

У *підрозділі 1.1 «Становлення та розвиток інформаційної безпеки України»* акцентовано увагу на тому, що проблематика забезпечення інформаційної безпеки України не втрачає своєї актуальності вже багато років. Сьогодні, в умовах інформаційної війни, яка ведеться російською федерацією проти нашої держави на рівні з повномасштабним військовим вторгненням, вона постала особливо гостро. Відмічено, що перш ніж проводити науково-теоретичне опрацювання нагальних проблемних питань інформаційної безпеки та засобів її забезпечення, доцільно поглянути на історико-правові умови становлення і розвитку зазначеної проблематики.

Наголошено, що період від проголошення державного суверенітету до прийняття Конституції України включно, тобто 1990 – 1996 роки 20-го століття, слід вважати першим етапом становлення та розвитку інформаційної безпеки України. Разом із тим відзначено: говорити про те, що саме у цей час почалося формування цілісного механізму забезпечення зазначеної безпеки, навряд чи доцільно, адже тоді ще не існувало чіткого розуміння сутності інформаційної безпеки як складової національної безпеки, не було закладено концептуальних і стратегічних засад організації, функціонування та розвитку механізму інформаційної безпеки.

З'ясовано, що другий період становлення і розвитку інформаційної безпеки України, який припадає на 1998 – 2006 роки, був не такий насичений за кількістю

прийнятих нових нормативно-правових актів з питань інформації та інформаційної діяльності, однак він ознаменувався перш за все тим, що саме на цьому етапі українська влада нарешті прямо позначила інформаційну безпеку як неодмінну і вкрай важливу складову національної безпеки. Також на даному етапі були вперше, з моменту проголошення незалежності України, сформульовані та закріплені на офіційному рівні деякі концептуальні засади та програмні цілі і завдання забезпечення інформаційної безпеки в нашій державі.

Аргументовано, що третій етап становлення та розвитку інформаційної безпеки, який тривав з 2007 по 2014 рік, характеризується тим що: було сформульоване і закріплене на законодавчому рівні поняття інформаційної безпеки; інформаційна безпека була віднесена до однієї із ключових і пріоритетних на даному етапі суспільного розвитку сфер державної політики; закріплено пріоритет національних інтересів у сфері інформаційної безпеки перед індивідуальними; визначено основні проблеми забезпечення інформаційної безпеки в Україні, а також засоби і шляхи їх усунення та подальшого удосконалення механізму інформаційної безпеки; починають впроваджуватися міжнародні стандарти і норми протидії злочинній активності у інформаційному (зокрема кібернетичному) просторі.

Відмічено, що четвертий етап становлення і розвитку інформаційної безпеки України розпочався у 2014 році після російської агресії проти нашої держави і триває до теперішнього часу. Саме ця подія досить чітко вказала на те: що війна може бути не лише у вигляді збройного протистояння, але й інформаційною, а фронт, відповідно може бути як військовий, так й інформаційний; що інформаційний суверенітет – це не якесь абстрактне, а цілком реальне явище, від забезпечення якого залежать і державність, і територіальна цілісність, і національна ідентичність; що для того, щоб захистити національні інтереси недостатньо запровадити заходи протидії лише окремим проявам злочинної активності в інформаційній сфері, натомість має бути сформований цілісний, комплексний, дієвий механізм, який би дозволяв вчасно виявляти та ефективно протистояти інформаційним загрозам будь-якого характеру і масштабу.

У *підрозділі 1.2 «Напрямки розвитку державної політики у сфері забезпечення реалізації інформаційної безпеки України»* підкреслено, що сьогодні, як і раніше, в нашій країні особлива увага приділяється розвитку інформаційного суспільства, комп'ютерних технологій та кіберпростору, однак при цьому, у реаліях війни росії проти України, яка ведеться як на фізичному полі бою, так і в інформаційному просторі (при чому інформаційний фронт проти нашої держави росія відкрила набагато раніше, аніж здійснила військове вторгнення), особливий акцент робиться на забезпеченні інформаційної безпеки держави та національних інтересів. З огляду на зазначене акцентовано увагу, що важливим напрямком теоретичних досліджень є вивчення питання розвитку державної політики у сфері забезпечення реалізації інформаційної безпеки України.

Спираючись на аналіз наукових поглядів вчених стосовно тлумачення понять «політика» та «державна політика», під державною політикою у сфері забезпечення інформаційної безпеки України запропоновано розуміти діяльність

(дії, комплекс дій, рішення тощо) суб'єктів публічної влади щодо визначення мети (цілей), завдань, пріоритетів, напрямків і засобів досягнення стабільності та захищеності національного інформаційного простору та інформаційних ресурсів від різного роду загроз як внутрішнього, так і зовнішнього характеру.

Здійснено комплексний аналіз «Стратегії інформаційної безпеки України», яка була затверджена Указом Президента України від 28 грудня 2021 року №685/2021, на основі чого було виокремлено такі ключові напрямки забезпечення реалізації інформаційної безпеки України: 1) ідеологічний; 2) нормативно-правовий; 3) організаційно-управлінський; 4) культурно-освітній; 5) налагодження ефективної, системної та систематичної внутрішньодержавної взаємодії та міжнародної співпраці з питань інформації та інформаційної безпеки; 6) інноваційний. Надано змістовну характеристику кожному виділеному напрямку.

У *підрозділі 1.3 «Сучасний стан правового регулювання забезпечення реалізації інформаційної безпеки України»* констатовано, що існуючий на сьогодні механізм правового регулювання інформаційної безпеки України не позбавлений недоліків. На підтвердження даної тези здійснено аналіз ряду наукових поглядів вчених, які у своїх працях розглядали окремі проблемні питання, присвячені проблемі правового регулювання реалізації інформаційної безпеки в нашій державі.

Здійснено аналіз чинного законодавства, норми якого спрямовані на регулювання інформаційної безпеки в Україні. З огляду на проведене дослідження було аргументовано, що наразі на законодавчому рівні не існує комплексного нормативно-правового акту з питань реалізації державної політики саме у сфері інформаційної безпеки України, що є суттєвою прогалиною як на теоретичному, так і практичному рівні.

У підсумку сучасний стан нормативно-правового регулювання забезпечення реалізації інформаційної безпеки України охарактеризовано як задовільний. Констатовано, що наразі інформаційна безпека на офіційному рівні визнана неодмінною і вкрай важливою складовою забезпечення національної, державної та воєнної безпеки держави, а нормативно-правові засади механізму забезпечення реалізації безпосередньо самої інформаційної безпеки розраховані не лише на боротьбу із конкретними нагальними загрозами і небезпеками, а на всебічне зміцнення і розвиток інформаційної сфери України з урахуванням як національних, так і міжнародних інтересів нашої держави. Втім, як недолік відзначено відсутність закону «Про інформаційну безпеку України», який мав би стати стрижневим у системі нормативно-правових актів з питань інформаційної безпеки, не сприяє узгодженій та послідовній реалізації цієї безпеки.

**Розділ 2. «Механізм організаційно-правового забезпечення реалізації інформаційної безпеки України»** складається із трьох підрозділів, в яких: розмежовано галузі права у правовому регулюванні забезпечення реалізації інформаційної безпеки України; надано характеристику системі суб'єктів забезпечення реалізації інформаційної безпеки України та встановлено місце серед них Служби безпеки України; визначено форми та методи реалізації інформаційної безпеки України.

У *підрозділі 2.1 «Розмежування галузей права у правовому регулюванні забезпечення реалізації інформаційної безпеки України»* відмічається, що механізм забезпечення реалізації інформаційної безпеки України являє собою складне, багаторівневе і багатоаспектне утворення, в межах якого переплітається та поєднується велика кількість різного роду суспільних відносин, для належного впорядкування і гарантування яких потрібне залучення засобів регулювання різних галузей права, що обумовлено як специфікою суб'єктного складу цих відносин, так і їх предметною основою. Саме тому важливе теоретичне значення мають дослідження, присвячені питанню розмежуванню галузей права у правовому регулюванні забезпечення реалізації інформаційної безпеки України.

З огляду на аналіз ряду наукових позицій вчених щодо визначення поняття та розуміння змісту предмета регулювання адміністративної та інформаційної галузей права, зроблено висновок про те, що засобами адміністративного права визначаються і регламентуються перш за все загальні матеріальні і процедурні засади організації та функціонування державної політики щодо забезпечення інформаційної безпеки. Підкреслено, що поряд із адміністративним та інформаційним правом, засобами яких регулюється забезпечення реалізації інформаційної безпеки, слід відмітити і конституційне право.

Узагальнено, що правове регулювання забезпечення реалізації інформаційної безпеки є явищем комплексним і його не можна зводити до засобів та (або) методів якоїсь окремої правової галузі, оскільки у механізмі цього забезпечення задіяна ціла низка суб'єктів різного рівня і статусу, а інструменти реалізації інформаційної безпеки мають юридичний, управлінський, технічний, культурний й інший характер, використання яких опосередковується правовідносинами, що мають як управлінську, так й іншу природу.

У *підрозділі 2.2 «Система суб'єктів забезпечення реалізації інформаційної безпеки України та місце серед них Служби безпеки України»* здійснено аналіз наукових поглядів вчених стосовно тлумачення понять «суб'єкт» та «система», на основі чого запропоновано авторське визначення поняття «система суб'єктів забезпечення реалізації інформаційної безпеки України».

З'ясовано, що система суб'єктів забезпечення реалізації інформаційної безпеки являє собою складний механізм, тобто сукупність активних, взаємопов'язаних і взаємодіючих суб'єктів, що перебувають у певній ієрархії та виконують відведене їм функціональне призначення. Обсяги і характер компетенції зазначених суб'єктів у досліджуваній сфері різняться залежно від того, чи є забезпечення реалізації інформаційної безпеки для них основним (одним із декількох основних) чи супутнім напрямом діяльності.

Здійснено класифікацію суб'єктів забезпечення реалізації інформаційної безпеки України, які запропоновано ділити за такими критеріями: 1) суб'єкти загальної компетенції, до яких належать Верховна Рада України, Президент України, Кабінет Міністрів України, місцеві державні адміністрації, органи місцевого самоврядування; 2) суб'єкти забезпечення реалізації інформаційної безпеки України міжгалузевої компетенції (суди та органи прокуратури); 3) суб'єкти галузевої компетенції; 4) суб'єкти спеціальної компетенції (Державна служба спеціального зв'язку та захисту інформації України, Національна поліція

України та Служба безпеки України). Надано змістовну характеристику правовому статусу кожному із визначених суб'єктів.

Аргументовано, що в системі відповідних суб'єктів самостійне та незалежне місце відводиться Службі безпеці України. Наведено низку аргументів на підтвердження даної тези.

У *підрозділі 2.3 «Форми та методи реалізації інформаційної безпеки України»* акцентовано увагу на важливості встановлення та подальшого вивчення форм реалізації інформаційної безпеки України. Здійснено аналіз наукових поглядів вчених стосовно тлумачення поняття «форма» з точки зору різних галузевих дисциплін, на основі чого запропоновано авторське визначення терміну «форми реалізації інформаційної безпеки України». Аргументовано, що відповідні форми є широкими за своїм змістом та сутністю, а відтак їх запропоновано поділити на: 1) нормативно-правові, 2) організаційно-управлінські, та 3) спеціальні форми, що властиві саме для реалізації інформаційної безпеки. Надано змістовну характеристику кожній із окреслених груп форм.

Відмічено, що реалізація окреслених вище форм передбачає використання низки встановлених нормами чинного законодавства інструментів та засобів, які прийнято називати методами. На підставі аналізу наукових поглядів вчених зроблено висновок, що під методами реалізації інформаційної безпеки України найбільш доцільно розуміти сукупність визначених у нормах чинного законодавства механізмів, інструментів та засобів, які використовують у своїй діяльності спеціально-уповноважені суб'єкти задля досягнення кінцевої мети у відповідній сфері. Виокремлено коло відповідних методів та надано їм змістовну характеристику.

Узагальнено, що саме наведені форми та методи відображають найбільш важливі практичні аспекти реалізації інформаційної безпеки в Україні. Так, якщо форми є зовнішнім проявом практичної діяльності спеціально уповноважених органів у відповідній сфері, то методи вказують, які при цьому були використані інструменти. Втім, як суттєвий недолік відмічено, що окреслені форми та методи не віднайшли своє законодавче закріплення, а відтак, дана прогалина потребує усунення шляхом внесення змін та доповнень до чинного законодавства, норми якого регулюють питання забезпечення та реалізації інформаційної безпеки в Україні.

**Розділ 3 «Шляхи вдосконалення організаційно-правового забезпечення реалізації інформаційної безпеки України»** складається із двох підрозділів, в яких: узагальнено міжнародний досвід правового регулювання забезпечення реалізації інформаційної безпеки та опрацьовано можливості його використання в Україні; з'ясовано напрямки вдосконалення організаційно-правового забезпечення реалізації інформаційної безпеки України.

У *підрозділі 3.1 «Міжнародний досвід правового регулювання забезпечення реалізації інформаційної безпеки та можливості його використання в Україні»* обґрунтовується важливість та необхідність проведення комплексних теоретичних досліджень, присвячених вивченню зарубіжного досвіду правового регулювання забезпечення реалізації інформаційної безпеки.

Значну увагу приділено досвіду Сполучених Штатів Америки, адже забезпечення інформаційної безпеки в цій країні має глибоке коріння. У XX столітті ця держава відіграла ключову роль у розвитку інформаційних технологій, що дозволило їм бути «першопрохідниками» у боротьбі з інформаційними загрозами. А відтак саме США була однією із перших країн, яка розробила державну політику і систему державного регулювання в інформаційній сфері.

Встановлено, що забезпечення інформаційної безпеки в Канаді визначається як один із найважливіших аспектів національної безпеки та економічного розвитку. Ця країна відзначається високим рівнем залученості до використання сучасних інформаційних технологій у різних сферах, включаючи бізнес, урядову діяльність та громадянські послуги.

Здійснено аналіз досвіду ряду Європейських держав, зокрема Великобританії, Німеччини та Франції. Узагальнено, що на сьогоднішній день всі провідні держави Європи та світу прагнуть створити належні правові та організаційні умови для забезпечення інформаційної безпеки. З огляду на проведене дослідження запропоновано авторське бачення щодо найбільш позитивного зарубіжного досвіду, який слід запровадити вітчизняному законодавцю з метою вдосконалення системи забезпечення реалізації інформаційної безпеки України.

У *підрозділі 3.2 «Напрямки вдосконалення організаційно-правового забезпечення реалізації інформаційної безпеки України»* констатується той факт, що на сьогоднішній день в Україні є наявною низка проблем правового та організаційного характеру у сфері забезпечення реалізації інформаційної безпеки. Наголошено, що важливим напрямком діяльності законодавця та вітчизняних науковців є вдосконалення: по-перше, чинного законодавства, норми якого спрямовані на регулювання суспільних відносин у відповідній сфері; по-друге, організаційних засад реалізації діяльності у галузі забезпечення інформаційної безпеки.

Здійснено аналіз наукових поглядів вчених, які у своїх наукових працях звертали увагу на окремі проблемні питання інформаційної безпеки в державі, на основі чого було відзначено, що переважна більшість теоретичних розробок: по-перше, втратили свою актуальність, оскільки були написані ще до повномасштабного вторгнення, а відтак не враховують всю специфіку сучасної інформаційної війни, яка наразі відбувається у медійному просторі; по-друге, переважна більшість робіт спрямована на покращення саме організаційного забезпечення інформаційної безпеки, в той час я покращенню норм чинного законодавства увага приділялась досить поверхнево.

Сформульовано авторське бачення щодо напрямів вдосконалення організаційно-правового забезпечення реалізації інформаційної безпеки України. В даному контексті першим кроком має бути розробка нової «Стратегії інформаційної безпеки України», яка буде враховувати набутий досвід протидії російській федерації. Доведена необхідність суттєвого розширення законодавчої бази у сфері забезпечення інформаційної безпеки, що має передбачати розробку та прийняття ряду законодавчих та підзаконних нормативно-правових актів.

Аргументовано, що покращення правового регулювання не може здійснюватись поза вдосконаленням організаційних засад забезпечення інформаційної безпеки в Україні. В даному контексті запропоновано вдосконалити систему кадрового забезпечення суб'єктів, що реалізують державну політику у досліджуваній сфері, а також якісно покращити фінансове та матеріально-технічне забезпечення відповідного напрямку національної безпеки.

## ВИСНОВКИ

У дисертації наведено теоретичне узагальнення та нове розв'язання наукового завдання, яке полягає у тому, щоб розкрити сутність та особливості організаційно-правових засад реалізації інформаційної безпеки України, на основі чого розробити пропозиції та рекомендації спрямовані на вдосконалення правових та організаційних засад здійснення відповідної діяльності. У результаті дослідження сформульовано низку нових наукових висновків, основні з них такі:

1. Виокремлено ключові етапи становлення та розвитку інформаційної безпеки України:

– перший етап (1990 – 1996 роки). На даному етапі відбувається визнання офіційною владою інформаційної сфери як окремої, самостійної і вкрай важливої галузі суспільного життя. Окрім того, в цей час закріплюється, що інформація та інформаційна діяльність не лише сприяють розвитку держави і суспільства, але можуть становити суттєву загрозу для їх інтересів;

– другий етап (1998 – 2006 роки), на якому було вперше з моменту проголошення незалежності України сформульовано та закріплено на офіційному рівні деякі концептуальні засади та програмні цілі і завдання забезпечення інформаційної безпеки в нашій державі;

– третій етап (2007 – 2014 роки). Даний етап характеризується тим, що в цей час було сформульоване і закріплено на законодавчому рівні поняття інформаційної безпеки; інформаційна безпека була віднесена до однієї із ключових і пріоритетних на даному етапі суспільного розвитку сфер державної політики; закріплено пріоритет національних інтересів у сфері інформаційної безпеки перед індивідуальними; визначено основні проблеми забезпечення інформаційної безпеки в Україні, а також засоби і шляхи їх усунення та подальшого удосконалення механізму інформаційної безпеки; починають впроваджуватися міжнародні стандарти і норми протидії злочинній активності у інформаційному (зокрема кібернетичному) просторі;

– четвертий етап, який розпочався у 2014 році після російської агресії проти нашої держави і триває до теперішнього часу. Саме ця подія досить чітко вказала на те: що війна може бути не лише у вигляді збройного протистояння, але й інформаційною, а фронт, відповідно може бути як військовий, так й інформаційний; що інформаційний суверенітет – це не якесь абстрактне, а цілком реальне явище, від забезпечення якого залежать і державність, і територіальна цілісність, і національна ідентичність; що для того, щоб захистити національні інтереси недостатньо запровадити заходи протидії лише окремим проявам

злочинної активності в інформаційній сфері, натомість має бути сформований цілісний, комплексний, дієвий механізм, який би дозволяв вчасно виявляти та ефективно протистояти інформаційним загрозам будь-якого характеру і масштабу.

2. З'ясовано, що ключовими напрямками забезпечення реалізації інформаційної безпеки України є: 1) ідеологічний; 2) нормативно-правовий; 3) організаційно-управлінський; 4) культурно-освітній; 5) налагодження ефективної, системної та систематичної внутрішньодержавної взаємодії та міжнародної співпраці з питань інформації та інформаційної безпеки; 6) інноваційний напрямок. Наголошено, що законодавець повинен здійснювати належне правове регулювання за всіма без винятку виокремленими напрямками забезпечення реалізації інформаційної безпеки.

3. Сучасний стан нормативно-правового регулювання забезпечення реалізації інформаційної безпеки України охарактеризовано як такий, що потребує подальшого вдосконалення, адже на сьогодні в нашій державі прийнято цілу низку нормативно-правових актів різної юридичної сили, які визначають концептуальні, матеріально-правові, процедурні аспекти реалізації зазначеної безпеки. Наразі інформаційна безпека на офіційному рівні визнана неодмінною і вкрай важливою складовою забезпечення національної, державної та воєнної безпеки держави, а нормативно-правові засади механізму забезпечення реалізації безпосередньо самої інформаційної безпеки розраховані не лише на боротьбу із конкретними нагальними загрозами і небезпеками, а й на всебічне зміцнення і розвиток інформаційної сфери України з урахуванням як національних, так і міжнародних інтересів нашої держави. Наголошено на необхідності прийняття закону України «Про інформаційну безпеку України», який мав би стати стрижневим у системі нормативно-правових актів з питань інформаційної безпеки, і сприяти узгодженій та послідовній реалізації цієї безпеки.

4. Констатовано, що правове регулювання забезпечення реалізації інформаційної безпеки є явищем комплексним і його не можна звести до засобів та (або) методів якоїсь окремої галузі права. Зокрема за допомогою адміністративно-правових засобів і механізмів врегульовані такі питання як: адміністративно-правовий статус центральних та територіальних органів виконавчої влади, які у тій чи іншій мірі залучені до забезпечення реалізації інформаційної безпеки в Україні; концептуальні та стратегічні засади забезпечення й розвитку інформаційної безпеки; пріоритетні напрямки діяльності та взаємодії суб'єктів публічної влади з питань інформаційної безпеки, а також координація їх діяльності; процедури та заходи протидії загрозам і викликам у сфері інформаційної безпеки України як на внутрішньому, так і зовнішньому рівнях; адміністративна відповідальність за порушення інформаційного законодавства та порядок притягнення до адміністративної відповідальності. У свою чергу нормами інформаційного права врегульовані ті відносини, процеси, факти, які стосуються: форм і способів створення (виготовлення, виробництва) інформації, її накопичення, зберігання, режимів використання і розповсюдження; реалізації індивідуальними і колективними суб'єктами своїх інформаційних прав та обов'язків; формування інформаційної культури населення та проведення

відповідної просвітницької діяльності. Акцентовано увагу, що поряд із нормами адміністративного та інформаційного права забезпечення реалізації інформаційної безпеки врегульовано нормами і конституційного права. Саме нормами Конституції України: встановлено загальне правове поле, в межах якого відбувається реалізація зазначеної безпеки; закріплено основоположні гарантії та пріоритети на яких ґрунтується суспільно-державне життя в цілому та його інформаційна сфера зокрема; врегульовано правове становище суб'єктів загальної компетенції, які визначають організаційно-правові, ідеологічні, управлінські та інші основи державної політики щодо забезпечення інформаційної безпеки.

5. Обґрунтовано, що на сьогодні в Україні створена та функціонує розгалужена і багаторівнева система суб'єктів забезпечення реалізації інформаційної безпеки. Всередині цієї системи існує доволі чітке розмежування компетенцій між зазначеними суб'єктами, кожен з яких виконує певний обсяг роботи, орієнтованої на забезпечення зазначеної безпеки. Так одні визначать загальні правові засади і принципи її забезпечення, другі – концептуальні засади, стратегічні напрямки та пріоритети зміцнення і розвитку інформаційної безпеки; треті – розробляють програми реалізації зазначених концептуальних і стратегічних засад, визначають матеріальні і процедурні аспекти виконання закріплених правових засад і принципів з огляду на реалії і потреби сьогодення; четверті – контролюють та координують практичну реалізацію заходів інформаційної безпеки у відповідності до вимог законності та ключових засад державної політики у цій сфері, а також опікуються питаннями ресурсного забезпечення діяльності, спрямованої на забезпечення інформаційної безпеки; п'яті – безпосередньо на практиці виконують конкретні заходи правового, організаційного, технічного та іншого характеру, спрямовані на протидію загрозам інформаційній безпеці України, зміцнення стійкості національного інформаційного простору, захист прав і законних інтересів його індивідуальних та колективних учасників, зокрема держави і суспільства в цілому. Наголошено, що особлива роль у сфері забезпечення реалізації інформаційної безпеки відводиться Службі безпеки України, яка має здійснювати комплекс заходів, що передбачають протидію ворожому впливу і агресії в інформаційному середовищі як шляхом відбиття атак, так і через здійснення активних атакуючих дій, спрямованих на ліквідацію чи пригнічення ворожих інформаційних ресурсів та інфраструктури, що забезпечує їх функціонування.

6. Встановлено, що форми реалізації інформаційної безпеки України являють собою зовнішній прояв практичної діяльності спеціально уповноважених суб'єктів, яка спрямована на створення правових та організаційних умов для забезпечення конфіденційності, цілісності та доступності інформації, а також на захист інформаційних ресурсів від несанкціонованого доступу, втрати, зміни, руйнування або розголошення. Констатовано, що відповідні форми найбільш доцільно поділити на три групи: 1) нормативно-правові (нормотворча, установча та правозастосовна форми); 2) організаційно-управлінські (проведення зборів (нарад); науково-практичних конференцій; розробка прогнозів, програм у сфері забезпечення інформаційної

безпеки; матеріально-технічне забезпечення); 3) спеціальні форми, що властиві саме для реалізації інформаційної безпеки (інформаційний патронат; інформаційна кооперація; інформаційне протиборство).

Під методами реалізації інформаційної безпеки України запропоновано розуміти сукупність визначених у нормах чинного законодавства механізмів, інструментів та засобів, які використовують в своїй діяльності спеціально-уповноважені суб'єкти задля досягнення кінцевої мети у відповідній сфері. Відповідні методи запропоновано поділити на дві групи: 1) загальні (переконання та примусу); та 2) спеціальні, зокрема: шифрування даних; аудит інформаційної безпеки; кіберзахист; управління доступом; інформаційна гігієна; моніторинг і виявлення загроз; метод кризового управління.

7. Узагальнено, що на сьогоднішній день всі провідні держави світу прагнуть створити належні правові та організаційні умови для забезпечення інформаційної безпеки. А відтак, з позитивного боку слід виділити такий зарубіжний досвід, який варто використати вітчизняному законодавцю в межах вдосконалення правового регулювання забезпечення реалізації інформаційної безпеки в українських реаліях: по-перше, вбачається необхідним значно розширити чинну нормативно-правову базу шляхом прийняття низки законодавчих актів, наприклад, законів, спрямованих на регулювання кіберзахисту урядових систем, критичних інфраструктур, тощо; по-друге, в окремих країнах, зокрема США, суттєва увага приділяється підготовці фахівців, що будуть здійснювати діяльність у сфері забезпечення інформаційної безпеки; по-третє, значний рівень фінансового забезпечення урядових програм, спрямованих на якісне покращення інформаційної безпеки в державі; по-четверте, розширення співпраці не тільки між різними органами державної влади, а й недержавними суб'єктами, зокрема фахівцями ІТ-сфери, а також іншими підприємствами, організаціями, які здійснюють свою діяльність у галузі інформаційних технологій; по-п'яте, в переважній більшості країн існують «просунуті» стратегії кібербезпеки, які постійно оновлюються та враховують виклики сучасності.

8. Обґрунтовано, що покращення забезпечення реалізації інформаційної безпеки України має здійснювати за двома ключовими напрямками:

1) вдосконалення законодавства у відповідній сфері, що має включати:

– розробку нової «Стратегії інформаційної безпеки України», адже незважаючи на те, що попередня Стратегія була прийнята у 2021 році і розрахована до 2025 року, перші півроку повномасштабної війни показали, що нашій державі досить складно протистояти зовнішньому ворогу. Втім, далі ситуація змінювалася у кращий бік і Україна отримала перевагу, а відтак, розроблення нової Стратегії буде здійснюватись з урахуванням набутого досвіду, та враховувати сучасні виклики та загрози;

– розробку та прийняття Законів України: «Про захист інформації в сфері охорони здоров'я»; «Про електронний підпис»; «Про мережу та інформаційну безпеку»; «Про кіберзахист критичних інфраструктур»; «Про кіберзахист урядових систем». Прийняття вказаних нормативно-правових актів дозволить: а) розширити сферу забезпечення інформаційної безпеки; б) створити сприятливі

умови для захисту інформації в окремих важливих галузях, наприклад, діяльності уряду, а також критичних інфраструктур;

– розробити та прийняти «Порядок взаємодії суб'єктів забезпечення інформаційної безпеки», який має бути спрямовано на визначення правових та організаційних засад здійснення спільної діяльності спеціально уповноважених суб'єктів у досліджуваній сфері.

2) покращення організаційно-управлінських аспектів здійснення відповідної діяльності, що має включати вдосконалення: а) кадрового забезпечення суб'єктів, що реалізують свою діяльність у напрямку реалізації інформаційної безпеки; б) системи інформаційного забезпечення; в) фінансового та матеріально-технічного забезпечення інформаційної безпеки.

## СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

***в яких опубліковані основні наукові результати дисертації:***

1. Вдовін І.О. До характеристики напрямків розвитку державної політики у сфері забезпечення реалізації інформаційної безпеки України. *Юридичний науковий електронний журнал.* 2022. № 10. С. 847–849. http://www.lsej.org.ua/10_2022/213.pdf

2. Вдовін І. Сучасний розвиток інформаційної безпеки України. *KELM*. 2022. № 7(51). С. 259–263.

3. Вдовін І.О. До характеристики сучасного стану правового регулювання забезпечення реалізації інформаційної безпеки України. *Науковий вісник публічного та приватного права.* 2023. Вип. 4. С. 86–90.

4. Вдовін І.О. До проблеми розмежування галузей права у правовому регулюванні забезпечення реалізації інформаційної безпеки України. *Науковий вісник публічного та приватного права.* 2023. Вип. 5. С. 91–95.

5. Vdovin I.O. The place of the Security Service of Ukraine in the system of entities ensuring information security. *Entrepreneurship, Economy and Law*. 2023. № 9. pp. 67–73.

***які засвідчують апробацію матеріалів дисертації:***

6. Вдовін І.О. До характеристики ідеологічного напрямку державної політики у сфері забезпечення реалізації інформаційної безпеки України. *Виклики сучасності та наукові підходи до їх вирішення*: матеріали міжнародної науково-практичної конференції (Київ, 12–13 серп. 2020 р.). Київ: Науково-дослідний інститут публічного права, 2020. С. 88–90.

7. Вдовін І.О. До характеристики правового статусу суб'єктів спеціальної компетенції забезпечення реалізації інформаційної безпеки України. *Науково-практичні засади розвитку наукової думки на сучасному етапі державотворення:* матеріали міжнародної науково-практичної конференції (Київ, 22–23 верес. 2021 р.). Київ: Науково-дослідний інститут публічного права, 2021. С. 71–74.

8. Вдовін І.О. Проблеми нормативно-правового напрямку формування та розвитку державної політики у сфері забезпечення реалізації інформаційної безпеки України. *Актуальні проблеми імплементації наукових досягнень у*

*практичну діяльність:* матеріали міжнародної науково-практичної конференції, (Київ, 19–20 січ. 2022 р.). Київ: Науково-дослідний інститут публічного права, 2022. С. 57–59.

## АНОТАЦІЯ

**Вдовін І.О. Організаційно-правові засади реалізації інформаційної безпеки України.** − *Кваліфікаційна наукова праця на правах рукопису.*

Дисертація на здобуття наукового ступеня кандидата юридичних наук за спеціальністю 12.00.07 «Адміністративне право і процес; фінансове право; інформаційне право». – Науково-дослідний інститут публічного права, Київ, 2024.

У дисертації наведено теоретичне узагальнення та нове вирішення наукового завдання, яке полягає у з'ясуванні сутності та розкритті особливостей організаційно-правових засад реалізації інформаційної безпеки України, а також опрацюванні напрямків вдосконалення організаційно-правового забезпечення відповідної сфери суспільних відносин.

Здійснено історико-правовий аналіз становлення та розвитку інформаційної безпеки України. Розкрито напрямки розвитку державної політики у сфері забезпечення реалізації інформаційної безпеки України. Оцінено сучасний стан правового регулювання забезпечення реалізації інформаційної безпеки України. Розмежовано галузі права у правовому регулюванні забезпечення реалізації інформаційної безпеки України. Надано характеристику системі суб'єктів забезпечення реалізації інформаційної безпеки України та встановлено місце серед них Служби безпеки України. Встановлено форми та методи реалізації інформаційної безпеки України. Узагальнено міжнародний досвід правового регулювання забезпечення реалізації інформаційної безпеки та опрацьовано можливості його використання в Україні. З'ясовано напрямки вдосконалення організаційно-правового забезпечення реалізації інформаційної безпеки України.

**Ключові слова**: інформація, інформаційна безпека, державна політика, правове регулювання, адміністративне право, інформаційне право, суб'єкти, форми, методи, міжнародний досвід, вдосконалення, правові засади, організаційні засади.

## SUMMARY

**Vdovin I. O. Organizational and Legal Principles of Implementing Information Security in Ukraine**. - *Qualification scientific work, manuscript*.

Thesis for obtaining a scientific degree of Candidate of Juridical Science in specialty 12.00.07 «Administrative Law and Process; Finance Law; Information Law». – Scientific Institute of Public Law, Kyiv, 2024.

The dissertation provides a theoretical generalization and a new solution to the scientific task, which involves clarifying the essence and revealing the peculiarities of the organizational and legal principles of implementing information security in Ukraine. It also analyzes the directions for improving the organizational and legal support of the relevant sphere of social relations.

A historical and legal analysis of the formation and development of information security in Ukraine is conducted. The directions of the development of state policy in the field of ensuring the implementation of information security in Ukraine are disclosed. The current state of legal regulation of ensuring the implementation of information security in Ukraine is evaluated. The branches of law in the legal regulation of ensuring the implementation of information security in Ukraine are delineated. A characteristic of the system of subjects ensuring the implementation of information security in Ukraine is provided, and their place among them, including the Security Service of Ukraine, is established. The forms and methods of implementing information security in Ukraine are determined. The international experience in the legal regulation of ensuring the implementation of information security is summarized, and the possibilities of its use in Ukraine are explored. The directions for improving the organizational and legal support of the implementation of information security in Ukraine are clarified.

**Keywords:** information, information security, state policy, legal regulation, administrative law, information law, subjects, forms, methods, international experience, improvement, legal principles, organizational principles.