НАУКОВО-ДОСЛІДНИЙ ІНСТИТУТ ПУБЛІЧНОГО ПРАВА

НІКОЛАЙЧИК ОЛЕКСАНДР СЕРГІЙОВИЧ

УДК 342.9(477)

АДМІНІСТРАТИВНІ ПРОЦЕДУРИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ В УКРАЇНІ

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:
доктор юридичних наук, професор, Заслужений діяч науки і техніки України
Дрозд Олексій Юрійович,
Бюро економічної безпеки України,
керівник Департаменту організаційного забезпечення діяльності

Офіційні опоненти:
доктор юридичних наук, професор, Заслужений юрист України
Сербин Руслан Андрійович,
Львівський державний університет внутрішніх справ,
проректор

кандидат юридичних наук, доцент
Шевченко Сергій Іванович,
Дніпровський державний університет внутрішніх справ,
заступник директора інституту післядипломної освіти та заочного навчання

Захист відбудеться «24» жовтня 2024 року о 9^{00} год 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» вересня 2024 р.

Учений секретар
спеціалізованої вченої ради Ксенія КУРКОВА

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Обґрунтування вибору теми дослідження. Протягом останніх десятиліть цифрові технології проникли в усі сфери суспільного життя та стали невід'ємною складовою функціонування держави й суспільства. Водночас розвиток останніх спричинив появу низки ризиків, пов'язаних із захистом даних та інформації, яка міститься в інформаційному просторі. У зв'язку з цим, важливим завданням світової спільноти, зокрема українського законодавця, стало створення належного рівня забезпечення кібербезпеки, за якого інтересам держави, а також правам і свободам фізичних та юридичних осіб у кіберпросторі не буде нічого загрожувати. Особливо ця проблема загострилася в умовах повномасштабного вторгнення російської федерації, яка постійно здійснює не лише атаки на критичну інфраструктуру нашої країни, а й кібератаки. З огляду на зазначене, проблема кібербезпеки має важливе значення для забезпечення безперервності роботи безпекового сектору нашої держави, а також її критичної інфраструктури, яка охоплює енергетичні мережі, водопостачання, фінансово-економічну систему і транспорт. Кібератаки на ці системи здатні призводити до значних перебоїв у їхній роботі, що може викликати економічний хаос, порушення громадського порядку та навіть загрожувати життю громадян.

Забезпечення кібербезпеки є складною за своєю сутністю та змістом діяльністю, що передбачає реалізацію низки процедур, які переважно мають адміністративний характер. Ці процедури визначають правила і порядок реагування на кібератаки, встановлюють вимоги до захисту інформації та забезпечують узгодженість дій між різними суб'єктами у сфері кібербезпеки. Таким чином, дотримання останніх має важливе значення з точки зору забезпечення законності й ефективності реалізації діяльності щодо забезпечення кібербезпеки в Україні.

Зв'язок теми дисертації із сучасними дослідженнями. Окремі проблемні аспекти, пов'язані із забезпеченням кібербезпеки в Україні, у своїх наукових працях розглядали: О. А. Баранов, Н. Л. Березовська, І. В. Діордіца, О. В. Джафарова, О. Ю. Дрозд, Ю. В. Гаруст, Є. А. Гетьман, О. В. Задерейко, О. Ф. Кобзар, О. В. Коваленко, В. К. Колпаков, О. В. Кузьменко, В. Г. Кундеус, В. І. Курило, К. М. Куркова, Ю. П. Лісовська, Н. І. Логінова, Л. І. Луценко-Миськів, А. А. Манжула, Л. В. Набока, О. В. Олійник, Ю. В. Прокоп, Р. А. Сербин, О. О. Середа, В. І. Сіверін, Є. Ю. Соболь, Л. В. Сорока, С. М. Стежко, В. М. Столбовий, О. Г. Трофіменко, Л. С. Харченко, Р. В. Шаповал, С. І. Шевченко, Т. О. Шевченко та багато інших. Проте, попри значний теоретичний доробок, у науковій літературі недостатньо опрацьованим є питання дослідження адміністративних процедур забезпечення кібербезпеки в Україні.

Отже, наявність низки прогалин і недоліків правового та організаційного характеру, пов'язаних із реалізацією адміністративних процедур забезпечення кібербезпеки, а також відсутність комплексних наукових досліджень, присвячених вказаній проблематиці, обумовлюють актуальність і своєчасність представленої дисертаційної роботи.

Зв'язок роботи з науковими програмами, планами, темами. Дисертаційне дослідження узгоджується з положеннями Стратегії інформаційної безпеки, затвердженої Указом Президента України від 28 грудня 2021 року № 685/2021; Стратегії кібербезпеки України, схваленої Указом Президента України від 26 серпня 2021 року № 447/2021; Стратегії зовнішньополітичної діяльності України, схваленої Указом Президента України від 26 серпня 2021 року № 448/2021; Цілей сталого розвитку України на період до 2030 року, затверджених Указом Президента України від 30 вересня 2019 року № 722/2019. 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 та завдання дослідження *Мета* дисертаційного дослідження полягає в тому, щоб на основі аналізу наукових поглядів учених, норм чинного законодавства та практики його реалізації з'ясувати сутність, зміст й особливості адміністративних процедур забезпечення кібербезпеки в Україні, а також, спираючись на позитивний вітчизняний і зарубіжний досвід, розкрити сучасні тенденції вдосконалення адміністративно-правового регулювання відповідної діяльності.

Досягнення поставленої мети зумовлює потребу у вирішенні таких *завдань*:

– схарактеризувати кібербезпеку як об'єкт адміністративно-правового регулювання;

– визначити поняття, розкрити особливості й виокремити види адміністративних процедур у сфері забезпечення кібербезпеки;

– окреслити коло суб'єктів реалізації адміністративних процедур у сфері забезпечення кібербезпеки;

– проаналізувати систему правового регулювання реалізації адміністративних процедур у сфері забезпечення кібербезпеки;

– розкрити адміністративні процедури, пов'язані зі змістом інформації, що обробляється в комунікаційних або в технологічних системах;

– схарактеризувати адміністративні процедури, пов'язані із захистом інформації, що становить державну таємницю, комунікаційні та технологічні системи, призначені для її оброблення;

– встановити коло адміністративних процедур захисту комунікаційних систем, які не взаємодіють з публічними мережами електронних комунікацій;

– здійснити порівняльний аналіз національних та міжнародних стандартів і практик забезпечення кібербезпеки;

– запропонувати шляхи вдосконалення правового регулювання адміністративних процедур у сфері забезпечення кібербезпеки.

Об'єктом дослідження є суспільні відносини, які виникають у процесі реалізації адміністративних процедур забезпечення кібербезпеки в Україні.

Предметом дослідження є адміністративні процедури забезпечення кібербезпеки в Україні.

Методи дисертаційного дослідження. Методологічну основу дисертаційної роботи становить сукупність загальних і спеціальних методів наукового пізнання, використання яких дало змогу комплексно підійти до виконання завдань дисертації. Так, за допомогою *логіко-семантичного* й *аналітичного* методів вдалося схарактеризувати кібербезпеку як об'єкт адміністративно-правового регулювання (підрозділ 1.1), а також визначити поняття, розкрити особливості та виокремити види адміністративних процедур у сфері забезпечення кібербезпеки (підрозділ 1.2). *Структурно-логічний* та *системно-функціональний* метод застосовано з метою окреслення кола суб'єктів реалізації адміністративних процедур у сфері забезпечення кібербезпеки (підрозділ 1.3) та узагальнення адміністративних процедур захисту комунікаційних систем, які не взаємодіють з публічними мережами електронних комунікацій (підрозділ 2.3). Метод *документального аналізу* дав змогу проаналізувати систему правового регулювання реалізації адміністративних процедур у сфері забезпечення кібербезпеки (підрозділ 1.4); розкрити адміністративні процедури, пов'язані зі змістом інформації, що обробляється в комунікаційних або в технологічних системах (підрозділ 2.1); визначити адміністративні процедури, пов'язані із захистом інформації, що становить державну таємницю, комунікаційні та технологічні системи, призначені для її оброблення (підрозділ 2.2). Щоб здійснити порівняльний аналіз національних та міжнародних стандартів і практик забезпечення кібербезпеки (підрозділ 3.1) було використано *порівняльно-правовий метод.* З'ясувати шляхи вдосконалення правового регулювання адміністративних процедур у сфері забезпечення кібербезпеки (підрозділ 3.2) вдалось за допомогою методів *моделювання* та *прогнозування*.

Нормативно-правовим підґрунтям дослідження є Конституція України, міжнародні нормативно-правові акти (ратифіковані у встановленому законом порядку), а також низка законодавчих і підзаконних актів, норми яких спрямовані на регулювання адміністративних процедур забезпечення кібербезпеки в Україні.

Науково-теоретичне підґрунтя становлять праці фахівців з галузі адміністративного та інформаційного права. Крім того, було використано напрацювання фахівців з інших галузевих дисциплін, таких як теорія держави і права, теорія управління, соціологія, філософія, психологія тощо.

Інформаційну та емпіричну основу дослідження становлять періодичні видання, статистичні матеріали тощо.

Наукова новизна отриманих результатів полягає в тому, що дисертаційне дослідження є першою спробою комплексно, на монографічному рівні з'ясувати сутність та особливості адміністративних процедур забезпечення кібербезпеки в Україні в сучасних умовах, на основі чого розробити пропозиції та рекомендації, спрямовані на вдосконалення нормативно-правового регулювання відповідної діяльності. У результаті проведеного дослідження сформульовано низку нових наукових положень і висновків, основні з них такі:

вперше:

– визначено особливості адміністративних процедур у сфері забезпечення кібербезпеки, до яких віднесено такі: по-перше, особлива сфера реалізації, а також

предмет, з приводу якого виникають відповідні суспільні відносини; по-друге, реалізовувати відповідні процедури мають право виключно спеціально уповноважені суб'єкти, посадові особи яких володіють набором специфічних професійних знань, умінь і навичок; по-третє, наявність спеціального набору нормативно-правових засад їх реалізації; по-четверте, переважна більшість адміністративних процедур пов'язані з обробкою персональних даних, що вимагає дотримання вимог законодавства про захист персональних даних; по-п'яте, наявність підвищеного рівня відповідальності суб'єктів, які відповідні процедури реалізовують; по-шосте, відповідні процедури застосовуються в різних сферах забезпечення кібербезпеки, що обумовлює наявність їх різновидів;

– встановлено, що адміністративні процедури у сфері кібербезпеки, пов'язані зі змістом інформації, яку обробляють у комунікаційних або технологічних системах, становлять окрему групу впорядкованих дій, заходів і процесів, що реалізуються уповноваженими суб'єктами та спрямовані на збір, обробку, зберігання, передачу та захист інформації у відповідних інформаційно-комунікаційних і технологічних системах. Ці процедури спрямовані на забезпечення конфіденційності, цілісності та доступності даних, а також на запобігання їх несанкціонованому доступу, розкриттю, модифікації або знищенню інформації;

– окреслено адміністративні процедури захисту комунікаційних систем, які не взаємодіють з публічними мережами електронних комунікацій, до яких віднесено такі: авторизацію та аутентифікацію визначеного переліку користувачів, що мають доступ до цієї системи; здійснення внутрішнього контролю (моніторинг та аудит системи); кадрові процедури; процедури управління та реагування на інциденти; захист даних і резервне копіювання;

удосконалено:

– теоретичний підхід щодо визначення поняття «забезпечення кібербезпеки», яким запропоновано вважати реалізований спеціально уповноваженими суб'єктами комплекс заходів, технологій, процесів та практик, спрямованих на захист інформаційних систем, мереж, даних і програм від несанкціонованого доступу, використання, розкриття, зміни, руйнування або втрати. Така діяльність включає забезпечення конфіденційності, цілісності й доступності інформації, а також протидію кіберзагрозам і кібератакам з боку зловмисників у цифровому просторі;

– твердження про те, що нормативно-правове підґрунтя реалізації адміністративних процедур у сфері кібербезпеки ґрунтується на двох групах нормативно-правових актів: 1) ті, що визначають правові, організаційні, матеріально-технічні та інші особливості процесу підтримки стану безпечного користування кіберпростором, комунікаційними та технологічними системами; 2) ті, що пояснюють зміст, значення та особливості реалізації безпосередньо адміністративних процедур у досліджуваній сфері;

– поняття суб'єктів реалізації адміністративних процедур у сфері забезпечення кібербезпеки, яким запропоновано вважати сукупність спеціально уповноважених органів державної влади (в особі їх посадових осіб), які відповідно до норм чинного законодавства наділені повноваженнями та необхідною компетенцією

щодо реалізації дій і заходів, спрямованих на створення необхідних умов для захисту інформаційних систем та мереж, а також координації дій щодо запобігання, виявлення та реагування на кіберзагрози;

дістало подальшого опрацювання:

– твердження про те, що зміст адміністративних процедур, пов'язаних з інформацією, що обробляється в комунікаційних або технологічних системах, охоплює низку оцінних, моніторингово-сканувальних, перевірочних, контрольних та експертно-дослідницьких заходів, реалізація яких дозволяє забезпечувати ефективність і безпечність роботи вказаних вище систем;

– науковий підхід щодо визначення поняття стандартів забезпечення кібербезпеки, яким запропоновано вважати набір правил, рекомендацій і вимог, що визначають методи й заходи для захисту інформаційних систем, мереж та даних від кібератак, несанкціонованого доступу, витоків даних та інших загроз кібербезпеці. Ці стандарти розроблені для встановлення загальних практик і політик, які можуть використовувати організації для забезпечення захисту своїх цифрових активів;

– обґрунтування необхідності розробки та прийняття Концепції розвитку системи забезпечення кібербезпеки в Україні, що дозволить: 1) забезпечити узгодженість і системність у правовому регулюванні адміністративних процедур у сфері кібербезпеки, усунути прогалини та суперечності в чинному законодавстві; 2) чітко визначити процедури й повноваження спеціально уповноважених суб'єктів, що спростить взаємодію між ними, забезпечить швидкість та якість прийняття управлінських рішень і зменшить бюрократичні бар'єри; 3) покращити систему правового регулювання у досліджуваній сфері, що сприятиме захисту прав суб'єктів господарювання, забезпечить прозорість та обґрунтованість рішень, які приймаються щодо них органами державної влади; 4) підвищити рівень довіри до державних органів; 5) ураховувати міжнародний досвід і стандарти у сфері кібербезпеки, що сприятиме інтеграції України в глобальний цифровий простір та поглибленню міжнародного співробітництва.

Практичне значення отриманих результатів полягає в тому, що викладені в дисертації висновки і пропозиції використовуються та можуть бути використані в:

– *науково-дослідній сфері* – як підґрунтя для проведення подальших теоретико-правових досліджень, присвячених адміністративним процедурам забезпечення кібербезпеки в Україні (акт впровадження Науково-дослідного інституту публічного права);

– *правотворчій сфері* – для розроблення нових та вдосконалення діючих законодавчих і підзаконних нормативно-правових актів, положення яких спрямовані на регулювання адміністративних процедур забезпечення кібербезпеки в Україні;

– *правозастосовній сфері* – з метою підвищення ефективності діяльності суб'єктів, які уповноважені реалізовувати адміністративні процедури у сфері забезпечення кібербезпеки в Україні;

– *освітньому процесі* – під час підготовки підручників і навчальних посібників з дисциплін «Адміністративне право»; «Інформаційне право»; «Кібербезпека» тощо.

Апробація матеріалів дисертації. Підсумки розроблення проблематики та відповідні висновки оприлюднено на міжнародних науково-практичних конференціях: «Актуальні проблеми взаємодії правової науки та практики її застосування» (м. Київ, 16–17 березня 2022 р.), «Науково-практичні засади розвитку юридичної науки на сучасному етапі державотворення» (м. Київ, 15–16 лютого 2023 р.), «Реформування українського законодавства: проблемні питання та шляхи їх вирішення» (м. Київ, 7–8 лютого 2024 р.).

Структура та обсяг дисертації. Дисертація складається зі вступу, трьох розділів, які містять дев'ять підрозділів, загальних висновків, списку використаних джерел, додатків. Загальний обсяг дисертації становить 216 сторінок. Список використаних джерел містить 193 найменування на 21 сторінці.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У **вступі** обґрунтовано вибір теми дисертації, визначено її зв'язок з науковими програмами, планами, темами, окреслено мету й завдання дослідження, об'єкт і предмет, методи дослідження, визначено наукову новизну та практичне значення отриманих результатів, наведено дані щодо апробації результатів дослідження та публікацій.

Розділ 1 «Загальна характеристика адміністративних процедур забезпечення кібербезпеки в Україні» складається з чотирьох підрозділів, у яких: надано характеристику кібербезпеки як об'єкта адміністративно-правового регулювання; визначено поняття, розкрито особливості й виокремлено види адміністративних процедур у сфері забезпечення кібербезпеки; окреслено коло суб'єктів реалізації адміністративних процедур у сфері забезпечення кібербезпеки; проаналізовано систему правового регулювання реалізації адміністративних процедур у сфері забезпечення кібербезпеки.

У *підрозділі 1.1 «Кібербезпека як об'єкт адміністративно-правового регулювання»* визначено поняття «безпека» як певний динамічний стан суспільного порядку, за якого кожна людина має психологічне відчуття захищеності, реальні гарантії недопущення негативного впливу на її права, свободи, інтереси, а також життя та здоров'я.

На підставі аналізу норм чинного законодавства та наукових поглядів учених аргументовано, що поняття «кібербезпека» найбільш доцільно розглядати в широкому та вузькому значенні. Зазначено, що забезпечення кібербезпеки – це реалізований спеціально уповноваженими суб'єктами комплекс заходів, технологій, процесів і практик, спрямований на захист інформаційних систем, мереж, даних і програм від несанкціонованого доступу, використання, розкриття, зміни, руйнування або втрати. Встановлено, що така діяльність передбачає

забезпечення конфіденційності, цілісності й доступності інформації, а також протидію кіберзагрозам і кібератакам з боку зловмисників у цифровому просторі.

Виокремлено чинники, які характеризують кібербезпеку як об'єкт адміністративно-правового регулювання. Для цього узагальнено низку наукових поглядів учених, а також проаналізовано чинне законодавство у вказаній сфері.

У *підрозділі 1.2 «Поняття, особливості та види адміністративних процедур у сфері забезпечення кібербезпеки»* зазначено, що в найбільш загальному значенні процедура – це регламентований нормами права прядок учинення уповноваженими суб'єктами юридично значущих дій з метою задоволення законних інтересів суспільства й держави.

Узагальнено наукові погляди вчених щодо змісту поняття «адміністративна процедура», на основі чого встановлено, що на сьогодні сформувалися дві відносно самостійні концепції щодо тлумачення змісту та призначення адміністративних процедур. Відповідно до першого підходу ця категорія охоплює всю публічно-управлінську діяльність органів державної влади й місцевого самоврядування із реалізації покладених на них законодавством повноважень щодо забезпечення прав, свобод і законних інтересів фізичних та юридичних осіб, а також внутрішньої організації своєї діяльності. Друга концепція відповідає законодавчому трактуванню та характеризує адміністративну процедуру як регламентований законодавством України порядок дій спеціально уповноважених суб'єктів з приводу забезпечення реалізації та захисту прав, свобод і законних інтересів фізичних та юридичних осіб, кінцевим етапом якого є прийняття адміністративного акта.

Сформульовано авторський підхід до розуміння категорії «адміністративні процедури у сфері забезпечення кібербезпеки». Зазначено, що відповідні процедури є різноманітними за своєю сутністю та змістом, на основі чого наголошено на необхідності здійснення їх класифікації.

Розкрито положення норм чинного законодавства, що визначає окремі проблемні аспекти реалізації адміністративних процедур у сфері забезпечення кібербезпеки, на основі чого констатовано, що останні найбільш доцільно поділити на чотири групи.

У *підрозділі 1.3 «Суб'єкти реалізації адміністративних процедур у сфері забезпечення кібербезпеки»* розкрито загальнотеоретичні підходи до розуміння категорії «суб'єкт». Особливу увагу приділено аналізу цього терміна з точки зору правової науки, на основі чого суб'єктами реалізації адміністративних процедур у сфері забезпечення кібербезпеки визначено сукупність спеціально уповноважених органів державної влади (в особі їх посадових осіб), які відповідно до норм чинного законодавства наділені повноваженнями та необхідною компетенцією щодо реалізації дій і заходів, спрямованих на створення необхідних умов для захисту інформаційних систем та мереж, а також координації дій щодо запобігання, виявлення та реагування на кіберзагрози.

Виокремлено коло суб'єктів, до компетенції яких належить безпосередня реалізація адміністративних процедур у сфері забезпечення кібербезпеки. З'ясовано, що попри широкий суб'єктний склад забезпечення кібербезпеки, який

включає значну кількість різноманітних державних, правоохоронних, військових та інших органів, основними суб'єктами реалізації адміністративних процедур у цій сфері є лише три публічно-правові відомства: Державна служба спеціального зв'язку та захисту інформації України, Національний банк України та Служба безпеки України. Саме вони наділені спеціальними правами та обов'язками у сфері забезпечення кібербезпеки, зокрема з питань реалізації адміністративних процедур відповідного типу, а їх правовий статус відповідає ознакам адміністративних органів, передбачених Законом України «Про адміністративну процедуру».

У *підрозділі 1.4 «Правове регулювання реалізації адміністративних процедур у сфері забезпечення кібербезпеки»* аргументовано, що правове регулювання реалізації адміністративних процедур у сфері забезпечення кібербезпеки – це здійснюваний за допомогою норм права регулюючий та упорядковуючий вплив на суспільні відносини, які виникають у досліджуваній сфері суспільного життя. Відповідний вплив здійснюється також за рахунок спеціальних юридичних інструментів і спрямований на забезпечення відповідності їх поведінки нормам чинного законодавства.

Схарактеризовано нормативно-правові акти різної юридичної сили, норми яких регулюють окремі аспекти реалізації адміністративних процедур у сфері забезпечення кібербезпеки.

Наголошено, що нормативно-правове підґрунтя реалізації адміністративних процедур у сфері кібербезпеки засновано на двох групах нормативно-правових актів: 1) ті, що визначають правові, організаційні, матеріально-технічні та інші особливості процесу підтримки стану безпечного користування кіберпростором, комунікаційними й технологічними системами; 2) ті, що пояснюють зміст, значення та особливості реалізації безпосередньо адміністративних процедур у досліджуваній сфері.

Констатовано, що на сьогодні система правового регулювання реалізації адміністративних процедур у сфері забезпечення кібербезпеки складається з низки нормативно-правових актів різної юридичної сили, кожен з яких регулює певний напрям досліджуваного питання. Зауважено, що попри значну увагу з боку законодавця та врегульованість досліджуваного питання, у зазначеній сфері залишається чимала кількість проблем.

Розділ 2 «Порядок здійснення окремих адміністративних процедур у сфері забезпечення кібербезпеки в Україні» складається з трьох підрозділів, у яких: розкрито адміністративні процедури, пов'язані зі змістом інформації, що обробляється в комунікаційних або в технологічних системах; окреслено адміністративні процедури, пов'язані із захистом інформації, що становить державну таємницю, комунікаційні та технологічні системи, призначені для її оброблення; встановлено коло адміністративних процедур захисту комунікаційних систем, які не взаємодіють з публічними мережами електронних комунікацій.

У *підрозділі 2.1 «Адміністративні процедури, пов'язані зі змістом інформації, що обробляється в комунікаційних або технологічних системах»* доведено, що інформація – це дані та відомості про певний об'єкт, явища або факти дійсності, які можуть набувати усної, письмової, електронної чи іншої форми. Зміст

інформації визначає її різновид і рівень доступу до неї. Відповідно, дані та відомості конфіденційного, таємного чи службового характеру обмежені для широкого загалу та додатково охороняються законом. Водночас інформація, зокрема з обмеженим доступом, зберігається та існує на відповідних носіях, а також передається між різноманітними суб'єктами вербально, документально, зокрема через технологічні й комунікаційні системи.

Акцентовано увагу на тому, що адміністративні процедури у сфері кібербезпеки пов'язані зі змістом інформації, що обробляється в комунікаційних або технологічних системах. Це – окрема група впорядкованих дій, заходів і процесів, що реалізуються уповноваженими суб'єктами та спрямовані на збір, обробку, зберігання, передачу й захист інформації у відповідних інформаційно-комунікаційних і технологічних системах. Зазначені процедури спрямовані на забезпечення конфіденційності, цілісності та доступності даних, а також на запобігання їх несанкціонованому доступу, розкриттю, модифікації або знищенню інформації. Виокремлено коло відповідних процедур і надано їм змістовну характеристику.

У *підрозділі 2.2 «Адміністративні процедури, пов'язані із захистом інформації, що становить державну таємницю, комунікаційні та технологічні системи, призначені для її оброблення»* наголошено, що найбільш специфічним та особливим різновидом адміністративних процедур у сфері кібербезпеки є ті, що пов'язані із захистом державної таємниці, а також комунікаційних, технологічних систем, призначених для її оброблення. Унікальні ознаки такої діяльності формуються завдяки наявності особливого правового статусу суб'єктів захисту інформації та спеціальних вимог щодо організації захисту зазначеної інформації, порівняно з іншими передбаченими законодавством типами відомостей і даних.

На основі аналізу норм чинного законодавства та наукових поглядів учених встановлено, що державна таємниця є особливо важливим різновидом інформації в суспільно значущих сферах (оборони, економіки, науки й техніки, міжнародних відносинах, галузі державної безпеки, охорони правопорядку тощо), порядок доступу до якої обмежено законодавством України з метою недопущення її несанкціонованого розголошення, що матиме шкідливі наслідки для національної безпеки.

Обґрунтовано такі основні ознаки державної таємниці: 1) її становлять не всі відомості, а лише ті, що безпосередньо віднесені до цієї категорії інформації в установленому законом порядку; 2) спеціальний захист державної таємниці передбачає особливий порядок надання уповноваженим суб'єктам доступу до відомостей і даних, які становлять зміст цієї категорії; 3) обробка, передача та збереження відомостей і даних, що становлять державну таємницю, зокрема в комунікаційних та технологічних системах, відбувається з дотриманням спеціальних правил і використанням заходів захисту.

Встановлено, що зазначені особливості впливають на перелік, зміст та особливості реалізації адміністративних процедур, пов'язаних із захистом інформації, що становить державну таємницю, комунікаційні та технологічні системи, призначені для її оброблення.

Запропоновано авторське визначення поняття адміністративних процедур, пов'язаних із захистом інформації, що становить державну таємницю, комунікаційних і технологічних систем, призначених для її оброблення. Виокремлено коло відповідних процедур і надано їм змістовну характеристику.

У *підрозділі 2.3 «Адміністративні процедури захисту комунікаційних систем, які не взаємодіють з публічними мережами електронних комунікацій»* наголошено, що комунікаційні системи, які не взаємодіють з публічними мережами електронних комунікацій, є закритими, або ізольованими, оскільки призначені для передачі інформації в межах певної організації або групи користувачів без підключення до загальнодоступних мереж, зокрема мережі Інтернет. Ці системи розроблені для забезпечення високого рівня безпеки, конфіденційності та надійності передачі даних, що робить їх особливо цінними в умовах, де необхідно захистити інформацію від несанкціонованого доступу, витоків або кібератак. Відсутність взаємодії із зовнішнім світом робить ці системи стійкими до більшості зовнішніх загроз та водночас потребує високого рівня внутрішнього контролю й управління для запобігання внутрішнім загрозам або помилкам.

Аргументовано, що адміністративні процедури захисту комунікаційних систем, які не взаємодіють з публічними мережами електронних комунікацій, переважно мають внутрішньосистемний характер і реалізуються безпосередньо користувачами відповідних систем, а також спрямовані на забезпечення безпеки інформації та запобігання несанкціонованому доступу або витоку даних. Ці процедури є частиною загальної системи безпеки, що забезпечує належний рівень захисту від загроз як зсередини, так і ззовні організації.

До вказаних процедур зараховано: формування політики безпеки; контроль та управління доступом; авторизація та аутентифікація визначеного переліку користувачів, що мають доступ до цієї системи; здійснення внутрішнього контролю (моніторинг та аудит системи); кадрові процедури; процедури управління та реагування на інциденти; захист даних і резервне копіювання. Надано змістовну характеристику кожній процедурі.

Розділ 3 «Сучасні тенденції вдосконалення адміністративно-правового регулювання здійснення окремих адміністративних процедур забезпечення кібербезпеки» складається з двох підрозділів, у яких здійснено порівняльний аналіз національних та міжнародних стандартів і практик забезпечення кібербезпеки; з'ясовано шляхи вдосконалення правового регулювання адміністративних процедур у сфері забезпечення кібербезпеки.

У *підрозділі 3.1 «Порівняльний аналіз національних та міжнародних стандартів і практик забезпечення кібербезпеки»* розкрито загальнотеоретичний зміст поняття «стандарт», на підставі чого встановлено, що стандарти забезпечення кібербезпеки – це набір правил, рекомендацій і вимог, які визначають методи й заходи щодо захисту інформаційних систем, мереж і даних від кібератак, несанкціонованого доступу, витоку даних та інших загроз кібербезпеці. Вказані стандарти встановлюють загальні практики, які організації можуть використовувати для забезпечення захисту власних цифрових активів.

Проаналізовано міжнародні стандарти у сфері забезпечення кібербезпеки. Надано характеристику міжнародним стандартам, які були адаптовані до національних реалій. Зауважено, що впровадження стандартів ISO для кібербезпеки передбачає визначення критичних інформаційних активів, оцінку ризиків, визначення засобів контролю безпеки, забезпечення відповідності нормативним вимогам і встановлення процедур для постійного вдосконалення. Наголошено, що ідентифікація активів є початковим кроком у процесі впровадження ISO, де компанії мають точно визначити інформаційні активи, важливі для їх діяльності та безпеки.

На підставі зіставлення національних та міжнародних стандартів і практик забезпечення кібербезпеки встановлено позитивні й негативні аспекти кожного з них.

Висвітлено досвід Сполучених Штатів Америки та Великої Британії у сфері забезпечення кібербезпеки, зокрема встановлено, що в цих країнах сформовано досить ефективні механізми в досліджуваній сфері, що дозволили вказаним країнам стати світовими лідерами та взірцем у цій галузі.

У *підрозділі 3.2 «Шляхи вдосконалення правового регулювання адміністративних процедур у сфері забезпечення кібербезпеки»* наголошено, що розв'язання проблем, пов'язаних із реалізацією адміністративних процедур у сфері забезпечення кібербезпеки, потребує комплексного покращення системи правового регулювання суспільних відносин, які виникають у досліджуваній сфері суспільного життя.

Акцентовано увагу на тому, що недоліки відповідного нормативно-правового регулювання обумовлені: 1) історичними та політичними чинниками; 2) технічними факторами; 3) соціальними факторами; 4) економічними чинниками; 5) війною в Україні, що спричинила: а) масовані кібератаки з боку російської федерації на критичну інфраструктуру, що призводить до значних збитків, а також перешкоджає нормальному функціонуванню всього державного апарату; б) дестабілізацію роботи не лише державного, а й приватного сектору, що значно шкодить фінансовому та економічному розвитку держави; в) відтік кваліфікованих кадрів у галузі кібербезпеки.

Здійснено аналіз низки стратегічних документів, на підставі чого аргументовано доцільність розроблення та прийняття Концепції розвитку системи забезпечення кібербезпеки в Україні, метою якої має бути створення та підтримка ефективного, стійкого й безпечного кіберсередовища, яке б захищало національні інтереси, сприяло сталому розвитку цифрової економіки та забезпечувало права та свободи громадян в інформаційному просторі. Наведено ключові завдання цієї Концепції.

Зауважено, що відповідно до вказаної вище Концепції слід доопрацювати Стратегію кібербезпеки України, яка має враховувати виклики та реалії сьогодення, а також набутий досвід кібератак на кіберпростір України в останні три роки. Доведено потребу в розробленні та прийнятті Стратегії забезпечення кібербезпеки в умовах воєнного стану.

Спираючись на аналіз наукових поглядів учених і норм чинного законодавства, запропоновано внести низку змін та доповнень до Закону України «Про основні засади забезпечення кібербезпеки України».

Наголошено, що, крім нормативних аспектів, суттєвого покрашення потребує організаційне забезпечення реалізації адміністративних процедур забезпечення кібербезпеки. У цьому контексті опрацьовано перспективні напрями покращення: кадрового, фінансового, матеріально-технічного та науково-методичного забезпечення суб'єктів реалізації адміністративних процедур у сфері кібербезпеки.

ВИСНОВКИ

У **висновках** дисертації наведено теоретичне узагальнення та нове вирішення наукового завдання, яке полягало в тому, щоб розкрити сутність, зміст та особливості адміністративних процедур забезпечення кібербезпеки в Україні, а також, спираючись на позитивний вітчизняний і зарубіжний досвід, розробити пропозиції та рекомендації, спрямовані на вдосконалення нормативно-правового регулювання суспільних відносин, що виникають у досліджуваній сфері суспільного життя. У результаті дослідження сформульовано низку нових наукових висновків, основні з них такі:

1. Констатовано, що кібербезпека як об'єкт адміністративно-правового регулювання означена такими особливостями: по-перше, становить особливу групу правовідносин, що виникають у специфічній сфері суспільного життя; по-друге, обумовлює необхідність здійснення низки різноманітних дій та заходів спеціально уповноваженими органами державної влади, а також приватними суб'єктами; по-третє, відповідна діяльність переважно регулюється нормами адміністративної галузі права; по-четверте, є сферою реалізації різноманітних процедур, які мають адміністративний характер.

2. Поняттям «адміністративні процедури у сфері забезпечення кібербезпеки» запропоновано вважати визначений законодавством України порядок дій, які реалізуються спеціально уповноваженими суб'єктами в напрямі забезпечення та захисту прав і законних інтересів фізичних та юридичних осіб, а також з метою реалізації публічних повноважень у сфері використання комунікаційних, технологічних систем, електронно-обчислювальної (комп'ютерної) техніки, програмного забезпечення та взаємодії в кіберпросторі.

Доведено, що особливостями адміністративних процедур у сфері забезпечення кібербезпеки є такі: по-перше, особлива сфера реалізації, а також предмет, з приводу якого виникають відповідні суспільні відносини; по-друге, реалізовувати відповідні процедури мають право виключно спеціально уповноважені суб'єкти, посадові особи яких володіють набором специфічних професійних знань, умінь і навичок; по-третє, наявність спеціального набору нормативно-правових засад їх реалізації; по-четверте, переважна більшість адміністративних процедур пов'язані з обробкою персональних даних, що вимагає дотримання вимог законодавства про захист персональних даних; по-п'яте, наявність підвищеного рівня

відповідальності суб'єктів, які відповідні процедури реалізовують; по-шосте, відповідні процедури застосовуються в різних сферах забезпечення кібербезпеки, що обумовлює наявність їх різновидів.

Адміністративні процедури у сфері забезпечення кібербезпеки запропоновано поділити на такі групи: 1) адміністративні процедури, пов'язані з організаційно-управлінським забезпеченням кібербезпеки; 2) адміністративні процедури, пов'язані зі змістом інформації, що обробляється в комунікаційних або технологічних системах; 3) адміністративні процедури, пов'язані із захистом інформації, що становить державну таємницю, комунікаційних і технологічних систем, призначених для її оброблення; 4) адміністративні процедури захисту комунікаційних систем, які не взаємодіють з публічними мережами електронних комунікацій.

3. Зауважено, що попри широкий суб'єктний склад забезпечення кібербезпеки, який охоплює значну кількість різноманітних державних, правоохоронних, військових та інших органів, основними суб'єктами реалізації адміністративних процедур у цій сфері є три публічно-правові відомства: Державна служба спеціального зв'язку та захисту інформації України, Національний банк України та Служба безпеки України. Саме вони наділені спеціальними правами та обов'язками у сфері забезпечення кібербезпеки, зокрема з питань реалізації адміністративних процедур відповідного типу, а їх правовий статус відповідає ознакам адміністративних органів, передбачених Законом України «Про адміністративну процедуру».

4. Обґрунтовано положення про те, що на сьогодні система правового регулювання реалізації адміністративних процедур у сфері забезпечення кібербезпеки складається з низки нормативно-правових актів різної юридичної сили, кожен з яких регулює певний напрям досліджуваного питання. Зауважено, що попри значну увагу з боку законодавця та врегульованість досліджуваного питання, у зазначеній сфері залишається чимала кількість проблем, зокрема: по-перше, невизначеним є перелік адміністративних процедур, які реалізуються у відповідній сфері суспільного життя; по-друге, коло та правовий статус суб'єктів, які здійснюють відповідну діяльність, є досить розмитими; по-третє, законодавцем недостатньо розроблено питання впровадження міжнародних стандартів у цій сфері.

5. Аргументовано, що адміністративні процедури у сфері кібербезпеки пов'язані зі змістом інформації, що обробляється в комунікаційних або технологічних системах. Це – окрема група впорядкованих дій, заходів і процесів, що реалізуються уповноваженими суб'єктами та спрямовані на збір, обробку, зберігання, передачу й захист інформації у відповідних інформаційно-комунікаційних і технологічних системах. Зазначені процедури спрямовані на забезпечення конфіденційності, цілісності та доступності даних, а також на запобігання їх несанкціонованому доступу, розкриттю, модифікації або знищенню інформації. Наголошено, що основними суб'єктами реалізації цих процедур є Державна служба спеціального зв'язку і захисту інформації України та Національний банк України. До відповідних процедур зараховано такі: оцінка

стану захищеності суб'єкта; сканування інформаційних ресурсів, розміщених у мережі Інтернет; експертиза; контрольні процедури.

6. Адміністративними процедурами, пов'язаними із захистом інформації, що становить державну таємницю, а також комунікаційних і технологічних систем, призначених для її оброблення, запропоновано вважати системну та систематизовану діяльність спеціально уповноважених органів державної влади, яка передбачає вчинення дій і заходів, спрямованих на організацію ефективного захисту та підтримки високого рівня безпеки під час оброблення та використання інформації, що становить державну таємницю у відповідних системах з метою запобігання та попередження її несанкціонованого витоку, що може завдати шкоди національним інтересам і безпеці. Серед відповідних процедур виокремлено: віднесення інформації до державної таємниці; надання дозволу на провадження діяльності, пов'язаної із секретними відомостями й даними; контроль за забезпеченням охорони державної таємниці; процедури погодження СБУ щодо створення, реорганізації чи ліквідації режимно-секретних органів.

7. Встановлено, що адміністративні процедури захисту комунікаційних систем, які не взаємодіють з публічними мережами електронних комунікацій, переважно мають внутрішньосистемний характер і реалізуються безпосередньо користувачами відповідних систем, а також спрямовані на забезпечення безпеки інформації та запобігання несанкціонованому доступу або витоку даних. Ці процедури є частиною загальної системи безпеки, що забезпечує належний рівень захисту від загроз як зсередини, так і ззовні організації. До вказаних процедур зараховано: формування політики безпеки; контроль та управління доступом; авторизація та аутентифікація визначеного переліку користувачів, що мають доступ до цієї системи; здійснення внутрішнього контролю (моніторинг та аудит системи); кадрові процедури; процедури управління та реагування на інциденти; захист даних і резервне копіювання.

8. З'ясовано, що Україна запровадила низку стандартів, пов'язаних із забезпеченням кібербезпеки. Водночас адаптація національних і міжнародних стандартів у досліджуваній сфері має певну специфіку, а саме:

1) охоплення та адаптивність. Так, міжнародні стандарти зазвичай є більш загальними й адаптивними, щоб задовольнити потреби широкого кола організацій по всьому світу, адже вони надають межі, які можна адаптувати відповідно до специфічних потреб організації. Національні стандарти, навпаки, часто розробляються та адаптуються з урахуванням конкретних загроз і регуляторних вимог, що робить їх більш конкретними щодо певної галузі або типу організації, правової культури тощо;

2) особливі регуляторні вимоги. У цьому контексті національні стандарти включають вимоги, необхідні для відповідності національному законодавству та нормативним актам, адже міжнародні стандарти зазвичай є більш універсальними й можуть використовуватися як основа для відповідності регуляторним вимогам у різних країнах;

3) застосування та сертифікація. Міжнародні стандарти, такі як ISO/IEC 27001, широко застосовуються для сертифікації в різних країнах і часто є основою для

підвищення глобальної довіри та визнання. Натомість національні стандарти мають обмежену географічну застосовність і можуть використовуватися переважно в межах однієї країни або регіону;

4) методологія та підхід до ризиків. Міжнародні стандарти зазвичай надають структурований підхід до управління ризиками з акцентом на ідентифікацію, оцінку та управління ризиками інформаційної безпеки. Національні стандарти можуть включати додаткові заходи або вимоги, що відображають місцеві загрози.

5) національні стандарти є більш гнучкими для адаптації до вітчизняних реалій, тоді як міжнародні – більш структуровані та формалізовані.

9. Доведено, що шляхи вдосконалення правового регулювання адміністративних процедур у сфері забезпечення кібербезпеки слід поділити на дві великі групи:

1) нормативно-правовий напрям, у межах якого необхідно: а) розробити та прийняти Концепцію розвитку системи забезпечення кібербезпеки в Україні; б) привести у відповідність до вказаної Концепції Стратегію кібербезпеки України, яка буде адаптована до сучасних умов, викликів і набутого досвіду ведення війни (зокрема кібервійни) проти російської федерації; в) прийняти Стратегію кібербезпеки України в умовах воєнного стану; г) внести зміни до Закону України «Про основні засади забезпечення кібербезпеки України», а саме: уточнити теоретичну частину Закону, зокрема визначити поняття «адміністративні процедури забезпечення кібербезпеки»; встановити коло адміністративних процедур, а також розкрити їх зміст; визначити сфери застосування цих адміністративних процедур; окреслити коло суб'єктів реалізації відповідних процедур, а також їх правовий статус;

2) організаційно-управлінський напрям, у межах якого варто: а) покращити систему кадрового забезпечення суб'єктів, що уповноважені реалізовувати діяльність у досліджуваній сфері; б) переглянути фінансове та матеріально-технічне забезпечення галузі кібербезпеки; в) удосконалити науково-методичне забезпечення досліджуваної сфери суспільного життя.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

в яких висвітлено основні наукові результати дисертації:

1. Ніколайчик О. С. До проблеми визначення поняття кібербезпеки як об'єкта адміністративно-правового регулювання. *Юридична наука*. 2020. № 1(103). Т. 2. С. 169–172.

2. Ніколайчик О. С. Адміністративні процедури, пов'язані із захистом інформації, що становить державну таємницю, комунікаційних та технологічних систем, призначених для її оброблення. *Юридична наука*. 2020. № 3(105). Т. 2. С. 61–67.

3. Ніколайчик О. С. Адміністративні процедури, пов'язані зі змістом інформації, що обробляється в комунікаційних або в технологічних системах. *Право і суспільство.* 2021. № 6. С. 207–211.

4. Ніколайчик О. С. Суб'єкти реалізації адміністративних процедур у сфері забезпечення кібербезпеки. *KELM*. 2022. № 7 (51). С. 343–346 (Республіка Польща).

5. Ніколайчик О. С. До характеристики системи правового регулювання реалізації адміністративних процедур у сфері забезпечення кібербезпеки. *Юридичний науковий електронний журнал.* 2023. № 6. С. 850–852.

які засвідчують апробацію матеріалів дисертації:

6. Ніколайчик О. С. Види адміністративних процедур у сфері забезпечення кібербезпеки. *Актуальні проблеми взаємодії правової науки та практики її застосування*: матеріали Міжнар. наук.-практ. конф. (Київ, 16–17 берез. 2022 р.). Київ: Наук.-дослід. ін-т публіч. права, 2022. С. 118–120.

7. Ніколайчик О. С. До характеристики адміністративних процедур забезпечення кібербезпеки, які не пов'язані із проведенням заходів захисту інформації у комунікаційних, технологічних системах, обробкою та обміном інформацією в кіберпросторі. *Науково-практичні засади розвитку юридичної науки на сучасному етапі державотворення:* матеріали Міжнар. наук.-практ. конф. (Київ, 15–16 лют. 2023 р.). Київ: Наук.-дослід. ін-т публіч. права, 2023. С. 117–121.

8. Ніколайчик О. С. Поняття адміністративних процедур у сфері забезпечення кібербезпеки. *Реформування українського законодавства: проблемні питання та шляхи їх вирішення*: матеріали Міжнар. наук.-практ. конф. (Київ, 7–8 лют. 2024 р.). Київ: Наук.-дослід. ін-т публіч. права, 2024. С. 171–173.

АНОТАЦІЯ

Ніколайчик О. С. Адміністративні процедури забезпечення кібербезпеки в Україні. – *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 розв'язання наукового завдання, яке полягає в тому, щоб розкрити сутність, зміст та особливості адміністративних процедур забезпечення кібербезпеки в Україні, а також, спираючись на позитивний вітчизняний та зарубіжний досвід, розробити пропозиції та надати рекомендації, спрямовані на вдосконалення нормативно-правового регулювання здійснення відповідної діяльності.

Надано характеристику кібербезпеки як об'єкта адміністративно-правового регулювання. Визначено поняття, особливості та види адміністративних процедур у сфері забезпечення кібербезпеки. Окреслено коло суб'єктів реалізації адміністративних процедур у сфері забезпечення кібербезпеки. Проаналізовано систему правового регулювання реалізації адміністративних процедур у сфері забезпечення кібербезпеки. Розкрито адміністративні процедури, пов'язані зі змістом інформації, що обробляється в комунікаційних або в технологічних системах. Визначено адміністративні процедури, пов'язані із захистом інформації, що становить державну таємницю, комунікаційних і технологічних систем,

призначених для її оброблення. Встановлено коло адміністративних процедур захисту комунікаційних систем, які не взаємодіють з публічними мережами електронних комунікацій. Здійснено порівняльний аналіз національних та міжнародних стандартів і практик забезпечення кібербезпеки. З'ясовано шляхи вдосконалення правового регулювання адміністративних процедур у сфері забезпечення кібербезпеки.

Ключові слова: кібербезпека, кіберпростір, об'єкт, адміністративно-правове регулювання, адміністративні процедури, суб'єкт, інформація, зміст інформації, комунікаційні системи, технологічні системи, державна таємниця, обробка інформації, стандарти, міжнародні стандарти, адміністративне законодавство.

SUMMARY

Nikolaichyk O.S. Administrative procedures for ensuring cyber security in Ukraine. – *Qualification scientific work on the rights of the manuscript***.**

Thesis for obtaining a scientific degree of candidate of juridical science in specialty 12.00.07 «Administrative Law and Procedure; Financial 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 consists in revealing the essence, content and features of administrative procedures for ensuring cyber security in Ukraine, as well as drawing on positive domestic and foreign experience to dev elop proposals and provide recommendations aimed at improving the regulatory - legal regulation of the relevant activity.

Cyber security is characterized as an object of administrative and legal regulation. The concept, features and types of administrative procedures in the field of cyber security are determined. The circle of subjects of implementation of administrative procedures in the field of cyber security is outlined. The system of legal regulation of the implementation of administrative procedures in the field of cyber security is characterized. Administrative procedures related to the content of information processed in communication or technological systems are disclosed. Administrative procedures related to the protection of information constituting a state secret, communication and technological systems designed for its processing are defined. A range of administrative procedures for the protection of communication systems that do not interact with public electronic communications networks is established. A comparative analysis of national and international standards and practices for ensuring cyber security is carried out. Ways to improve the legal regulation of administrative procedures in the field of cyber security are being explored.

Keywords: cyber security, cyberspace, object, administrative and legal regulation, administrative procedures, subject, information, content of information, communication systems, technological systems, state secret, information processing, standards, international standards, administrative legislation.