МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ

БУХАРЄВ Владислав Вікторович

УДК: 342.95 (477)

АДМІНІСТРАТИВНО-ПРАВОВІ ЗАСАДИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ УКРАЇНИ

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

АВТОРЕФЕРАТ
дисертації на здобуття наукового ступеня
кандидата юридичних наук

Суми – 2018

Дисертацією є рукопис.

Робота виконана в Університеті сучасних знань.

Науковий керівник: доктор юридичних наук, професор, заслужений юрист України **КУЛІШ Анатолій Миколайович**, Сумський державний університет, директор навчально-наукового інституту права.

Офіційні опоненти: доктор юридичних наук, професор, заслужений юрист України **МУЗИЧУК Олександр Миколайович**, Харківський національний університет внутрішніх справ, декан факультету № 1;

кандидат юридичних наук, заслужений юрист України, **БОНДАР Сергій Олександрович**, Сумський окружний адміністративний суд, суддя-спікер.

Захист відбудеться 24 грудня 2018 р. о 10 годині на засіданні спеціалізованої вченої ради К 55.051.07 Сумського державного університету за адресою: 40007, м. Суми, вул. Римського-Корсакова, 2.

З дисертацією можна ознайомитися в бібліотеці Сумського державного університету за адресою: 40007, м. Суми, вул. Римського-Корсакова, 2.

Автореферат розісланий 24 листопада 2018 р.

Учений секретар спеціалізованої вченої ради **О. М. Рєзнік**

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Обґрунтування вибору теми дослідження. Одним із пріоритетних напрямків розвитку України на її сучасному історичному етапі є розбудова інформаційного суспільства. Заходи із втілення даного кроку передбачають активне впровадження інформаційно-комунікаційних технологій, розвиток кібернетичного простору. Передовий зарубіжний досвід свідчить про те, що переведення частини суспільних відносин у кібернетичний простір має низку переваг, зокрема сприяє підвищенню відкритості та прозорості діяльності суб'єктів публічної влади, оперативності та ефективності їх взаємодії між собою та з представниками громадськості, міжнародною спільнотою. Однак водночас швидкий розвиток інформаційних, інформаційно-телекомунікаційних засобів, технологій, систем і мереж характеризується і значними негативними аспектами, зокрема появою нової сфери для процвітання злочинності. Сприятливість даної сфери для злочинної діяльності обумовлена цілим рядом факторів, наприклад: розвиток комп'ютерних та інформаційно-комунікаційних технологій випереджає розвиток законодавства, яке регулює відносини в даній сфері; необмеженість державними кордонами, що створює сприятливі умови для процвітання транснаціональної злочинності; складність виявлення безпосереднього суб'єкта злочинної діяльності та доведення його вини.

Указані та інші аспекти комп'ютеризації, кібернетизації значної частини суспільного життя змушують кожну сучасну державу особливу увагу приділяти своїй кібернетичній безпеці. Зрозуміло, що Україна в цьому питанні не є виключенням, що обумовлює необхідність суттєвого вдосконалення національного механізму забезпечення кібербезпеки. Одним із основних етапів покращення якості та ефективності організації і функціонування даного механізму є поліпшення його адміністративно-правового забезпечення, яке передбачає покращення відповідного законодавства та перегляд системи суб'єктів, що опікуються питаннями кібербезпеки. Протягом останніх років у наукових колах все частіше мали місце думки щодо назрілої потреби зміцнення національної кібербезпеки, що є цілком зрозумілим, адже із такими кібернетичними загрозами, які є сьогодні, Україна раніше не зіштовхувалася, як результат – відсутність необхідного досвіду і нездатність ефективно протидіяти даним загрозам. Зазначене вказує на актуальність проведення комплексного вивчення адміністративно-правових засад забезпечення кібернетичної безпеки в Україні з метою виокремлення існуючих проблем у даному механізмі та визначення пріоритетів і перспективних напрямків його подальшого розвитку з урахуванням реалій і викликів сьогодення.

Варто відзначити, що загальним питанням адміністративно-правового забезпечення кібербезпеки присвячено наукові праці Г. О. Андрощук, І. В. Арістової, О. А. Баранова, О. І. Безпалової, Ю. П. Битяка, В. О. Бойко, С. О. Бондаря, С. М. Братуся, В. Л. Бурячка, С. А. Буяджи, Л. Є. Виноградова, О. К. Волох, М. В. Гайворонського, Ю. В. Гаруста, Є. А. Гетьмана, С. О. Гнатюка, Б. В. Деревянка, А. А. Демцова, О. В. Джафарової, Б. В. Дзюндзюк, В. Б. Дзюндзюк, І. В. Діордіци, О. Л. Добржанської, А. В. Долинного, І. В. Європіної, А. В. Кірмач, О. М. Клюєва, Н. В. Коваленка,

О. В. Коломоєць, В. К. Колпакова, А. Т. Комзюка, Ю. А. Копитова, О. Є. Користіна, О. Г. Корченка, Т. М. Кравцової, Р. О. Куйбіди, О. В. Кузьменка, А. М. Куліша, В. І. Курила, Є. В. Курінного, О. С. Лагоди, В. А. Ліпкана, М. В. Лошицького, Д. М. Лук'янця, Р. В. Лук'янчука, П. С. Лютікова, В. В. Маркова, О. М. Мельника, О. М. Музичука, В. Я. Настюка, В. І. Олефіра, В. В. Пахомова, Т. О. Проценка, Д. М. Притики, А. В. Руденка, О. Ю. Синявської, М. В. Старинського, В. В. Сухоноса, В. Б. Толубка та ін. Однак, незважаючи на наявність ряду наукових праць, присвячених розвитку кібернетичного простору, забезпеченню кібербезпеки, спеціальні комплексні дослідження, в яких визначаються особливості адміністративно-правового забезпечення кібербезпеки в Україні, і які ґрунтуються на оновленому законодавстві у цій сфері, є недостатніми.

Таким чином, необхідність удосконалення кібербезпеки в Україні, недосконаліть правового регулювання у зазначеній сфері, з одного боку, та відсутність комплексних досліджень з цієї проблематики – з іншого, обумовлюють своєчасність та актуальність комплексного дослідження адміністративно-правових засад забезпечення кібербезпеки України.

Зв'язок роботи з науковими програмами, планами, темами, грантами. Дисертаційне дослідження виконане відповідно до основних положень Стратегії сталого розвитку «Україна – 2020», схваленої Указом Президента України від 12 січня 2015 р. № 5/2015, Стратегії кібербезпеки України, затвердженої Указом Президента України від 15 березня 2016 р. № 96/2016, Стратегії розвитку наукових досліджень Національної академії правових наук України на 2016 – 2020 роки, затвердженої постановою загальних зборів Національної академії правових наук України від 3 березня 2016 р., Пріоритетних напрямів наукових досліджень Університету сучасних знань на 2017 – 2022 рр. (протокол Вченої ради Університету сучасних знань № 3 від 08.12.2016).

Мета і завдання дослідження. Метою дисертаційного дослідження є визначення сутності та особливостей адміністративно-правових засад забезпечення кібербезпеки в Україні, а також шляхів їх удосконалення.

Для досягнення зазначеної мети в дисертаційному дослідженні необхідно було виконати такі основні *завдання*:

– визначити поняття та з'ясувати особливості кібербезпеки як об'єкта адміністративно-правової охорони;

– здійснити історико-правовий аналіз розвитку та становлення правового інституту кібербезпеки;

– встановити види об'єктів кібербезпеки та кіберзахисту;

– охарактеризувати правові засади забезпечення кібербезпеки України та з'ясувати місце серед них адміністративно-правового забезпечення;

– окреслити систему суб'єктів забезпечення кібербезпеки України та особливості їх адміністративно-правового статусу;

– систематизувати адміністративно-правові форми та методи забезпечення кібербезпеки України;

– виокремити види та особливості юридичної відповідальності за порушення законодавства у сфері кібербезпеки України;

– узагальнити зарубіжний досвід забезпечення кібербезпеки та запропонувати можливості його використання в Україні;

– опрацювати напрямки вдосконалення адміністративного законодавства, яке регулює забезпечення кібербезпеки в Україні;

– встановити способи оптимізації системи суб'єктів забезпечення кібербезпеки України та напрямки вдосконалення взаємодії між ними.

Об'єктом дослідження є суспільні відносини, що виникають під час забезпечення кібербезпеки в Україні.

Предметом дослідження є адміністративно-правові засади забезпечення кібербезпеки України.

Методи дослідження. В дисертаційному дослідженні використано такі методи наукового пізнання: а) логіко-семантичний, за допомогою якого визначено поняття «кібербезпека як об'єкт адміністративно-правової охорони» (підрозділ 1.1), «кібербезпека» та «кіберзахист» (підрозділ 1.3), «адміністративно-правові форми забезпечення кібербезпеки України» та «адміністративно-правові методи забезпечення кібербезпеки України» (підрозділ 2.2), «суб'єкти забезпечення кібербезпеки України» (підрозділ 3.2); б) історико-правовий – під час аналізу становлення та розвитку правового інституту кібербезпеки (підрозділ 1.2); в) системно-структурний, за допомогою якого систематизовано види об'єктів кібербезпеки та кіберзахисту, окреслено коло суб'єктів забезпечення кібербезпеки України, особливості їх адміністративно-правового статусу та види юридичної відповідальності за порушення законодавства у сфері кібербезпеки України (підрозділи 1.3, 2.1, 2.3); г) порівняльно-правовий, що використовувався з метою з'ясування правових підстав становлення правового інституту кібербезпеки, виявлення особливостей адміністративно-правового забезпечення кібербезпеки України, опрацювання напрямків удосконалення адміністративно-правових засад забезпечення кібербезпеки в Україні (підрозділи 1.2, 1.4, 3.1 – 3.3); ґ) структурного аналізу, який застосовано під час окреслення особливостей адміністративно-правового статусу суб'єктів забезпечення кібербезпеки та шляхів оптимізації їх системи (підрозділи 2.1, 3.3). В роботі використано низку інших методів наукового пізнання.

Науково-теоретичне підґрунтя дисертації становлять праці вчених різної галузевої належності, які вивчали проблеми теорії та практики забезпечення кібербезпеки в Україні та світі. Нормативною основою дослідження є Конституція України, норми міжнародних нормативно-правових актів, закони та підзаконні нормативно-правові акти, які визначають адміністративно-правові засади забезпечення кібербезпеки в Україні. Інформаційну та емпіричну основу роботи становлять узагальнення

практики забезпечення кібербезпеки, довідкові видання, статистичні матеріали.

Наукова новизна отриманих результатів визначається тим, що представлене дисертаційне дослідження є однією з перших спроб комплексно, з урахуванням аналізу наукових праць учених та чинного законодавства України визначити сутність та особливості адміністративно-правових засад забезпечення кібербезпеки України та запропонувати напрямки вдосконалення відповідного законодавства. У результаті проведеного дослідження сформульовано низку нових наукових положень та висновків, запропонованих особисто здобувачем. Основні з них такі:

вперше:

– визначено, що адміністративно-правова охорона у сфері забезпечення кібербезпеки – це діяльність відповідних державних органів, що здійснюється на засадах імперативності та ієрархічності і направлена на підтримання та забезпечення належного стану захищеності прав, інтересів та інформації відповідних суб'єктів у кіберпросторі;

– обґрунтовується, що розмежування адміністративно-правового забезпечення кібербезпеки та адміністративно-правового забезпечення кіберзахисту є принципово важливим питанням, адже воно прямо пов'язане з процесом їх реалізації, що при неправильному підході може завдати шкоди охоронюваним законом інтересам та правам людей, які здійснюють різні операції з інформацією в кіберпросторі;

– доведено позицію автора, згідно з якою суб'єкти забезпечення кібербезпеки є учасниками не інформаційних, а адміністративних правовідносин, оскільки, по-перше, відносини між ними будуються на основі влади і підпорядкування, а по-друге, останні реалізують механізм кіберзахисту шляхом використання примусу, який їм надано чинним законодавством. Крім цього, аналіз адміністративно-правового статусу суб'єктів забезпечення кібербезпеки просто неможливо здійснювати поза межами адміністративної галузі права;

удосконалено:

– розуміння того, що історія становлення та розвитку кібербезпеки як юридичного інституту прямо пов'язана з еволюцією інформаційних технологій та Інтернету, який дав людству можливість обробляти та обмінюватися колосальною кількістю даних на відстані;

– обґрунтування того, що правові засади забезпечення кібербезпеки – це весь масив керівних ідей, засад та положень, закріплених у нормативно-правових актах різної юридичної сили, які визначають механізм правового регулювання забезпечення кібербезпеки;

– характеристику основних адміністративно-правових форм забезпечення кібербезпеки України, під якими запропоновано розуміти зовнішній вираз діяльності уповноважених органів державної влади, який виявляється у вчиненні ними комплексу дій, які спрямовані на створення

таких умов, за яких буде забезпечено безпеку комп'ютерних систем у всій країні в цілому;

– розуміння оптимізації системи суб'єктів забезпечення кібербезпеки, яка являє собою процес, що передбачає: по-перше, створення оптимальної кількості таких суб'єктів, яких буде достатньо для виконання завдань у сфері забезпечення кібербезпеки; по-друге, належну організацію діяльності відповідних суб'єктів шляхом збільшення або зменшення кількості їх повноважень;

– характеристику ознак взаємодії суб'єктів забезпечення кібербезпеки, до яких віднесено: 1) єдину мету спільної діяльності; 2) наявність декількох або більше суб'єктів; 3) обов'язковість законодавчого підґрунтя діяльності; 4) чітко визначений адміністративно-правовий статус кожного суб'єкта; 5) узгодженість заходів щодо мети, місця, часу, методів діяльності;

– розуміння форм взаємодії суб'єктів забезпечення кібербезпеки в Україні, до яких запропоновано віднести: 1) проведення спільних міжвідомчих нарад; 2) обмін оперативною інформацією щодо стану забезпечення кібербезпеки, а також щодо заходів, які були вже реалізовані кожним суб'єктом взаємодії; 3) розроблення спільних програм щодо протидії кіберправопорушенням та окреслення основних напрямків спільної діяльності; 4) спільну участь у проведенні окремих слідчих та розшукових дій; 5) утворення спільних консультативно-дорадчих та експертних органів, рад, комісій;

– визначення поняття «методи взаємодії суб'єктів забезпечення кібербезпеки», під яким запропоновано розуміти сукупність способів та прийомів, які спрямовуються на налагодження ефективної взаємодії між суб'єктами, що уповноважені забезпечувати кібербезпеку в Україні;

дістали подальшого розвитку:

– обґрунтування того, що кібербезпека є складним правовим явищем, у рамках якого діє механізм кіберзахисту, що являє собою систему заходів організаційного, нормативно-правового, воєнного, оперативного, технічного та іншого характеру;

– розуміння того, що з прийняттям Закону України «Про основні засади забезпечення кібербезпеки України» вперше з'явилось нормативне визначення поняття «кібербезпека», що, у свою чергу, дозволило виробити стратегію захисту кібербезпеки в адміністративно-правовому порядку та закріпити засади, суб'єктний склад механізму забезпечення вказаної категорії, що, безперечно, є позитивною новацією у сфері забезпечення кіберпростору та процесу використання інноваційних технологій;

– обґрунтування того, що питання юридичної відповідальності за порушення законодавства у сфері кібербезпеки України є недостатньо врегульованим, що, безперечно, можна вважати суттєвою прогалиною, яка сприяє зростанню рівня кіберзлочинності в нашій державі. Зокрема, питання притягнення правопорушника у сфері кібербезпеки до цивільної та адміністративної відповідальності регулюється цілою низкою нормативно-

правових актів, у кожному з яких містяться різні підстави притягнення особи до відповідальності. Така розгалуженість, у свою чергу, ускладнює застосування стягнень до винних осіб органами державної влади;

– характеристика методів взаємодії суб'єктів забезпечення кібербезпеки, до яких віднесено: 1) кадровий метод, який передбачає активне навчання представників одних органів специфіці роботи інших, що, у свою чергу, сприяє налагодженню ефективної взаємодії між відомствами; 2) метод взаємного інформаційного забезпечення, який полягає в наданні суб'єктами співпраці один одному всієї необхідної інформації для більш відкритої та ефективної взаємодії; 3) метод контролю, завдяки якому сторони (суб'єкти) взаємодії мають змогу здійснювати взаємне контролювання один одного під час спільної діяльності; 4) методи планування та прогнозування; 5) економічний метод, який передбачає створення відповідної матеріальної бази для проведення спільних заходів.

Практичне значення отриманих результатів полягає в тому, що викладені в даному дисертаційному дослідженні висновки і пропозиції можуть бути використані у:

– науково-дослідній сфері – для подальшого розроблення теоретико-методологічних та правових питань забезпечення кібербезпеки України (*акт впровадження Кримінологічної асоціації України від 05.01.2018 р.*);

– правотворчості – як основа для вдосконалення адміністративного законодавства, що регламентує забезпечення кібербезпеки України (*акт впровадження Науково-дослідного інституту публічного права від 17.01.2018 р.*);

– правозастосовній діяльності – з метою удосконалення окремих напрямків, форм та методів забезпечення кібербезпеки України (*акт впровадження результатів дисертаційного дослідження у практичну діяльність Навчально-тренувального центру боротьби з кіберзлочинністю та моніторингу кіберпростору Харківського національного університету внутрішніх справ від 26.01.2018 р.*);

– навчальному процесі – під час підготовки підручників та навчальних посібників із дисциплін «Адміністративне право», «Адміністративний процес», «Публічне адміністрування» та інших дисциплін адміністративно-правового характеру, в ході підготовки відповідних їх розділів (*акт впровадження Сумського державного університету від 10.09.2018 р.*).

Апробація матеріалів дисертації. Підсумки розроблення проблеми в цілому, окремих її аспектів, одержані узагальнення і висновки було оприлюднено на міжнародних, всеукраїнських та регіональних науково-практичних конференціях, семінарах, круглих столах, зокрема: «Сучасні правові системи світу в умовах глобалізації: реалії та перспективи» (Київ, 2015); «Розвиток сучасного права в умовах глобальної нестабільності» (Одеса, 2016); «Розвиток державності та права в Україні: реалії та перспективи) (Львів, 2018).

Публікації. Основні результати дисертаційного дослідження викладено в семи статтях, опублікованих у наукових фахових виданнях України та

наукових періодичних виданнях інших держав, та трьох тезах наукових повідомлень на науково-практичних конференціях.

Структура та обсяг дисертації. Дисертація складається зі вступу, трьох розділів, що містять 10 підрозділів, висновків, списку використаних джерел, додатків. Повний обсяг дисертації становить 221 сторінку. Список використаних джерел включає 225 найменувань та розміщений на 23-х сторінках, додатки розташовано на дев'яти сторінках.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У **вступі** обґрунтовується вибір теми дисертації, визначається її зв'язок з науковими програмами, планами та темами, окреслюються мета і завдання, об'єкт і предмет, методи дослідження, вказується на наукову новизну та практичне значення отриманих результатів, наводяться дані щодо апробації результатів дослідження та публікацій.

Розділ 1 «Методологічні засади забезпечення кібербезпеки України» присвячений дослідженню поняття та особливостей кібербезпеки як об'єкта адміністративно-правової охорони; вивченню історико-правових основ і умов становлення та розвитку правового інституту кібербезпеки; з'ясуванню видів об'єктів кібербезпеки та кіберзахисту; аналізу правових засад забезпечення кібербезпеки України та встановленню місця серед них адміністративно-правового забезпечення.

У *підрозділі 1.1 «Поняття та особливості кібербезпеки як об'єкта адміністративно-правової охорони»* зазначається, що одним з основних напрямків розвитку України з моменту проголошення незалежності стали технологічний прогрес та впровадження інформаційних технологій, які сьогодні суттєво полегшують процеси пошуку та оперування інформацією. Запровадження новітніх інформаційних технологій відкриває величезні можливості для якісного та швидкого розвитку держави і суспільства. Однак «цифрова» революція характеризується не лише позитивними, але й негативними моментами, зокрема виникненням та процвітанням такого виду протизаконної активності, як кіберзлочинність, що вимагає від держави активізації заходів з удосконалення та зміцнення системи кібербезпеки. Перш за все, необхідно розробити якісне та змістовне нормативно-правове підґрунтя для ефективного та дієвого проведення державної політики із забезпечення кібернетичної безпеки.

Наголошено на відсутності в чинному законодавстві визначень таких понять, як «кібербезпека» та «адміністративно-правова охорона». Досліджено наукові підходи до розуміння сутності та ключових характеризуючих аспектів адміністративно-правової охорони. Запропоновано наступне визначення адміністративно-правової охорони: це системне явище адміністративного права, сутність якого полягає у діяльності публічних органів, спрямованій на забезпечення прав громадян або підтримання відповідного легального режиму в тій чи іншій сфері суспільного буття.

Проаналізовано нормативно-правові та доктринальні джерела на предмет визначення сутнісного змісту та характерних ознак кібербезпеки. Визначено інститут адміністративно-правової охорони кібербезпеки як

діяльність окремих державних органів, що здійснюється на засадах імперативності та ієрархічності, направлена на підтримання та забезпечення належного стану захищеності прав, інтересів та інформації відповідних суб'єктів у кіберпросторі. Висвітлено особливості проблеми забезпечення кібербезпеки як об'єкта адміністративно-правової охорони.

У *підрозділі 1.2 «Історико-правовий аналіз розвитку та становлення правового інституту кібербезпеки»* зазначається, що становленню кібербезпеки передувала ціла низка подій, які обумовили розвиток її юридичного виразу у правовій системі держави. Тому з метою більш повного розуміння природи та значення даного інституту, визначення перспектив та пріоритетів його розвитку слід піддати аналізу не лише його поточний стан, але й історичні передумови та умови становлення і розвитку кібербезпеки.

Наголошено, що історія становлення та розвитку досліджуваного правового інституту безпосередньо пов'язана з еволюцією інформаційних технологій та Інтернету. Досліджено суспільно-політичні та організаційно-правові умови і засади, з урахуванням яких, починаючи із середини XX століття, відбувався процес становлення та подальшого розвитку кібербезпеки. Прослідковано загальні та специфічні аспекти нормативно-правового забезпечення протидії кібернетичній злочинності на міжнародному та національному рівнях. Висловлено власне бачення щодо позитивних та проблемних аспектів еволюції правового інституту кібербезпеки.

У *підрозділі 1.3 «Види об'єктів кібербезпеки та кіберзахисту»* звернено увагу на питання співвідношення кібербезпеки та кіберзахисту. Наголошено на тому, що досить часто представлені явища сприймаються як цілком ідентичні, що не відповідає дійсності. Проаналізовано сутність поняття кіберзахисту, задля чого вивчено відповідні наукові точки зору і позиції, а також положення офіційних документів із цього приводу. Встановлено, що кіберзахист є складовим елементом кібербезпеки. Запропоновано під кіберзахистом розуміти систему (механізм) засобів різного характеру, за допомогою яких здійснюються підтримка та забезпечення інституту кібербезпеки.

Досліджено доктринальні підходи до тлумачення понять «об'єкт», «об'єкт правовідносин». Зазначається, що об'єктний склад кібербезпеки становлять суспільні відносини з приводу використання кіберпростору, а також організації безпечного пошуку, обробки та передачі інформації у цій сфері. У свою чергу, об'єктами механізму кіберзахисту виступають матеріальні та нематеріальні блага, на які спрямовано дію заходів забезпечення кібербезпеки, що входять до складу цього механізму.

До об'єктів кіберзахисту віднесено: об'єкти критичної інформаційної інфраструктури; інформаційно-телекомунікаційні системи, в яких здійснюється обробка державних інформаційних ресурсів; інформаційно-телекомунікаційні системи, в яких здійснюється обробка інформації, вимоги щодо захисту якої встановлені законом. Охарактеризовано зміст кожного із зазначених видів об'єктів кіберзахисту.

У *підрозділі 1.4 «Правові засади забезпечення кібербезпеки України та місце серед них адміністративно-правового забезпечення»* зазначається, що

механізм забезпечення кібербезпеки ґрунтується та функціонує на цілому ряді принципів, від правильності визначення яких значним чином залежать якість та ефективність роботи даного механізму.

Досліджено наукові підходи до розуміння сутності понять «принцип» та «принцип права». Вивчено запропоновані у правовій літературі точки зору щодо класифікації правових принципів. На підставі проведеного дослідження визначено правові засади механізму забезпечення кібербезпеки як весь масив керівних ідей, існуючих у положеннях нормативних актів різного ступеня ієрархії, які визначають роль механізму у правовій системі, а також його сферу та способи застосування.

Проаналізовано чинне законодавство на предмет закріплення у ньому принципів забезпечення кібербезпеки. Виокремлено коло принципів механізму забезпечення кібербезпеки України: 1) верховенства права, законності, поваги до прав людини і основоположних свобод та їх захисту в порядку, визначеному законом; 2) забезпечення національних інтересів України; 3) відкритості, доступності, стабільності та захищеності кіберпростору, розвитку мережі Інтернет та відповідальних дій у кіберпросторі; 4) державно-приватної взаємодії, широкої співпраці з громадянським суспільством у сфері кібербезпеки та кіберзахисту, зокрема шляхом обміну інформацією про інциденти кібербезпеки, реалізації спільних наукових та дослідницьких проектів, навчання та підвищення кваліфікації кадрів у цій сфері; 5) пріоритетності запобіжних заходів.

З'ясовано сутність адміністративно-правового регулювання та його місце (роль) у визначенні засад механізму забезпечення кібербезпеки. Встановлено, що адміністративно-правове регулювання кібербезпеки являє собою спрямований законодавством вплив норм адміністративного права, в рамках якого використовуються, застосовуються спеціальні засоби та провадяться запобіжні заходи з метою забезпечення відносин суб'єктів у кіберпросторі, а також охорони їх прав та законних інтересів. Визначено співвідношення заходів адміністративного припинення та адміністративних запобіжних заходів.

Розділ 2 «Адміністративно-правовий механізм забезпечення кібербезпеки України» присвячений вивченню системи суб'єктів забезпечення кібербезпеки України та встановленню особливостей їх адміністративно-правового статусу; аналізу адміністративно-правових форм і методів забезпечення кібербезпеки України; дослідженню різновидів та особливостей юридичної відповідальності за порушення законодавства у сфері кібербезпеки України.

У *підрозділі 2.1 «Система суб'єктів забезпечення кібербезпеки України та особливості їх адміністративно-правового статусу»* з метою з'ясування сутності та структури системи суб'єктів забезпечення кібербезпеки звернено увагу на загальноправову категорію «суб'єкти правовідносин», з приводу чого вивчено відповідні наукові думки і позиції. Встановлено, що суб'єктами забезпечення інституту кібербезпеки є державні органи та посадові особи останніх, наділені владними повноваженнями та відповідними обов'язками щодо охорони об'єктів кібербезпеки.

Проаналізовано чинне законодавство з метою визначення кола суб'єктів, уповноважених на забезпечення кібербезпеки. Розподілено

суб'єктів забезпечення кібербезпеки на дві групи: загальну та спеціальну. До першої включено органи державної влади, органи місцевого самоврядування, суб'єктів господарювання, громадян України та об'єднання громадян, інших осіб, які провадять діяльність та/або надають послуги, пов'язані з національними інформаційними ресурсами, інформаційними електронними послугами, здійсненням електронних правочинів, електронними комунікаціями, захистом інформації та кіберзахистом. Зміст другої групи становлять органи влади, які формують систему кібербезпеки України: Служба безпеки України, Національна поліція, Національний банк тощо. Досліджено правовий статус (завдання та повноваження) суб'єктів забезпечення кібербезпеки в Україні.

У *підрозділі 2.2 «Адміністративно-правові форми та методи забезпечення кібербезпеки України»* наголошено, що надзвичайно важливим аспектом для якісного забезпечення кібернетичної безпеки є правильне визначення основних форм і методів здійснення даного забезпечення. У зв'язку із цим з'ясовна загальнотеоретична сутність понять «форма» та «метод», а також вивчені відповідні наукові та навчальні джерела. Запропоновано під адміністративно-правовими формами забезпечення кібербезпеки України розуміти зовнішній вираз діяльності уповноважених органів державної влади, який виявляється у вчиненні ними комплексу дій, які спрямовані на створення таких умов, за яких буде забезпечено безпеку комп'ютерних систем у всій країні в цілому.

Проаналізовано доктринальні підходи та положення чинного законодавства щодо кола та змісту форм забезпечення кібербезпеки, на підставі чого виокремлено наступні форми зазначеного забезпечення: нормотворчість; прийняття індивідуальних актів у сфері забезпечення кібербезпеки; адміністративний договір; правореалізація. Охарактеризовано сутнісний зміст та значення кожної форми для забезпечення кібербезпеки.

З'ясовано наукові позиції щодо розуміння поняття та ролі адміністративно-правових методів. Висвітлено суть та значення для забезпечення кібербезпеки таких методів, як: адміністративний примус; позитивне зобов'язання; дозвіл та заборона; адміністративний контроль; ліцензування діяльності у сфері захисту відомостей, що становлять державну таємницю; сертифікація та стандартизація; реєстрація.

У *підрозділі 2.3 «Види та особливості юридичної відповідальності за порушення законодавства у сфері кібербезпеки України»* підкреслено, що серед інших засобів забезпечення кібербезпеки особливе місце посідає юридична відповідальність. Вивчено доктринальні підходи до розуміння поняття та основних властивостей (ознак) юридичної (або правової) відповідальності. На підставі цього запропоновано розуміти юридичну відповідальність за порушення законодавства у сфері кібербезпеки України як застосування заходів примусового характеру, які визначені нормами чинного законодавства, до осіб, що вчинили правопорушення у кіберпросторі.

Проаналізовано норми чинного законодавства на предмет урегулювання ним відповідальності за вчинення протиправних дій у кібернетичному просторі. Встановлені види юридичної відповідальності, що можуть бути застосовані за порушення зазначеного законодавства, а саме: цивільна, адміністративна та кримінальна. Розглянуто сутнісний зміст та

значення для забезпечення кібербезпеки кожного з указаних видів відповідальності. Висловлено власні думки щодо стану законодавчої регламентації юридичної відповідальності за порушення кібербезпеки. Виокремлено найбільш характерні особливості юридичної відповідальності за порушення законодавства у сфері кібербезпеки.

Розділ 3 «Удосконалення адміністративно-правових засад забезпечення кібербезпеки України» присвячений дослідженню зарубіжного досвіду забезпечення кібербезпеки та з'ясуванню можливостей його використання в Україні; визначенню напрямків удосконалення адміністративного законодавства, яке регулює забезпечення кібербезпеки в Україні; вивченню проблем оптимізації системи суб'єктів забезпечення кібербезпеки України та удосконалення взаємодії між ними.

У *підрозділі 3.1 «Зарубіжний досвід забезпечення кібербезпеки та можливості його використання в Україні»* наголошено на тому, що існуючий в Україні сьогодні механізм забезпечення кібербезпеки є недосконалим та потребує удосконалення. Встановлено, що необхідність вивчення зарубіжного досвіду забезпечення кібербезпеки визначається курсом України на європейську інтеграцію, що обумовлює необхідність впровадження на національному рівні європейських норм і стандартів організації і функціонування основних сфер суспільного життя, зокрема це стосується і вимог щодо протидії злочинності у кібернетичному просторі та забезпечення кібербезпеки.

Враховуючи зазначене проведено дослідження досвіду в зазначеній сфері таких європейських країн, як: Великобританія, Німеччина, Франція, Польща; також проаналізовано досвід США, Японії, КНР. Розглянуто політико-правові та організаційно-управлінські засади діяльності системи кібернетичної безпеки у даних країнах. На підставі проведеного дослідження виокремлено перспективні напрямки розвитку інституту забезпечення кібербезпеки в Україні: збільшення фінансування суб'єктів, діяльність яких спрямована на забезпечення кібербезпеки в державі; кардинальне оновлення Стратегії кібербезпеки України.

У *підрозділі 3.2 «Напрямки удосконалення адміністративного законодавства, яке регулює забезпечення кібербезпеки в Україні»* наголошено на тому, що чинне законодавство України з питань кібербезпеки має ряд недоліків і прогалин, що не дозволяє йому належним чином урегулювати відносини у даній сфері.

За результатами аналізу чинного адміністративного законодавства з питань кібербезпеки виокремлено його недоліки та запропоновано певні кроки щодо його вдосконалення, зокрема: визначити у Законі «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 р. орган, до повноважень якого повинно бути віднесено оперативне управління всіма іншими суб'єктами у досліджуваній сфері; удосконалити понятійно-термінологічний апарат у зазначеному законодавстві (наприклад, відсутні визначення термінів «кіберправопорушення» та «кіберпроступок»); закріпити види кіберзагроз, чіткий перелік кіберзлочинів; удосконалити організаційно-процедурні засади забезпечення кібербезпеки. Акцентовано увагу на проблемних аспектах Доктрини інформаційної безпеки України та Стратегії

кібербезпеки України. Висловлені пропозиції щодо перспектив розвитку національного адміністративного законодавства з питань кібербезпеки.

У *підрозділі 3.3 «Оптимізація системи суб'єктів забезпечення кібербезпеки України та удосконалення взаємодії між ними»* підкреслено, що важливим етапом на шляху вдосконалення національного адміністративно-правового механізму забезпечення кібербезпеки є оптимізація системи суб'єктів, що уповноважені здійснювати діяльність у цій сфері, а також налагодження ефективної взаємодії між ними. У зв'язку із цим проаналізовано наукові та навчальні джерела на предмет визначення сутнісного змісту понять «оптимізація» та «взаємодія». Встановлено, що оптимізація системи суб'єктів забезпечення кібербезпеки являє собою процес, який передбачає: по-перше, створення оптимальної кількості таких суб'єктів, яких буде достатньо для виконання завдань у сфері забезпечення кібербезпеки; по-друге, належну організацію діяльності відповідних суб'єктів шляхом звуження або розширення їх компетенцій. Акцентовано увагу на необхідності створення єдиного суб'єкта, який був би наділений повноваженнями щодо координації діяльності всіх суб'єктів забезпечення кібербезпеки України. Наголошено, що численність суб'єктів, які забезпечують кібербезпеку в Україні, є чи не однією із найбільших у Європі та світі, що, у свою чергу, суттєво ускладнює налагодження взаємодії між ними.

Взаємодію суб'єктів забезпечення кібербезпеки визначено як їх спільну взаємоузгоджену діяльність, яка спрямована на досягнення єдиної мети – забезпечення належного стану кібернетичної безпеки в Україні. Виокремлено характерні ознаки даної взаємодії. Досліджено положення чинного законодавства на предмет урегулювання ним взаємодії між суб'єктами забезпечення кібербезпеки України. Акцентовано увагу на необхідності більш змістовної законодавчої регламентації: 1) взаємних прав та обов'язків суб'єктів під час здійснення спільної діяльності; 2) напрямків взаємодії; 3) форм та методів взаємодії; 4) повноважень суб'єкта, який буде координувати спільну діяльність суб'єктів забезпечення кібербезпеки в Україні. Наголошується на доцільності розроблення положення «Про порядок взаємодії суб'єктів забезпечення кібербезпеки в Україні». Визначено коло форм, які слід включити до даного положення: 1) проведення спільних міжвідомчих нарад; 2) обмін оперативною інформацією щодо стану забезпечення кібербезпеки, а також щодо заходів, які були вже реалізовані кожним суб'єктом взаємодії; 3) розроблення спільних програм щодо протидії кіберправопорушенням та окреслення основних напрямків спільної діяльності; 4) утворення спільних консультативно-дорадчих та експертних органів, рад, комісій. Окреслено сутність та коло методів взаємодії.

ВИСНОВКИ

У дисертації наведено теоретичне узагальнення та нове вирішення наукового завдання, яке полягає у визначенні сутності та особливостей адміністративно-правових засад забезпечення кібербезпеки України, а також опрацюванні напрямків удосконалення адміністративного законодавства, яке регулює забезпечення кібербезпеки в Україні. У

результаті дослідження сформульовано низку нових теоретичних та практичних положень, основні з них такі:

1. Аргументовано, що кібербезпека як об'єкт адміністративно-правової охорони являє собою певний правовий інститут, охорона якого відбувається в межах норм адміністративного права та здійснюється окремими державними органами на засадах імперативності та ієрархічності.

Наведено такі особливості кібербезпеки як об'єкта адміністративно-правової охорони: а) відсутність чіткого визначення змісту адміністративно-правової охорони кібербезпеки; б) адміністративно-правова охорона кібербезпеки хоча і являє собою єдиний юридичний інститут, проте закріплюється у нормах різних нормативно-правових актів, якими регулюється діяльність відповідних органів державної влади; в) її забезпечення здійснюється не тільки у правовідносинах, які виникають у сфері вчинення адміністративних правопорушень. Інститут має більш широкий обсяг застосування, який передбачає не тільки припинення відповідних порушень, а також їх попередження; г) основні засади забезпечення кібербезпеки лише нещодавно знайшли своє закріплення у відповідному нормативно-правовому акті – Законі України «Про основні засади забезпечення кібербезпеки України»; ґ) має місце спеціальний понятійний апарат.

2. Історико-правовий аналіз становлення та розвитку інституту кібербезпеки дозволив переконатись у тому, що достатньо тривалий час інституту кібербезпеки на території України фактично не існувало. Наголошено, що становлення інституту кібербезпеки безпосередньо пов'язане з еволюцією інформаційних технологій. Тож, найпершим комп'ютерним законом, положеннями якого вже було передбачено різного роду правопорушення з використанням комп'ютерів, став Закон «Про боротьбу з комп'ютерними шахрайствами та комп'ютерними зловживаннями», прийнятий у 1986 р. у США. Відзначено, що у подальшому розвиток правового інституту кібербезпеки здійснювався на міжнародному рівні, зокрема, у: Віденській декларації про злочинність та правосуддя, Конвенції про взаємодопомогу в кримінальних справах між членами ЄС, Резолюції Генеральної Асамблеї ООН (щодо створення глобальної культури кібербезпеки від 2002 р.), Женевській декларації принципів побудови інформаційного суспільства тощо. З'ясовано, що в Україні кібербезпека як окремий правовий інститут з'явилася після ратифікації у 2005 р. Конвенції про кіберзлочинність. Наступним кроком на шляху її розвитку стало розроблення Стратегії кібербезпеки України, яка була введена в дію рішенням Ради національної безпеки і оборони України. На сучасному етапі кібербезпека повною мірою отримала нормативний прояв у положеннях Закону України «Про основні засади забезпечення кібербезпеки України».

3. Доведено, що до об'єктного складу кібербезпеки входять: а) правовідносини у сфері розвитку належної інформаційної інфраструктури у

державі; б) правовідносини у сфері налагодження міжнародних зав'язків з метою обміну досвідом у галузі розбудови кібербезпеки; в) правовідносини з приводу регулювання, координації і контролю діяльності правоохоронних органів та інших суб'єктів забезпечення кібербезпеки в процесі виконання покладених на них обов'язків; г) правовідносини у сфері впровадження інформаційних технологій в основних галузях життєдіяльності суспільства та налагодження процесу їх безпечного використання; ґ) правовідносини у сфері розвитку науки та техніки з метою розбудови предметної основи інституту кібербезпеки, тобто розроблення новітніх технологій, які б сприяли підвищенню безпеки при роботі у кіберпросторі; д) правовідносини у сфері імплементації у законодавство України правових механізмів забезпечення кібербезпеки з урахуванням міжнародного досвіду у цій галузі; е) правовідносини у сфері підвищення інформаційної обізнаності суспільства при роботі з інформацією у кіберпросторі.

З'ясовано, що об'єктами кіберзахисту є: а) об'єкти критичної інформаційної інфраструктури; б) інформаційно-телекомунікаційні системи, в яких здійснюється обробка державних інформаційних ресурсів; в) інформаційно-телекомунікаційні системи, в яких здійснюється обробка інформації, вимоги щодо захисту якої встановлені законом.

4. Встановлено, що адміністративно-правове регулювання кібербезпеки – це цілеспрямований вплив норм адміністративного законодавства на суспільні відносини, які виникають у сфері забезпечення кібербезпеки, в межах якого застосовуються спеціальні засоби та запобіжні заходи з метою недопущення правопорушень у кіберпросторі.

Роль адміністративно-правового регулювання у сфері забезпечення кібербезпеки полягає в тому, що саме відповідно до норм адміністративного законодавства здійснюється правове регулювання діяльності суб'єктів забезпечення кібербезпеки в Україні.

5. Суб'єктів забезпечення кібербезпеки запропоновано об'єднати у дві групи: загальні та спеціальні. До загальної належать усі органи державної влади, органи місцевого самоврядування, суб'єкти господарювання, громадяни України та об'єднання громадян, інші особи, які провадять діяльність та/або надають послуги, пов'язані з національними інформаційними ресурсами, інформаційними електронними послугами, здійсненням електронних правочинів, електронними комунікаціями, захистом інформації та кіберзахистом. До кола спеціальних суб'єктів віднесено органи влади, котрі становлять систему суб'єктів кібербезпеки України, перелік яких закріплено в Законі України «Про основні засади забезпечення кібербезпеки України».

Наголошено, що всі суб'єкти забезпечення кібербезпеки наділені як комплексом специфічних, так і комплексом загальних повноважень. Серед загальних ознак суб'єктів забезпечення кібербезпеки виділено наступні: по-перше, вони у своїй діяльності використовують владний примус з

метою реалізації передбачених законодавством функцій; по-друге, суб'єкти забезпечення кібербезпеки перебувають у системному взаємозв'язку з іншими учасниками адміністративних правовідносин, який будується на засадах ієрархічності; по-третє, діяльність суб'єктів забезпечення кібербезпеки спрямована не тільки на припинення правопорушень у цій сфері, а й на забезпечення умов, коли такі порушення неможливі, що реалізується шляхом проведення контрольних заходів.

6. Виокремлено та охарактеризовано такі форми забезпечення кібербезпеки України: а) нормотворчість (тобто прийняття нормативно-правових актів у сфері забезпечення кібербезпеки); б) прийняття індивідуальних актів у сфері забезпечення кібербезпеки; в) укладення адміністративних договорів; г) правореалізація.

Доведено, що нормотворчість є однією з ключових форм забезпечення кібербезпеки в Україні, оскільки за її допомогою вбачається можливим створити таке правове поле, яке буде виключати будь-які можливості для суб'єктів відповідних правовідносин вчинити правопорушення у досліджуваній сфері. Акцентовано увагу на тому, що індивідуальні акти у сфері забезпечення кібербезпеки дозволяють оперативно вирішити нагальні проблеми, що з'являються у вказаній сфері суспільних відносин. Їх перевага полягає у тому, що вони спрямовані на конкретного суб'єкта, а тому за їх допомогою можливо вирішити більш конкретні проблемні питання. Визначено, що адміністративний договір, як адміністративно-правова форма забезпечення кібербезпеки, являє собою добровільну угоду між декількома суб'єктами адміністративного права, які наділені владними повноваженнями, з метою координації їх спільної діяльності, що в результаті приводить до виникнення, зміни або припинення взаємних прав та обов'язків сторін відповідного договору. З'ясовано, що правореалізація передбачає безпосереднє втілення норм адміністративного права в діяльність суб'єктів, функції яких полягають у забезпеченні кібербезпеки в Україні. При цьому кожен із таких суб'єктів повинен в обов'язковому порядку дотримуватись визначених суб'єктивних прав та виконання своїх зобов'язань.

На основі аналізу норм чинного законодавства та наукових поглядів учених виокремлено та охарактеризовано такі методи забезпечення кібербезпеки: а) адміністративний примус (ключове значення вказаного методу полягає в тому, що він спрямований на попередження виникнення правопорушень у досліджуваній сфері. Проте застосування методу адміністративного примусу спрямовано не лише на попередження виникнення протиправної поведінки, а й покликано забезпечити захист інформаційних, приватних, комп'ютерних ресурсів тощо); б) метод позитивного зобов'язання; в) метод дозволу та заборон; г) метод адміністративного контролю; ґ) метод контролю доступу; д) метод

ліцензування діяльності; е) метод сертифікації та стандартизації; є) реєстраційний метод.

7. Виокремлено найбільш характерні особливості юридичної відповідальності за порушення законодавства у сфері кібербезпеки: а) специфічний предмет правопорушення та/або кіберзлочину, яким є інформація, тобто відомості та/або дані, які зберігаються у мережі Інтернет або на якихось носіях (серверах, жорстких дисках, картах пам'яті тощо); б) складність виявлення суб'єкта правопорушення, що потребує серйозного матеріально-технічного та кадрового забезпечення; в) найбільш поширеним видом відповідальності є кримінальна, що обумовлюється високим рівнем шкоди в результаті здійснення кіберзлочину; г) зазвичай, правопорушення у вказаній сфері спрямовуються не на конкретну особу, тобто не є персоніфікованими; ґ) шкода від вчинення кіберзлочину, як правило, має матеріальний характер та не шкодить фізичному здоров'ю людини.

Розкрито сутність та особливості таких видів юридичної відповідальності за порушення законодавства у сфері кібербезпеки, як адміністративна, кримінальна та цивільно-правова. Основний акцент зроблено на характеристиці адміністративної відповідальності за порушення законодавства у сфері кібербезпеки, у зв'язку з чим визначено, що адміністративна відповідальність за порушення законодавства у сфері кібербезпеки – це застосування до особи, що вчинила правопорушення, санкцій, передбачених нормами адміністративного права. Зазвичай, санкції за вчинення адміністративного проступку мають матеріальний (грошовий) характер.

8. На підставі узагальнення зарубіжного досвіду забезпечення кібербезпеки констатовано, що сьогодні світові тенденції розвитку інформаційного суспільства спонукають всі держави світу вжити заходів щодо забезпечення кібербезпеки. Не є виключенням і Україна, яка нині знаходиться лише на перших етапах розвитку цього інституту. Аналіз досвіду вказаних вище країн дав змогу виокремити наступні напрямки розвитку інституту забезпечення кібербезпеки в Україні: по-перше, необхідно збільшити фінансування суб'єктів, діяльність яких спрямована на забезпечення кібербезпеки в державі; по-друге, покращити якість освіти працівників кіберполіції; по-третє, кардинального оновлення потребує Стратегія кібербезпеки України. На наше переконання, вона повинна бути ширшою та охоплювати більше коло питань у цій сфері, а не обмежуватись лише базовими питаннями. В цьому контексті цікавим є досвід Великобританії та Німеччини, чиї стратегії забезпечення кібербезпеки охоплюють, практично, всі питання та є основними документами у цій сфері; по-четверте, необхідно розширювати міжнародне співробітництво у сфері забезпечення кібербезпеки, не обмежуючись співпрацею з однією конкретною країною (в нашому випадку – США); по-п'яте, слід посилити контроль у мережі Інтернет (на

прикладі Китаю). Така наша пропозиція, в першу чергу, обґрунтовується тим, що сьогодні в мережу «викидається» дуже багато так званих «фейкових» новин, які лише вводять в оману населення та підривають довіру до окремих органів державної влади (досить часто ними є правоохоронні органи) та держави взагалі.

9. З метою вдосконалення адміністративного законодавства, яке регулює забезпечення кібербезпеки в Україні, запропоновано: а) закріпити види кіберзагроз на законодавчому рівні, що має важливе значення не лише з теоретичної, а й з практичної точки зору, адже це, по-перше, унеможливлює неоднозначне тлумачення окремих правових норм; по-друге, дозволяє більш якісно формулювати положення інших нормативно-правових актів у цій сфері, наприклад положення Стратегії кібербезпеки України; б) внести зміни до Закону України «Про основні засади забезпечення кібербезпеки України» та додати терміни «кіберправопорушення» та «кіберпроступок», вказавши, що кіберправопорушення – це суспільно небезпечне діяння, яке було здійснено за допомогою застосування кіберпростору через використання, створення, обробку чи знищення інформації (комп'ютерних даних, носіїв інформації тощо) та здійснення якого тягне за собою настання негативних наслідків у вигляді юридичної відповідальності. Що ж стосується кібепроступку, то під ним необхідно розуміти кіберправопорушення, яке не несе в собі суспільну небезпеку та за яке передбачена відповідальність; в) у Стратегії кібербезпеки України, по-перше, чітко закріпити строки реалізації стратегії; по-друге, приділити увагу кадровому питанню суб'єктів, що уповноважені забезпечувати кібербезпеку в Україні. В ній повинні бути вказані наступні аспекти: кількість фахівців, яку планується підготувати для здійснення діяльності у досліджуваній сфері; напрямки підготовки фахівців; відповідальні особи (державні органи), які повинні відповідати за розроблення програм підготовки та перепідготовки кадрів; джерела фінансування.

10. З метою оптимізації системи суб'єктів забезпечення кібербезпеки України запропоновано створити єдиний державний орган, який був би наділений повноваженнями щодо координації діяльності всіх суб'єктів забезпечення кібербезпеки України.

З'ясовано, що на законодавчому рівні мало уваги приділяється взаємодії конкретних суб'єктів забезпечення кібербезпеки. Зокрема, недостатньо розробленим є механізм такої взаємодії, який включає: 1) визначення взаємних прав та обов'язків суб'єктів під час здійснення спільної діяльності; 2) визначення напрямків взаємодії; 3) окреслення форм та методів взаємодії; 4) визначення повноважень суб'єкта, який буде координувати спільну діяльність суб'єктів забезпечення кібербезпеки в Україні.

Враховуючи постійну динаміку розвитку кіберпростору обґрунтована необхідність прийняття окремого положення «Про порядок взаємодії суб'єктів забезпечення кібербезпеки в Україні», в якому необхідно передбачити всі аспекти такої взаємодії.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ:

Статті у наукових фахових виданнях:

1. Бухарєв В. В. Адміністративно-правові форми забезпечення кібербезпеки в Україні. *Науковий вісник Ужгородського національного університету. Серія «Право»*. 2015. Вип. 33. Ч. 2. С. 61–66.
2. Бухарєв В. В. Види юридичної відповідальності за порушення законодавства у сфері кібербезпеки України. *Науковий вісник Херсонського державного університету. Серія «Юридичні науки»*. 2016. Вип. 6-2. Т. 2. С. 188–192.
3. Бухарєв В. В. Зарубіжний досвід забезпечення кібербезпеки та можливості його використання в Україні. *Науковий вісник Ужгородського національного університету. Серія «Право»*. 2017. Вип. 43. Т. 3. С. 128–133.
4. Бухарєв В. В. Напрямки вдосконалення адміністративного законодавства, яке регулює забезпечення кібербезпеки в Україні. *Наше право*. 2018. № 2. С. 52–57.
5. Бухарєв В. В. Поняття та особливості кібербезпеки як об'єкту адміністративно-правової охорони. *Європейські перспективи.* 2018. № 3. С. 11–16.

Статті у зарубіжних періодичних наукових виданнях:

1. Бухарєв В. В. Напрямки удосконалення взаємодії суб'єктів забезпечення кібербезпеки України. *Верховенство права*. 2018. № 3. С.71–76.
2. Бухарев В. В. Историко-правовой анализ развития законодательства в сфере обеспечения кибербезопасности. *Legea si viata*. 2018. № 11/2. С. 23–26.

Наукові праці, які засвідчують апробацію матеріалів дисертації:

1. Бухарєв В. В. Адміністративно-правові методи забезпечення кібербезпеки в Україні. *Сучасні правові системи світу в умовах глобалізації: реалії та перспективи*: Міжнародна науково-практична конференція, м. Київ, 13-14 березня 2015 р. – К.: Центр правових наукових досліджень, 2015. С. 59–62.
2. Бухарєв В. В. Нормотворчість як адміністративно-правова форма забезпечення кібербезпеки в Україні. *Розвиток сучасного права в умовах глобальної нестабільності*: Матеріали міжнародної науково-практичної конференції (м. Одеса, Україна, 9-10 вересня 2016 р.) – Одеса: ГО «Причорноморська фундація права», 2016. С. 78–79.
3. Бухарєв В. В. Адміністративний договір як важлива адміністративно-правова форма забезпечення кібербезпеки в Україні. *Розвиток державності та права в Україні: реалії та перспективи*: Матеріали міжнародної науково-практичної конференції, м. Львів, 14–15 вересня 2018 р. – Львів: Західноукраїнська організація «Центр правничих ініціатив», 2018. С. 59–62.

АНОТАЦІЯ

Бухарєв В. В. Адміністративно-правові засади забезпечення кібербезпеки України. – *На правах рукопису.*

Дисертація на здобуття наукового ступеня кандидата юридичних наук за спеціальністю 12.00.07 – адміністративне право і процес; фінансове право; інформаційне право. – Сумський державний університет. – Суми, 2018.

У дисертації наведено теоретичне узагальнення та нове вирішення наукового завдання, яке полягає у визначенні сутності та особливостей адміністративно-правових засад забезпечення кібербезпеки України, а також опрацюванні напрямків удосконалення адміністративного законодавства, яке регулює забезпечення кібербезпеки в Україні.

Визначається поняття та з'ясовуються особливості кібербезпеки як об'єкта адміністративно-правової охорони. Здійснюється історико-правовий аналіз розвитку та становлення правового інституту кібербезпеки. Встановлюються види об'єктів кібербезпеки та кіберзахисту. Характеризуються правові засади забезпечення кібербезпеки України та з'ясовується місце серед них адміністративно-правового забезпечення. Окреслюється коло суб'єктів забезпечення кібербезпеки України та особливості їх адміністративно-правового статусу. Систематизуються адміністративно-правові форми та методи забезпечення кібербезпеки України. Виокремлюються види та особливості юридичної відповідальності за порушення законодавства у сфері кібербезпеки України. Узагальнюється зарубіжний досвід забезпечення кібербезпеки та пропонуються можливості його використання в Україні. Опрацьовуються напрямки вдосконалення адміністративного законодавства, яке регулює забезпечення кібербезпеки в Україні. Пропонуються способи оптимізації системи суб'єктів забезпечення кібербезпеки України та напрямки вдосконалення взаємодії між ними.

Ключові слова: кібербезпека, кіберзахист, адміністративно-правова охорона, правовий інститут, адміністративно-правові засади, суб'єкти забезпечення кібербезпеки, адміністративно-правовий статус, юридична відповідальність, форми, методи, взаємодія.

АННОТАЦИЯ

Бухарев В. В. Административно-правовые основы обеспечения кибербезопасности Украины. – *На правах рукописи*.

Диссертация на соискание ученой степени кандидата юридических наук по специальности 12.00.07 – административное право и процесс; финансовое право; информационное право. – Сумской государственный университет. – Сумы, 2018.

В диссертации приведены теоретическое обобщение и новое решение научной задачи, которая заключается в определении сущности и особенностей административно-правовых основ обеспечения кибербезопасности Украины, а также разработке направлений совершенствования административного законодательства, регулирующего обеспечение кибербезопасности в Украине.

Определяется понятие и выясняются особенности кибербезопасности как объекта административно-правовой охраны. Осуществляется историко-правовой анализ развития и становления правового института кибербезопасности. Устанавливаются виды объектов кибербезопасности и киберзащиты. Характеризуются правовые основы обеспечения кибербезопасности Украины и выясняется место среди них административно-правового обеспечения. Определяется круг субъектов обеспечения кибербезопасности Украины и особенности их административно-правового статуса. Систематизируются административно-правовые формы и методы обеспечения кибербезопасности Украины. Выделяются виды и особенности юридической ответственности за

нарушение законодательства в сфере кибербезопасности Украины. Обобщается зарубежный опыт обеспечения кибербезопасности и предлагаются возможности его использования в Украине. Прорабатываются направления совершенствования административного законодательства, регулирующего обеспечение кибербезопасности в Украине. Предлагаются способы оптимизации системы субъектов обеспечения кибербезопасности Украины и направления совершенствования взаимодействия между ними.

Ключевые слова: кибербезопасность, киберзащита, административно-правовая охрана, правовой институт, административно-правовые основы, субъекты обеспечения кибербезопасности, административно-правовой статус, юридическая ответственность, формы, методы, взаимодействие.

SUMMARY

Bukhariev V. V. Administrative and Legal Principles of Ensuring Cyber Security of Ukraine. — *Manuscript.*

The thesis for a candidate's degree by the specialty 12.00.07 – administrative law and procedure; financial law; informational law. – Sumy State University. – Sumy, 2018.

The author of the dissertation has provided theoretical generalization and a new solution of the scientific problem, which consists in determining the essence and peculiarities of administrative and legal principles of ensuring cyber security of Ukraine, as well as working out the directions of improving administrative legislation that regulates the provision of cyber security in Ukraine.

The author has determined the concept and clarified the features of cyber security as an object of administrative and legal protection. The historical and legal analysis of the development and formation of the legal institution of cyber security has been carried out. The types of objects of cyber security and cyber protection have been established. The author has characterized the legal principles of ensuring cyber security of Ukraine and has clarified the place of administrative and legal provision among them. The range of subjects of ensuring cyber security of Ukraine and the peculiarities of their administrative and legal status have been outlined. Administrative and legal forms and methods of ensuring cyber security of Ukraine have been systematized. The types and peculiarities of legal liability for the violations of legislation in the sphere of cyber security of Ukraine have been singled out. International experience of ensuring cyber security has been generalized; the author has offered the possibilities of its application in Ukraine. Areas of improvement of administrative legislation regulating the provision of cyber security in Ukraine have been worked out. The ways for the optimization of the system of subjects of ensuring cyber security of Ukraine and directions of the improvement of interaction between them have been offered.

Key words: cyber security, cyber protection, administrative and legal protection, legal institution, administrative and legal principles, subjects of ensuring cyber security, administrative and legal status, legal liability, forms, methods, interaction.

Відповідальний за випуск
БУХАРЄВ Владислав Вікторович.

Підписано до друку 20.11.2018.
Формат 60х90/16. Обл.-вид. арк. 1,9. Гарнітура
Times. Тираж 100 пр. Вид. № 101/18.

Віддруковано у видавництві «Ярославна».
40030, м. Суми, вул. Горького, 2.
Свідоцтво суб'єкта видавничої справи:
серія ДК, № 332 від 09.02.2001 р.