МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
ОДЕСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ

ВЕСЕЛОВА ЛІЛІЯ ЮРІЇВНА

УДК 342.951

АДМІНІСТРАТИВНО-ПРАВОВІ ОСНОВИ КІБЕРБЕЗПЕКИ В УМОВАХ ГІБРИДНОЇ ВІЙНИ

12.00.07 «Адміністративне право і процес;
фінансове право; інформаційне право»

Автореферат дисертації на здобуття наукового ступеня доктора юридичних наук

Одеса – 2021

Дисертацією є рукопис.

Роботу виконано в Одеському державному університеті внутрішніх справ, Міністерство внутрішніх справ України.

Науковий консультант:
доктор юридичних наук, професор
заслужений діяч науки і техніки України
Користін Олександр Євгенійович,
Державний науково-дослідний інститут Міністерства внутрішніх справ України,
головний науковий співробітник науково-дослідної лабораторії
кримінологічних досліджень та проблем запобігання злочинності.

Офіційні опоненти:
доктор юридичних наук, професор
Марущак Анатолій Іванович,
Національна академія Служби безпеки України,
професор спеціальної кафедри № 8 Навчально-наукового інституту
перепідготовки та підвищення кваліфікації кадрів;

доктор юридичних наук, професор
Гуржій Тарас Олександрович,
Київський національний торговельно-економічний університет,
завідувач кафедри адміністративного, фінансового та інформаційного права;

доктор юридичних наук, професор
Свиридюк Наталія Петрівна,
Національний авіаційний університет,
професор кафедри міжнародного права та порівняльного правознавства.

Захист відбудеться «26» березня 2021 року о 10^{00} на засіданні спеціалізованої вченої ради Д 41.884.04 Одеського державного університету внутрішніх справ за адресою: 65014, м. Одеса, вул. Успенська, 1.

З дисертацією можна ознайомитись у бібліотеці Одеського державного університету внутрішніх справ за адресою: 65000, м. Одеса, пров. Сабанський, 4.

Автореферат розісланий «24» лютого 2021 року.

Учений секретар
спеціалізованої вченої ради О.М. Заєць

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Обґрунтування вибору теми дослідження. У сучасному суспільстві проблематика кібербезпеки привертає все більше уваги. Актуальність адміністративно-правового забезпечення кібербезпеки визначається сучасним розвитком інформаційного суспільства, який переходить від традиційного публічного адміністрування до урядування через електронні форми, утворення нових форм інформаційної діяльності, що призводить до суттєвого розширення обсягів інформації, проникнення її складових у різні сфери суспільної діяльності. Водночас розвиток інформаційного суспільства та сформовані правові інструменти забезпечують реалізацію інформаційних прав і обов'язків громадян, визначають ступінь розвитку інформаційної сфери України, стан інформаційного правопорядку, рівень забезпечення правової охорони і захисту соціальних цінностей.

За даними американської транснаціональної компанії Cisco, що спеціалізується у галузі високих технологій та телекомунікацій, майже кожна четверта організація, яка піддалася кібератаці, втрачає бізнес-можливості, а близько 30% підприємств втратили прибуток. В Україні зазначена проблема підсилюється станом гібридної війни проти нашої країни. Ключовим гібридним інструментом агресор використовує саме інформаційні технології та системи комунікацій у кіберпросторі. За даними Держспецзв'язку України щодо захисту державних інформаційних ресурсів лише за останніх 9 місяців зареєстровано більше ніж 60 мільйонів підозрілих подій та більше 3 млн. атак різних видів, які система захищеного доступу державних органів до мережі Інтернет заблокувала. Щотижня фіксується від 600 тис. до 900 тис. підозрілих подій, а система захищеного доступу державних органів до мережі Інтернет блокує більш 0,5 млн. різних видів атак.

За умови гібридизації кіберзагроз, їх зовнішнього характеру, санкції кримінальних законів є безперспективними та малоефективними. Національна безпека загалом, зокрема її інформаційна складова (кібербезпека), потребують формування безпекового кіберпростору та системного упровадження правових інструментів превентивного характеру. Зазначене реалізується саме адекватним механізмом адміністративно-правового регулювання, визначенням відповідного адміністративно-правового статусу суб'єктів національної системи кібербезпеки в Україні, удосконаленням форм та методів адміністративно-правового регулювання у сфері протидії гібридним кіберзагрозам.

Ураховуючи зазначене, дослідження щодо адміністративно-правових основ кібербезпеки в умовах гібридної війни набуває суттєвого практичного значення та викликає значний інтерес у науково-теоретичному та практичному аспектах означеної проблеми.

Теоретичне підґрунтя дослідження склали наукові здобутки та погляди багатьох учених. Адміністративно-правове спрямування предмета дослідження забезпечено аналізом здобутків провідних учених-адміністративістів: В.Б. Авер'янова, С.М. Алфьорова, О.Ф. Андрійко, А.І. Берлача, Л.Р. Білої-Тіунової, Ю.П. Битяка, В.М. Гаращука, В.Л. Грохольського, Т.О. Гуржія, Денисова А.В., Д.П. Калаянова, Р.А. Калюжного, Т.О. Коломоєць, В.К. Колпакова, А.Т. Комзюка, С.О. Кузніченка, О.В. Кузьменко, Є.В. Курінного, Я.В. Лазура, Р.С. Мельника, О.В. Негодченка, Є.В. Петрова, Н.П. Свиридюк, О.І. Харитонової, Х.П. Ярмакі та інших.

Вагомий внесок щодо розуміння окремих аспектів забезпечення кібербезпеки України, проблем інформаційної безпеки, розбудови системи правового забезпечення інформаційної та кібербезпеки зроблено у наукових працях вітчизняних науковців: Арістової І.В., Архипова О.Є., Баранова О.А., Безкоровайного М.М., Березовської І.Р., Бєлякова К.І., Бірюкова Д.С., Брижка В.М., Бутузова В.М., Бухарєва В.В., Галинської К.Ю., Горбуліна В., Діордіци І.В., Довганя О.Д., Дороніна І.М., Дубова Д.В., Заярного О.А., Користіна О.Є., Кормича Б.А., Лісовської Ю.П., Леонідова О.О, ЛогіноваО.В., Марущака А.І., Орлова О.В., Олійник О.В., Пилипчука В.Г., Рудник Л.І., Резнікової О.О., Стоєцького О.В., Тихомирова О.О., Хахановського В.Г., Цимбалюка В.С., Швеця М.Я. та інших. Однак, попри наявні здобутки, з'ясування та вирішення проблем забезпечення кібербезпеки, зокрема в умовах гібридної війни, зазначені праці в комплексі не висвітлюють питання щодо особливостей формування адміністративно-правових основ системи кібербезпеки в умовах гібридної війни, що зумовлює актуальність обраної теми наукової роботи та важливість ґрунтовного дослідження на монографічному рівні.

Все вищенаведене, а також недостатня розробленість на теоретичному рівні цієї проблематики та наявність організаційних і правових прогалин у досліджуваній сфері, зумовлює актуальність обраної теми та потребує правового унормування окремих проблемних аспектів, а також обумовлює необхідність у проведенні комплексного дослідження питань адміністративно-правових основ кібербезпеки в умовах гібридної війни на основі як наук юридичного циклу, так і з врахуванням сучасної наукової думки суміжних наук.

Емпіричну основу дослідження становлять: аналітичні та методичні матеріали міжнародних, національних та зарубіжних інституцій; статистичні дані Національної поліції України, Державної служби спеціального зв'язку та захисту інформації України, Урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA; єдині звіти Офісу Генерального прокурора про кримінальні правопорушення по державі та про осіб, які

вчинили кримінальні правопорушення за 2020 р.; відомості річних звітів Cisco з інформаційної безпеки за 2017 та 2018 роки; результати узагальнення анкетування експертів, а саме кіберполіцейських та фахівців спеціального відділу СБУ (320 респондентів).

Нормативно-правову основу дослідження становлять законодавство України, міжнародно-правові та окремі нормативні акти зарубіжних країн у сфері кібербезпеки.

Зв'язок роботи з науковими програмами, планами, темами, грантами. Дисертацію виконано відповідно до основних положень Стратегії сталого розвитку «Україна–2020», затвердженої Указом Президента України від 12.01.2015 № 5/2015; Концепції розвитку сектору безпеки і оборони, затвердженої Указом Президента України від 14.03.2016 р.; Стратегії розвитку органів системи МВС на період до 2020 р., затвердженої розпорядженням Кабінету Міністрів України від 15.11.017 № 1023-р; Плану заходів реалізації Стратегії розвитку органів Міністерства внутрішніх справ на період до 2020 року, затвердженого розпорядженням Кабінету Міністрів України від 21.08.2019 № 693-р; Переліку пріоритетних напрямів наукового забезпечення діяльності органів внутрішніх справ України на період 2015–2019 рр., затвердженого наказом МВС України від 16.03.2015 № 275, а також комплексної теми наукових досліджень кафедри адміністративного права та адміністративного процесу Одеського державного університету внутрішніх справ «Пріоритетні напрями розвитку реформування правоохоронних органів в умовах розгортання демократичних процесів у державі» (державний реєстраційний номер 0116U006773).

Тема дисертації затверджена на засіданні Вченої ради Одеського державного університету внутрішніх справ (протокол № 4 від «26» грудня 2018 р.), а також розглянуто координаційним бюро відповідного відділення Національної академії правових наук України і вона отримала позитивний відгук щодо актуальності, коректності формулювання і доцільності дослідження у вигляді дисертації за спеціальністю 12.00.07 – адміністративне право і процес; фінансове право; інформаційне право.

Мета та завдання дослідження відповідно до предмета та об'єкта дослідження. *Метою* роботи є здійснення комплексного наукового дослідження адміністративно-правових основ кібербезпеки в умовах гібридної війни на основі аналізу чинного національного та міжнародного законодавства, практики його застосування та реалізації, а також на основі узагальнення основних положень сучасних зарубіжних та вітчизняних наукових праць. Для досягнення зазначеної мети під час дослідження поставлено та вирішено наступні *завдання:*

- охарактеризувати сучасний стан кібербезпеки України на основі її актуалізації в умовах гібридної війни;

- з’ясувати методологічні та безпекознавчі засади пізнання кібербезпеки та окреслити напрями її дослідження;

- окреслити особливості сучасної адміністративно-правової парадигми забезпечення кібербезпеки;

- розкрити ключові аспекти механізму застосування адміністративно-правових заходів забезпечення кібербезпеки;

- розкрити зміст адміністративно-правової охорони у сфері забезпечення кібербезпеки;

- проаналізувати сутнісні характеристики адміністративної відповідальності у сфері забезпечення кібербезпеки;

- визначити роль адміністративно-правових відносин у сфері забезпечення кібербезпеки України;

- проаналізувати адміністративно-правовий статус суб’єктів забезпечення кібербезпеки України з виділенням проблемних питань;

- окреслити форми міжвідомчої та державно-приватної взаємодії у системі забезпечення кібербезпеки України;

- виявити особливості щодо нових технологій й загроз у сфері кібербезпеки та визначити стратегічні цілі й складові її правового забезпечення;

- виокремити та оцінити сучасні світові тенденції розвитку адміністративно-правового та організаційного забезпечення кібербезпеки;

- визначити та обґрунтувати стратегічні напрями за досвідом ЄС та НАТО у формуванні адміністративно-правового механізму протидії гібридним загрозам у сфері забезпечення кібербезпеки та сформулювати відповідні рекомендації.

Об’єктом дослідження є суспільні відносини у сфері забезпечення кібербезпеки.

Предметом дослідження є адміністративно-правові основи кібербезпеки в умовах гібридної війни.

Методи дослідження. Методологічне забезпечення дослідження зумовлене його метою та завданнями й базується на використанні сукупності загальнонаукових та спеціальних методів наукового пізнання, що забезпечило повноту та достовірність отриманих результатів.

Методологічну основу роботи заклали системно-структурний метод та метод сходження від абстрактного до конкретного. У поєднанні з методом аналізу вони стали дієвим інструментом у дослідженні теоретико-методологічних засад адміністративно-правового забезпечення кібербезпеки України (підрозділи 1.1, 1.2, 2.1, 2.2, 3.1).

Філософського-світоглядну основу дослідження становить *діалектичний метод* наукового пізнання кібербезпки, як правової категорії в суперечностях та змінах, що створило можливість оцінити історичний розвиток розуміння, становлення правового інституту та формування сучасної адміністративно-правової парадигми забезпечення кібербезпеки. За допомогою *формально-*

юридичного методу були обґрунтовані дефініції щодо сутності досліджувальних категорій, сформовано понятійно-категоріальний апарат (підрозділи 1.1, 1.2, 1.3, 2.1, 2.2, 3.3). *Порівняльно-правовий метод* використовувався під час дослідження вітчизняного та зарубіжного законодавства, з питань законодавчої регламентації правового забезпечення кібербезпеки в умовах гібридизації кіберзагроз та практики застосування адміністративної відповідальності у сфері забезпечення кібербезпеки України (підрозділи 2.1, 2.3, 3.1, 3.3). *Статистичний та соціологічний методи* використовувалися для отримання та аналізу емпіричних даних щодо предмету дослідження, характеристики явищ, аналізу правозастосування та обґрунтування загальних висновків по підрозділах дисертації (розділи 2, 3). *Метод наукової абстракції* дозволив сформувати обґрунтовані заходи щодо формування адміністративно-правового механізму протидії гібридним загрозам у сфері забезпечення кібербезпеки.

Наукова новизна отриманих результатів полягає в тому, що дисертація є першим комплексним дослідженням адміністративно-правових основ кібербезпеки України в умовах гібридної війни, а також обґрунтовуються напрями оптимізації та вдосконалення її забезпечення. У результаті виконання дослідження було сформульовано та обґрунтовано низку наукових положень, які є новими для вітчизняної правової доктрини та правозастосовної практики, а саме:

уперше:

- на основі гносеологічного підходу обґрунтовується сучасне розуміння розвитку суспільних відносин у кіберпросторі, їх дуалістичний зміст для України, що формується як на основі загальноцивілізаційних тенденцій, притаманних інформаційному суспільству, так і особливостями, що є результатом гібридної агресії на територію держави та потребує врахування безпекової складової з адекватним методологічним та змістовним наповненням;
- на основі порівняльного аналізу зарубіжного законодавства, норм міжнародного права та рекомендацій міжнародних організацій обґрунтовано методологічне значення формування адміністративних заходів запобігання на основі правового врегулювання зобов'язань суб'єктів національної системи кібербезпеки щодо визначення ризиків кібербезпеки та упровадження ризик-орієнтованої стратегії кібербезпеки;
- доведено необхідність підвищення обізнаності щодо гібридних кіберзагроз на основі визначення вразливості суспільства щодо них, скоординованої діяльності щодо оцінювання зазначених загроз та ризиків, що впливають на інститути та мережі, а також виявлення ключових вразливостей, враховуючи конкретні гібридні показники;
- обґрунтовано необхідність упровадження та розкрито зміст ключових складових забезпечення кібербезпеки України в умовах гібридної війни:

«ризик-орієнтований підхід щодо забезпечення кібербезпеки», «ризик-орієнтований підхід щодо захисту критичної інфраструктури»;

- обґрунтовано необхідність законодавчих змін, спрямованих на покращання адміністративно-правового забезпечення кібербезпеки України в умовах гібридної війни, а саме: внесення змін та доповнень до проекту Закону України «Про критичну інфраструктуру та її захист» та Кодексу України про адміністративні правопорушення.

удосконалено:

- підходи до обґрунтування ключових напрямів розвитку чинної правової бази забезпечення кібербезпеки України, підкреслюючи необхідність формування понятійно-термінологічного апарату адміністративно-правового забезпечення кібербезпеки та його узгодженість не лише з термінологією чинного вітчизняного законодавства та міжнародних актів, а й з адекватним щодо гібридності кіберзагрози змістовним наповненням;

- підходи до обґрунтування сутності та визначення поняття «кібербезпека», під якою запропоновано розуміти цілісну систему забезпечення стану захищеності життєво важливих інтересів громадян, суспільства та держави, а також мінімізації ймовірності реальних і потенційних кіберзагроз, їх наслідків та підвищення стійкості суспільства у кіберпросторі, а також забезпечення сталого розвитку особистості, суспільства та держави;

- підходи до тлумачення сутнісної характеристики адміністративно-правової охорони у сфері забезпечення кібербезпеки, яка визначена у якості адміністративно-правового явища, зміст якого базується на впорядкованій нормами адміністративного права діяльності суб'єктів забезпечення кібербезпеки, що спрямована на забезпечення прав і свобод громадян, суспільства та держави у кіберпросторі, запобігання їх порушення, виявлення кіберзагроз та відновлення порушених прав, свобод та законних інтересів осіб, що здійснюються засобами адміністративного права з можливістю застосування заходів адміністративного примусу та притягнення винних до адміністративної відповідальності;

- тлумачення щодо подальшого безпекового розвитку адміністративно-правових форм та методів як ключових у реалізації адміністративно-правового механізму у сфері забезпечення кібербезпеки України, що потребує подальшого комплексного використання усіх зазначених адміністративно-правових інструментів та формування високого рівня спроможності державно-правового впливу на безпеку відносин у кіберпросторі;

дістали подальшого розвитку:

- підходи до розкриття змісту механізму адміністративно-правового забезпечення кібербезпеки, під яким запропоновано розуміти сукупність правових

засобів, заходів та способів, за допомогою яких забезпечується функціонування та розвиток взаємодії суб'єктів національної системи кібербезпеки;

- підходи до сприйняття змісту та визначення поняття заходів адміністративно-правового забезпечення кібербезпеки як законодавчо визначеної сукупності взаємопов'язаних організаційно-правового й спеціального характеру заходів державно-владного впливу суб'єктів національної системи кібербезпеки, спрямованих на забезпечення кібербезпеки людини, суспільства та держави;

- характеристика заходів запобігання в механізмі адміністративно-правового забезпечення кібербезпеки, що застосовуються суб'єктами національної системи кібербезпеки, на підставі положень чинного законодавства з питань забезпечення кібербезпеки, за відсутності очевидних порушень, з метою профілактики і недопущення правопорушень у кіберпросторі;

- підходи щодо розуміння адміністративно-правових форм у сфері забезпечення кібербезпеки України як зовнішнього вияву конкретних дій, що здійснюються органами виконавчої влади, суб'єктами забезпечення кібербезпеки, та спрямовуються на реалізацію поставлених перед ними завдань щодо створення необхідних умов безпеки інформаційних та телекомунікаційних систем у кіберпросторі;

- підходи щодо розкриття безпекового змісту адміністративної відповідальності у сфері забезпечення кібербезпеки України як різновиду юридичної відповідальності, що є засобом адміністративно-правової охорони відносин у кіберпросторі, є наслідком винного антисуспільного діяння у сфері забезпечення кібербезпеки, і головне призначення якого у примусовому припиненні протиправних дій, що стосуються незаконного втручання в комп'ютерні та телекомунікаційні системи й порушення при цьому прав та свобод людини, інтересів держави та суспільств;

- характеристика адміністративно-правових відносин у сфері забезпечення кібербезпеки – суспільних відносин, що виникають з приводу діяльності об'єктів у кіберпросторі, які характеризуються стійкими правовими зв'язками між суб'єктами забезпечення кібербезпеки, що виникають у процесі реалізації ними суб'єктивних прав та обов'язків на підставі приписів адміністративно-правових норм, якими вони встановлені та гарантовані;

- пропозиції щодо розкриття змісту правовідносин, що характеризують діяльність суб'єктів забезпечення кібербезпеки України, з'ясовано їх адміністративно-правовий статус та співвідношення співзвучних загалом юридичних термінів «суб'єкти правовідносин», «учасник правовідносин» й «суб'єкт права»;

- підходи щодо розкриття змісту поняття та структури правового статусу суб'єктів забезпечення кібербезпеки;

- обґрунтування стратегічних цілей й складових правового забезпечення кібербезпеки України на основі аналізу особливостей новітніх технології й загроз у сфері кібербезпеки.

Практичне значення отриманих результатів полягає в тому, що вони становлять науково-теоретичний і практичний інтерес. Сформульовані положення, пропозиції та висновки використані та можуть бути застосовані в:

– науково-дослідній сфері для формування теоретичного підґрунтя подальших наукових розвідок за відповідними напрямами (акт впровадження у наукову діяльність ДНДІ МВС України від 05.03.2020);

– правотворчості як основа для реформування національного адміністративного законодавства щодо забезпечення кібербезпеки (довідки Комітету Верховної Ради України з питань правоохоронної діяльності від 16.06.2020 № 04-27/12-2020/77348; 16.07.2020 № 04-27/12-2020/108767);

– правозастосовній діяльності для підвищення ефективності публічного адміністрування у сфері кібербезпеки;

– освітньому процесі як інформаційне підґрунтя для формування змістовного наповнення і викладання таких навчальних дисциплін, як «Актуальні питання інформаційного права», «Безпека технічних джерел», «Сучасні інформаційні технології», «Сучасні інформаційні технології в юридичних дослідженнях» (акт впровадження в освітній процес ОДУВС від 16.03.2020).

Особистий внесок здобувача. Дисертація є самостійною науковою роботою. Основні теоретичні положення та розробки, які характеризують наукову новизну дослідження, теоретичне й практичне значення його результатів одержані дисертантом особисто. Особистий внесок здобувача в публікаціях, підготовлених у співавторстві, становить не менш як 50 %. Ідеї та розробки співавторів у дисертації не використовувалися.

Апробація матеріалів дисертації. Основні результати дослідження оприлюднено та обговорено на міжнародних і всеукраїнських наукових і науково-практичних конференціях, семінарах і круглих столах, зокрема: «Актуальні завдання та напрями розвитку юридичної науки у XXI столітті» (Львів, 18-19.10.2019); «Проблеми правової реформи та розбудови громадянського суспільства в Україні» (Харків, 18-19.10.2019); «Стан та перспективи розвитку адміністративного права України» (Одеса, 23.10.2019); «Економіка, облік, фінанси та право: аналіз тенденцій та перспектив розвитку» (Полтава, 24.10.2019); «Актуальні проблеми розвитку науки в контексті глобальних трансформацій інформаційного суспільства» (Київ, 25-26.10.2019); «Актуальні питання розвитку державності та правової системи в сучасній Україні» (Запоріжжя, 25-26.10.2019); «Науковий потенціал та перспективи розвитку юридичної науки» (Запоріжжя, 27-28.03.2020); «Актуальні проблеми прав людини, держави та вітчизняної правової системи» (Дніпро, 03-04.04.2020); «Громадське суспільство в Україні: проблеми забезпечення правотворчої діяльності» (Харків, 03-04.04.2020); «Протидія організованій злочинній діяльності» (Одеса, 14.06.2020).

Публікації. Основні теоретичні й практичні висновки, положення та пропозиції, сформульовані за результатами дисертаційної роботи, викладено у 34 публікаціях: 1 монографії, 23 наукових статтях, з них 14 – у періодичних виданнях, включених МОН України до Переліку наукових фахових видань із юридичних наук, 9 – у зарубіжних наукових періодичних виданнях, а також у 10 тезах доповідей на науково-практичних конференціях, семінарах і круглих столах.

Структура та обсяг дисертації. Дисертація складається з анотації, вступу, чотирьох розділів, що включають 12 підрозділів, висновків, списку використаних джерел та додатків. Загальний обсяг дисертації становить 500 сторінок, з них основна частина тексту викладена на 390 сторінках. Список використаних джерел нараховує 892 найменування і викладений на 83 сторінках, додатки – на 10 сторінках.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У **Вступі** обґрунтовано актуальність дослідження, зазначається зв'язок роботи із науковими планами та програмами; визначено мету та задачі, об'єкт та предмет дослідження; надано характеристику методологічним основам роботи; розкрито ступінь наукової новизни одержаних результатів, характер та результати їхньої апробації; структуру та обсяг дисертації.

Розділ 1 «Теоретико-методологічні засади адміністративно-правового забезпечення кібербезпеки України» містить три підрозділи й присвячений комплексному аналізу основних категорій та понять інституту забезпечення кібербезпеки в Україні.

У підрозділі 1.1. «Концептуалізація гібридизації загроз кібербезпеці України» наголошується, що технологічні можливості формують низку якостей, які спрощують, забезпечують анонімність та доступність для людей, але, у той же час, приваблюють злочинців для вчинення протиправних дій. Разом з тим, наслідком зростаючого використання інформаційних технологій є одночасне зростання та поширення кіберзагроз, зокрема, і у формі кіберзлочинів. З'ясовано, що особливим видом кіберзагрози у сучасних умовах є поширення кібертероризму.

Із врахуванням предмету дослідження, доводиться, що ключовою проблемою залишається правова регламентація використання кіберпростору. Правовим регулюванням держава має сприяти підвищенню відповідальності провайдерів і власників сайтів щодо розміщення недостовірної та завідомо шкідливої інформації, а також закріплювати механізм впливу на недобросовісних суб'єктів інформаційних правовідносин в кіберпросторі.

Науковий пошук у межах дослідження дав змогу зробити висновок, що сучасний стан розвитку суспільних відносин у кіберпросторі для України характеризується низкою як загальноцивілізаційних ознак, характерних

інформаційному суспільству, так і певними особливостями, що є результатом гібридної агресії на територію України. Дуалізм зазначеної характеристики кіберпростору для вітчизняних користувачів інформаційно-телекомунікаційними системами, перш за все, притаманний безпековій складовій інформаційних суспільних відносин.

Зазначено, що кібербезпека України умовно розглядається у двох площинах: технологічний прогрес (не лише сприяє стрімкому розвиткові інформаційних комунікацій та послуг, а й формує свої специфічні загрози – кіберзагрози, що є надбанням усього глобального людства та певним чином невідворотною кармою сучасного інформаційного суспільства); з іншого боку, Україна у стані війни, яка характеризується агресивними нападами не лише у воєнній сфері, інша складова агресії проти України, можливо навіть попереду всього іншого, базується на сучасних інформаційних технологіях і гібридизує усталені конвенційні канони війни.

Підрозділ 1.2. «Методологічні та безпекознавчі засади пізнання кібербезпеки» акцентує увагу на тому, що характеризуючи концептуальні підходи до розуміння феномену «кібербезпека», вітчизняні й зарубіжні вчені надзвичайно ґрунтовно та всебічно визначають предмет наукового пошуку та формують відповідну методологічну базу. Крім того, міждисциплінарний характер кібербезпеки як проблеми, так і предмета наукового пізнання зумовлює залежність від неї значного спектру та сегментів суспільних відносин.

Зазначається, що останніми десятиліттями проблема безпеки взагалі, інформаційної й кібербезпеки, зокрема, є надзвичайно актуальною й поширюється настільки швидко, що певним чином неможливо зосередитись на сутності нового явища та межах його використання у контексті правового забезпечення. Тому виникає необхідність конкретизувати та більш глибоко розкрити сутність розуміння проблеми кібербезпеки через ретроспективний аналіз інформаційної безпеки до сучасних безпекознавчих засад кібербезпеки на основі надбань найбільш відомих представників наукової думки у цій сфері.

Акцентовано на тому, що національна безпека України істотно залежить від забезпечення кібербезпеки. У ході еволюції технічного прогресу та кіберпрогресу дана залежність дедалі зростатиме. Крім того, законодавче регулювання відносин у кіберпросторі потребує постійного оновлення, що є об’єктивно необхідним процесом, який має супроводжувати стрімкий технологічний розвиток інформаційного суспільства.

Із врахуванням аналізу вітчизняного законодавства з’ясовано, що законодавче забезпечення кібербезпеки потребує вирішення проблем правових колізій й прогалин правового регулювання, наслідком яких є неефективна правоохоронна діяльність щодо заподіяної шкоди інформації, інформаційно-телекомунікаційним мережам та репутації громадян тощо.

З врахуванням категорійної невизначеності і неготовності чинної правової бази протистояти новим загрозам, підкреслено на необхідності термінологічного урегулювання та унормування понятійного апарату у системі адміністративно-правового забезпечення кібербезпеки, на основі забезпечення адекватності його змістовного наповнення, відповідності вимогам, що висуваються до правової термінології, а також погодження термінології чинного вітчизняного законодавства з міжнародними актами.

У підрозділі 1.3. «Становлення правового інституту та формування сучасної адміністративно-правової парадигми забезпечення кібербезпеки» акцентовано увагу на розкритті змісту поняття «кібербезпека», що забезпечувалося дослідженням відповідних стратегій кібербезпеки, які розробляють та приймають розвинені країни світу (США, Німеччина, Франція, Канада, Австралія тощо), наукових розробок, аналітичних звітів, виступів на форумах, конференціях, семінарах національного та міжнародного рівнів, опублікованих наукових робіт, присвячених найрізноманітнішим аспектам кібербезпеки. Що дало можливість обґрунтувати очевидність того, що національні підходи до визначення кібербезпеки та й у міжнародних директивних документах суттєво відрізняються як щодо змісту, так і заходів щодо забезпечення кібербезпеки. Поряд з тим, глобальний характер кіберзагроз визначає необхідність правового врегулювання щодо уніфікації підходів до визначення сутності кібербезпеки та стандартизації заходів забезпечення задля ефективної співпраці та координації зусиль на національному та міжнародному рівнях.

Узагальнюючи наукові здобутки знаних вчених у досліджуваній сфері щодо визначення дефініції «кібербезпека», пропонується під кібербезпекою розуміти цілісну систему забезпечення стану захищеності життєво важливих інтересів громадян, суспільства та держави, а також мінімізації ймовірності реальних і потенційних кіберзагроз, їх наслідків та підвищення стійкості суспільства у кіберпросторі, а також забезпечення сталого розвитку особистості, суспільства та держави. Таким чином, зазначається, що кібербезпека є системним й цілеспрямованим явищем, яке забезпечує захист, стійкість та спроможність до розвитку суб'єктів кіберпростору.

Акцентується, що сучасний етап формування вітчизняного законодавства є надзвичайно активним та результативним. На основі аналізу низки нормативно-правових актів України у сфері кібербезпеки зроблено висновок, що становлення національного правового інституту кібербезпеки, напряму пов'язується з розвитком міжнародного права у цій сфері і, перш за все, європейського, яке слугувало певним стандартом у сфері інформаційної та телекомунікаційної захищеності суспільства.

Установлено, що усі зазначені положення мають важливий методологічний зміст щодо розуміння проблем кібербезпеки і не лише в

контексті інших видів безпеки. У свою чергу, складнощі з визначенням поняття кіберпростору обумовлюють проблеми щодо розуміння кібербезпеки та кібервійни. Поряд з тим, за умов сучасного технологічного розвитку кіберсфери, методологічні засади адміністративно-правового забезпечення кібербезпеки потребують подальшого вдосконалення.

Розділ 2 «Методологічні засади адміністративно-правового забезпечення кібербезпеки в умовах гібридизації кіберзагроз» об'єднує в собі три підрозділи.

У підрозділі 2.1. «Механізм застосування адміністративно-правових заходів забезпечення кібербезпеки» досліджено думки науковців-адміністративістів щодо тлумачення змісту, поняття механізму адміністративно-правового регулювання та його структури. На підставі аналізу різноманітних позицій вчених та підсумовуючи систему знань у сфері кібербезпеки, обґрунтованим вважається під механізмом адміністративно-правового забезпечення кібербезпеки розуміти сукупність правових засобів, заходів та способів, за допомогою яких забезпечується функціонування та розвиток взаємодії суб'єктів національної системи кібербезпеки.

Зазначено на необхідності постійного функціонального моніторингу новостворених суб'єктів кібербезпеки так як, незважаючи на те, що національна система кібербезпеки своєю метою і визначає певні гарантії ефективної протидії кіберзагрозам в умовах гібридної війни, на практиці, нерідко спостерігається відсутність чіткої та повної взаємодії, що пов'язується з певним функціональним дублюванням у діяльності окремих суб'єктів національної системи кібербезпеки та невиправданістю бюджетних витрат, які у такій високотехнологічній сфері є надзвичайно великими.

Зосереджено увагу на детальній характеристиці елементів механізму адміністративно-правового забезпечення кібербезпеки: адміністративно-правових нормах, що закріплюють права та обов'язки суб'єктів національної системи кібербезпеки; адміністративно-правових відносинах, що є особливою формою взаємозв'язку суб'єктів національної системи кібербезпеки на основі їх прав та обов'язків; актах реалізації прав й обов'язків суб'єктів національної системи кібербезпеки, що закріплюють та реалізують положення адміністративно-правових норм у процесі взаємодії суб'єктів національної системи кібербезпеки.

Акцентовано на важливості використання адміністративно-попереджувальних заходів щодо запобігання кіберзагрозам в умовах гібридної війни. Зазначається на необхідності формування заходів запобіжного характеру на основі упровадження ризик-орієнтованої стратегії кібербезпеки. Саме в межах адміністративних заходів запобігання, необхідним є правове врегулювання зобов'язання суб'єктів національної системи кібербезпеки щодо визначення ризиків кібербезпеки. Зазначені

ризики не можуть обмежуватися лише технічними ризиками, комп'ютерних та телекомунікаційних систем, мають також включати аналіз ризиків стратегічного та операційного характеру, соціальної, економічної, інфраструктурної сфер тощо.

Формування механізму адміністративно-правового забезпечення кібербезпеки із врахуванням аналізу ризиків запроваджує як заходи запобігання, так і заходи щодо виправлення ситуації.

У підрозділі 2.2. «Адміністративно-правова охорона, форми й методи у сфері забезпечення кібербезпеки» акцентовано, що розвиток системи охорони прав та свобод людини, охорони суспільних відносин в державі є невід'ємною складовою національної політики розвинутих країн, а результативність такої політики залежить від здатності урядів країн правильно та своєчасно обирати механізми її реалізації з урахуванням зростаючої ролі безпекового характеру сучасного цивілізаційного розвитку.

Зазначено, що адміністративно-правова охорона у сфері забезпечення кібербезпеки реалізується не лише нормами КУпАП та базового закону «Про основні засади забезпечення кібербезпеки України», а й нормами цілої низки, пов'язаних правоохоронною, інформаційною, телекомунікаційною та іншими сферами, законодавчих актів. У зв'язку з цим, забезпеченням кібербезпеки займаються різні відомства та установи в процесі виконання своїх функцій та покладених обов'язків. Крім того, особливістю забезпечення кібербезпеки як об'єкта адміністративно-правової охорони є її здійснення не лише у правовідносинах, що мають місце у зв'язку із вчиненням адміністративних правопорушень. Зазначене реалізується у більш широкому обсязі, що передбачає і запобігання, і припинення правопорушень.

Визначено, що адміністративно-правовими формами у сфері забезпечення кібербезпеки України є зовнішній вияв конкретних дій, що здійснюються органами виконавчої влади, суб'єктами забезпечення кібербезпеки, спрямованих на реалізацію поставлених перед ними завдань щодо створення необхідних умов безпеки інформаційних та телекомунікаційних систем у кіберпросторі.

Виділено та охарактеризовано адміністративно-правові форми у сфері забезпечення кібербезпеки (нормотворчість, прийняття індивідуальних актів, адміністративний договір, правореалізація), які є об'єктивним практичним відображенням діяльності суб'єктів кібербезпеки України. На основі думок знаних вчених-адміністративістів проаналізовано адміністративно-правові методи у сфері забезпечення кібербезпеки України. Доведено, що досліджені адміністративно-правові форми та методи є ключовими у реалізації адміністративно-правового механізму у сфері забезпечення кібербезпеки України, але подальший безпековий розвиток зазначеної сфери потребує подальшого комплексного використання усіх зазначених адміністративно-

правових інструментів та формування високого рівня спроможності державно-правового впливу на безпеку відносин у кіберпросторі.

У підрозділі 2.3. «Адміністративна відповідальність у сфері забезпечення кібербезпеки України» проаналізовано низку наукових праць, які стосуються різних видів юридичної відповідальності у сфері кібербезпеки та обґрунтовано, що велике коло питань, які стосуються юридичної відповідальності як засобу правової охорони відносин у кіберпросторі, потребують ґрунтовного та комплексного теоретичного дослідження.

Охарактеризовано загальні засади адміністративної відповідальності у сфері забезпечення кібербезпеки та проаналізовано окремі адміністративні правопорушення у зазначеній сфері. Зокрема, враховуючи методологічні акценти у дисертації щодо безпекового змісту діяльності із забезпечення кібербезпеки, обґрунтованим вбачається під адміністративною відповідальністю у сфері забезпечення кібербезпеки України розуміти різновид юридичної відповідальності, що є засобом адміністративно-правової охорони відносин у кіберпросторі, є наслідком винного антисуспільного діяння у сфері забезпечення кібербезпеки, і головне призначення якого у примусовому припиненні протиправних дій, що стосуються незаконного втручання в комп'ютерні та телекомунікаційні системи й порушення при цьому прав та свобод людини, інтересів держави та суспільства. Крім того, зазначається, що адміністративним проступком у сфері забезпечення кібербезпеки є протиправне, винне діяння (бездіяльність), що завдає значної шкоди відносинам у сфері кіберпростору, порушує права людини й інтереси суспільства і держави у цій сфері та встановлений правопорядок використання інформаційних й телекомунікаційних систем, а також за яке законодавством передбачено особливий вид державного примусу – адміністративну відповідальність.

Дослідивши поняття адміністративної відповідальності у сфері забезпечення кібербезпеки та адміністративного проступку у цій же сфері, на основі аналізу основних ознак адміністративної відповідальності та характеристики складів адміністративних правопорушень щодо правопорядку у кіберпросторі, виведено специфічні ознаки, що зумовлюються юридичною природою адміністративної відповідальності у сфері забезпечення кібербезпеки.

Розділ 3 «Правовідносини у сфері забезпечення кібербезпеки України та адміністративно-правовий статус суб'єктів» складається з трьох підрозділів.

У підрозділі 3.1. «Адміністративно-правові відносини у сфері забезпечення кібербезпеки України» здійснено аналіз адміністративно-правових відносин у сфері забезпечення кібербезпеки України та тлумачення означеного поняття з позиції адміністративно-правової науки. Акцентовано

увагу, що лише частина, управлінських відносин, яка того потребує, врегульовується адміністративно-правовими нормами.

Увагу зосереджено на аналізі структури адміністративно-правових відносин, що виникають у сфері забезпечення кібербезпеки, достатньо повно розкривають специфіку зазначеного явища, зумовлені низкою суттєвих ознак, які створюють можливість вирізнення правових зв'язків з усієї сукупності відносин, що складаються у процесі діяльності щодо забезпечення кібербезпеки України, а саме: суб'єкти адміністративно-правових відносин; об'єкти адміністративно-правових відносин; зміст адміністративно-правових відносин; юридичні факти як підстави для виникнення, зміни та припинення адміністративно-правових відносин у сфері забезпечення кібербезпеки.

Обґрунтовано поділ суб'єктів адміністративно-правових відносин у сфері забезпечення кібербезпеки України на три групи: суб'єкти загальної компетенції; суб'єкти спеціальної компетенції – основні суб'єкти національної системи кібербезпеки; суб'єкти, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки. Згідно чинного законодавства виділяється три групи об'єктів адміністративно-правових відносин у сфері забезпечення кібербезпеки України: загальнонаціональні суспільні та соціально-економічні інтереси; об'єкти кіберзахисту – інформаційні та телекомунікаційні системи; об'єкти критичної інфраструктури. Змістом адміністративно-правових відносин щодо забезпечення кібербезпеки є взаємозв'язок суб'єктивних прав та юридичних обов'язків учасників цих відносин.

На основі матеріалу дослідження щодо аналізу особливостей адміністративно-правових відносин у сфері забезпечення кібербезпеки України зазначається, що вони: поряд із загальними ознаками, мають цілий ряд специфічних рис, які визначають їх видову відмінність; виникають виключно на основі норм права та проявляють зв'язок між суб'єктами, який виникає через їх суб'єктивні юридичні права і обов'язки; цей зв'язок має індивідуальний, конкретно визначений характер і забезпечується та гарантується примусовою силою держави; мають особливості, що властиві їм як адміністративно-правовим відносинам, та підкреслюють їх специфіку і виділяють їх серед інших правовідносин. Крім того, виділено особливості адміністративно-правових відносин щодо забезпечення кібербезпеки.

Підрозділ 3.2. «Адміністративно-правовий статус суб'єктів забезпечення кібербезпеки України» присвячений проблемам визначення поняття та структури правового статусу суб'єктів забезпечення кібербезпеки та наданні оцінки суттєвим недолікам, що пов'язані з урегулюванням найважливіших питань щодо вирішення проблем вдосконалення організації діяльності суб'єктів даних правовідносин, корегування їх місця у

національній системі забезпечення кібербезпеки та підвищення результативності усієї системи у цілому.

Стверджується, що суб'єкти забезпечення кібербезпеки України, як суб'єкти адміністративно-правових відносин, включають органи державної влади та органи місцевого самоврядування, державні та недержавні підприємства, установи й організації, громадян та інших осіб, які наділені повноваженнями щодо здійснення діяльності із забезпечення стану захищеності життєво важливих інтересів особи, суспільства та держави у кіберсфері. При цьому, суб'єкти забезпечення кібербезпеки є складовою національної системи забезпечення кібербезпеки, сформовані сукупністю відповідних органів влади та громадських ініціатив, які згідно чинного законодавства діють з визначеною законом метою шляхом виконання певних завдань, реалізуючи конкретні функції.

Акцентовано на тому, що зміст адміністративно-правового статусу розкривається сукупністю обов'язкових елементів, серед яких – права і обов'язки. Поряд з цим, враховуючи розвиток наукової думки, варто адміністративно-правовий статус суб'єктів забезпечення кібербезпеки розкривати із врахуванням додаткових елементів: адміністративна правосуб'єктність; права; обов'язки; відповідальність, а також адміністративно-правові гарантії. Адміністративна правосуб'єктність суб'єктів забезпечення кібербезпеки розкривається через їх адміністративну правоздатність (виникає з моменту набрання чинності нормативно-правових актів, на підставі яких вони створюються, або з моменту державної реєстрації) та адміністративну дієздатність суб'єктів забезпечення кібербезпеки (здатність реалізовувати надані їм права і виконувати покладені на них обов'язки щодо забезпечення кібербезпеки).

Зазначено, що великий перелік, визначений чинним законодавством суб'єктів забезпечення кібербезпеки України, передбачає розмежування суб'єктів у різні групи, що характеризуються певними особливостями, які і обумовлюють специфіку їх правового статусу. Зосереджено увагу та доведено, що суб'єктів забезпечення кібербезпеки України, згідно з визначеними повноваженнями чинним вітчизняним законодавством та сформованим, таким чином, адміністративно-правовим статусом, доречно розділити у чотири групи: загального статусу; спеціального статусу; галузевого статусу; індивідуального статусу.

У підрозділі 3.3. «Міжвідомча та державно-приватна взаємодія у системі забезпечення кібербезпеки України» в логічній послідовності досліджено питання щодо взаємодії органів, служб та підрозділів у сфері забезпечення кібербезпеки, а також можливості впровадження та вдосконалення кібербезпеки шляхом використання механізмів державно-приватного партнерства як одного із головних інструментів ефективної

системи кіберзахисту країни. Автором досліджено основоположний документ у сфері забезпечення кібербезпеки – Закон України «Про основні засади забезпечення кібербезпеки України», у якому досить детально визначені напрями взаємодії суб'єктів забезпечення кібербезпеки України.

Вивчено зарубіжну практику партнерських відносин у кіберсфері, а саме досвід: США, для якої кіберзагрози є одним із найсерйозніших національних і економічних викликів, а питання кібербезпеки створюють все більше проблем щодо розвитку цифрової економіки країни; Німеччини, федеральний уряд якої у 2005 році розробив та запровадив План державно-приватного партнерства KPITIC («Umsetzungsplan KRITIS»).

З'ясовано та констатовано, що ефективна протидія загрозам національній безпеці у кіберсфері можлива лише за умови комплексного використання всього арсеналу правових засобів забезпечення кібербезпеки, за всіма структурними елементами державного управління та на всіх етапах обігу інформації. Крім того, максимального ефекту у взаємодії суб'єктів забезпечення кібербезпеки України можливо досягти виключно шляхом використання цілісного системного механізму адміністративно-правових методів та засобів, завдяки якому здійснюється реалізація державної політики у сфері забезпечення кібербезпеки як складового елементу національної безпеки України.

Визначено, що найбільш важливим кроком на етапі цілком сформованої законодавчої основи забезпечення кібербезпеки України доцільним є розроблення та якнайшвидше прийняття Державної цільової програми забезпечення кібербезпеки України, прийняття якої слугуватиме відправною точкою в реалізації реальної взаємодії суб'єктів забезпечення кібербезпеки України. Акцентовано увагу на основних напрямах державної політики з протидії кіберзагрозам, що повині стати відмінною особливістю Державної цільової програми забезпечення кібербезпеки України.

Розділ 4 «Напрями удосконалення адміністративно-правового забезпечення кібербезпеки України в умовах гібридної війни» об'єднує у собі три підрозділи.

У підрозділі 4.1. «Нові технології й загрози у сфері кібербезпеки та стратегічні цілі й складові її правового забезпечення» зосереджено увагу на вирішенні комплексних та багатоманітних проблем кібербезпеки, пов'язаних з інформаційними мережами та відкритими системами, а також акцентується на найбільш актуальних загрозах у кіберпросторі за сучасних умов життєдіяльності суспільства та на вирішенні нагальних проблемних питань щодо удосконалення пріоритетних напрямів інноваційної діяльності в Україні. Означено, що підвищення небезпеки та ризиків змушує приватних осіб, організації та цілі країни приймати заходи, вводити процедури та

набувати інструменти для покращання управління технологічними та комп'ютерними ризиками.

Акцентовано, що пристрої, які постійно перебувають в мережі Інтернет є мішенню для деструктивних дій у вигляді спрямованого втручання та атак, зокрема, у процес управління комунікаціями, що передбачають можливість ускладнення управління пристроєм або технічного збою передачі інформації, або ж підміну даних геолокації пристрою. Зокрема, має місце велика кількість інформації щодо захоплення управління пристроями іншими суб'єктами, тобто хакерські дії в мережах GSM, перехоплення в GPRS та втручання через Bluetooth, Wi-Fi або інфрачервоні порти.

Звертається увага на новітні загрози у сфері кібербезпеки, зокрема, на впровадження технології Інтернету речей, та пропонується врахування зарубіжного досвіду, звітів фахівців у цій сфері та відповідного прогнозування розвитку ситуації. За такої умови, вітчизняне законодавство повинно також характеризуватися певним чином новаціями правового регулювання, розробленими фахівцями, із врахуванням кращих зразків світової практики.

На основі вивчення досвіду розвинених країн з означеної проблематики та низки міжнародних документів щодо вирішення проблем довіри до Інтернету як до відкритого середовища акцентується: забезпечення кібербезпеки, у зв'язку з використанням технології Інтернету речей, в ЄС є менш регламентованим ніж у США, що і визначає відповідну державну правову політику; на відміну від ЄС у КНР досить значна увага приділяється заходам з вдосконалення державної політики у сфері регуляції питань застосування технології Інтернету речей, в першу чергу на технічному рівні.

Розглянувши низку прикладів щодо можливого виникнення проблем правового регулювання в умовах упровадження новітніх технологій, зокрема, Інтернету речей, визначено необхідність, при подальшому просуванні суспільства у напрямі розвитку технологічного прогресу, вирішення певної системи прикладних проблем саме засобами правового регулювання.

Визначено, що правове регулювання упровадження та використання новітніх технологій на основі розподіленої обробки даних (блокчейн) має враховувати її подвійну функцію: по-перше, зазначені новітні технології, з однієї сторони, є об'єктом кібератак у зв'язку із надзвичайним поширенням її технологічних продуктів, зокрема, Інтернет речей, криптовалют тощо, поряд з цим, з іншої сторони, зазначена технологія виводить на більш високий рівень захист інформації від незаконного втручання у кіберпросторі, а тому є також інструментом підвищення кібербезпеки. Указано, що різні країни по різному підходять до правового регулювання обігу криптовалют, зокрема вивчено досвід США щодо трактування правового статусу цифрових валют та охарактеризовано правове регулювання використання криптовалют у Європейському Союзі. Зроблено висновок, що у розвинених країнах світу достатньо поширеними є системи на

основі сучасних технологій розподіленого реєстру, хоча правове регулювання суттєво відстає від розвитку технологій. Кім того, розроблені нормативно-правові акти США та країнами ЄС не мають однозначності у правовому регулюванні блокчейну, так само як і немає єдиних міжнародних стандартів. У свою чергу, суди по-різному розуміють правовий статус віртуальних валют, вважаючи їх або товарами, або валютами, або цінними паперами. Крім того, враховуючи, що блокчейн ще проходить етап свого становлення і правове регулювання діяльності блокчейн-компаній у майбутньому обов'язково зміниться, основні акценти їх правової регламентації зосереджуються на дотриманні загальних стандартів у сфері протидії відмиванню коштів та захисту персональних даних.

Встановлено, що нормативно-правова база в Україні все ж таки формує офіційну позицію щодо факту існування криптовалюти як певного об'єкта права та фінансового інструмента, що регламентується в межах підзаконних нормативно-правових актів.

У підрозділі 4.2. «Сучасні світові тенденції розвитку адміністративно-правового та організаційного забезпечення кібербезпеки», використовуючи зарубіжний досвід (США, Велика Британія, Німеччина) зосереджено увагу на вивченні правового регулювання у сфері забезпечення кібербезпеки, що є складовою національної системи права та обумовлено традиціями нормотворчості окремої країни. З урахуванням специфіки та сукупності історичних чинників, політичного і економічного розвитку, фінансових і матеріальних ресурсів, що впливають в цілому на розбудову інформаційного суспільства та забезпечення кібербезпеки, особливу увагу приділено національним стратегіям, нормативно-правовим актам окремих зарубіжних країн, ініціативам і законодавству ЄС щодо активної позиції у сфері забезпечення кібербезпеки та протидії гібридизації кіберзагроз, а також, створеним провідною міжнародною організацією безпеки (НАТО), дієвим механізмам правового та організаційного забезпечення кібербезпеки.

Надано оцінку відповідним підрозділам спеціальних органів – суб'єктів кібербезпеки в системі кіберзахисту окремих зарубіжних країн (U.S. Cyber Command (США), Cyber Security Operations Centre (Велика Британія), Internet Crime Unit (Німеччина), Federal Office for Information Security, The Cyber security operations centre (Австралія) тощо), які створено з метою адміністративно-правового забезпечення кібербезпеки в країні.

Виходячи з аналізу досвіду зарубіжних країн констатовано, що адміністративно-правове забезпечення кібербезпеки в умовах гібридизації міжнародних відносин та з метою протидії дедалі зростаючого числа злочинів у кіберсфері є загальноприйнятою практикою в багатьох державах світу. Зокрема, обґрунтованим є висновок щодо реально сформованого міжнародного консенсусу розвинених країн світу на основі визнання його

об'єктивної необхідності в умовах стрімкого зростання кіберзагроз як на національному, так і міжнародному рівнях.

У підрозділі 4.3. «Стратегічні напрями за досвідом ЄС та НАТО у формуванні адміністративно-правового механізму протидії гібридним загрозам у сфері забезпечення кібербезпеки» акцентовано увагу на розумінні типів гібридних загроз, які можуть бути застосовані проти держави та протидії їм. Особливу увагу приділено питанням діяльності НАТО та Європейського Союзу, які вважають протидію гібридним загрозам пріоритетом для міжнародної співпраці. Проаналізовано низку документів ЄС, які формують чітку уяву щодо гібридності кіберзагроз та основних напрямів адміністративно-правового та організаційного забезпечення кібербезпеки, зокрема, щодо протидії гібридним кіберзагрозам в країнах Європейського Союзу.

Розкрито та обґрунтовано думку щодо проблем ризику, що базується на усвідомленні феномену ризику, що є сталим атрибутом людської життєдіяльності, з широким спектром прояву та масштабами, що пов'язані із соціально-історичним розвитком суспільства, і є певним чином віддзеркаленням його інтенсивності. Акцентовано увагу на тому, що для сучасного сприйняття важливим є розуміння того, що в інформаційному суспільстві за рахунок поширення інфогенних ризиків, посилюються характерні для індустріальної стадії суспільного розвитку соціальні ризики.

На основі аналізу зроблено висновок, що на сучасному етапі розвитку суспільства сформувалися підстави щодо утвердження стійкого сприйняття проблеми ризику як одного з утворюючих факторів сучасного і особливо майбутнього суспільства, що також набуває все більшого загальносоціального значення. Ризик має місце у діяльності суб'єктів управління в ситуації невизначеності, а тому є постійним атрибутом управлінської діяльності. При цьому, еволюційні перетворення, що мають місце з утвердженням інформаційного суспільства, потребують упровадження науково обґрунтованої системи заходів прогнозування суспільного розвитку у будь-якій сфері життєдіяльності.

Розвиваючи питання підвищення обізнаності щодо гібридних кіберзагроз, зроблено акценти на визначенні вразливості суспільства щодо них та скоординованої діяльності щодо оцінювання зазначених загроз. Для виявлення ключових вразливостей, враховуючи конкретні гібридні показники, необхідним є здійснення аналізу ризиків, що впливають на інститути та мережі.

Наголошується, що вітчизняна нормативна база має суттєві недоліки та потребує упровадження відповідних норм щодо запровадження ризик-орієнтованого підходу у діяльності щодо забезпечення кібербезпеки України, а також запропоновано визначення основних термінів («ризик-орієнтований

підхід щодо забезпечення кібербезпеки», «ризик-орієнтований підхід щодо захисту критичної інфраструктури», «ризики», «управління ризиками»).

Розкрито сутність та зміст терміну «стійкість», який набув практичного застосування у стратегічних документах у сфері безпеки та за своєю сутністю є новітнім концептом сучасної теорії національної безпеки, що має прикладне значення для формування політики держави в умовах безпекового середовища та важливе значення для практики забезпечення безпеки у кіберпросторі, тому що саме наявність гібридних загроз у кіберпросторі, яким неможливо запобігти, спричиняє потребу у формуванні нового підходу, зокрема, формування «стійкості», що в свою чергу має бути імплементованим в державну кібербезпекову політику.

На основі дослідження щодо *формування адміністративно-правового механізму протидії гібридним загрозам у сфері забезпечення кібербезпеки* вказано на правові прогалини, які потребують врегулювання та, перш за все, концептуального підходу та визначення на рівні національної Стратегії. За змістом Стратегія повинна включати питання забезпечення кібербезпеки України в умовах гібридної війни на основі мінімізації ризиків поширення агресором кіберзагроз на основі впровадження комплексу заходів з формування та реалізації державного управління у зазначеній сфері щодо визначення уразливості та забезпечення стійкості суспільства й держави. Запропоновано основні напрями та ключові заходи зазначеної Стратегії, а саме: підвищення обізнаності, забезпечення стійкості, запобігання, реагування на кризу та відновлення, нарощування співробітництва з ЄС та НАТО, а також іншими зарубіжними та міжнародними партнерськими організаціями.

ВИСНОВКИ

У дисертації здійснено теоретичне узагальнення і нове вирішення наукової проблеми щодо адміністративно-правових основ кібербезпеки України в умовах гібридної війни. У результаті проведеного дослідження сформовано низку висновків, пропозицій і рекомендацій, спрямованих на досягнення поставленої мети.

1. Обґрунтовується, що гібридна війна значно посилює вплив кіберзагроз на українське суспільство та на фоні глобальних тенденцій загрози у кіберпросторі актуалізує небезпеку від цілеспрямованих кібератак як інструменту агресії проти нашої держави. Зазначене, перш за все, потребує адекватного розуміння проблеми кіберзагроз в умовах гібридної війни, що виходить за межі традиційного сприйняття глобальних безпекових тенденцій та акцентує увагу на кіберзагрозах, що є цілеспрямованою агресією у кіберпросторі та порушує права і свободи громадян України, інтереси українського суспільства та держави Україна.

2. На основі підходів та напрямів щодо формування методологічних засад дослідження феномену кібербезпеки, а також враховуючи зв'язки з інформаційною безпекою, зазначено, що розгалуженість безпекознавчих наукових досліджень, міждисциплінарні зв'язки, актуальність та інтенсивність формують надзвичайно важливий аспект методологічного базису – комплексність, багатогранність та соціальну всеосяжність забезпечення кібербезпеки. Підкреслено, що розвиток інформаційного простору та інформаційно-телекомунікаційних технологій, їх вплив на реальність, різноманітність інформаційних явищ та процесів, є, перш за все, своєрідними й особливими за своєю природою, але все ж потребують універсального та комплексного підходу, оскільки взаємопов'язані з різноманітними сферами суспільних відносин.

Кіберсфера набуває загрозливих масштабів, що зумовлює необхідність охоплення її регуляторними та охоронними функціями права, а також підвищує увагу до кібербезпеки як до окремої складової національної безпеки України. Окрім того, формування механізму адміністративно-правового забезпечення кібербезпеки наражається на проблеми, обумовлені інноваційним характером кібербезпекової проблематики.

3. Сучасна адміністративно-правова парадигма забезпечення кібербезпеки формується із врахуванням того, що безпека у кіберпросторі стосується як громадян, так і суспільства у цілому, тому є стратегічною проблемою держави, що потребує на основі адміністративно-правового регулювання створення комплексної системи забезпечення кібербезпеки та інформаційного суверенітету, налагодження стратегічних комунікацій суб'єктів національної системи кібербезпеки, розбудови спроможностей протидії кіберзагрозам, формування відповідної інфраструктури вітчизняного інформаційного простору.

Крім того, очевидними є суттєві відмінності змістовного наповнення правових актів в Україні та міжнародних директивних документів щодо забезпечення кібербезпеки. За умов глобалізації кіберзагроз обґрунтованою є уніфікація підходів до правового регулювання у сфері забезпечення кібербезпеки та стандартизація заходів забезпечення задля ефективної співпраці та координації зусиль на національному та міжнародному рівнях.

4. Обґрунтовується, що механізм адміністративно-правового забезпечення кібербезпеки має велике значення в контексті формування ефективної системи протидії гібридним загрозам у кіберпросторі, так як дозволяє виокремити проблемні питання, що потребують вирішення та врегулювання. При цьому, об'єктом адміністративно-правових відносини суб'єктів національної системи кібербезпеки є спільна діяльність щодо виявлення, запобігання та усунення загроз кібербезпеці в Україні. А формами реалізації прав та обов'язків, які притаманні суб'єктам національної системи

кібербезпеки у процесі застосування адміністративно-правових засобів, є: додержання норм права, зокрема, отримання суб'єктами національної системи кібербезпеки даних та інформації в установленому законом порядку; використання норм права, зокрема, право суб'єктів національної системи кібербезпеки здійснювати спільні заходи щодо забезпечення кібербезпеки; право проводити спільні наукові дослідження; виконання норм права, зокрема, обов'язок суб'єктів національної системи кібербезпеки оприлюднювати достовірну інформацію про діяльність органів виконавчої влади у сфері забезпечення кібербезпеки.

Кіберзагрози в умовах гібридної війни, а також певним чином пов'язані із цим об'єктивні неузгодженості правового й організаційно характеру, вимагають впровадження якісних і кількісних змін у структурі адміністративно-правового забезпечення кібербезпеки України, зокрема, і в частині розвитку заходів адміністративного запобігання гібридним кіберзагрозам. Констатовано, що адміністративно-правові засоби забезпечення кібербезпеки реалізуються відповідним адміністративно-правовим механізмом забезпечення кібербезпеки, низкою адміністративно-правових норм і здійснюваними на їх основі спеціальними юридичними діями у цій сфері. У свою чергу, адміністративно-правові заходи забезпечення кібербезпеки є діяльною частиною нормативно визначених адміністративно-правових засобів.

5. Розкриваючи сутнісну характеристику терміну «адміністративно-правова охорона» зазначено, що адміністративно-правова охорона у сфері забезпечення кібербезпеки – це адміністративно-правове явище, зміст якого базується на впорядкованій нормами адміністративного права діяльності суб'єктів забезпечення кібербезпеки, що спрямована на забезпечення прав і свобод громадян, суспільства та держави у кіберпросторі, запобігання їх порушення, виявлення кіберзагроз та відновлення порушених прав, свобод та законних інтересів осіб, що здійснюються засобами адміністративного права з можливістю застосування заходів адміністративного примусу та притягнення винних до адміністративної відповідальності.

6. Враховуючи методологічні засади щодо безпекового змісту діяльності із забезпечення кібербезпеки, обґрунтованим вбачається під адміністративною відповідальністю у сфері забезпечення кібербезпеки України розуміти різновид юридичної відповідальності, що є засобом адміністративно-правової охорони відносин у кіберпросторі, є наслідком винного антисуспільного діяння у сфері забезпечення кібербезпеки, і головне призначення якого у примусовому припиненні протиправних дій, що стосуються незаконного втручання в комп'ютерні та телекомунікаційні системи й порушення при цьому прав та свобод людини, інтересів держави та суспільств.

7. Адміністративно-правові відносини у сфері забезпечення кібербезпеки – це суспільні відносини, що виникають з приводу діяльності об'єктів у кіберпросторі, які характеризуються стійкими правовими зв'язками між суб'єктами забезпечення кібербезпеки, що виникають у процесі реалізації ними суб'єктивних прав та обов'язків на підставі приписів адміністративно-правових норм, якими вони встановлені та гарантовані.

Суб'єкти адміністративно-правових відносин у сфері забезпечення кібербезпеки України поділяються на три групи: суб'єкти загальної компетенції; суб'єкти спеціальної компетенції – основні суб'єкти національної системи кібербезпеки; суб'єкти, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки. Згідно чинного законодавства виділяється три групи об'єктів адміністративно-правових відносин у сфері забезпечення кібербезпеки України: загальнонаціональні суспільні та соціально-економічні інтереси; об'єкти кіберзахисту – інформаційні та телекомунікаційні системи; об'єкти критичної інфраструктури.

8. Зосереджено увагу та доведено, що суб'єктів забезпечення кібербезпеки України, згідно з визначеними повноваженнями (правами та обов'язками) чинним вітчизняним законодавством та сформованим, таким чином, адміністративно-правовим статусом доречно розділити у чотири групи: *загальний статус* (Президент України, Кабінет Міністрів України, Рада національної безпеки та оборони України); *спеціальний статус (*Державна служба спеціального зв'язку та захисту інформації України, Національна поліція України, Служба безпеки України, розвідувальні органи України, а також контррозвідувальні органи та суб'єкти оперативно-розшукової діяльності); *галузевий статус* (Міністерство оборони України, Генеральний штаб Збройних Сил України, Національний банк України, міністерства та інші центральні органи виконавчої влади; місцеві державні адміністрації; органи місцевого самоврядування; підприємства, установи та організації, віднесені до об'єктів критичної інфраструктури; 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); *індивідуальний статус* (Державний центр кіберзахисту, урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA; Департамент кіберполіції НПУ; Ситуаційний центр забезпечення кібербезпеки СБУ; центр кіберзахисту Національного банку України).

При цьому, важливо розуміти надзвичайне значення реалізації адміністративно-правового статусу суб'єктами забезпечення кібербезпеки України саме в умовах гібридної війни. Враховуючи необхідність

забезпечення проактивного та запобіжного характеру адміністративно-правового регулювання у зазначеній сфері, обґрунтованим є запровадження активних форм та методів протидії кіберзагрозам, виділяючи при цьому важливість забезпечення адміністративно-правового статусу суб'єктів забезпечення кібербезпеки України спеціального та індивідуального статусу.

9. Реалізацію конкретних напрямів у правильному визначенні державно-приватного партнерства у сфері забезпечення кібербезпеки України доцільно здійснювати у формах: здійснення технічних експертиз, предметом яких виступають засоби телекомунікації та комп'ютерної техніки; сприяння фахівців у галузі забезпечення кібербезпеки щодо здійснення оперативно-розшукової діяльності; збір цифрових доказів; розробка та впровадження програмного забезпечення з метою виявлення та попередження кіберзагроз. Виходячи з проаналізованих законодавчих приписів, здійснення державно-приватної взаємодії у сфері кібербезпеки поки не має адекватного нормативно-правового фундаменту та має ряд дискусійних питань. При цьому, одним із найбільш важливих та перспективних напрямів даної сфери є освітній напрям – підготовка кваліфікованих кадрів на основі формування відповідних компетентностей.

10. Потребою сьогодення є врахування та вирішення низки проблем насамперед правового та безпекового характеру, а саме: правове регулювання щодо забезпечення кібербезпеки, насамперед, має базуватися на загальній безпеці суспільства, з ключовим акцентом на правових нормах, що превентивно забороняють деструктивні технології; запровадження та стимулювання перспективних досліджень у галузі правової науки, прогнозування щодо стану правового регулювання суспільних відносин, пошук можливих шляхів вивчення прогнозованих проблем, враховуючи неочевидність деструктивності і можливих помилок в оцінці сутності та наслідків нових технологій; відповідальність держави за функціонування систем на основі новітніх технологій із врахуванням того, що ніхто не може контролювати у цілому зазначені системи; стимулювання та економічна підтримка функціонування систем на основі новітніх технологій; обґрунтоване надання різноманітних преференцій розвитку інноваційної діяльності та відхід від декларативного характеру провадження державної політики у цьому напрямі; за умови упровадження новітніх технологій, характерною тенденцією кіберзагроз є їх постійна модифікація та інтенсифікація; захист інформації від втрати і спотворення та забезпечення довготривалого зберігання у відкритому для користування стані; необхідність значного оновлення законодавства і вирішення низки правових проблем.

11. Для України є надзвичайно актуальним впровадження міжнародного досвіду у сфері адміністративно-правового та організаційного забезпечення кібербезпеки, який є необхідним у якості успішного прикладу щодо формування відповідної політики і побудови власної системи правового та організаційного

забезпечення кібербезпеки, у першу чергу, в умовах гібридної війни. Успіх та ефективність адміністративно-правового забезпечення кібербезпеки забезпечується одночасними заходами, спрямованими як у напрямі співпраці з фаховими міжнародними інституціями щодо забезпечення кібербезпеки, так і у напрямі формування адекватного викликам гібридної війни національного законодавства у цій сфері.

12. Аналіз чинного законодавства України у сфері забезпечення кібербезпеки показав повне ігнорування питань щодо правового регламентування ризик-орієнтованого підходу у протидії гібридним загрозам, особливо у сфері кібербезпеки, визначення вразливості та розбудови стійкості українського суспільства.

Для України вивчення і використання позитивного зарубіжного досвіду щодо управління ризиками та забезпечення стійкості держави і суспільства у сфері національної безпеки обумовлене, перш за все, необхідністю формування нової якості вітчизняного сектору безпеки і оборони, який повинен мати риси, притаманні стійким системам.

У сучасних умовах забезпечення кібербезпеки України стійкість як суспільно-культурний феномен перетворюється на складний багатовимірний концепт, який в якості основоположного принципу визначає вирішальну роль самих об'єктів безпеки, які одночасно стають ключовими суб'єктами забезпечення кібербезпеки. При цьому, кібербезпека в умовах гібридної війни першочергово залежить не від характеру чи рівня кіберзагрози, а від здатності суб'єктів кібербезпеки їм протистояти, уразливості та спроможності національної системи забезпечення кібербезпеки в умовах щодо кібератак, кіберзлочинів тощо. Стійкість практично може бути досягнута на основі формування державно-приватного партнерства та необхідної культури у суб'єктів забезпечення кібербезпеки.

Стійкість у сфері забезпечення кібербезпеки в умовах гібридної війни формується, виходячи з розуміння кіберпростору як такого, що має принципові невизначеності щодо характеру та форм прояву гібридних кіберзагроз, часу їх прояву та поширення, а тому набуває змісту цільової установки на засадах нормативного впровадження ефективного механізму адміністративно-правового регулювання та за умови провадження у якості запобіжних заходів системи оцінювання ризиків прояву гібридних загроз та визначення уразливості суспільства.

13. Внести зміни та доповнення до:

проекту Закону України «Про критичну інфраструктуру та її захист»:

Стаття 1. Визначення основних термінів

1. У цьому Законі терміни вживаються в такому значенні:

20) ризик-орієнтований підхід – принцип захисту критичної інфраструктури, на основі оцінювання ризиків порушення безпеки критичної

інфраструктури, а також вжиття відповідних заходів щодо управління ризиками у спосіб та в обсязі, що забезпечують мінімізацію таких ризиків залежно від їх рівня;

21) ризики – рівень реальної загрози порушення безпеки критичної інфраструктури;

22) управління ризиками – комплекс заходів, що вживаються операторами критичної інфраструктури: виявлення та оцінювання загроз й вразливості критичної інфраструктури, оцінювання ризиків поширення загроз, - та прийняття на цій основі відповідних управлінських рішень щодо мінімізації ризиків порушення безпеки критичної інфраструктури;

Стаття 4. Засади державної політики захисту критичної інфраструктури

2. Державна політика у сфері захисту критичної інфраструктури ґрунтується на засадах:

9) застосування ризик-орієнтованого підходу.

Кодексу України про адміністративні правопорушення в частині підвищення санкції покарання за вчинення адміністративного правопорушення передбаченого ст. 212^6 «Здійснення незаконного доступу до інформації в інформаційних (автоматизованих) системах, незаконне виготовлення чи розповсюдження копій баз даних інформаційних (автоматизованих) систем».

14. На основі дослідження адміністративно-правового механізму протидії гібридним загрозам у сфері забезпечення кібербезпеки вказано на необхідність концептуального національного підходу щодо формування та упровадження відповідної Стратегії, з наступними ключовими напрямами її реалізації:

підвищення обізнаності шляхом формування методологічних засад ідентифікації й оцінювання гібридних загроз та створення спеціальних механізмів для обміну інформацією між суб'єктами забезпечення кібербезпеки;

забезпечення стійкості на основі стратегічних рішень у сфері забезпечення кібербезпеки та запровадження постійного моніторингу національної системи кібербезпеки з метою ідентифікації кіберзагроз, визначення вразливостей системи та оцінювання відповідних ризиків;

нарощування співробітництва з ЄС та НАТО, а також іншими зарубіжними та міжнародними партнерськими організаціями у спільних зусиллях щодо протидії гібридним загрозам у сфері забезпечення кібербезпеки при дотриманні принципів інклюзивності та автономності процесу прийняття рішень кожною організацією.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Праці, у яких опубліковано основні наукові результати дисертації:

1. Веселова Л.Ю. Кібернетична безпека в умовах гібридної війни: адміністративно-правові засади: монографія. Видавн. «Гельветика», 2020. 488 с.

2. Veselova L. The Relationship between Law and Order Legal Liability in the Cybernetic Field. *European Reforms Bulletin*. 2018. № 2. С. 53-56.

3. Веселова Л.Ю. Принципи права в методології адміністративно-правового забезпечення кібербезпеки. *Держава та регіони. Серія: Право*. 2018. Вип 2(23). Т. 3. С. 131-134.

4. Veselova L.Administrative-legal status subjects of administrative legal relation in the sphere of cyber security in Ukraine. *European Reforms Bulletin*. 2019. № 1. С. 40-44.

5. Веселова Л.Ю. Особливості державної політики України у сфері забезпечення кібернетичної безпеки в умовах гібридної війни. *Науковий вісник Херсонського державного університету. Серія «Юридичні науки»*. 2019. № 2. С. 23-27.

6. Veselova L. Administrative and legal protection in the field of cyber security. *European Reforms Bulletin*. 2019. № 2. С. 54-58.

7. Veselova L. Fatures of administrative-legal regulation in the field of cyber security support. *European Reforms Bulletin*. 2019. № 3. С. 49-52.

8. Veselova L. Legal assignment of cyber security terms. *European Reforms Bulletin*. 2019. № 4. С. 75-79.

9. Веселова Л.Ю. Методологічні засади пізнання кібернетичної безпеки. *Південноукраїнський правничий часопис*. 2019. № 4. Ч. 2. С. 162-165.

10. Веселова Л.Ю. Особливості взаємодії спеціальних органів, служб та підрозділів у сфері забезпечення кібернетичної безпеки. *Актуальні проблеми вітчизняної юриспруденції*. 2019. № 5. С. 51-55.

11. Веселова Л.Ю. Компетенція суб'єктів адміністративно-правового забезпечення національної безпеки України у кібернетичній сфері. *Право і суспільство*. 2019. № 5. Ч. 2. С. 14-20.

12. Веселова Л.Ю. Понятійно-термінологічний апарат у системі адміністративно-правового забезпечення кібербезпеки. *Науковий вісник публічного та приватного права*. 2019. № 5. С. 138-143.

13. Veselova L. The questionnaire for the formation and implementation of the administrative policy in the field of the cyber. *Visegrad Journal on Human Rights*. 2019. № 5(2). С. 45-49.

14. Веселова Л.Ю. Адміністративно-правові заходи у сфері забезпечення кібербезпеки. *Науковий вісник публічного та приватного права*. 2019. № 6. С. 148-152.

15. Веселова Л.Ю. Зміст та ролі інституційного механізму забезпечення кібернетичної безпеки України. *Науковий вісник Ужгородського національного університету. Серія «Право».* 2019. № 58. Т. 1. С. 204-207.

16. Веселова Л.Ю. Зміст адміністративно-правових заходів забезпечення безпеки в кібернетичній сфері. *Правничий часопис Донбасу.* 2020. № 1(70). С. 89-97.

17. Веселова Л.Ю. Становлення правового інституту кібернетичної безпеки в Україні. *Економічна теорія та право*. 2020. № 1(40). С. 113-126.

18. Веселова Л.Ю. Актуалізація інформаційної безпеки та глобальної кібернетичної загрози. Наука і правоохоронна. № 1. 2020. С. 175-181.

19. Veselova L. Administrative legal status of cybersecurity entities in Ukraine. *European Reforms Bulletin*. 2020. № 1. С. 70-74.

20. Веселова Л.Ю. Термінологічний консенсус у формуванні адміністративно-правової парадигми кібернетичної безпеки *Експерт: парадигми юридичних наук і державного управління*. 2020. № 2(8). С. 106-114.

21. Веселова Л.Ю. Кібернетичні загрози у контексті сучасного сприйняття їх в Україні. *Вісник Харківського національного університету імені В. Н. Каразіна. Серія «Право»*. 2020. Вип. 29. С. 169-175.

22. Веселова Л.Ю. Механізм адміністративно-правового забезпечення кібербезпеки. *Науковий вісник Міжнародного гуманітарного університету. Серія «Юриспруденція».* 2020. Вип. 43. С. 56-59.

23. Веселова Л.Ю. Терминологические подходы формирования понятийного аппарата в области кибербезопасности. *Юридические науки и образование.* 2020. № 62. С. 54-63.

24. Veselova L. Improving Ukraine's fdministrative-legal support for cyber security: EU and NATO experience in countering hybrid cyber threats. *Public Administration and Law Review*. 2020. № 3. С. 67-73.

Праці, які засвідчують апробацію матеріалів дисертації:

25. Веселова Л.Ю. Інститут юридичної відповідальності в сфері забезпечення кібернетичного правопорядку. *Актуальні завдання та напрями розвитку юридичної науки у XXI столітті*: матеріали міжнародної науково-практичної конференції, м. Львів, 18-19 жовтня 2019 р, Львів, 2019, С. 74-76.

26. Веселова Л.Ю. Адміністративно-правове забезпечення кібербезпеки як одне з пріоритетних завдань державної політики. *Проблеми правової реформи та розбудови громадянського суспільства в Україні*: матеріали міжнародної науково-практичної конференції, м. Харків, 18-19 жовтня 2019 р., Харків, 2019, С. 31-33.

27. Веселова Л.Ю. Ключові форми реалізації державно-приватного партнерства у сфері забезпечення кібербезпеки України. *Економіка, облік, фінанси та право: аналіз тенденцій та перспектив розвитку*: матеріали міжнародної науково-практичної конференції, м. Полтава, 24 жовтня 2019 р., Полтава, 2019, С. 55-56.

28. Веселова Л.Ю. Деякі прогалини в законодавстві щодо визначення та функцій основних суб'єктів забезпечення кібербезпеки України. *Актуальні проблеми розвитку науки в контексті глобальних трансформацій інформаційного суспільства*: матеріали міжнародної науково-практичної конференції, м. Київ, 25-26 жовтня 2019 р., Киїів, 2019, С. 112-114.

29. Веселова Л.Ю. Щодо адміністративно-правового статусу суб'єктів адміністративно-правових відносин у кіберсфері. *Актуальні питання розвитку державності та правової системи в сучасній Україні*: матеріали міжнародної науково-практичної конференції, м. Запоріжжя, 25-26 жовтня 2019 р., Запоріжжя, 2019, С. 54-57.

30. Веселова Л.Ю. Формування державної політики в сфері забезпечення кібернетичної безпеки. *Стан та перспективи розвитку адміністративного права України*: матеріали IV Міжнародної науково-практичної інтернет-конференції, м. Одеса, 23 жовтня 2019 р., Одеса, 2019, С. 30-32.

31. Веселова Л.Ю. Щодо проблеми понятійного апарату у сфері забезпечення кібернетичної безпеки. *Науковий потенціал та перспективи розвитку юридичної науки*: матеріали міжнародної науково-практичної конференції, м. Запоріжжя, 27-28 березня 2020 р., Запоріжжя, 2020, С. 52-55.

32. Веселова Л.Ю. Вплив адміністративно-правових норм чинного законодавства на суспільні відносини щодо забезпечення кібербезпеки. *Актуальні проблеми прав людини, держави та вітчизняної правової системи*: матеріали міжнародної науково-практичної конференції, м. Дніпро, 3-4 квітня 2020 р., Дніпро, 2020, С. 52-54.

33. Веселова Л.Ю. Поняття та елементи механізму адміністративно-правового забезпечення кібербезпеки. *Громадське суспільство в Україні: проблеми забезпечення правотворчої діяльності*: матеріали міжнародної науково-практичної конференції, м. Харків, 3-4 квітня 2020 р., Харків, 2020, С. 67-70.

34. Веселова Л.Ю. Щодо поняття адміністративно-правової охорони в сфері забезпечення кібернетичної безпеки. *Протидія організованій злочинній діяльності:* матеріали IV всеукраїнської науково-практичної інтернет-конференції, м. Одеса, 14 травня 2020 р., Одеса, 2020, С. 22-24.

АНОТАЦІЯ

Веселова Л. Ю. Адміністративно-правові основи кібербезпеки в умовах гібридної війни. – *Кваліфікаційна наукова праця на правах рукопису*.

Дисертація на здобуття наукового ступеня доктора юридичних наук за спеціальністю 12.00.07 «Адміністративне право і процес; фінансове право; інформаційне право». – Одеський державний університет внутрішніх справ, Одеса, 2021.

У межах об'єкта та предмета дослідження розкрито широке коло проблемних питань від методологічних засад пізнання феномену «кібербезпеки» до сучасної парадигми адміністративно-правового забезпечення кібербезпеки в умовах гібридної війни. Обґрунтовується сучасне розуміння розвитку суспільних відносин у кіберпросторі, їх дуалістичний зміст для України. Розкрито історичні аспекти формування та проаналізовано сучасний стан нормативно-правового забезпечення у зазначеній сфері. Акцентовано на суттєвих правових колізіях та прогалинах

вітчизняного законодавства у сфері кібербезпеки і особливо в умовах гібридної війни. Підкреслено на необхідності формування понятійно-термінологічного апарату адміністративно-правового забезпечення кібербезпеки.

Змістовно розкрито юридико-функціональні аспекти формування національної системи кібербезпеки: ключові аспекти механізму застосування адміністративно-правових заходів забезпечення кібербезпеки; зміст адміністративно-правової охорони, її форми й методи у сфері забезпечення кібербезпеки; сутнісні характеристики адміністративної відповідальності у сфері забезпечення кібербезпеки; зміст та особливості адміністративно-правових відносин у сфері забезпечення кібербезпеки України; адміністративно-правовий статус суб'єктів забезпечення кібербезпеки України з виділенням проблемних питань; загальну тенденцію та особливості міжвідомчої та державно-приватної взаємодії у системі забезпечення кібербезпеки України.

Обґрунтовано методологічне значення формування механізму адміністративно-правового регулювання у зазначеній сфері на основі правового врегулювання зобов'язань суб'єктів національної системи кібербезпеки щодо визначення ризиків кібербезпеки та упровадження ризик-орієнтованої стратегії кібербезпеки. Узагальнено міжнародний досвід стратегічного характеру щодо формування безпекового середовища та стійкості суспільства в умовах гібридизації міжнародних відносин та сформульовано пропозиції удосконалення адміністративно-правового забезпечення кібербезпеки в Україні.

Ключові слова: *адміністративно-правові основи, кібербезпека, гібридна війна, гібридні загрози, кіберзагрози, адміністративно-правовий механізм, суб'єкти забезпечення кібербезпеки, ризик-орієнтований підхід, стійкість суспільства, вразливість.*

АННОТАЦИЯ

Веселова Л. Ю. Административно-правовые основы кибербезопасности в условиях гибридной войны. – *Квалификационный научный труд на правах рукописи.*

Диссертация на соискание учёной степени доктора юридических наук по специальности 12.00.07 «Административное право и процесс; финансовое право, информационное право». – Одесский государственный университет внутренних дел, Одесса, 2021.

В рамках объекта и предмета исследования раскрыто широкий круг проблемных вопросов от методологических основ познания феномена «кибербезопасности» до современной парадигмы административно-правового обеспечения кибербезопасности в условиях гибридной войны. Обосновывается современное понимание развития общественных отношений

в киберпространстве, их дуалистический смысл для Украины. Раскрыто исторические аспекты формирования и проанализировано современное состояние нормативно-правового обеспечения в указанной сфере. Акцентировано на существенных правовых коллизиях и пробелах отечественного законодательства в сфере кибербезопасности и особенно в условиях гибридной войны. Подчеркнуто необходимость формирования понятийно-терминологического аппарата административно-правового обеспечения кибербезопасности.

Содержательно раскрыто юридико-функциональные аспекты формирования национальной системы кибербезопасности: ключевые аспекты механизма применения административно-правовых мер обеспечения кибербезопасности; содержание административно-правовой охраны, ее формы и методы в области обеспечения кибербезопасности; сущностные характеристики административной ответственности в сфере обеспечения кибербезопасности; содержание и особенности административно-правовых отношений в сфере обеспечения кибербезопасности Украины; административно-правовой статус субъектов обеспечения кибербезопасности Украины с выделением проблемных вопросов; общую тенденцию и особенности межведомственного и государственно-частного взаимодействия в системе обеспечения кибербезопасности Украины.

Обоснованно методологическое значение формирования механизма административно-правового регулирования в указанной сфере на основе правового регулирования обязательств субъектов национальной системы кибербезопасности по определению рисков кибербезопасности и внедрения риск-ориентированной стратегии кибербезопасности. Обобщен международный опыт стратегического характера по формированию среды безопасности и устойчивости общества в условиях гибридизации международных отношений и сформулированы предложения совершенствования административно-правового обеспечения кибербезопасности в Украине.

Ключевые слова: *административно-правовые основы, кибербезопасность, гибридная война, гибридные угрозы, киберугрозы, административно-правовой механизм, субъекты обеспечения кибербезопасности, риск-ориентированный подход, стойкость общества, уязвимость.*

SUMMARY

Veselova L. Yu. Administrative-legal bases of cyber security in the context of hybrid war. – *Qualifying scientific work on the rights of a manuscript.*

The thesis for a degree of Doctor of Juridical Sciences in the specialty 12.00.07 «Administrative Law and Process; Financial Law; Informational Law». – Odesa State University of Internal Affairs, Odesa, 2021.

Within the object and subject of the research a wide range of problematic issues is revealed, from the methodological bases of knowledge of "cybersecurity" phenomenon to the actual paradigm of administrative-legal support of cybersecurity in the hybrid war's context. The nowadays understanding of the development of social relations in cyberspace, their dualistic content for Ukraine is substantiated. The historical aspects of the formation are revealed and the current state of regulatory-legal support in this area is analyzed. Emphasis is placed on significant legal conflicts and gaps in domestic legislation in the field of cybersecurity and especially in hybrid war. Emphasis is placed on the need to form a conceptual and terminological apparatus of administrative-legal support of cybersecurity.

The legal-functional aspects of the national cybersecurity system formation are substantially revealed: key aspects of application mechanism of administrative-legal measures to ensure cybersecurity; the content administrative-legal protection, its forms and methods in the field of cybersecurity; essential characteristics of administrative responsibility in the field of cybersecurity; content and features of administrative-legal relations in the field of cyber security of Ukraine; administrative-legal status of the subjects of cyber security of Ukraine with the allocation of problematic issues; general tendency and features of interdepartmental and public-private cooperation in the cyber security system of Ukraine.

The methodological significance of the mechanism's formation of administrative-legal regulation in this area based on legal settlement of obligations of the national cybersecurity system to identify cybersecurity risks and implement a risk-oriented cybersecurity strategy is substantiated. The international experience of strategic character concerning formation of the security environment and stability of society in the context of hybridization of international relations is generalized and offers of perfection of administrative-legal maintenance of cybersecurity in Ukraine are formulated.

***Keywords**: administrative-legal bases, cybersecurity, hybrid war, hybrid threats, cyber threats, administrative-legal mechanism, subjects of cybersecurity, risk-oriented approach, social stability, vulnerability.*

Підписано до друку 19.02.2021. Формат 60х90/16. Папір офсетний.
Гарн. «Times New Roman». Друк різографічний. Ум. друк. арк. 1,9.
Наклад 100 прим.
Видавництво ОДУВС
м. Одеса, вул. Успенська, 1
Свідоцтво суб'єкта видавничої справи ДК № 3507 від 25.06.2009 р.
тел. 0487431393; 0949464393 email – 7431393@gmail.com