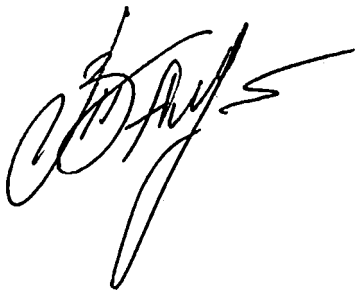
ДЕРЖАВНА НАУКОВА УСТАНОВА
«ІНСТИТУТ ІНФОРМАЦІЇ, БЕЗПЕКИ І ПРАВА НАЦІОНАЛЬНОЇ АКАДЕМІЇ ПРАВОВИХ НАУК УКРАЇНИ»

ТАРАСЮК Анатолій Васильович



УДК 336.7:340.5:347.7

ТЕОРЕТИКО-ПРАВОВІ ОСНОВИ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ УКРАЇНИ

12.00.07 – адміністративне право і процес; фінансове право;
інформаційне право (081 – Право)

АВТОРЕФЕРАТ
дисертації на здобуття наукового ступеня
доктора юридичних наук

Київ – 2021

Дисертацією є рукопис.

Робота виконана в Державній науковій установі «Інститут інформації, безпеки і права Національної академії правових наук України».

Науковий консультант – заслужений діяч науки і техніки України, доктор юридичних наук, професор **ДОВГАНЬ Олександр Дмитрович**, Державна наукова установа «Інститут інформації, безпеки і права НАПрН України», радник при дирекції.

Офіційні опоненти:

доктор юридичних наук, професор **ЛЮТІКОВ Павло Сергійович**, Університет митної справи та фінансів, завідувач кафедри адміністративного та митного права

доктор юридичних наук, доцент **ЗАЯРНИЙ Олег Анатолійович**, Інститут права Київського національного університету імені Тараса Шевченка, професор кафедри інтелектуальної власності та інформаційного права;

доктор юридичних наук, доцент **ТКАЧУК Тарас Юрійович**, Навчально-науковий інститут інформаційної безпеки Національної академії Служби безпеки України, заступник завідувача кафедри.

Захист відбудеться «8» липня 2021 р. о 11^{00} годині на засіданні спеціалізованої вченої ради Д 26.501.01 в Державній науковій установі «Інститут інформації, безпеки і права Національної академії правових наук України» за адресою: 03039, м. Київ, вул. Фрометівська, 2.

З дисертацією можна ознайомитись у бібліотеці Державної наукової установи «Інститут інформації, безпеки і права Національної академії правових наук України» за адресою: 01032, м. Київ, вул. Саксаганського, 110-В.

Автореферат розіслано «7» червня 2021 р.

Вчений секретар спеціалізованої вченої ради **М. В. Беланюк**

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми дослідження. Сучасний етап розвитку світового співтовариства нерозривно пов’язаний з упровадженням цифрових технологій. Відповідно створюються умови для виникнення нових правовідносин.

Водночас сучасний етап стратегічної конкуренції і нові загрози вимагають удосконалення стратегії забезпечення кібербезпеки України, що має відповідати новим викликам, забезпечувати можливості процвітання Українського народу і бути фактором стримування для супротивників. Варто зауважити, що протягом 2020 року Службою безпеки України нейтралізовано понад 600 кіберінцидентів і кібератак на інформаційні ресурси органів влади й об’єкти критичної інфраструктури. Окрім цього, триває активна протидія кіберзагрозам з боку Росії. Відповідно, основоположне значення для втілення в життя нашої стратегії має забезпечення безпеки національного кіберпростору, що вимагає впровадження новітніх досягнень технічного прогресу, а також адміністративної ефективності держави і приватного сектора. Одного тільки технократичного підходу щодо кіберпростору недостатньо для розв’язання проблем, що виникають. Мають бути розроблені широкі інструменти ефективних заходів примусу, що дозволять запобігти можливій ескалації і забезпечать стримування структур, які здійснюють недружні дії. А з іншого боку, на постійній основі повинна тривати просвітницька робота. Метою якої має бути розвиток інформаційної культури людини, критичного мислення серед населення, екологія інформації та інформаційна гігієна.

Перспективним напрямом у вивченні проблем кібербезпеки України вважаємо якісно новий підхід, який би розглядав кібернетичну безпеку не тільки в конкретно прикладних аспектах, а і як внутрішній стан усієї соціальної системи. Діюча система кібербезпеки України має гарантувати рівноправну участь усіх суб’єктів інформаційної взаємодії в системі глобальної безпеки й забезпечити захист їхніх основних прав і свобод. У зв'язку із застосуванням сучасних інформаційних технологій потрібна зміна підходу до правового регулювання суспільних відносин у процесі забезпечення кібербезпеки. Зважаючи на це, важливість досліджень теоретико-правових основ забезпечення кібербезпеки України лише зростає. Цим обумовлюється й авторська мотивація вибору зазначеного напряму наукового дослідження.

Актуальність теми дослідження визначається, насамперед, новизною самої проблеми кібербезпеки, особливо її правової, соціально-філософської та методологічної складових, акцентованих на забезпеченні безпеки людини, суспільства, держави, дослідженні її ціннісних уподобань. Ці питання особливо актуалізуються у наш час, коли слід активно протидіяти симбіозу бойових дій у кіберпросторі та інформаційним операціям, механізми якої активно застосовуються Росією у ході гібридної війни проти України. Зазначена проблематика певною мірою вже розроблялася вченими у

правничій науці, де кожен із дослідників зробив свій внесок у загальну стратегію забезпечення кібербезпеки нашої країни. Це обумовлено значними трансформаціями, що відбуваються в сучасному світі в умовах розвитку інформаційно-комунікаційних технологій. При цьому держава і право в даних умовах не статичні, вони досить динамічні, постійно розвиваються і удосконалюються разом з розвитком суспільства. З плином часу з'являються нові суспільні відносини, які потребують правового врегулювання та наукового осмислення, особливо у контексті розвитку технологій штучного інтелекту. Зокрема це питання розробки асиметричних механізмів протидії розвідувально підривній діяльності у кіберпросторі та кібертероризму, протидії кіберзлочинності, посилення кіберзахисту критичної інфраструктури, забезпечення безпеки цифрових послуг, державно-приватного партнерства особливо в частині взаємодії учасників системи кібербезпеки, обміну інформацією про кіберзагрози на міжнародному та національному рівнях, необхідність впровадження системи тренінгів та професійного навчання, підвищення рівня кіберкультури тощо.

Теоретичною базою дослідження стали пов’язані з проблематикою обраного наукового напряму праці в таких галузях і таких учених:

– *філософії:* А. Бергсон, Г. Гроцій, Р. Ієрінг, Н. Макіавеллі, Р. Оуен, Плутарх, Платон, Б. Рассел, Сенека, Сунь-цзи, А. Сен-Сімон;

– *інформаційного права*: І. Арістова, О. Баранов, К. Бєляков, В. Брижко, І. Бондар, С. Бондаренко, О. Довгань, С. Домбровська, О. Заярний, М. Згуровський, О. Золотар, І. Корж, Р. Калюжний, Б. Кормич, О. Костенко, В. Клочко, О. Логінов, А. Марущак, Є. Мануйлов, О. Морозов, А. Нашинець-Наумова, В. Остроухов, І. Панова, В. Пилипчук, В. Петрик, В. Політанський, М. Присяжнюк, Ю. Размєтаєва, В. Рубан, Ю. Руденко, Г. Сащук, Я. Собків, О. Тихомиров, Т. Ткачук, В. Фурашев, С. Феденько, Л. Харченко, О. Хілько, В. Шамрай, Р. Шаповал, В. Шатун, О. Ярема та ін.

– *інших галузей права*: вітчизняні вчені – В. Білоус, В. Горбулін, В. Григор’єв, В. Гулай, О. Дзьобань, Т. Карабін, А. Качинський, Я. Лазур, А. Легеза, Ю. Лісовська, І. Лях, Я. Малик, Й. Мастяниця, С. Мельник, Н. Нижник, Д. Прокоф’єва-Янчиленко, Г. Ситник, М. Савчин, О. Соснін, Л. Шиманський; зарубіжні вчені: С. Алексєєв, Дж. Барбер, Н. Вінер, В. Герхард, К. Геерс, Дж. Данн, К. Демпсі, Л. Козер, П. Корніш, А. Кемпф, Р. Оуен, В. Піллітері, Б. Рассел, А. Робертс, Ф. Сталдер, М. Лібіскі, О. Лукашов, А. Левін, Х. Міллінгтон, М. Нільес, К. Шенон, К. Шилде, Р. Ярґер та ін.

На основі аналізу джерельної бази виявлено теоретичні та практичні проблеми – від браку достатніх теоретичних основ до відсутності системності й недостатньої ефективності відповідних практик забезпечення кібербезпеки України, необхідності правового врегулювання нових суспільних відносин, які виникають у досліджуваній сфері та адаптації національного законодавства до законодавства ЄС та НАТО.

Зв’язок роботи з науковими програмами, планами, темами. Дисертацію виконано відповідно до Пріоритетних напрямів розвитку

правової науки на 2016–2020 рр., затверджених постановою загальних зборів Національної академії правових наук України від 03.03.2016 р., Плану законодавчого забезпечення реформ в Україні, схваленого Постановою Верховної Ради України від 04.06.15 № 509-VIII, а також у межах планової науково-дослідної роботи Науково-дослідного інституту інформатики і права Національної академії правових наук України «Теоретичні та організаційно-правові основи забезпечення кібербезпеки в Україні» (номер державної реєстрації 0116U007745).

Результати дослідження було розглянуто й обговорено в ході науково-практичного семінару в Науково-дослідному інституті інформатики і права НАПрН України, протокол № 2 від 25 лютого 2021 р.

Мета і завдання дослідження. *Мета* – сформувати теоретичну модель стратегії забезпечення кібернетичної безпеки України, запропонувати на цій основі теоретико-правові засади механізму забезпечення кібернетичної безпеки людини, суспільства, держави в сучасних умовах.

Окреслена дослідницька мета асоційована з розв'язанням вагомої *наукової проблеми* **–** формування теоретичної моделі стратегії забезпечення кібернетичної безпеки України та розробки теоретико-правових засад механізму забезпечення кібернетичної безпеки людини, суспільства, держави в сучасних умовах.

Досягнення поставленої мети передбачає розв'язання таких наукових *завдань*:

– дослідити генезис наукових поглядів забезпечення кібербезпеки України;

– на основі понятійно-категоріального синтезу з'ясувати змістовну сутність основних понять у національному законодавстві;

– з'ясувати особливості співвідношення кібербезпеки та інформаційної безпеки на сучасному етапі;

– дослідити методологічні засади правового забезпечення кібербезпеки України;

– дослідити стан правового регулювання кібербезпеки в Україні;

– охарактеризувати систему суб'єктів забезпечення кібербезпеки в Україні та дослідити практику правового регулювання їхньої діяльності;

– вивчити питання протидії кіберзагрозам на національному та глобальному рівнях, дослідити відповідний досвід законодавчого забезпечення зарубіжних країнах;

– на основі теоретико-правового аналізу дослідити загрози кібербезпеці людини під час використання кіберпростору та запропонувати правові механізми протидії їм;

– на основі порівняльно-правового дослідження дослідити особливості забезпечення кібербезпеки людини на міжнародному рівні;

– узагальнити теоретичні підходи до аналізу концепцій інформаційного суспільства;

– дати оцінку правовому чиннику у запобіганні кіберзагрозам сучасному українському суспільству;

– визначити теоретико-правове підґрунтя системи соціального регулювання в інформаційному суспільстві;

– виокремити концептуальні засади правового регулювання кібербезпеки України на сучасному етапі розвитку глобальних інформаційних процесів;

– запропонувати й обґрунтувати конкретні пріоритети розвитку правових основ державної політики України у сфері кібербезпеки;

– розробити напрями правового регулювання окремих елементів інформаційної інфраструктури на національному та міжнародному рівнях забезпечення кібербезпеки.

Об'єктом дослідження є суспільні відносини у процесі забезпечення кібернетичної безпеки України.

Предмет дослідження – теоретико-правові основи забезпечення кібербезпеки України.

Методи дослідження. Як методологічна основа дослідження використані філософські (діалектичний), загальнотеоретичні, (гносеологічний, структурно-функціональний), спеціальні (порівняльно-правовий, індуктивний) та міжгалузеві методи наукового пізнання (історичний, аналітичний), застосування яких зумовлюється системним підходом.

За допомогою *філософських методів*, що стали онтологічною основою наукової праці, зокрема *діалектики*, досліджено кібернетичну безпеку України як важливу складову інформаційної в широкому розумінні та національної безпеки України, з'ясовано взаємозв'язки основних складових кібернетичної безпеки України, обґрунтовано взаємозалежність стану інформаційного законодавства та правового забезпечення кібербезпеки України (підрозд. 1.1–1.4). *Історичний метод* дав змогу дослідити генезис теорій і концепції забезпечення кібернетичної безпеки України (підрозд. 1.1). Використання *аналітичного методу* сприяло класифікації загроз кібернетичній безпеці України, розробці механізмів протидії їм (підрозд. 2.4, 2.5, 3.2, 4.2, 5.4), а також аналізу функціонування суб'єктів забезпечення кібернетичної безпеки України (підрозд. 2.3). *Порівняльно-правовий метод* покладено в основу дослідження міжнародного досвіду забезпечення кібернетичної безпеки (підрозд. 2.5, 4.3.1, 5.2). *Формально-юридичний метод* застосовувався при тлумаченні норм права для з'ясування їхньої суті, змісту та вираженої в них волі законодавця (підрозд. 2.1, 3.1). *Структурно-функціональний аналіз* дав можливість визначити відповідність нормативно-правових актів, з якими асоційована сучасна система правового забезпечення кібернетичної безпеки України реальним суспільним відносинам у цій сфері та міжнародним стандартам (підрозд. 5.2, 5.3). Використання *індуктивного методу*, *методів правового моделювання та прогнозування* дало змогу підтвердити висновок про необхідність удосконалення правового забезпечення кібернетичної безпеки України (підрозд. 5.3, 5.4).

Наукова новизна одержаних результатів. Дисертаційна робота є одним з перших у вітчизняній правничій науці комплексним дослідженням

теоретико-правових основ забезпечення кібернетичної безпеки людини, суспільства, держави. Основними науковими добутками нашої праці стали:

вперше:

– *розроблено* структуру та зміст Концепції кібернетичної безпеки людини. Визначено її головні правові принципи формування, завдання, механізми реалізації й очікувані результати державної політики у сфері правового регулювання кібернетичної безпеки людини;

– *обґрунтовано* існування комплексного міжгалузевого інституту інформаційного законодавства, яким є інститут забезпечення кібербезпеки. *Охарактеризовано* такі його властивості: 1) сформований і розвивається на базі матеріальних та процесуальних норм інформаційного, конституційного, цивільного, адміністративного, кримінального, процесуального, фінансового й інших галузей законодавства; 2) як самостійний інститут формується на основі нечисленної сукупності юридичних норм, що регулюють специфічне коло суспільних відносин стосовно забезпечення безпекових інтересів людини, суспільства, держави в інформаційній сфері; 3) як складова підгалузі правового регулювання інформаційної безпеки в системі інформаційного законодавства взаємопов'язаний з іншими інститутами цієї підгалузі – охороною комерційної та державної таємниці, захисту персональних даних і низка інших; 4) в основі змісту лежать норми зазначених вище галузей права, що об'єднані спрямованістю на забезпечення безпекових інтересів людини, суспільства, держави в кіберпросторі;

– *розроблено* концептуальні засади правового регулювання кібербезпеки України на сучасному етапі розвитку глобальних інформаційних процесів;

– *запропоновано* логічну схему співвідношення кібернетичної та інформаційної безпеки. Обґрунтовано, що кібербезпека формується в реляційних відносинах з безпекою мереж, безпекою інтернету і безпекою додатків, а також здійснює підтримку безпеки критичної інформаційної інфраструктури в частині, що її стосується;

– *виокремлено* та *систематизовано* складові національних інтересів України в кіберпросторі: 1) дотримання конституційних прав і свобод людини та громадянина у сфері отримання інформації та користування нею, сприяння духовному оновлення держави, збереження та зміцнення моральних цінностей суспільства, традицій гуманізму і патріотизму, наукового і культурного потенціалу країни; 2) інформаційне забезпечення державної політики, що пов'язане з доведенням до міжнародної громадськості правдивої інформації про державну національну політику, офіційну позицію держави щодо соціально-значимих подій держави та міжнародного життя, із наданням громадянам доступу до відкритих національних інформаційних ресурсів; 3) застосування новітніх інформаційних технологій, створення вітчизняної індустрії інформації, зокрема й індустрії засобів інформатизації, телекомунікації та зв'язку, задоволення потреб внутрішнього ринку її продукцією, а також забезпечення накопичення, ефективного використання та збереження національних

інформаційних ресурсів; 4) захист інформаційних ресурсів від несанкціонованого доступу, забезпечення безпеки телекомунікаційних й інформаційних систем, як створюваних, так і тих, що функціонують на території України;

– *розроблено* нові механізми співпраці між приватним сектором та державними органами у процесі забезпечення кібербезпеки України. Виокремлено такі пріоритетні напрями: розвиток кіберрозвідки, аудит кібербезпеки, взаємний обмін інформацією щодо кіберзагроз, заміна нормативних документів в галузі технічного захисту інформації на ефективніший та сучасніший базовий стандарт і запровадження галузевих стандартів кібернетичної безпеки, створення галузевих центрів з реагування на кібернетичні інциденти (Security Operations Center (SOC)) та центрів інформаційного обміну про кібернетичні атаки (Information Systems Audit and Control Association (ISACA)), створення на базі національних навчальних закладів тренінгових центрів для налагодження ефективного діалогу у рамках державно-приватного партнерства з протидії кіберзагрозам.

удосконалено:

– базові поняття дослідження: «кібернетична безпека України», «забезпечення кібернетичної безпеки України», «кібератака», «кіберпростір», «кіберзлочин», «стан захищеності», «кіберзагроза», «інформаційна інфраструктура України», «критична інформаційна інфраструктура» що дозволить упорядкувати понятійно-категоріальний апарат інформаційного права;

– тлумачення терміна «*культура кібербезпеки*», під яким розуміється система переконань, уявлень та етичних норм щодо ведення інформаційної діяльності в кіберпросторі, знань, умінь і навичок із забезпечення кібербезпеки, а також вимоги до професійно-психологічних якостей осіб, що необхідні для безпечної інформаційної діяльності у кіберпросторі;

– підхід до системно-функціонального аналізу суб'єктів забезпечення кібернетичної безпеки України, у частині розвитку державно-приватного партнерства, розширення функціональних повноважень Національного координаційного центру кібербезпеки, удосконалення функціональних завдань Служби безпеки України;

– критерії класифікації кіберзагроз державі, зокрема: загрози існуванню нації, за деструктивним впливом на основні сегменти національного кіберпростору, за посяганням на національні цінності кібербезпеки (життєво важливі інтереси людини і громадянина, суспільства та держави);

– теоретичний підхід у рамках якого кіберпростір може розглядатися одночасно як об'єкт правового захисту і як джерело загроз. На цій основі у пріоритеті рівнів кібербезпеки (безпека людини, суспільства й держави, в основу якого покладені конституційні принципи захисту життєво важливих інтересів зазначених суб'єктів) стосовно кібербезпеки запропоновано надати пріоритет інтересам держави, оскільки від цього безпосередньо залежатиме й реалізація інтересів особи й суспільства.

Забезпечення кібербезпеки держави є передумовою особистісної та громадської кібернетичної безпеки

– критерії класифікації загроз кібербезпеці людини, у частині їх впливу на національну свідомість; за посяганням на національні цінності; за природою виникнення;

– роль правового чинника, як єдиного регулятора процесів та відносин у сфері роботи глобальної мережі Інтернет, розвитку Інтернету-речей (IoT), інтелектуалізації робототехніки, використання можливостей кіберсистем, мікрочіпів, нанотехнологій, їх упровадження в інформаційні процеси управління, взаємодії людини і влади, у повсякденній життєдіяльності «цифрової людини»;

– систему забезпечення кібербезпеки людини, суспільства, держави в контексті доповнення до її структури соціальної та морально-етичної складових;

– пріоритетні напрями розвитку правових основ державної політики у процесі забезпечення кібернетичної безпеки з урахуванням досвіду європейських країн і сучасної обстановки в нашій державі.

дістали подальшого розвитку:

– теоретичні засади утвердження інформаційного права як самостійної галузі права та розширення меж його правового впливу, у частині удосконалення законодавства про забезпечення кібернетичної безпеки України;

– теоретичні положення щодо розвитку інформаційно-правових досліджень правового регулювання кібернетичної безпеки України;

– теоретичні підходи до змісту, динаміки розвитку сучасних загроз кібернетичній безпеці України та механізмів протидії їм;

– узагальнення зарубіжного досвіду забезпечення кібернетичної безпеки, що створює правову базу побудови системи кібернетичної безпеки в Україні, здійснення гармонізації національного законодавства з міжнародними стандартами та європейським законодавством.

Практичне значення одержаних результатів. Висновки і пропозиції були впроваджені та можуть бути використані:

– *у правотворчій діяльності* – при підготовці змін і доповнень до законодавчих та відомчих нормативно-правових актів, що стосуються питань забезпечення кібернетичної безпеки України;

– *у правоохоронній діяльності* – при удосконаленні практичних засад забезпечення кібернетичної безпеки України *(акт впровадження від 05.03.2021р. Департаменту контррозвідувального захисту інтересів держави у сфері інформаційної безпеки СБ України*);

– *у правозастосовній практиці* – під час реалізації завдань аналітичної діяльності, прогнозування й моніторингу кіберзагроз в Україні *(акт впровадження від 13.01.2021р. № 12 Міжвідомчого науково-дослідного центру з проблем боротьби з організованою злочинністю РНБО України)*;

– *у науково-дослідній діяльності* – як основа для подальших теоретичних і практичних розробок системи забезпечення кібербезпеки, а також опрацювання проблемних питань інформаційного права. Окремі положення дослідження враховано в науково-дослідній роботі Науково-дослідного інституту інформатики і права НАПрН України *(акт впровадження від 16.12.2020р.)*;

– *у навчальному процесі* – під час розробки й оновлення навчально-методичного забезпечення навчальних дисциплін «Кібербезпека», «Інформаційне право», «ІТ-право».

Особистий внесок здобувача. Дисертаційна робота є самостійною науковою працею. Викладені в дисертації наукові положення, висновки і рекомендації, що винесені на захист, отримані дисертантом самостійно. Для обґрунтування деяких висновків використано праці інших учених, на які зроблено посилання. Із праць, опублікованих у співавторстві, використано ідеї та положення, що одержані особисто здобувачем. Особистий внесок автора в наукові праці, виконані у співавторстві, становить: «Глобальна культура кібербезпеки в системі запобігання кіберзлочинності в Україні» (60 %), «Корпоративна культура кібербезпеки суб'єктів наукової та науково-технічної діяльності» (60 %), «Протидія загрозам кібербезпеці держави на глобальному рівні» (60 %); «Національні інтереси України в кібернетичній сфері» (70 %).

Апробація результатів дослідження. Результати досліджень, викладені в дисертації, були представлені у вигляді доповідей і виступів на таких наукових заходах, як:

– *міжнародні науково-практичні конференції*: «Досудове розслідування: актуальні проблеми та шляхи їх вирішення» (м. Харків, 26.10.2018); «Правове забезпечення оперативно-службової діяльності: актуальні проблеми та шляхи їх вирішення» (м. Харків, 23.05.2019); «Актуальні проблеми правових наук в євроінтеграційному вимірі» (Харків, 20–21.12.2019); «Теоретичні та практичні проблеми правового регулювання суспільних відносин (м. Харків, 17–18.01.2020); «Реформування національного та міжнародного права: перспективи та пріоритети» (м. Одеса, 17–18.01.2020); «Нові завдання та напрями розвитку юридичної науки у XXI столітті» (м. Одеса, 21–22.02.2020); «Міжнародне та національне законодавство: способи удосконалення» (м. Дніпро, 3–4.04.2020); «Міжнародні та національні правові виміри забезпечення стабільності» (м. Львів, 17–18.04.2020); «Права людини та проблеми організації і функціонування публічної адміністрації в умовах становлення громадянського суспільства в Україні» (м. Запоріжжя, 24–25.04.2020); «Розбудова правової держави в Україні: реалії та перспективи» (м. Одеса, 29.05.2020); «Кібербезпека в Україні: правові та організаційні питання» (м. Одеса, 26.11.2020);

– *всеукраїнські науково-практичні конференції*: «Освіта і наука у сфері національної безпеки: проблеми та пріоритети розвитку» (м. Острог, 14.05.2019); «Актуальні проблеми управління інформаційною безпекою

держави» (м. Київ, 30.03.2018); «Актуальні проблеми управління інформаційною безпекою держави» (м. Київ, 4.04.2019); «Захист прав, свобод і безпеки людини в інформаційній сфері в сучасних умовах» (м. Київ, 21.05.2020); «Соціальна і цифрова трансформація: теоретичні та практичні проблеми правового регулювання» (м. Київ, 10.12.2020).

Публікації. Основні положення та висновки дисертації викладено в 40 наукових працях, зокрема в 2 індивідуальних монографіях, у розділі в 1 колективній монографії, у 22 статтях, що опубліковані у фахових виданнях України, наукових періодичних виданнях інших держав і наукових періодичних вітчизняних виданнях, що внесені до міжнародних наукометричних баз даних (6 із яких – у наукових періодичних виданнях інших держав), у 15 тезах доповідей на конференціях.

Структура та обсяг дисертації зумовлена метою й завданнями дослідження та складається зі вступу, п’яти розділів, що містять 19 підрозділів, висновків до кожного розділу та загальних висновків, списку використаних джерел і додатків. Загальний обсяг дисертації становить 461 сторінку, з яких основного тексту – 381 сторінка. Список використаних джерел розміщено на 41 сторінці (407 найменувань), додатки – на 8 сторінках.

ОСНОВНИЙ ЗМІСТ ДИСЕРТАЦІЇ

У **Вступі** обґрунтовано актуальність теми дисертаційного дослідження; висвітлено зв’язок із науковими програмами, планами, темами; проаналізовано загальний стан наукової розробленості теми; окреслено мету й завдання дослідження; сформульовано об’єкт і предмет, основні методологічні підходи до дослідження, наукову новизну, теоретичне й практичне значення роботи; наведено відомості про апробацію та публікацію результатів дослідження, його структуру.

Розділ 1 «Теоретико-методологічні засади дослідження кібербезпеки України» складається із чотирьох підрозділів.

Підрозділ 1.1 «Ґенеза наукових поглядів забезпечення кібербезпеки України» присвячено аналізу основних теоретичних підходів до предмета дослідження. У ході вивчення й аналізу основних теоретичних підходів до правового регулювання кібербезпеки людини, суспільства, держави виокремлено рівень корпоративної та глобальної культури кібербезпеки. У першому випадку йдеться про компетентність та корпоративні цінності, пов’язані із забезпеченням особистої та корпоративної безпеки в кіберпросторі відповідно до визначеної політики кібербезпеки окремої особистості чи установи. На особисту кібербезпеку співробітника установи спрямовані основні заходи формування корпоративної культури кібербезпеки, орієнтовані на засвоєння необхідних умінь і навичок захисту, що стосуються як технічних, так і психологічних аспектів, так званої соціальної інженерії і можливостей інформаційно-психологічного впливу.

Доведено, що формування глобальної культури кібербезпеки є дієвим механізмом запобігання кіберзлочинності, який спрямовано на запобігання,

виявлення й усунення причин та умов, що сприяють учиненню кіберзлочинів. Ідеться про системні заходи забезпечення життєво важливих інтересів осіб у кіберпросторі з позицій захисту інформації та інформаційно-психологічного захисту. Глобальну культуру кібербезпеки визначено як шлях вирішення проблеми підвищення рівня кіберзахисту особи і суспільства з використанням соціальних заходів на міжнародному і національному рівнях.

У ***підрозділі 1.2 «Понятійно-категоріальний синтез забезпечення кібербезпеки України в науці інформаційного права»*** виявлено низку прогалин законодавчого тлумачення основних термінів сфери кібербезпеки. Зокрема, визначений законодавцем підхід до змісту кібербезпеки із предмета свого безпосереднього правового впливу усуває досить важливу складову, що проявляється внаслідок дії загроз кібербезпеки – це запобігання шкоді. Обґрунтовано, що таке усунення не дозволяє в повній мірі визначити мету правового регулювання.

На основі аналізу різних теоретичних підходів запропоновано зміст категорії «кібербезпека України» з погляду функціонально-діяльнісного підходу розуміти як безпечність об'єктів кіберпростору й захищеність життєво важливих інтересів людини, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі, а також постійний процес запобігання та протидії відповідним загрозам.

Доведено, що кібернетична безпека є унікальним, універсальним явищем, продуктом світової цивілізації, розвиток якого потребує глибокого наукового осягнення, належного нормативно-правового врегулювання та створення відповідних структур, що мають забезпечувати національну безпеку України у глобальному кібернетичному просторі.

У ***підрозділі 1.3 «Співвідношення кібербезпеки та інформаційної безпеки»*** доведено, що кібербезпека, як певний процес та правове явище, виникла як складова частина інформаційної безпеки. Проте, у ході розвитку даних процесів, кібербезпека набуває ознак самостійного виду національної безпеки. Зроблено припущення, що в наш час кібербезпека – це еволюція інформаційної безпеки, оскільки від захисту процесів, інформації та діяльності в кіберпросторі залежить значно більше, ніж просто втрата інформації.

Автором запропоновано логічну схему еволюції кібербезпеки як окремого виду безпеки: кібербезпека формується в реляційних відносинах з безпекою мереж, безпекою інтернету і безпекою додатків, кібербезпека також здійснює підтримку безпеки інфраструктури критичної інформації, критичної інфраструктури в частині, що її стосується.

У ***підрозділі 1.4 «Методологічні засади забезпечення кібербезпеки України»*** зазначено, що основними методологічними підходами дослідження стали: загальнофілософський, соціологічний, технічний, аксіологічний і правовий. На основі поданого методологічного інструментарію визначено,

що провідною гіпотезою є залежність, взаємна зумовленість, кореляція ефективності розвитку людини, суспільства, держави в умовах інформатизації й глобалізації. Факторний аналіз, який є основним методом пропонованої наукової роботи, базується на вивченні чинників, що у глобальному інформаційному суспільстві впливають на результативність реалізації особою своїх інтересів і становлять для неї небезпеку. Вихідним предметом дослідження визначено правове забезпечення кібернетичної безпеки в умовах глобального інформаційного суспільства.

У розділі наголошується, що з метою узагальнення висновків проведеної роботи за допомогою аналізу інформаційного законодавства, його систематизації, з'ясування змісту основних понять застосовується інструментарій формально-логічного або юридичного методу. Дослідженню правового регулювання кібернетичної безпеки України за допомогою виявлення тенденцій, порівняльного аналізу підходів до зазначеної проблематики в законодавствах іноземних держав та в міжнародно-правових документах сприяє застосування порівняльно-правового методу. Завдяки використанню історичної (історично-правової) методики досягається мета здобуття й узагальнення даних щодо сутності й закономірностей розвитку інформаційного права, його інститутів у контексті інформаційно-безпекової проблематики. За допомогою засобів системного аналізу здійснюється, зокрема, оцінювання підходів до забезпечення інформаційної безпеки особи, що усталилися у вітчизняній юриспруденції, їхня кореляція з актуальними суспільними відносинами. Водночас виявити й оцінити чинники, що впливають на правову поведінку особи, дає змогу соціологічний метод. Прогностичний метод, зі свого боку, дозволяє за допомогою моделювання окреслити перспективи, передбачити ймовірні шляхи розвитку галузевого законодавства у сфері кібербезпеки України, її правового забезпечення.

Забезпечення кібернетичної безпеки України розглянуто як самостійний комплексний міжгалузевий інститут інформаційного законодавства.

Розділ 2 «Нормативно-правове забезпечення кібербезпеки України» складається із п'яти підрозділів.

У ***підрозділі 2.1 «Стан правового регулювання кібербезпеки в Україні»*** визначено такі особливості стану правового регулювання кібербезпеки України: глобальний розвиток кіберпростору, що призвело до виникнення нових типів суспільних відносин, які потребують правового врегулювання; прагнення України до вступу в Європейський Союз і НАТО ставить завданням наближення нормативно-правового регулювання заходів безпеки до рівня вимог Європейського Союзу та стандартів НАТО; динамічність загроз кібербезпеці України зумовлює потребу оперативного реагування, в тому числі й за допомогою правового чинника.

У підрозділі, на основі аналізу національного законодавства у сфері кібербезпеки, виокремлено низку недоліків, зокрема, запропоноване визначення «кіберпростору» в Законі «Про основні засади забезпечення кібербезпеки України» усуває з поля правового впливу автономні

автоматизовані системи управління (наприклад, об'єктів атомної енергетики), які, саме з огляду на вимоги безпеки, є автономними.

Запропоноване визначення терміна «кіберпростір» також суб'єктно обмежує «простір» лише інформаційними (автоматизованими), телекомунікаційними й інформаційно-телекомунікаційними системами, тобто автоматизованими системами. Крім того, у законі не надано визначення терміна «середовище», що призводить до невизначеності у тлумаченні терміна «кіберпростір».

У визначенні терміна «*кіберзлочин*» доведено доцільність заміни словосполучення «міжнародними договорами» словосполученням «міжнародним правом». Зазначений підхід забезпечить єдність термінологічного тлумачення на рівні національного права та законодавства зарубіжних країн.

Встановлено, що законодавчий зміст терміна *«критично важливі об'єкти інфраструктури (критичні інфраструктурні об'єкти),* не передбачає виділення саме об'єктів такої інфраструктури, а вказує лише на «підприємства, установи й організації незалежно від форм власності». Тут ми підтримуємо думку тих дослідників, які відстоюють доцільність ухвалення Закону України «Про об'єкти критично важливої інформаційної інфраструктури».

Обґрунтовано, що визначення терміна *«кіберзагроза»* не співвідноситься за обсягом інформації, поданої в терміні «кібербезпека», та не відповідає визначенню цього терміна.

Наведено науково обґрунтовані аргументи, що Закон України «Про основні засади забезпечення кібербезпеки України» є, радше, дорожньою картою для розробки майбутніх нормативних актів, а не всеосяжним законом про кібербезпеку, який регулює повний спектр питань кібербезпеки та відповідає міжнародним стандартам і найкращим практикам.

У ***підрозділі 2.2 «Теоретико-правові засади визначення об'єктів кібербезпеки України»*** акцентовано увагу на тому, що в контексті визначення об'єктів забезпечення кібербезпеки України кіберпростір є, водночас, й об'єктом захисту, скажімо, інформаційних ресурсів, відповідних апаратних і програмних засобів тощо, і джерелом загрози для інших об'єктів національної безпеки. Отже, кібернетичну безпеку слід розглядати як самостійний вид безпеки, оскільки реалії сьогодення переконливо свідчать, що ця науково-правова категорія вийшла за межі інформаційного протиборства та військової безпеки і є елементом інформаційної сфери загалом.

Еволюція сучасного кіберпростору супроводжується виникненням нових загроз безпеці інформації та інформаційних технологій, а також виробленням відповідних захисних заходів. Зазначені тенденції закономірно приводять до розширення об'єкта правового регулювання кібербезпеки. Отже, кібербезпека розглядається у розділі і як спрямована на цифрове середовище нова стадія еволюції інформаційної безпеки, яку нині переживає людство. Кібербезпека охоплює не тільки власне захист інформації, а й

захист інформаційного-технологічного простору (поля комп'ютерних технологій) загалом й усіх його складових.

Поширення «інтернету речей», криптовалют, криптобірж, систем електронного урядування й виборів, «розумних контрактів» та інших новітніх ІТ-технологій докорінно змінює кібернетичний простір, та, відповідно, розширює межі правового впливу.

Аргументовано, що визначити об'єкти правового регулювання кібербезпеки України як завершену систему чи класифікацію неможливо. Така структура є динамічною та мінливою відповідно до національних і глобальних тенденцій змін у кіберпросторі. Зважаючи на це, перед кожною державою постає потреба створення ефективних засобів забезпечення своєї кібербезпеки.

У ***підрозділі 2.3 «Система суб'єктів забезпечення кібербезпеки в Україні»*** обґрунтовано, що систему суб'єктів забезпечення кібербезпеки людини, суспільства, держави, слід розглядати в комплексному взаємозв'язку міжнародних і регіональних організацій, недержавних організацій, галузевих організацій, держави, приватного сектору та безпосередньо громадян. За такого комплексного підходу структуру суб'єктів забезпечення кібербезпеки можна відобразити так: міжнародні регіональні організації, недержавні організації, галузеві організації, держава, приватний сектор, громадяни.

Запропоновано розробити оптимальні механізми співпраці між приватним сектором і державними органами у сфері забезпечення кібербезпеки. У цьому контексті виокремлено такі пріоритетні напрями: розвиток кіберрозвідки, аудит кібербезпеки, взаємний обмін інформацією щодо кіберзагроз, заміна НД ТЗІ на ефективніший та сучасніший базовий стандарт і запровадження галузевих стандартів кібернетичної безпеки, створення галузевих центрів з реагування на кібернетичні інциденти (SOC) та центрів інформаційного обміну про кібернетичні атаки (ISAC), започаткування незалежних платформ для співпраці – кіберцентрів, з метою ефективної протидії кібернетичним загрозам.

Досить дієвим з огляду практики його втілення є, зокрема, розроблений у США NIST Cybersecurity Framework, яким, крім Сполучених Штатів, користуються японський та ізраїльський уряди. До того ж організації можуть обирати й запроваджувати NIST, ISO, Cobit та ін. Розв'язання питань, пов'язаних з регулюванням і контролем, можна покласти на галузеві регулятори або саморегулюючі організації. Прикладом останніх є NERC CIP у Сполучених Штатах, якими були розроблені галузеві стандарти з кібернетичної безпеки в енергетичному секторі. Іншим позитивним прикладом галузевого регулювання, який варто було б розглядати з погляду можливого запровадження в Україні, є Health Insurance Portability and Accountability Act (HIPAA) із підтримки безпеки медичної інформації на електронних носіях у галузі охорони здоров'я або Ofcom для телекомунікаційної сфери тощо.

У розділі запропоновано конкретні умови розвитку індустрії кібернетичної безпеки: у фінансовій (забезпечення пільгами, прозорими

тендерами на отримання бюджетного фінансового забезпечення, розвиток технопарків, співпраця закладів вищої освіти та приватного ІТ-сектору тощо); в організаційній площині (прозорі та зрозумілі правила, що диктує цей ринок). Дієвим механізмом у цьому напрямі вбачаємо укладання відповідних меморандумів між суб'єктами забезпечення кібербезпеки. Прикладом такої співпраці може слугувати підписаний Службою безпеки України із приватним акціонерним товариством «Укргідроенерго» та національною енергетичною компанією «Укренерго» Меморандум щодо протидії кіберзагрозам і розвитку ефективної системи кібербезпеки держави.

Автором наведені аргументи для подальшого розвитку системи збирання й обробки інформації щодо інцидентів кібербезпеки й обміну технічними даними про ідентифікатори компрометації інформаційних систем об'єктів критичної інфраструктури між суб'єктами сектору безпеки в режимі реального часу в межах Ситуаційного центру забезпечення кібербезпеки СБУ на базі платформи з відкритим програмним кодом MISP (Malware Information Sharing Platform). Цю платформу широко використовують в усьому світі. Вона відповідає міжнародним стандартам ЄС та НАТО і застосовується основними міжнародними суб'єктами у сфері кібербезпеки FIRST, CIRCL, CiviCERT, NATO NCI Agency.

У ***підрозділі 2.4 «Актуальні питання протидії кіберзагрозам у сучасному кіберпросторі»*** на основі системного підходу класифіковано такі основні кіберзагрози існуванню нації та кіберзагрози за деструктивним впливом на основні сегменти національного кіберпростору: *держави*, що використовують відповідні кіберзасоби для збирання інформації та розвідувальної діяльності (зокрема, економічне шпигунство задля отримання переваг в економічній, політичній, військовій та інших сферах); *бізнесові структури*: приватні компанії-конкуренти, що прагнуть здобути важливі дані стосовно опонентів задля отримання ринкових переваг – виробництво, ціни, розробки, асортимент тощо; *кримінальні угруповання*, що вдаються до кібернетичних атак з метою грошового зиску; *міжнародне корпоративне шпигунство*, метою якого є економічне, промислове шпигунство, викрадення значних коштів; нерідко користуються послугами хакерів, надаючи їм відповідні засоби; *мережеві оператори*, що використовують ботнет (мережу) дистанційно керованих зламаних систем задля розповсюдження спаму, фішингу, провадження узгоджених атак тощо; *розробники шкідливих програм і програм стеження* – окремі особи чи організації, які створюють і застосовують зазначений продукт із протиправною метою; *розробники фішингових схем*, що створюють і застосовують їх для викрадення коштів, персональних даних тощо; працівники підприємств (компаній, установ), які мають доступ до внутрішньої конфіденційної інформації (інсайдери), зокрема до комп'ютерних систем, а тому можуть викрадати дані або завдавати шкоди. До цих суб'єктів належать також некваліфіковані чи халатні співробітники, тимчасово наймані працівники, що можуть неумисно зашкодити системі через необережність; *спамери*, які використовують схеми фішингу, поширюють у мережі повідомлення, що містять приховані або

хибні дані, а також кібератаки здійснюють шпигунські й вірусні програми (приміром, «відмова в обслуговуванні» – DDoS); *терористи*, що ставлять за мету виведення з ладу чи руйнацію об'єктів критичної інфраструктури або ж втручання в їхнє функціонування, що може призвести до значних людських жертв, становить серйозну загрозу національній безпеці через підрив економіки країни, морально-психологічного стану суспільства; *хакери*, які зламують закриті інформаційні системи й мережі з різних мотивів. Це може бути перевірка фахових здібностей, самоствердження, демонстрація певної громадянської позиції, отримання незаконного фінансового зиску; *хактивісти*, що атакують поштові сервери та веб-сторінки з метою розміщення матеріалів політичного характеру.

На основі узагальнення даних щодо загроз кібербезпеці на глобальному та національному рівнях у пропонованому дослідженні сформульовано загальну концепцію загроз кібернетичній безпеці, що містить такі складові, як інформаційні війни, кібернетичне шпигунство, кібертероризм, кібернетична злочинність. У розділі зіставлено зазначені види загроз із їхніми головними суб'єктами, досліджено переважну мотивацію зловмисного використання інформаційно-комунікативних технологій та основні об'єкти можливих кібератак.

Підрозділ 2.5 «Досвід забезпечення кібербезпеки у зарубіжних країнах» присвячено аналізу нормативних документів різних країн, що стосуються питань забезпечення кібербезпеки. За результатами дослідження пріоритетних напрямів Стратегії кібербезпеки Європейського Союзу, зроблено висновок, що кібербезпека є спільною справою всіх: самої людини, приватного сектора, суспільства і держави. Тільки у межах цього симбіозу вбачається можливість побудови суспільства, у якому індивіди будуть почувати себе безпечно в кіберпросторі. Досягнути цього можливо за умови низки складових: тісної взаємодії держави, в особі відповідальних за кібербезпеку органів, та приватного сектору і громадян. Така співпраця першочергово полягає у взаємному обміні інформацією; у розвитку та практичному втіленні таких категорій, як «екологія інформації», «інформаційна гігієна», «критичне мислення у споживачів інформації», у розвитку інформаційної культури, а також усвідомленні необхідності навчання дітей та молоді інформаційній культурі та гігієні.

Констатовано, що найбільш передовими в галузі розробки і застосування національних стратегій кібербезпеки серед країн – членів ЄС є Норвегія, Естонія, ФРН, Австрія, Угорщина, Нідерланди. Найменш успішні у сфері кібербезпеки серед країн, що входять до ЄС, Румунія, Болгарія, Бельгія, Португалія, Греція. У Нідерландах найрозвиненіша система кібернетичної безпеки, як з погляду правової підтримки, так і з погляду технологій та організації. Ця країна через кожні два роки здійснює перегляд своєї Національної стратегії кібербезпеки, а Національним центром кібербезпеки, що є національним CERT (англ. ***c**omputer **e**mergency **r**esponse **t**eam*) з низкою додаткових повноважень, здійснюється розробка та запровадження усіх процедурних і технологічних питань стосовно безпеки в кіберпросторі.

Центром також проводиться активна співпраця з Аналітичними та інформаційними центрами (ISACs), які дбають про те, щоб критична інформаційна інфраструктура за секторами була в безпеці. Саме Нідерланди були ініціаторами створення загальноєвропейських мереж «гарячих ліній» – InHope і перші впровадили їх у своїй національній практиці.

Аргументовано, що позитивними прикладами для України можуть служити практичні знання, яких набула Естонія. Естонцями було створено такі стандарти кібернетичної безпеки, які згодом перейняло НАТО задля впровадження у власному оборонному та безпековому сегменті. Нині у світі є 32 центри, що користуються саме естонськими стандартами. На теперішній час у державі, що має населення 1,2 млн осіб, функціонує п'ять кібернетичних центрів.

З огляду на аналіз правового регулювання та практики забезпечення кібербезпеки у зарубіжних країнах, запропоновано доповнити Положення про Національний координаційний центр кібербезпеки, затверджене Указом Президента України від 7 червня 2016 р. № 242/2016 у частині вдосконалення основних завдань органу. У цьому контексті пропонуємо розширити п. 3 згаданого положення, додавши до основних завдань центру такі: упровадження в Україні стандартів безпеки мережевих та інформаційних систем; визначення критеріїв, за якими буде складатися перелік операторів базових послуг і провайдерів цифрових послуг; контроль за дотримання мережевої нейтральності та міжнародних і європейських стандартів та заборон уведення окремих національних стандартів у сфері кібербезпеки, які не є сумісними з європейськими та міжнародними стандартами; аудит системи мережевої та інформаційної безпеки; організація та підтримка системи сповіщення про кіберінциденти, системи аудиту й упровадження заходів мережевої та інформаційної безпеки; забезпечення належного дотримання вимог щодо збереження конфіденційності, зокрема стосовно персональних даних і захисту комерційних інтересів операторів та провайдерів.

Розділ 3 «Теоретико-правовий аналіз сучасних загроз кібербезпеці людини під час використання кіберпростору» складається із трьох підрозділів.

У ***підрозділі 3.1 «Системний аналіз правового регулювання кібербезпеки людини»*** наголошено, що право людини на кібербезпеку – це своєрідна, специфічна сукупність прав, що реалізуються, зокрема, за допомогою цифрових, інформаційно-телекомунікаційних технологій з метою захисту приватної, особистої інформації від несанкціонованого доступу та запобігання шкідливим впливам на особистість. Формування зазначеної сукупності прав належить до четвертого покоління прав людини й зумовлене технологізацією й інформатизацією суспільства.

Подано авторське тлумачення поняття «інформаційна дієздатність людини», яке визначено як спроможність особи своїми діями в інформаційній галузі, у сфері використання кіберпростору набувати прав,

брати на себе певні правові обов'язки, а також нести юридичну відповідальність у разі неправомірної поведінки.

Систематизовано основні права людини на кібербезпеку, що полягають у: 1) можливості реалізації «права на забуття», тобто обов'язку оператора пошукової системи мережі інтернет на вимогу користувача – фізичної особи припинити надання відомостей про покажчики сторінок сайту в мережі, що дають змогу отримати доступ до певної інформації про заявника, якщо вона є недостовірною, неактуальною, такою, що втратила для особи значущість, або розповсюджується з порушеннями встановлених законодавством вимог. Це дозволяє особі – користувачу інтернету видаляти певну інформацію про себе, контролюючи поширення її в мережі; 2) можливості «цифрового спілкування» з державними та самоврядними органами, отримання державних адміністративних послуг в електронному вигляді. Нині ця форма закріплена законодавчо, поступово вдосконалюється й набуває дедалі більшої популярності, дозволяючи громадянам заощаджувати час, матеріальні, фізичні та психологічні ресурси; 3) захисті персональних даних, конфіденційної інформації у процесі користування інформаційним (кібернетичним) простором, здійснення особою своєї цифрової ідентичності. З погляду права така ідентифікація є унікальною сукупністю, вираженою в цифровій формі інформації про особу, за допомогою якої відбуваються міжособистісні стосунки, правові відносини, реалізуються права й обов'язки; 4) захисті інформації, що циркулює в системах інтернет-банкінгу, від несанкціонованого доступу. У цьому разі засобами забезпечення інформаційної (кібернетичної) безпеки особи є аутентифікація особи, застосування цифрового підпису й зовнішніх електронних пристроїв, шифрування інформації тощо; 5) захисті від негативного інформаційного впливу, поширення протиправного контенту (зокрема і в інтернеті), що забезпечується дією автоматизованої інформаційної системи ведення й використання бази даних про сайти, які містять інформацію, заборонену до розповсюдження в Україні, певне обмеження анонімності в мережі інтернет тощо.

Підрозділ 3.2 «Критерії класифікації загроз безпеці людини у кіберпросторі» присвячений дослідженню правових механізмів протидії загрозам кібернетичній безпеці людини.

Підкреслено, що існує декілька критеріїв класифікації форм і видів загроз безпеці людині в кіберпросторі. З огляду на сучасні тенденції, виокремлено такі основні: за впливом на національну свідомість, загрози кібербезпеці людини, які посягають на національні цінності, за природою виникнення.

Крім того, вивчення сучасних інформаційно-телекомунікаційних технологій дало змогу виявити специфічну групу загроз, пов'язаних із цифровою економікою, фінансово-банківською сферою (зокрема, з обігом електронних грошей, криптовалют – BitCoin, LitCoin, OneCoin тощо), конфіденційністю персональних даних (загрози від найсучаснішої онлайн-реклами Real-TimeBidding (RTB), спеціальних файлів cookie та ін). Нині

найнагальнішим вважаємо вирішення проблем, пов'язаних із розвитком новітніх технологій (на кшталт універсальної інноваційної платформи Blockchain), удосконалення систем ідентифікації й аутентифікації особи в кібернетичному просторі тощо.

Спираючись на проведене системне наукове дослідження, розроблено структуру та зміст Концепції кібернетичної безпеки людини. Визначено її головні принципи формування, завдання, механізми реалізації й очікувані результати державної політики у сфері забезпечення кібернетичної безпеки людини, її можливі структуру та зміст, а також потребу долучення до її складу документів стратегічного планування України. Запропоноване структурно-змістовне наповнення зазначеного документа містить головні принципи формування, завдання, механізми реалізації й очікувані результати державної політики у сфері забезпечення кібербезпеки особи. Крім того, обґрунтовано мету гармонізації інформаційних відносин, підвищення відповідальності держави в цій сфері, створення умов для формування сприятливого кібернетичного середовища як стратегічну спрямованість концепції.

Доцільність розробки Концепції кібернетичної безпеки людини зумовлена необхідністю вдосконалення національного законодавства про кібернетичну безпеку в сенсі закріплення поняття кібернетична безпека людини, правового забезпечення кібернетичної безпеки людини, формування системи забезпечення безпеки людини в інформаційній сфері як сукупності відповідних сил і засобів.

У ***підрозділі 3.3 «Порівняльно-правове дослідження правового регулювання кібербезпеки людини на міжнародному рівні»*** проведено аналіз норм міжнародного права про кібербезпеку. Виявлено, що натепер відсутній єдиний, загальний для всієї світової спільноти міжнародно-правовий документ щодо кібернетичної безпеки. Однак керівні принципи стосовно методів підвищення рівня безпеки в кібернетичному просторі містять Конвенція ООН проти транснаціональної організованої злочинності (2000), Статут Міжнародного союзу електрозв'язку (1992) та Доповідь ООН про кібербезпеку (2015).

Єдиний регіональний обов'язковий у юридичному сенсі документ – Будапештська конвенція про кіберзлочинність (2001). Наша держава є учасницею цієї конвенції, а тому більшість її норм матеріального права імплементовані в національне законодавство. Водночас, на нашу думку, задля ефективної реалізації всіх положень Будапештської конвенції слід удосконалити кібербезпековий понятійно-термінологічний апарат Кримінального процесуального кодексу України.

Констатовано, що Директива NIS не є обов'язковою для України, яка поки що не входить до Євросоюзу, проте окремі її положення беруться до уваги у правозастосовній практиці, а деякі були частково впроваджені у вітчизняне законодавство. Вважаємо, що імплементацію Директиви NIS можна провести в межах механізму, встановленого Угодою про асоціацію між Україною та Європейським Союзом.

Розділ 4 «Правова захищеність суспільства у контексті глобальних трансформацій у кіберпросторі» складається із трьох підрозділів.

У ***підрозділі 4.1 «Аналіз концепцій інформаційного суспільства»*** обґрунтовано пріоритет розвитку суспільства на сучасному етапі – захист прав і свобод людини має бути головним пріоритетом у застосуванні інформаційних технологій й у використанні кіберпростору. На цій теоретичній основі виокремлено низку кібервикликів і кіберзагроз глобальному інформаційному суспільству: деструктивний вплив на різних суб'єктів (пропаганда); економічна свобода; зіткнення культур; правозастосовні проблеми в умовах кібернетичної транскордонності; надмірна соціальна мобільність, інформаційне відчуження, сугестія, зомбування.

Констатовано, що на сферу прав і свобод людини безпосередньо впливає висока оперативність новацій у сфері інформаційних технологій і використання кіберпростору, зокрема це й технології «інтернету речей», штучного інтелекту, нанотехнології, інформаційно-комунікаційні технології тощо. З огляду на це набуває неабиякої ваги проблема наслідків їх застосування, актуалізується потреба аналізувати й ураховувати ці обставини, налаштовуючи, зокрема, новітні технології на дотримання загальнолюдських цінностей.

Обґрунтовано та підтверджено, що реальні загрози глобальному інформаційному суспільству й кожній людині несуть: мілітаризація кіберпростору, розв'язування широкомасштабних інформаційних війн, поширення маніпулятивних матеріалів, деструктивні інформаційно-психологічні впливи на індивідуальну, групову й суспільну свідомість тощо. Доведено гіпотезу, що в таких умовах успішне розв'язання згаданих глобальних соціально-економічних, політичних, безпекових та інших проблем можливе тільки в разі об'єднаних плідних зусиль усього світового співтовариства.

У ***підрозділі 4.2 «Правовий чинник у попередженні кіберзагроз сучасному українському суспільству»*** визначено такі актуальні проблеми правового регулювання кібербезпеки, що потребують невідкладного й кардинального розв'язання:

1) виконання відповідного законодавства, зокрема в частині кваліфікації комп'ютерних злочинів і призначення покарання, а також складнощі в його застосуванні;

2) узгодження національного законодавства з міжнародно-правовими нормами й відповідними стандартами правозастосування. Транскордонність і транснаціональність глобальної мережі значно ускладнюють реалізацію приписів національного законодавства й контроль за його дотриманням, спричиняють юрисдикційні суперечності при розв'язанні багатьох питань – технологічних, технічних, економічних, культурологічних та інших, що виникають при використанні кіберпростору;

3) керовані комп'ютерною технікою автоматизовані кібернетичні системи стають нині повноцінними суб'єктами інформаційної взаємодії (це,

насамперед, сфера IoT). У наукових дискурсах дедалі частіше лунає думка, що нинішній світоустрій утворено саме за допомогою розумних машин і штучного інтелекту. Відповідно, серйозну небезпеку може становити можливість шляхом віддаленого управління через зазначених суб'єктів делегувати певні повноваження, реалізовувати, ба, навіть їх перекручувати та спотворювати. Відповідно тепер, в умовах тотального поширення інформаційно-телекомунікаційних технологій і використання кіберпростору часом важко визначити справжнє джерело управління й контролю – людина це чи машина, і виявити при цьому якісь відмінності.

Аналізуючи проблеми використання кіберпростору, роботу глобальної електронної мережі, що є своєрідною технологічною картою розвитку IoT, інтелектуалізації робототехніки, обґрунтовано необхідність приділення особливої уваги можливостям кіберсистем, мікрочіпів, гібридів, нанотехнологій. У глобальному інформаційному суспільстві вбачається неминучим упровадження таких недержавних суб'єктів в інформаційну взаємодію, в управлінські процеси, у життєдіяльність «цифрової» людини й соціуму. З огляду на це актуальність проблем щодо влади, впливу, контролю в контексті використання кіберсередовища не викликає сумнівів, а особливої ваги набуває правовий чинник, який має стати надійним регулятором подібних процесів і відносин.

Доведено, що забезпечення кібернетичного середовища слід розглядати і як об'єкт морально-правового регулювання. Сутність останнього полягає в налагодженні суспільних відносин, урегулювання яких базується на нормах права та моралі. Із цією метою держава, як основний регулятор, виконує такі основні завдання:

1) удосконалення існуючих, розробка й упровадження в законодавство нових правових норм, що відповідають сучасним потребам людини, суспільства й держави і спрямовані на правове регулювання використання кіберпростору, узгодження національного й міжнародного інформаційного законодавств тощо;

2) утвердження й упорядкування доцільних суспільних відносин у сфері державного управління інформаційним середовищем, зокрема, питань таємниці даних, інтелектуальної власності, авторського права тощо, шляхом упровадження морально-етичних і правових норм;

3) захист передбачених законодавством відносин у процесі користування інформаційними технологіями, кіберпростором, зокрема і визначення відповідальності за їхнє порушення;

4) регулювання суспільних відносин, пов'язаних з еволюцією інформаційного суспільства, шляхом формування суспільної думки, створення морально-етичних кодексів тощо.

У ***підрозділі 4.3 «Теоретико-правове підґрунтя системи соціального регулювання в інформаційному суспільстві»*** констатовано зростання в кібербезпеці ролі соціальної складової. Зазначений факт зумовлює потребу запровадження принципово нового виду захисних інформаційно-безпекових заходів – соціальних. Якісною новизною такий вид захисту кібербезпеки

людини, суспільства й держави зобов'язаний складній, багаторівневій системі механізмів і поведінкових форм, сукупність яких і має цю безпеку забезпечити.

Доведено, що задля успішного розв'язання проблем забезпечення кібернетичної безпеки необхідне впровадження комплексу заходів, а саме: здійснення активного наукового пошуку в межах розвитку інформаційної етики – нової галузі етичного знання, що перебуває на етапі свого становлення; освітні та виховні заходи з кібербезпеки; усебічна популяризація в суспільній свідомості способів, моделей і форм морально-етичної поведінки у глобальному кіберсередовищі із застосуванням при цьому найсучасніших цифрових технологій, із залученням усіх можливих ЗМІ й активною участю державних структур й освітніх закладів.

Розділ 5 «Напрями розвитку правового регулювання кібербезпеки держави» складається із чотирьох підрозділів.

Підрозділ 5.1 «Концептуальні засади правового регулювання кібербезпеки України на сучасному етапі розвитку глобальних інформаційних процесів» присвячено характеристиці основних напрямів правового забезпечення кібернетичної безпеки України на сучасному етапі. Підкреслено, що беззаперечним пріоритетом державної політики у сфері забезпечення кібербезпеки є і має бути подальша інтеграція в НАТО. Серед останніх добутків нашої держави на цьому шляхи слід вважати надання у червні 2020 р. Північноатлантичною радою статусу партнера з розширеними можливостями (Enhanced Opportunities Partner, EOP). EOP дозволяє країні-партнеру досягти так званої секторальної (оперативної) взаємосумісності з НАТО (на рівні системи логістики, зв'язку, управління військами, конкретних родів військ тощо). Крім того, EOP надає запрошеним до неї країнам-партнерам низку особливих можливостей взаємодії з НАТО.

Розроблено чотири основні складові національних інтересів України в кібернетичній сфері. *Перша складова* – забезпечення дотримання конституційних прав і свобод людини та громадянина у сфері отримання інформації та користування нею, сприяння духовному оновленню держави, збереження та зміцнення моральних цінностей суспільства, традицій гуманізму і патріотизму, наукового і культурного потенціалу країни. *Другий компонент* передбачає інформаційне забезпечення державної політики, що пов'язане з доведенням до міжнародної громадськості та народу України правдивої інформації про державну національну політику, офіційну позицію держави щодо соціально-значимих подій держави та міжнародного життя, із наданням громадянам доступу до відкритих національних інформаційних ресурсів. *Третя складова* забезпечує застосування новітніх інформаційних технологій, створення вітчизняної індустрії інформації, зокрема й індустрії засобів інформатизації, телекомунікації та зв'язку, задоволення потреб внутрішнього ринку її продукцією, а також забезпечення накопичення, ефективного використання та збереження національних інформаційних ресурсів. *Четвертий компонент* національних інтересів України в кібернетичній сфері передбачає захист інформаційних ресурсів від

несанкціонованого доступу, забезпечення безпеки телекомунікаційних й інформаційних систем, як створюваних, так і тих, що функціонують на території України.

У ***підрозділі 5.2 «Міжнародні аспекти кібербезпеки України»*** обґрунтовано, що кожне інформаційне протистояння на світовій арені має цілком визначену мету. Водночас їхній аналіз дозволив виявити цілі загальнішого характеру, що властиві глобальному інформаційному суперництву в нинішніх умовах. До них належить: забезпечення національної безпеки держави у глобальному кіберпросторі; просування і захист національних інтересів в інформаційній сфері; забезпечення кібербезпеки як важливої складової системи національної безпеки; посилення міжнародної кібербезпеки шляхом зменшення у глобальному кібернетичному просторі можливостей для ворожого використання інформаційно-комунікаційних технологій.

Для досягнення зазначених цілей у процесі глобального інформаційного протистояння використовують відповідні методи і способи боротьби, серед яких: інформаційне домінування або досягнення переваги в кіберпросторі; інформаційна асиметрія як базовий принцип інформаційного впливу, що використовується як відповідь на зовнішній вплив, так і при здійсненні впливу на іншу сторону інформаційного суперництва; зовнішній контроль кіберпростору держави й управління інформаційними процесами, що здійснюється з іноземних центрів; інформаційне стримування як спосіб управління кризовими ситуаціями в зонах конфліктів; кіберагресія, в основі якої лежить незаконне здійснення однією державою інформаційного впливу на кіберпростір іншої держави, що завдає шкоди її суверенітету, життєдіяльності в різних сферах та політичній незалежності; кібервійна, що є найгострішою формою інформаційного протистояння між державами, здійснюваного насильницькими засобами і способами впливу на інформаційну сферу супротивника з метою досягнення стратегічних завдань. Нині сутність кібервійни полягає у прихованому управлінні економічними, політичними, військовими й іншими процесами держави-супротивника.

У ***підрозділі 5.3 «Пріоритети розвитку правових основ державної політики забезпечення кібербезпеки України»*** запропоновано такі конкретні заходи, які доцільно реалізувати міжнародним співтовариством на глобальному рівні для посилення кібербезпеки: 1) розробка й упровадження правових повноважень, юрисдикційних правил та інших процедурних положень для забезпечення ефективного розслідування злочинів, скоєних за допомогою ІКТ, зокрема: коригування норм збирання, зберігання, засвідчення і використання у кримінальному розслідуванні електронних доказів; ухвалення положень, що регулюють проведення внутрішніх і міжнародних обшуків; розробка положень, що стосуються міжнародних і національних відстежень повідомлень; ухвалення положень, що стосуються перехоплення повідомлень, переданих через комп'ютерні мережі й аналогічні засоби масової інформації тощо; 2) для подолання розриву між швидкістю, з якою працюють кіберзлочинці, і темпами реагування правоохоронних

органів слід здійснити розширення міжнародної співпраці між правоохоронними органами, прокуратурою та судовими органами, а також з інтернет-провайдерами; 3) реалізація за умови наявності ресурсів міжнародних проектів технічної взаємодії та допомоги. Зазначені проекти могли б об'єднати експертів у галузі законодавства, запобігання злочинності, судового переслідування, комп'ютерної безпеки, методів розслідування і суміжних питань з державами, що потребують інформації або допомоги в цих сферах; 4) розробка освітньої програми, що сприятиме підвищенню рівня знань та поінформованості про протидію кіберзлочинності.

У ***підрозділі 5.4 «Нормативно-правове забезпечення окремих елементів інформаційної інфраструктури на національному та міжнародному рівнях забезпечення кібербезпеки»*** запропоновано визначення «інформаційна зброя» внести до переліку основних термінів, що містяться в Законі України «Про основні засади забезпечення кібербезпеки України». У широкому розумінні, з погляду інформаційного права, зазначений термін визначено як інформаційні технології, засоби і методи, призначені для ведення інформаційної війни.

Обґрунтовано доцільність доповнення ст. 14 згаданого Закону України «Про основні засади забезпечення кібербезпеки України» таким змістом: «*основною загрозою в галузі міжнародної інформаційної безпеки є використання інформаційно-комунікаційних технологій для вчинення різних протиправних дій, зокрема і як інформаційну зброю у військово-політичних цілях. Умови, що створюють можливості протидії загрозам використання ІКТ, належать до основних напрямів державної політики*».

Запропоновано під «інформаційною інфраструктурою України» розуміти сукупність об'єктів інформатизації, інформаційних систем, мереж зв'язку і сайтів у мережі інтернет, розміщених на території України, а також на територіях, що перебувають під юрисдикцією України або використовуваних на підставі міжнародних договорів України. Обґрунтовано доцільність законодавчого закріплення терміна «критична інформаційна інфраструктура», що відрізняється від інформаційної інфраструктури наявністю автоматизованої системи управління суб'єктів критичної інформаційної інфраструктури і систем електронного зв'язку в ролі об'єктів критичної інформаційної інфраструктури.

Доведено, що забезпечення кібербезпеки критичної інформаційної інфраструктури можливе, насамперед, шляхом визначення її об'єктів, розв'язання проблеми кібербезпеки об'єктів зі значним життєвим циклом, розробки методики модернізації критичної інформаційної інфраструктури для кожної організації, інформаційні структури та технології якої є об'єктами критичної інформаційної інфраструктури. Крім того, необхідно систематизувати акти Уряду України й органів виконавчої влади, виявивши положення, що не відповідають забезпеченню кібербезпеки інформаційних технологій у міжвідомчій взаємодії, а також уточнити визначення понять «інформаційна система» й «інформаційно-телекомунікаційна мережа». Обґрунтовано необхідність надати правову оцінку діяльності віртуальних й

анонімних спільнот. Їхнє функціонування має схожі риси із функціонуванням адміністративно-територіальних утворень, але здійснюється в інтернеті. Адміністрування діяльності зазначених спільнот можливе в межах інформаційної технології, на базі якої вони об'єднані. Водночас з огляду на те, що термін «територія» не може бути застосований для характеристики інтернет-відносин, назріло визначення правового терміна «транскордонний простір». А віртуальні спільноти слід визнати «адміністративно транснаціональними утвореннями».

ВИСНОВКИ

У дисертації здійснено теоретичне узагальнення та вирішено актуальну наукову проблему формування теоретичної моделі стратегії забезпечення кібернетичної безпеки України та розробки теоретико-правових засад механізму забезпечення кібернетичної безпеки людини, суспільства, держави в сучасних умовах.

Положення дисертації можуть стати теоретичними орієнтирами для удосконалення нормотворчої та правозастосовної практики забезпечення кібербезпеки України, розвитку інформаційного права та юридичної науки. Отримані в ході дослідження результати дають підстави стверджувати про досягнення поставленої мети і реалізацію визначених завдань та сформулювати такі основні висновки:

1. Спираючись на отримані результати дослідження генезису правового регулювання кібербезпеки людини, суспільства й держави у роботі запропоновано авторське трактування терміна «*культура кібербезпеки*». Під цим терміном ми розуміємо систему переконань, уявлень та етичних норм щодо ведення інформаційної діяльності у кіберпросторі, знань, умінь і навичок із забезпечення кібербезпеки, а також вимоги до професійно-психологічних якостей осіб, що необхідні для безпечної інформаційної діяльності в кіберпросторі.

«Глобальну культуру кібербезпеки», зі свого боку, у роботі розглянуто як наднаціональну масову культуру кібербезпеки людини, суспільства, держави.

Водночас доведено, що основною *метою формування глобальної культури кібербезпеки* є досягнення такого стану соціальної взаємодії між суб'єктами інформаційної діяльності, коли заходи із забезпечення кібербезпеки стають повсякденною звичкою кожного користувача сервісів кіберпростору.

2. На основі понятійно-категоріального аналізу правового регулювання кібербезпеки України з'ясовано, що термін «кібербезпека» – похідний від родового терміна «безпека», відтак «кібербезпека» є частиною загальнішого поняття «безпека», що вирізняється специфічними особливостями, й одночасно має бути результатом синтезу поняття «безпека» та прикметника «кібернетична» (скороч. – «кібер»).

Базовою категорією у дослідженні кібербезпеки є категорія «безпека». В

основу авторського підходу до сутності категорії «кібербезпека» покладено наукові уявлення видатних учених сучасності, зокрема О. Довганя, В. Пилипчука, О. Баранова, І. Коржа, які поняття «кібербезпека» розглядають у соціальному розумінні «безпеки», що означає збалансований стан функціонування соціальної системи (людини, держави, світового співтовариства), антропогенних, природних систем тощо, за якого людина завдяки знанням про навколишнє природне середовище і тенденції його розвитку своїми діями спроможна своєчасно виявити та мінімізувати негативний вплив наявних і потенційних загроз або уникнути їх, що, з іншого боку, дає їй можливість зберігати систему своїх цінностей і забезпечувати подальший їхній розвиток. Зазначений підхід у дисертації взятий як базовий у дослідженні змісту кібербезпеки.

На цій теоретичній основі удосконалено такі категорії:

– «*кібербезпеку»* визначено як безпечність об’єктів кіберпростору й захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, у процесі чого забезпечено розвиток інформаційного суспільства, розвиток кіберкультури людини, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз безпеці України у кіберпросторі, а також постійний процес попередження й протидії відповідним загрозам;

– *«забезпечення кібербезпеки»* – це діяльність відповідних суб’єктів із досягнення такого стану захищеності життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, що унеможливлює його порушення;

– *кіберзагрози* – це такі явища, дії, чинники й умови, що становлять небезпеку для життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, яка полягає в можливості порушення властивостей одного чи декількох із зазначених складників;

– *кібератака* – це дії з метою порушення захищеності життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору.

Обґрунтовано гіпотезу, що сучасний рівень розвитку інформаційної сфери зумовлює потребу у перспективі виокремлення кібернетичної безпеки в самостійного виду безпеки, що дасть змогу, ураховуючи особливості відповідних систем і процесів управління, реалізувати правові, організаційні й технічні можливості захисних заходів. Це також передбачає підвищення вимог до захисту згаданих систем і процесів залежно від їхнього призначення, рівня, складу тощо.

3. Доведено, що кібернетична безпека – це також сукупність умов, які у фізичному, емоційно-психічному, духовно-освітньому, професійному, фінансовому, політичному й інших аспектах гарантовано забезпечують захищеність усіх компонентів інформаційних систем від якомога більшої кількості загроз і негативних впливів у кіберпросторі або ж від руйнівних наслідків у разі похибок, нещасних випадків, псування, аварій та іншої

шкоди в цій сфері.

Аргументовано, що до предмета вивчення безпекової науки стосовно кіберсередовища належать: природні, соціально-економічні, соціально-політичні та техногенні процеси в контексті їхнього розвитку, взаємодії й утворення нових об'єктів і явищ, та їхніх елементів з навколишнім середовищем задля виявлення існуючих і потенційних небезпек, оцінювання відповідних ризиків та розробки адекватних методів і способів протидії, а також розробки належної нормативної бази для належної правової регламентації вимог, методик, механізмів, алгоритмів, застосування яких гарантує досягнення мети захищеності інтересів людини, суспільства й держави від наявних і можливих загроз.

4. На основі теоретичного аналізу співвідношення кібербезпеки й інформаційної безпеки розроблено логічну схему підпорядкованості різного роду безпек, зокрема кібербезпеку визначено нами як складову частину інформаційної безпеки. Кібербезпека формується в реляційних відносинах із безпекою мереж, безпекою інтернету і безпекою додатків, а також здійснює підтримку безпеки критичної інформаційної інфраструктури у частині, що її стосується; кіберзлочинність і безпечну діяльність у кіберпросторі (насамперед дітей і молоді в інтернеті). Кіберзлочинність має вплив на інформаційну безпеку та, відповідно, кібернетичну безпеку. Безпечну діяльність у кіберпросторі визначається певним орієнтиром ідеальної поведінки.

У поняття «кібербезпека» входить широкий спектр практичних прийомів, інструментів і концепцій, тісно пов'язаних із технологіями інформаційної та операційної безпеки. Відмітна риса кібербезпеки полягає в тому, що вона передбачає використання інформаційних технологій в наступальних цілях для атак противника. Запропоновано, що кібербезпека повинна охоплювати не тільки заходи оборони та контрзахисту, а й наступу. Що стосується сучасного стану кібербезпеки України – її пріоритетним напрямом мають стати заходи активної оборони. Термін кібербезпека слід використовувати тільки для позначення практичних методів забезпечення безпеки, що поєднують у собі заходи наступального й оборонного характеру, які є сукупністю або системою інформаційних технологій, або ґрунтуються на них.

5. На основі аналізу базових категорій, що наведені в Законі України «Про основні засади забезпечення кібербезпеки України», виявлено низку невідповідностей, а також протиріч базисних категорій кібербезпеки. На цій основі обґрунтовано пропозиції визначити на законодавчому рівні такі поняття:

– «*стан захищеності*», яке є системоутворюючим до категорії «безпека» та її еквівалентом. Запропоновано під цим терміном розуміти наявність параметрів, відповідно до яких об'єкти кібербезпеки перебувають під захистом. Основними параметрами визначено дотримання прав особи в кіберпросторі, реалізація національних інтересів в інформаційній сфері, здатність суб'єктів забезпечення кібербезпеки діяти і застосовувати засоби

для усунення або зниження рівня небезпеки для об’єктів кібербезпеки та кіберзахисту;

– запропоновано у визначенні терміна «*кіберзлочин*» словосполучення «міжнародними договорами» замінити словосполученням «міжнародним правом». Зазначений підхід забезпечить єдність термінологічного тлумачення на рівні національного законодавства та міжнародного права;

– обґрунтовано, що законодавче визначення терміна «кіберзагроза» не співвідноситься за обсягом інформації, наведеної в терміні «кібербезпека», та не відповідає визначенню цього терміна. Адже кіберзагроза – це також злочинний акт, метою якого є пошкодження, викрадення цінних даних, доступ до несанкціонованих файлів або порушення цифрового життя загалом. Під кіберзагрозою слід також розуміти тактику, техніку та процедуру, що використовується під час кібератаки.

6. Досліджуючи систему суб’єктів забезпечення кібербезпеки України, запропоновано розглядати таку систему як органічне поєднання спільною метою державних і недержавних інституцій, а також інших суб’єктів, що беруть участь у здійсненні заходів, спрямованих на забезпечення кібербезпеки. У цьому контексті важливе значення має розвиток державно-приватного партнерства, яке може мати різні форми: обмін інформацією, консультації, експертизи, сприяння в захисті інформації з обмеженим доступом тощо. Першочерговим завданням сьогодення є розробка оптимальних механізмів співпраці між приватним сектором і державними органами у сфері забезпечення кібербезпеки України.

7. На основі системного підходу удосконалено критерії класифікації кіберзагроз в Україні, зокрема виокремлено нові критерії класифікації: загрози існуванню нації, за деструктивним впливом на основні сегменти національного кіберпростору, за посяганням на національні цінності кібербезпеки (життєво важливі інтереси людини і громадянина, суспільства та держави).

8. З огляду на аналіз правового регулювання кібербезпеки у зарубіжних країнах, запропоновано доповнити Положення про Національний координаційний центр кібербезпеки, затверджене Указом Президента України від 7 червня 2016 р. № 242/2016 у частині вдосконалення основних завдань органу. У цьому контексті пропонуємо розширити п. 3 зазначеного положення, додавши до основних завдань центру такі: упровадження в Україні стандартів безпеки мережевих й інформаційних систем; визначення критеріїв, за якими буде складатися перелік операторів базових послуг і провайдерів цифрових послуг; контроль за дотриманням мережевої нейтральності та міжнародних і європейських стандартів і заборон уведення окремих національних стандартів у сфері кібербезпеки, які не є сумісними з європейськими та міжнародними стандартами; аудит системи мережевої й інформаційної безпеки; організація та підтримка системи сповіщення про кіберінциденти, системи аудиту й упровадження заходів мережевої та інформаційної безпеки; забезпечення належного дотримання вимог щодо збереження конфіденційності, зокрема щодо персональних даних і захисту

комерційних інтересів операторів та провайдерів.

9. У межах дослідження правових засад кібербезпеки людини *інформаційну дієздатність,* як складову інформаційної правосуб'єктності, визначено як спроможність особи своїми діями в інформаційній галузі, у сфері використання кіберпростору набувати прав, брати на себе певні правові обов'язки, а також нести юридичну відповідальність у разі неправомірної поведінки.

10. На основі теоретичного аналізу правової природи відносин у процесі забезпечення кібернетичної безпеки людини комплексно досліджено усі її складові – суб'єкт (людина у глобальному інформаційному просторі, яка потребує належного правового регулювання своєї безпеки при користуванні кібернетичним простором), об'єкт (стан захищеності особи від внутрішніх і зовнішніх загроз під час використання кіберпростору) та зміст (сукупність прав та обов'язків усіх учасників зазначених суспільних відносин).

Удосконалено зміст поняття «кібернетична безпека людини», яке запропоновано розуміти як стан її захищеності, що визначається спроможністю особи протистояти внутрішнім і зовнішнім негативним інформаційним впливам, а також здатністю інформаційної держави й інформаційного суспільства забезпечувати її інформаційну безпеку.

Наголошено, що найбільш уразливим суб'єктом інформаційних правовідносин є людина. Зумовлено це постійним виникненням нових викликів і загроз інформаційній безпеці особи, пов'язаних із недосконалістю інформаційно-телекомунікаційних технологій, інформаційно-психологічними впливами, використанням інформації для досягнення геополітичних, терористичних та інших протиправних, руйнівних цілей. Отже, в умовах глобального інформаційного суспільства особистість у процесі задоволення своїх потреб найбільш яскраво виявляє свою соціальну складову, і, з огляду на нові безпекові виклики й загрози, змушена на основі культури інформаційної безпеки виробляти відповідні заходи протидії.

Визначено декілька основних критеріїв класифікації загроз кібербезпеці людини. Зокрема: за впливом на національну свідомість; за посяганням на національні цінності; за природою виникнення.

11. Усебічне дослідження новітніх викликів і загроз кібербезпеки в глобальному інформаційному суспільстві, а також небезпечних тенденцій у цій сфері дало змогу виокремити критерії їх можливої класифікації: джерело загрози (виклику), залежність від джерела загрози, розташування джерела загрози стосовно об'єкта, характер впливу. На цій основі, з метою вдосконалення вітчизняної системи правового забезпечення кібернетичної безпеки людини, запропоновано авторську класифікацію видів відповідних викликів і загроз. Зокрема, з огляду на значущість соціальних мереж, визначено джерела загроз в інтернеті, а саме: сайти, що становлять небезпеку для особистості (мають на меті вплив на свідомість індивіда, рекламовані задля отримання зиску та ін.); спам, тотальне розсилання реклами й іншої інформації без бажання користувача тощо.

Крім того, вивчення сучасних інформаційно-телекомунікаційних технологій дало змогу виявити специфічну групу загроз, пов'язаних із цифровою економікою, фінансово-банківською сферою (зокрема, з обігом електронних грошей, криптовалют – BitCoin, LitCoin, OneCoin та ін.), конфіденційністю персональних даних (загрози від найсучаснішої онлайн-реклами Real-TimeBidding (RTB), спеціальних файлів cookie тощо).

12. Запропоновано теоретичну модель Концепції кібернетичної безпеки людини, а також потребу долучення до її складу документів стратегічного планування України. Подано пропозиції зі структурно-змістовного наповнення зазначеної концепції, зокрема її головні принципи формування, завдання, механізми реалізації й очікувані результати державної політики у сфері забезпечення інформаційної безпеки особи. Крім того, обґрунтовано мету гармонізації інформаційних відносин, підвищення відповідальності держави в цій сфері, створення умов для формування сприятливого кібернетичного середовища як стратегічну спрямованість концепції.

Визначено, що доцільність розробки Концепції кібернетичної безпеки людини зумовлена необхідністю вдосконалення національного законодавства про кібернетичну безпеку в сенсі закріплення поняття «кібернетична безпека людини», правового регулювання кібернетичної безпеки людини, формування системи забезпечення безпеки особи в інформаційній сфері як сукупності відповідних сил і засобів.

13. Зазначено, що недосконалість вітчизняного інформаційного законодавства, неузгодженість системи міжнародної кібербезпеки, брак дійового інструментарію протидії викликам і загрозам в інформаційному (кібернетичному) просторі залишаються основними чинниками, які, з огляду на динаміку відповідних правопорушень, а також викликів і загроз, що негативно впливають на головного суб'єкта інформаційних відносин – людину, здійснюють значний вплив на характер цих відносин у суспільстві.

14. Теоретичний аналіз основних концепцій інформаційного суспільства дозволив з'ясувати, що реальні загрози глобальному інформаційному суспільству на сучасному етапі сконцентровані в таких сферах: мілітаризація кіберпростору, розв'язування широкомасштабних інформаційних війн, поширення екстремістських і маніпулятивних матеріалів, деструктивні інформаційно-психологічні впливи на індивідуальну, групову й суспільну свідомість тощо. На цій основі обґрунтовується висновок, що успішне розв'язання зазначених глобальних соціально-економічних, політичних, безпекових та інших проблем можливе тільки в разі об'єднаних зусиль усього світового співтовариства.

15. Досліджуючи роль правового чинника в запобіганні кіберзагрозам сучасному українському суспільству, доведено необхідність створення оптимального співвідношення між правом особи на захист від зловживань її персональними даними й іншою конфіденційною інформацією і небезпекою несанкціонованого доступу до неї. Такий підхід визначається важливим аспектом інформаційної політики всіх держав у сучасних умовах.

На сучасному етапі розвитку суспільство потребує (у межах прийнятої

моделі кібернетичної безпеки) розроблення державної соціальної стратегії застосування інформаційних технологій і використання кіберпростору, що вказувала б на головні пріоритети прогресивного розвитку суспільства і закладала базис для створення механізму координування соціальних норм. На цій основі правове забезпечення кібернетичного середовища розглянуто і як об'єкт морально-правового регулювання. Сутність останнього полягає в налагодженні суспільних відносин, урегулювання яких базується на нормах права та моралі.

16. Доведено та науково обґрунтовано, що важливим елементом забезпечення кібернетичної безпеки України на сучасному етапі державотворення має стати освітня і просвітницька діяльність за активного й дієвого державного сприяння. Для продуктивної інформаційної взаємодії конче потрібна належна освіченість користувачів та їхня поінформованість щодо відповідних прав й обов'язків. Провідною ідеєю сучасної інформаційно-технологічної освіти є гуманізм, усвідомлення того, що головна мета розвитку суспільства – людина, її фізичне, інтелектуальне, духовне і психологічне зростання, яке визначає її потреби, пріоритети, інтереси й, урешті-решт, сенс життя.

17. Концептуальними засадами правового регулювання кібербезпеки України на сучасному етапі розвитку глобальних інформаційних процесів визначено: розвиток державно-приватного партнерства у сфері взаємодії державних органів із громадськими організаціями та громадянами з метою забезпечення кібербезпеки України; інформаційно-просвітницьку, ідеологічну й освітню роботу із протидії радикальній ідеології та екстремізму; удосконалення нормативно-правового забезпечення протидії використанню інтернету в терористичних й екстремістських цілях, а також забезпечення національних інтересів суверенної України в інформаційній сфері; розвиток міжнародного чинника з метою утвердження України як повноправного учасника глобальних інформаційних процесів заради подальшої інтеграції в НАТО та поліпшення іміджу нашої держави серед міжнародних партнерів; створення, розвиток і забезпечення безпеки національних інформаційних ресурсів; практичну реалізацію на рівні законодавчого забезпечення національних інтересів України в кіберсфері.

18. З урахуванням міжнародного досвіду та на основі аналізу національної практики запропоновано основні складові національних інтересів України в кіберсфері: 1) дотримання конституційних прав і свобод людини та громадянина у сфері отримання інформації та користування нею, сприяння духовному оновленню держави, збереження та зміцнення моральних цінностей суспільства, традицій гуманізму та патріотизму, наукового і культурного потенціалу країни; 2) інформаційне забезпечення державної політики, що пов'язане з доведенням до міжнародної громадськості та народу України правдивої інформації про державну національну політику, офіційну позицію держави щодо соціально-значимих подій держави та міжнародного життя, із наданням громадянам доступу до відкритих національних інформаційних ресурсів; 3) застосування новітніх

інформаційних технологій, створення вітчизняної індустрії інформації, зокрема й індустрії засобів інформатизації, телекомунікації та зв'язку, задоволення потреб внутрішнього ринку її продукцією, а також забезпечення накопичення, ефективного використання та збереження національних інформаційних ресурсів; 4) захист інформаційних ресурсів від несанкціонованого доступу, забезпечення безпеки телекомунікаційних й інформаційних систем, як створюваних, так і тих, що функціонують на території України.

19. Щодо пріоритетів розвитку правових основ державної політики України у сфері кібербезпеки та правового регулювання окремих елементів інформаційної інфраструктури акцентовано увагу, що в Україні досі не ухвалений Закон «Про критичну інфраструктуру і її захист», не розроблені норми кіберзахисту, рекомендації щодо їхньої реалізації, методики контролю за їхнім дотриманням для недержавного сектора, хоча варто визнати, що уповноваженими державними органами України робота в цьому напрямі ведеться.

Обґрунтовано доцільність прискорення процесу прийняття ініційованого Національною поліцією України і СБ України спільно розробленого законопроекту про внесення змін і доповнень до Кримінального процесуального кодексу України в частині, що стосується цифрових доказів.

Доведено позицію стосовно необхідності додати до основних термінів, що містяться в законі України «Про основні засади забезпечення кібербезпеки України», поняття «інформаційної зброї». У широкому розумінні, з погляду інформаційного права, під інформаційною зброєю пропонуємо розуміти інформаційні технології, засоби і методи, призначені для ведення інформаційної війни. Також обґрунтовано необхідність доповнити згаданий закон текстом такого змісту: «*основною загрозою в галузі міжнародної інформаційної безпеки є використання інформаційно-комунікаційних технологій для вчинення різних протиправних дій, зокрема і як інформаційну зброю у військово-політичних цілях. Умови, що створюють можливості протидії загрозам використання ІКТ, належать до основних напрямів державної політики*».

На основі аналізу основних підходів державної політики з реформування СБ України, доведено, що з метою підвищення ефективності організаційного забезпечення кіберзахисту об'єктів критичної інфраструктури та критичної інформаційної інфраструктури серед функціональних завдань СБ України необхідно передбачити такі заходи: здійснювати правове регулювання діяльності національного координаційного центру кібербезпеки; вносити пропозиції про вдосконалення нормативно-правового забезпечення; оцінювати безпеку критичної інформаційної інфраструктури; координувати дії суб'єктів критичної інформаційної інфраструктури в напрямі обміну і надання інформації про комп'ютерні інциденти, щодо використання коштів, призначених для запобігання, виявлення і ліквідації наслідків комп'ютерних атак та реагування на

комп'ютерні інциденти.

20. Запропоновано такі перспективні напрями подальших наукових пошуків: дослідження у сфері оцінювання загроз кібернетичній безпеці України; визначення місця кібернетичної безпеки України в системі чинників національної безпеки; дослідження основних завдань кібернетичної безпеки України і напрямів її функціонування; розробки критеріїв оцінки негативного впливу на кібернетичну безпеку України; дослідження складових ІТ-права та його місця в національній і міжнародній системі права; обґрунтування правових основ функціонування штучного інтелекту.

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Наукові праці, в яких опубліковані основні наукові результати дисертації:

Монографії:

1. Тарасюк А.В. Кібербезпека України на сучасному етапі державотворення: теоретико-правові основи : монограф. Одеса : Фенікс, 2020. 404 с.

2. Тарасюк А.В. Доказування у справах про несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку у стадії досудового розслідування : монограф. Х. : Вид-во «ФІНН», 2011. 192 с.

Підрозділи у колективних монографіях:

3. Пилипчук В.Г., Брижко В.М., Доронін І.М. та ін. Захист прав, приватності та безпеки людини в інформаційну епоху : монографія; за заг. ред. акад. НАПрН України В.Г. Пилипчука. Київ-Одеса : Фенікс, 2020. 260 с., підр. 5.2.

Статті в наукових фахових виданнях України з юридичних наук, зокрема і в тих, що зареєстровані у міжнародних наукометричних базах:

4. Довгань О.Д., Тарасюк А.В. Глобальна культура кібербезпеки в системі запобігання кіберзлочинності в Україні. *Інформація і право*. 2018. № 3 (26). С. 94–103.

5. Довгань О.Д., Тарасюк А.В. Корпоративна культура кібербезпеки суб'єктів наукової та науково-технічної діяльності *Інформація і право*. 2018. № 2 (25). С. 51–61.

6. Тарасюк А.В. Співвідношення інформаційної та кібернетичної безпеки. *Інформація і право*. 4(31)/2019. С. 73–82.

7. Тарасюк А.В. Досвід забезпечення кібербезпеки у зарубіжних країнах. *Науковий вісник публічного та приватного права* : зб. наук. праць. 2019. № 4. С. 204–209.

8. Тарасюк А.В. Понятійно-категоріальний синтез правового забезпечення кібербезпеки України. *Порівняльно-аналітичне право*. №5. 2019. С. 296-298. URL : http://www.pap.in.ua/5_2019/77.pdf.

9. Тарасюк А.В. Стан правового забезпечення кібербезпеки в Україні. *Наукові записки ЛУБП*. Серія «Право». 2019. Вип. 23. С. 201–206.

10. Тарасюк А.В. Система суб'єктів забезпечення кібербезпеки в Україні. *Вчені записки Таврійського національного університету імені В.І. Вернадського.* Серія «Юридичні науки». 2020. Т. 31 (70), № 2. С. 119–124.

11. Тарасюк А.В. Пріоритети правового забезпечення кібербезпеки в Україні на сучасному етапі. *Прикарпатський юридичний вісник*. 2020. № 1. С. 133–136.

12. Довгань О.Д., Тарасюк А.В. Протидія загрозам кібербезпеці держави на глобальному рівні. *Інформація і право*. 2020. № 2. С. 85–98.

13. Тарасюк А.В. Системний підхід у дослідженні правових основ кібербезпеки. *Прикарпатський юридичний вісник*. 2020. № 2. С. 108–111.

14. Тарасюк А.В. Методологічні підходи до вивчення проблеми безпеки людини у кіберпросторі. *Підприємництво, господарство і право*. 2020. № 7. С. 254–258.

15. Тарасюк А.В. Забезпечення кібернетичної безпеки людини: міжнародно-правовий аспект. *Юридичний вісник*. 2020. № 3. С. 254–261.

16. Тарасюк А.В. Місце концепції «суспільства знань» у процесах забезпечення кібернетичної безпеки. *Юридичний науковий електронний журнал*. 2020. № 6. С. 156–169. URL : http://www.lsej.org.ua/6_2020/40.pdf.

17. Тарасюк А.В. Правовий чинник у попередженні кіберзагроз на міжнародному та національному рівнях. *Вісник Запорізького національного університету.* Юридичні науки. 2020. № 4. Т. 1. С. 168–173.

18. Тарасюк А.В. Теоретико-правове підґрунтя інформаційної етики у системі забезпечення кібербезпеки. *Правова позиція*. 2020. № 4 (29). С. 48–52.

19. Довгань О.Д., Тарасюк М.В. Національні інтереси України в кібернетичній сфері. *Інформація і право*. 2021. № 1. С. 134-142

Статті в наукових періодичних виданнях із юридичних наук інших держав:

20. Тарасюк А.В. Актуальні проблеми забезпечення кібербезпеки на глобальному та національному рівнях. *Visegrad Journal on Human Rights*. 2020. № 1. С. 167–172.

21. Тарасюк А.В. Актуальні питання правового забезпечення кібербезпеки України. *Recht der Osteuropäischen Staaten*. 4/2019. С. 164–168.

22. Тарасюк А.В. Пріоритети забезпечення кібербезпеки: досвід окремих країн. *Інтернаука* : міжнар. наук. журн. Серія «Юридичні науки». 2020. 4. С. 42–49. URL : https://doi.org/10.25313/2520-2308-2020-4-5818.

23. Тарасюк А.В. Окремі аспекти соціального чинника в забезпеченні кібербезпеки суспільства. *KELM (Knowledge, Education, Law, Management)*. 2020. № 3 (31). С. 206–211.

24. Тарасюк А.В. Місце та роль України у глобальних інформаційних процесах: питання кібербезпеки. *Інтернаука* : міжнар. наук. журн. Серія

«Юридичні науки». 2020. XI (43). С. 46–52. URL : https://doi.org/10.25313/2520-2308-2020-11-6528.

25. Тарасюк А.В. Пріоритети національної політики України у сфері забезпечення міжнародної кібербезпеки. *Visegrad Journal on Human Rights*. 2021. № 1. С. 48-53.

Наукові праці, які засвідчують апробацію матеріалів дисертації:

26. Тарасюк А.В. Актуальні питання протидії кіберзлочинності в сучасних умовах. *Досудове розслідування: актуальні проблеми та шляхи їх вирішення* : мат. постійно діючого наук.-практ. Семінару. м. Харків, 26 жовт. 2018 р. 2018. С. 251–254.

27. Тарасюк А.В. Кібербезпека – один із важливих напрямків захисту держави. *Правове забезпечення оперативно-службової діяльності: актуальні проблеми та шляхи їх вирішення* : мат. постійно діючого наук.-практ. семінару, м. Харків, 23 трав. 2019 р. / редкол.: С.О. Гриненко (голов. ред.) та ін. Х. : Право, 2019. Вип. 10. С. 44–47.

28. Тарасюк А.В. Законодавчі підходи до кібернетичної безпеки України. *Актуальні проблеми правових наук в євроінтеграційному вимірі* зб. мат. Міжнародної наук.-практ. конф. м. Харків, 20–21 груд. 2019 р. С. 87–90.

29. Тарасюк А.В. Пріоритетні питання забезпечення кібербезпеки України. *Освіта і наука у сфері національної безпеки: проблеми та пріоритети розвитку* : зб. мат. III Міжнародної наук.-практ. конф., м. Острог, 14 черв. 2019 р. / упорядн.: С.О. Дорогих, І.М. Доронін, О.Д. Довгань, О.В. Лебединська, В.Г. Пилипчук, О.Г. Радзієвська, М.С. Романов ; НУОА, НДІІП НАПрН України. К. : ТОВ «Вид. дім «АртЕк», 2019. С. 181–185.

30. Тарасюк А.В. Новації у сфері кібербезпеки великої Британії. *Актуальні проблеми управління інформаційною безпекою держави* : зб. тез наук. доп. X Всеукраїнської наук.-практ. конф. м. Київ, 4 квіт. 2019 р. С. 217–218.

31. Тарасюк А.В. Окремі питання політики європейських країн щодо правового забезпечення кібербезпеки. *Теоретичні та практичні проблеми правового регулювання суспільних відносин* : зб. мат. Міжнародної наук.-практ. конф. м. Харків, 17–18 січ. 2020 р. С. 61–64.

32. Тарасюк А.В. Теоретико-правові конструкції правового забезпечення кібербезпеки України. *Реформування національного та міжнародного права: перспективи та пріоритети : зб. мат. Міжнародної наук.-практ. конф.* м. Одеса, 17–18 січ. 2020 р. С. 107–110.

33. Тарасюк А.В. Кіберпростір як об’єкт кібербезпеки держави. *Нові завдання та напрями розвитку юридичної науки у XXI столітті* : зб. мат. Міжнародної наук.-практ. конф. м. Одеса 21–22 лют. 2020 р. С. 115–118.

34. Тарасюк А.В. Окремі питання забезпечення кібербезпеки: досвід Європейського Союзу. *Міжнародне та національне законодавство: способи удосконалення* : зб. мат. Міжнародної наук.-практ. конф. м. Дніпро 3–4 квіт. 2020 р. С. 159–163.

35. Тарасюк А.В. Онтологічні засади поняття «кібербезпека». *Управління інформаційною безпекою* : зб. мат. Науково-практичної конф. НА СБУ. 15 травня 2020 р. К., С. 197-199

36. Тарасюк А.В. Окремі питання функціональних завдань суб'єктів забезпечення кібербезпеки. *Міжнародні та національні правові виміри забезпечення стабільності* : зб. мат. Міжнародної наук.-практ. конф. м. Львів, 17–18 квіт. 2020 р. С. 72–76.

37. Тарасюк А.В. Окремі аспекти співпраці державного та приватного секторів безпеки у забезпеченні кібербезпеки. *Права людини та проблеми організації і функціонування публічної адміністрації в умовах становлення громадянського суспільства в Україні* : зб. мат. Міжнародної наук.-практ. конф. м. Запоріжжя, 24–25 квіт. 2020 р. С. 77–81.

38. Тарасюк А.В. Міжнародно-правові засади протидії кіберзагрозам *Розбудова правової держави в Україні: реалії та перспективи* : зб. мат. Міжнародної наук.-практ. конф. Одеса, 29 трав. 2020 р. С. 133–135.

39. Тарасюк А.В. Забезпечення кібербезпеки України як пріоритетне завдання цифрової дипломатії. *Кібербезпека в Україні: правові та організаційні питання» :* зб. мат. ІІ Міжнародної наук.-практ. конф. м. Одеса, 26 листоп. 2020 р. С. 23–24.

40. Тарасюк А.В. Питання кібербезпеки України на сучасному етапі розвитку глобальних інформаційних процесів. *Соціальна і цифрова трансформація: теоретичні та практичні проблеми правового регулювання* : мат. наук.-практ. конф., м. Київ, 10 груд. 2020 р. / упоряд.: О.А. Баранов, В.М. Фурашев, С.О. Дорогих. К. : Фенікс, 2020. С. 241–246.

АНОТАЦІЯ

Тарасюк А.В. Теоретико-правові основи забезпечення кібербезпеки України. – *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. – Державна наукова установа «Інститут інформації, безпеки і права Національної академії правових наук України». – Київ, 2021.

Дисертацію присвячено дослідженню проблеми правового забезпечення кібербезпеки України, також у роботі здійснено порівняння відповідних практик у європейських країнах. На цьому теоретичному та емпіричному ґрунті у дисертаційному дослідженні запропоновано розв'язання актуальної наукової проблеми – розроблення концептуальних правових засад забезпечення кібербезпеки України, та надані практичні рекомендації щодо вдосконалення механізмів її реалізації.

Розроблено логічну схему співвідношення кібернетичної та інформаційної безпеки, а також підпорядкованості різного роду безпек. Запропоновано розробити Концепцію кібернетичної безпеки людини та подано її обґрунтування. Визначено структуру та зміст концепції, а також потребу долучення до її складу документів стратегічного планування

України. Подано пропозиції зі структурно-змістовного наповнення зазначеної концепції, зокрема її головні принципи формування, завдання, механізми реалізації й очікувані результати державної політики у сфері забезпечення інформаційної безпеки людини. Крім того, обґрунтовано мету гармонізації інформаційних відносин, підвищення відповідальності держави в цій сфері, створення умов для формування сприятливого кібернетичного середовища як стратегічну спрямованість концепції.

Визначено забезпечення кібернетичної безпеки як самостійного комплексного міжгалузевого інституту інформаційного права. Охарактеризовано його властивості.

Розроблено концептуальні засади правового забезпечення кібербезпеки України на сучасному етапі розвитку глобальних інформаційних процесів. Виокремлено та систематизовано складові національних інтересів України в кіберпросторі.

Запропоновано нові механізми співпраці між приватним сектором і державними органами у сфері забезпечення кібербезпеки України. Доведено, що кіберпростір є одночасно об’єктом захисту і джерелом загроз.

Ключові слова: кібербезпека, кіберзагрози, забезпечення кібербезпеки, кібербезпека людини, кібербезпека суспільства, кібербезпека України.

АННОТАЦИЯ

Тарасюк А.В. Теоретико-правовые основы обеспечения кибербезопасности Украины. – ***Квалификационный научный труд на правах рукописи.***

Диссертация на соискание ученой степени доктора юридических наук по специальности 12.00.07 – административное право и процесс; финансовое право, информационное право. – Государственное научное учреждение «Институт информации, безопасности и права Национальной академии правовых наук Украины». – Киев, 2021.

Диссертация посвящена исследованию проблемы правового обеспечения кибербезопасности Украины, также в работе проведено сравнение соответствующих практик в европейских странах. На этой теоретической и эмпирической почве в диссертационном исследовании предложено решение актуальной научной проблемы – разработка концептуальных правовых основ обеспечения кибербезопасности Украины, и даны практические рекомендации по совершенствованию механизмов ее реализации.

Разработана логическая схема соотношения кибернетической и информационной безопасности, а также подчиненности разного рода безопасностей. Предложено разработать Концепцию кибернетической безопасности человека и представлены ее обоснования. Определена структура и содержание концепции, а также потребность добавления в ее состав документов стратегического планирования Украины. Представлены предложения по структурно-содержательном наполнении указанной

концепции, в частности ее главные принципы формирования, задания, механизмы реализации и ожидаемые результаты государственной политики в сфере обеспечения информационной безопасности человека. Кроме того, обосновано цель гармонизации информационных отношений, повышение ответственности в этой сфере, создание условий для формирования благоприятной кибернетической среды как стратегическую направленность концепции.

Определено обеспечение кибернетической безопасности как самостоятельного комплексного межотраслевого института информационного права. Охарактеризованы его свойства.

Разработаны концептуальные основы правового обеспечения кибербезопасности Украины на современном этапе развития глобальных информационных процессов. Выделены и систематизированы составляющие национальных интересов Украины в киберпространстве.

Предложены новые механизмы сотрудничества между частным сектором и государственными органами в области обеспечения кибербезопасности Украины. Доказано, что киберпространство выступает одновременно объектом защиты и источником угроз.

Ключевые слова: кибербезопасность, киберугрозы, обеспечение кибербезопасности, кибербезопасность человека, кибербезопасность общества, кибербезопасность Украины.

SUMMARY

Tarasyuk A.V. Theoretical and legal bases of cyber security of Ukraine. – ***Qualifying scientific work as a manuscript.***

The dissertation on competition of a scientific degree of the doctor of legal sciences on a specialty 12.00.07 – administrative law and process; finance law; information law. – State Scientific Institution "Institute of Information, Security and Law of the National Academy of Legal Sciences of Ukraine". – Kyiv, 2021.

The dissertation is devoted to the research of the problem of legal provision of cyber security of Ukraine, the corresponding practices in the European countries are comparatively considered. On this theoretical and empirical basis, the dissertation proposes a solution to a topical scientific problem - the development of conceptual legal framework for cybersecurity in Ukraine and practical recommendations for improving the mechanisms of its implementation in Ukraine.

A logical scheme of the relationship between cyber and information security, as well as the subordination of various types of security. It is proposed and substantiated to develop the Concept of human cyber security. Its structure and content are determined, as well as the need to include in its composition the strategic planning documents of Ukraine. The structural and substantive content of this Concept is proposed, in particular its main principles of formation, tasks, implementation mechanisms and expected results of the state policy in the field of information security. In addition, the goal of harmonization of information relations, increasing the responsibility of the state in this area, creating conditions

for the formation of a favorable cyber environment as a strategic direction of the Concept is substantiated.

The provision of cyber security as an independent complex intersectoral institute of information law is determined. Its properties are described. The role of the legal factor as a single regulator of processes and relations in the field of global electronic network, IoT development, robotics intellectualization, use of cybersystems, microchips, hybrids, nanotechnologies, their implementation in information management processes, human-government interaction, in everyday life has been improved "digital person".

Conceptual bases of legal support of cybersecurity of Ukraine at the present stage of development of global information processes are developed. The components of Ukraine's national interests in cyberspace are singled out and systematized.

New mechanisms of cooperation between the private sector and public authorities in the field of cyber security of Ukraine are proposed. The following priority areas have been identified: development of cyber intelligence, cyber security audit, mutual exchange of information on cyber threats, replacement of ND TCI with a more effective and modern basic standard and introduction of industry standards of cyber security, creation of industry centers for responding to cyber incidents (SOC) attacks (ISAC), the creation of independent platforms for cooperation on the basis of educational institutions – cybercenters, in order to effectively combat cyber threats.

The approach to the system-functional analysis of the subjects of cyber security of Ukraine has been improved, in terms of development of public-private partnership, expansion of functional powers of the National Coordination Center for Cyber Security, improvement of functional tasks of the Security Service of Ukraine. Cyberspace has been shown to be both a source of protection and a source of threats. On this basis, in the priority of cybersecurity levels (security of man, society and state, which is based on the constitutional principles of protection of vital interests of these entities), in relation to cybersecurity argued to give priority to state interests, as it directly affects the interests of individual and society. Ensuring the cyber security of the state is a prerequisite for personal and public cyber security.

Key words: cybersecurity, cyberthreats, cybersecurity, human cybersecurity, cybersecurity of society, cybersecurity of Ukraine.

Гарнітура Таймс. Формат 60х84/16.
Наклад 100. Папір офсетний. Ум.-др. арк. 1,9.
Підписано до друку 05.04.2021. Замовлення 159.

Надруковано в «МП Леся».
Свідоцтво про внесення до Державного реєстру
суб'єктів видавничої справи серія ДК № 892 від 08.04.2002.
«МП Леся»
03148, Київ, а/с 115.
Тел./факс: (066) 60-50-199, (098) 455-41-17
E-mail: lesya3000@ukr.net