

До спеціалізованої вченої ради Д 26.501.01

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

## Відгук

доктора юридичних наук, доцента Заярного Олега Анатолійовича на  
дисертаційну роботу Тарасюка Анатолія Васильовича на тему:  
**«Теоретико-правові основи забезпечення кібербезпеки України», подану на  
здобуття наукового ступеня доктора юридичних наук за спеціальністю  
12.00.07 – адміністративне право і процес, фінансове право; інформаційне  
право**

Актуальність теми дисертації обумовлена назрілою необхідністю концептуального переосмислення теоретико-правових основ забезпечення кібербезпеки України виходячи з сучасних процесів цифрової трансформації та правової реформи, що тривають у нашій державі.

Побудова інформаційного суспільства в Україні, міжнародна конкуренція, глобалізація інформаційних процесів, суттєве зростання ролі інформаційної інфраструктури у різних сферах суспільного життя неодмінно сприяють ефективному соціально-економічному розвитку, задоволенню конституційних прав на інформацію, однак, разом з цим, інформаційні системи публічної та приватної сфер стають надзвичайно вразливими від реалізації кіберзагроз та кібератак.

У сучасних умовах кібербезпека набуває дедалі більшої ваги та стає одним із найважливіших елементів національної та інформаційної безпеки. При забезпеченні належного рівня кібербезпеки можливим є сталий розвиток інформаційного суспільства та цифрового середовища, а також захист життєво важливих інтересів людини, громадянини, суспільства та держави під час використання кіберпростору.

У свою чергу, заходи із забезпечення кібербезпеки України жодним чином не можуть суперечити принципу гарантування прав та свобод людини і громадянина, в тому числі права на недоторканність приватного життя, свободи спілкування, що закріплені ст. 12 Загальної декларації прав людини, ст. 8 Конвенції про захист прав людини і основоположних свобод, а також ст. ст. 32, 34 Конституції України.

Аналіз інформаційного законодавства України, наукових джерел, правозастосованої практики суб'єктів владних повноважень, а також судової практики дає підстави стверджувати, що нинішній стан розв'язання проблем правового забезпечення кібербезпеки України свідчить про потребу розроблення якісно нових підходів до розуміння теоретико-правових зasad подальшого удосконалення цього механізму.

Про актуальність проблематики дисертаційного дослідження Тарасюка Анатолія Васильовича свідчить також триваюча в юридичній літературі дискусія щодо засобів і форм правового забезпечення кібербезпеки України в умовах триваючої гібридної війни з Російською федерацією, цифровими трансформаціями процесів державного управління, національної економіки, освіти, співвідношення їх із приватно-правовими інструментами забезпечення стану захищеності інтересів суспільства і окремих осіб у кібернетичному просторі.

Підготовлена Тарасюком Анатолієм Васильовичем дисертаційна робота є одним із перших у вітчизняній правничій науці комплексним дослідженням теоретико-правових основ забезпечення кібернетичної безпеки людини, суспільства, держави, на підставі якого сформульовано нові наукові положення, висновки та пропозиції.

Ступінь обґрунтованості наукових положень, висновків, рекомендацій, викладених в дисертаційній роботі.

Чітко визначивши об'єкт і предмет наукового дослідження (с. 29, 30 дисертації, с. 6, автореферату), дисертант визначив метою дисертаційного дослідження, 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 кібернетичної безпеки України та розробки теоретико-правових зasad механізму забезпечення кібернетичної безпеки людини, суспільства, держави в сучасних умовах (с. 28 дисертаційної роботи, с. 5 автореферату).

Завдяки вирішенню комплексу складних теоретико-прикладних проблем, зокрема: дослідженню генезису наукових поглядів на забезпечення кібербезпеки України, з'ясуванню змістової сутності основних понять у національному законодавстві, визначеню особливостей співвідношення кібербезпеки та інформаційної безпеки на сучасному етапі, дослідженню методологічних засад правового забезпечення кібербезпеки України, а також стану правового регулювання кібербезпеки в Україні, характеристиці систему суб'єктів забезпечення кібербезпеки в Україні та дослідженню практики правового регулювання їхньої діяльності, вивченю питання протидії кіберзагрозам на національному та глобальному рівнях, аналізу відповідного досвіду законодавчого забезпечення зарубіжних країнах, дослідженню загроз кібербезпеці людини під час використання кіберпростору, , особливостей забезпечення кібербезпеки людини на міжнародному рівні, узагальненню теоретичних підходів до аналізу концепцій інформаційного суспільства, визначеню теоретико-правового підґрунтя системи соціального регулювання в інформаційному суспільстві, виокремленню концептуальних засад правового регулювання кібербезпеки України на сучасному етапі розвитку глобальних інформаційних процесів, обґрунтуванню конкретних пріоритетів розвитку правових основ державної політики України у сфері кібербезпеки, розробленню напрямів правового регулювання окремих елементів інформаційної інфраструктури на національному та міжнародному рівнях забезпечення

кібербезпеки (с. 28 – 29 дисертаційної роботи, с. 5, 6 автореферату), дисидентом була досягнута поставлена мета проведеного дослідження.

Це сталося за допомогою і завдяки вмілому використанню здобувачем загально-наукових та спеціальних методів наукового пізнання, зокрема: 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 (підрозділи 1.1–1.4). Історичний метод дав змогу дослідити генезис теорій і концепцій забезпечення кібернетичної безпеки України (підрозділ 1.1). Використання аналітичного методу сприяло класифікації загроз кібернетичній безпеці України, розробці механізмів їхній протидії (підрозділи 2.4, 2.5, 3.2, 4.2, 5.4), а також аналізу функціонування суб'єктів забезпечення кібернетичної безпеки України (підрозділ 2.3). Порівняльно-правовий метод покладено в основу дослідження міжнародного досвіду забезпечення кібернетичної безпеки (підрозділи 2.5, 4.3, 5.2). Формально-юридичний метод застосовано при тлумаченні норм права для з'ясування їхньої сутності, змісту та вираженої в них волі законодавця (підрозділи 2.1, 3.1). Структурно-функціональний аналіз дав змогу визначити відповідність нормативно-правових актів, з якими асоційована сучасна система правового забезпечення кібернетичної безпеки України, реальним суспільним відносинам у цій сфері та міжнародним стандартам (підрозділи 5.2, 5.3). Використання індуктивного методу, методів правового моделювання та прогнозування дало змогу підтвердити висновок про необхідність удосконалення правового забезпечення кібернетичної безпеки України (підрозділи 5.3, 5.4).

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 (підрозділи 1.1–1.4). Історичний метод дав змогу дослідити генезис теорій і концепцій забезпечення кібернетичної безпеки України (підрозділ 1.1). Використання аналітичного методу сприяло класифікації загроз кібернетичній безпеці України, розробці механізмів їхній протидії (підрозділи 2.4, 2.5, 3.2, 4.2, 5.4), а також аналізу функціонування суб'єктів забезпечення кібернетичної безпеки України (підрозділ 2.3). Порівняльно-правовий метод покладено в основу дослідження міжнародного досвіду забезпечення кібернетичної безпеки (підрозділи 2.5, 4.3, 5.2). Формально-юридичний метод застосовано при тлумаченні норм права для з'ясування їхньої сутності, змісту та вираженої в них волі законодавця (підрозділи 2.1, 3.1). Структурно-функціональний аналіз дав змогу визначити відповідність нормативно-правових актів, з якими асоційована сучасна система правового забезпечення кібернетичної безпеки України, реальним суспільним відносинам у цій сфері та міжнародним стандартам (підрозділи 5.2, 5.3). Використання індуктивного методу, методів правового моделювання та прогнозування дало змогу підтвердити висновок про необхідність удосконалення правового забезпечення кібернетичної безпеки України (підрозділи 5.3, 5.4).

Дисертація А. В. Тарасюка виконана 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 р. № 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» (ДР № 0116U007745).

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

Структура дисертації зумовлена метою й завданнями дослідження та складається зі вступу, п'яти розділів, що містять 15 підрозділів, висновків до кожного розділу та загальних висновків, списку використаних джерел і додатків. Загальний обсяг дисертації становить 462 сторінки, з яких основного тексту – 392 сторінки. Список використаних джерел розміщено на 42 сторінках (410 найменувань), додатки – на 8 сторінках.

Достовірність і новизна наукових положень, висновків, рекомендацій, сформульованих у дисертації.

Усі розділи та підрозділи роботи за своїм змістом і висновками, перспективами подальшого дослідження і використання для розвитку доктрини правового забезпечення кібербезпеки України, науки інформаційного права, законодавства України у відповідній сфері правового регулювання, слід вважати вагомими і вдало викладеними.

Дисертація виконана здобувачем самостійно з використанням останніх досягнень теорії права, інформаційного права. Усі сформульовані в ній положення і висновки обґрунтовано на основі особистих досліджень автора. Ідеї та розробки дисертації належать автору.

При цьому Розділи 1 та 2, які присвячені теоретико-методологічним засадам дослідження кібербезпеки України та проблемам нормативного забезпечення у цій сфері становлять значний теоретичний інтерес, а розділи 3 - 5, в яких проведене дослідження сучасних загроз для кібербезпеки людини, проблематики захисту суспільства від глобальних загроз у кіберпросторі, а також напрямів подальшого удосконалення правового регулювання у сфері кібербезпеки, мають значну практичну цінність для правозастосування у відповідній галузі інформаційної діяльності.

Дослідження змісту дисертації Тарасюка А. В. дозволяє проаналізувати процес втілення ідей і думок автора в тексті наукової роботи, виділити

найбільш переконливі аргументи, а також питання, які потребують подальших досліджень.

Так, зокрема, аналіз змісту розділу 1 дисертаційної роботи дозволяє детально охарактеризувати генезу розвитку вчень про правове забезпечення кібербезпеки України, дослідити її сутність та зміст, особливості співвідношення понять «інформаційна безпека» та «кібербезпека», охарактеризувати підходи до класифікації загроз кібербезпеки, з'ясувати методологічні засади вивчення цих категорій науки інформаційного права.

Отримані дисертантом у межах першого розділу результати розкривається через наступні висновки та положення наукової новизни дисертаційної роботи:

Уперше:

– обґрутовано 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 тощо; 5) в основі змісту лежать норми зазначених вище галузей права, що об’єднані спрямованістю на забезпечення безпекових інтересів людини, суспільства, держави в кіберпросторі, (с. 31 дисертаційної роботи, с. 7 автореферату);

– розроблено концептуальні засади правового регулювання кібербезпеки України на сучасному етапі розвитку глобальних інформаційних процесів, (с. 31 – 32 дисертаційної роботи, с. 7 автореферату).

– 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 (с. 32 дисертаційної роботи, с. 8 автореферату).

Актуальними та такими, що поглиблюють наукове вивчення теоретико-правових зasad дослідження понятійного апарату механізму правового забезпечення кібербезпеки України, удосконалені у межах першого розділу положення наукової новизни, зокрема:

- базові поняття дослідження: «кібернетична безпека України», «забезпечення кібернетичної безпеки України», «кібератака», «кіберпростір», «кіберзлочин», «стан захищеності», «кіберзагроза», що дасть змогу упорядкувати понятійно-категоріальний апарат інформаційного права, (с. 33 дисертації, с. 8 автореферату);
- тлумачення терміну «культура кібербезпеки» як системи 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, (с. 33 дисертаційної роботи, с. 8 автореферату).

Дістали подальший розвиток наступні положення:

- теоретичні засади утвердження інформаційного права як самостійної галузі права, та розширення меж його правового впливу у частині удосконалення законодавства про забезпечення кібернетичної безпеки України (с. 33 дисертації, с. 8 автореферату);
- теоретичні положення щодо розвитку інформаційно-правових досліджень правового регулювання кібернетичної безпеки України, (с. 34 дисертаційної роботи);

– теоретичні підходи до змісту, динаміки розвитку сучасних загроз кібернетичній безпеці України та механізмів їхній протидії, (с. 34 дисертації, с. 8 дисертації).

В межах первого розділу автором виокремлено питання, які не охоплювалися наявними дослідженнями та яким в дисертаційній роботі було приділено значну увагу. Йдеться серед іншого про наступні аспекти теоретико-методологічних зasad правового забезпечення кібербезпеки України: 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.

Вирішення у межах первого розділу цих наукових завдань стало можливим завдяки вдалому використанню діалектичного підходу та його принципам, що дістало вияв у концептуальному розумінні правового забезпечення кібербезпеки як комплексного інституту права та правового механізму захисту держави, суспільства та людини від кіберзагроз, а також їхній характеристиці.

Заслуговує на увагу викладений у першому розділі авторський погляд на тлумачення змісту поняття «інформаційна культура» у вузькому та широкому розумінні виходячи з характеристики ознак цього поняття, зокрема, від навичок володіння окремими інформаційними технологіями (комп’ютерної грамотності) до опанування знань та навичок майже у всіх сферах людської діяльності. На основі вказаної в дисертаційній роботі аргументації, Тарасюк А. Т. обґрунтовує авторську позицію щодо необхідності розуміння поняття «інформаційна культура», що більшою мірою відповідає потребам забезпечення кібербезпеки України, (с. 43 – 44 дисертації).

Обґрунтованою та такою, що відображає найбільш поширені в науці інформаційного права погляди є розвинена у межах первого розділу наукова позиція, відповідно до якої: «Термін «кібербезпека» є похідним від родового

терміну «безпека», відтак «кібербезпека» становить частину більш загального поняття «безпека», що вирізняється специфічними особливостями, і одночасно має виступати результатом синтезу поняття «безпека» та прикметника «кібернетична» (скорочено – «кібер»)» (с. 62 дисертації).

Заслуговує на увагу та такою, що становить науковий інтерес є думка автора, згідно з якою: «Відмінність інформаційної безпеки від кібернетичної, таким чином, полягає в тому, що перша спрямована на комплексний захист інформаційних ресурсів у будь-якій із можливих форм їх існування, тоді як кібербезпека опікується захистом виключно цифрових форм даних», (с. 80 дисертаційної роботи).

Аналіз змісту розділу 2 дисертаційної роботи дозволяє чітко прослідкувати розвиток наукової позиції дисертанта щодо формування нормативних зasad правового забезпечення кібербезпеки України, виокремити конкретні висновки, які логічно та послідовно розкривають зміст наукової новизни дисертаційної роботи.

Зокрема, вперше 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 оновленню держави, збереженню та зміцненню 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-значущих 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 телекомуникаційних й інформаційних систем, як створюваних, так і тих, що функціонують на території України, (с. 32 дисертаційної роботи, с. 7 - 8 автореферату).

Поряд з цим в межах розділу 2 дисертаційної роботи дисертантом було вперше 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 у 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, (с. 32 – 33 дисертації, с. 8 автореферату).

Виокремлення в межах дисертаційної роботи пріоритетних напрямів забезпечення кібербезпеки у авторській інтерпритації відображає сучасні тенденції розвитку державної політики у цій сфері а також здобутки науки інформаційного права, що вказує на практичну важливість та теоретичну цінність відповідних положень дисертаційної роботи.

У другому розділі дисертаційної роботи автором було удосконалено ряд концептуальних положень механізму правового забезпечення кібербезпеки України, які є актуальними для науки інформаційного права та законодавства України у цій сфері правового регулювання.

Так, зокрема, були удосконалені такі основоположні поняття інституту правового забезпечення інформаційної безпеки, як: «забезпечення кібернетичної безпеки України», «кібербезпека України», «критична

інформаційна інфраструктура», «національні інтереси України у кіберпросторі (с. 33 дисертаційної роботи, с. 8 автореферату).

Поряд з цим у другому розділі удосконалені положення щодо:

- 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, (с. 33 дисертаційної роботи);
- 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), (с. 33 дисертаційної роботи).

Наведені положення наукової новизни проведеного дослідження мають важливе значення для подальшого удосконалення законодавства України про кібербезпеку, запровадження більш спеціалізованого механізму протидії окремим видам кіберзагроз. Також, удосконалені у межах другого розділу положення наукової новизни з позицій розширення суб'єктного складу забезпечення кібербезпеки України мають важливе методологічне значення. Йдеться, зокрема про використання механізму забезпечення кібербезпеки України на основі державно-приватного партнерства.

У розділі 3 дисертаційної роботи були розроблені, удосконалені та одержали подальший розвиток доктринальні положення, що складають теоретичну основу дослідження проблематики правового забезпечення кібербезпеки людини у сучасному кібернетичному просторі.

Зокрема, вперше на доктринальному рівні 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, (с. 31 дисертаційної роботи, с. 7 автореферату).

Зважаючи на визначені дисертантом завдання проведеного дослідження важливим для науки інформаційного права та таким, що має істотне значення для правотворчої діяльності є сформульоване на сторінці 33 дисертаційної роботи положення наукової новизни за змістом якого удосконалений теоретичний підхід, у рамках якого кіберпростір може розглядатися одночасно як об'єкт правового захисту, і як джерело загроз. На цій основі автором констатовано, що у пріоритеті рівнів кібербезпеки (безпека людини, суспільства й держави, в основу якого покладені конституційні принципи захисту життєвоважливих інтересів зазначених суб'єктів, с. 8, 9 автореферату)

В межах третього розділу дисертаційної роботи також були удосконалені критерії класифікації загроз кібербезпеці людини у частині їх впливу на національну свідомість. Виходячи з таких теоретико-методологічних позицій, автором було запропоновано наступні критерії поділу загроз для кібербезпеці людині: за посяганням на національні цінності; за природою виникнення, (с. 34 дисертаційної роботи, с. 9 автореферату). Окреслені критерії мають принципово важливе значення а аспекті забезпечення кібербезпеки людини на національному рівні, сприяння повсюдному утвердженню принципу відповідальності держави перед людиною за свою діяльність.

В контексті формування теоретико-правових зasad кібербезпеки людини обґрунтованим та таким, що має значну наукову цінність є викладене на сторінці 219 дисертації положення, відповідно до якого, право людини на кібербезпеку – це своєрідна, специфічна сукупність прав, котрі реалізуються, зокрема, за допомогою цифрових, інформаційно-телекомунікаційних технологій з метою захисту приватної, особистої інформації від несанкціонованого доступу та запобігання шкідливим впливам на особистість.

З позицій обґрунтування особливостей правовідносин у сфері забезпечення кібербезпеки людини, заслуговує викладений на сторінках 222 та 256 дисертації авторський підхід до визначення змісту поняття «інформаційна діездатність». На думку дисертанта, це поняття необхідно розглядати 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.

На виконання мети і завдань дослідження, здобувачем у межах третього розділу було також 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, (с. 258 дисертації).

Зазначене положення дисертації відповідає змісту норми, передбаченої у частині першій статті 17 Конституції України та узгоджується з пріоритетними напрямами забезпечення кібербезпеки людини, закріпленими в нормах національного законодавства України.

У розділі 4 дисертаційної роботи ґрутовне наукове та прикладне вирішення одержали концептуальні проблеми розвитку інформаційного суспільства в умовах розвитку цифрових трансформацій та прояву глобальних кіберзагроз.

Дисертантом чітко узагальнено теоретичні підходи до аналізу концепцій інформаційного суспільства, оцінку правовому чиннику у запобіганні кіберзагрозам сучасному українському суспільству, визначено теоретико-правове підґрунтя системи соціального регулювання в інформаційному суспільстві. На цій основі Тарасюком А. В. було запропоновано вперше, удосконалено або надано подальшого розвитку наступним положенням наукової новизни:

– 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 оновленню держави, збереженню та зміцненню 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-значущих 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, (с. 32 дисертаційної роботи, с. 7 автореферату);

– тлумачення терміну «культура кібербезпеки» – це 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, (с. 33 дисертаційної роботи);

Серед сформульованих в межах розділу 4 дисертаційної роботи положень ключове наукове та методологічне значення мають зокрема такі висновки:

Запропоновані дисертантом на сторінках 275 – 276 дисертації ознаки сучасного інформаційного суспільства. Як зазначає дисерант: «Це, насамперед наявність високорозвинених інформаційних технологій, їх значну поширеність серед населення, у бізнесових колах, в державних і самоврядних органах. Подруге, це отримання пересічними громадянами та іншими суб'єктами суспільства очевидних переваг від застосування новітніх інформаційних технологій, а саме: вільного й рівноправного доступу до інформаційних ресурсів і кібернетичних технологій; розвитку інформаційно-телекомунікаційних систем, баз даних, мереж тощо; упровадження інноваційних технологій, зокрема, підвищення за рахунок цього ефективності

роботи органів державного управління й місцевого самоврядування при неодмінному забезпеченні інформаційної, кібернетичної безпеки особи, суспільства й держави».

Зважаючи на мету дисертаційної роботи та реалізовані здобувачем межах четвертого розділу проведеного дослідження, заслуговує на увагу запропонований поділ кібервикликів та кіберзагроз у глобальному інформаційному суспільстві. До них дисертант відносить: деструктивний вплив на різних суб'єктів (пропаганда); економічна свобода; зіткнення культур; правозастосовні проблеми в умовах кібернетичної транскордонності; надмірна соціальна мобільність, інформаційне відчуження, сугестія, зомбування, (с. 279 – 280 дисертації).

Важливими як для подальшого розвитку інформаційного суспільства в Україні, так, і для протидії сучасним кіберзагрозам є розроблені дисертантом основні напрями застосування засобів забезпечення кібербезпеки. До них А. Т. Тарасюк відносить: по-перше: формування в негативної суспільної думки щодо правопорушень у кіберпросторі та інформаційній сфері загалом; унормування, чітке визначення відповідальності за кожен із видів вказаних правопорушень. Другий напрям, на думку здобувача, має включати заходи з координування зусиль щодо підвищення рівня освіченості й поінформованості громадянського суспільства у сфері інформаційної та кібернетичної безпеки, (с. 306 дисертації).

У розділі 5 основну увагу дисертанта сфокусовано на сучасних теоретико-методологічних проблемах правового регулювання кібербезпеки України. На цій основі дисертантом було виокремлено концептуальні засади правового регулювання кібербезпеки України на сучасному етапі розвитку глобальних інформаційних процесів, запропоновано та обґрунтовано конкретні пріоритети розвитку правових основ державної політики України у відповідній сфері, розроблено напрями правового регулювання окремих елементів інформаційної інфраструктури на національному та міжнародному рівнях забезпечення кібербезпеки.

В межах цього розділу Тарасюком А. В. були запропоновані вперше, удосконалені або дістали подальший розвиток наукові положення в яких:

- розроблено концептуальні засади правового регулювання кібербезпеки України на сучасному етапі розвитку глобальних інформаційних процесів, (с. 31 дисертаційної роботи, с. 7 авторефрату);
- пріоритетні напрями розвитку правових основ державної політики у процесі забезпечення кібернетичної безпеки, з урахуванням досвіду європейських країн і сучасної ситуації у нашій державі, (с. 34 дисертаційної роботи, с. 8, 9 авторефрату);
- узагальнення іноземного досвіду забезпечення кібернетичної безпеки, що створює правову базу побудови системи кібернетичної безпеки в Україні, здійснення гармонізації національного законодавства з міжнародними стандартами та європейським законодавством, (с. 35 дисертаційної роботи, с. 9 авторефрату).

Важливe теоретичne і практичne значення в контексті реалізації мети і завдань дослідження мають сформульовані дисертантом в межах розділу 5 на сторінці 337 складові кібербезпеки є, до яких автор пропонує віднести: стан безпеки кіберпростору, за якого забезпечується його формування і розвиток в інтересах держави, організацій та громадян; стан безпеки інформаційної інфраструктури, за якого інформація використовується суворо за призначенням і при цьому не здійснює негативного впливу на об'єкт; стан безпеки самої інформації, за якого унеможливлюється або суттєво ускладнюється погіршення таких її характеристик, як конфіденційність, доступність, цілісність.

Обґрунтованим та таким, що має важливe значення для подальшого удосконалення механізму забезпечення транскордонної кібербезпеки є сформульованих на сторінці 398 дисертаційної роботи науковий висновок, згідно з яким, Увага міжнародного співтовариства має бути зосереджена на забезпеченні кібербезпеки у сфері інформаційних технологій, оскільки більшість відносин базується на цифрових транскордонних технологіях.

Цікавим та таким, що може бути застосований в цілях подальшого удосконалення норм Закону України «Про основні засади забезпечення кібербезпеки України» підхід до розуміння змісту поняття «інформаційна зброя» у його широкому розумінні. Згідно з авторською інтерпретацією згаданого поняття під інформаційною зброєю розуміють інформаційні технології, засоби і методи, призначені для ведення інформаційної війни, (с 399 дисертаційної роботи).

Публікації. Основні положення та висновки дисертації викладено в 40 наукових працях, зокрема в 2 індивідуальних монографіях, у розділах 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 наукометрических баз даних (6 із яких – у наукових періодичних виданнях інших держав), у 15 тезах доповідей на конференціях.

Оцінюючи обґрунтованість наукових положень дисертації, слід наголосити на тому, що висновки, положення і пропозиції здобувача є новими, достовірними і належно обґрунтованими. Наукова новизна одержаних результатів обумовлюється тим, що дисертація є комплексним теоретико-прикладним монографічним дослідженням теоретичних та практичних проблем формування механізму правового забезпечення кібербезпеки України

Наукова новизна, поза сумнівами, визначається також сучасною постановкою проблеми, дослідженням нових ідей та тенденцій в аспекті теми дисертації.

В роботі дістали подальший розвиток раніше проаналізовані положення, а також сформульовані нові наукові висновки, які запропоновані автором особисто і внесені ним на захист.

Позитивно оцінюючи актуальність і науковий рівень проведеного дисертантом дослідження, наукову новизну, обґрунтованість і достовірність, теоретичний рівень і теоретичну та практичну значимість його результатів для вирішення правових проблем, пов'язаних із визначенням закономірностей

формування теоретико-правових основ забезпечення кібернетичної безпеки України як правового механізму та комплексного інституту права, можна висловити наступні зауваження щодо окремих положень роботи:

1. Формулюючи на сторінках 30 – 31 дисертаційної роботи положення наукової новизни, дисертант зазначає, що ним уперше розроблено концептуальні засади правового регулювання кібербезпеки України на сучасному етапі розвитку глобальних інформаційних процесів, проте, не конкретизує про які процеси йдеться та в чому виявляється сутність сучасних концептуальних зasad забезпечення кібербезпеки України. Уточнення авторської позиції щодо окресленої проблематики під час прилюдного захисту дисертації може значно посилити ступень розробленості вказаних положень наукової новизни роботи та сприятиме більш повному розкриттю предмета дисертаційного дослідження.

2. На сторінці 33 дисертаційної роботи, дисертант зазначає, що ним було удосконалено підхід до системно-функціонального аналізу суб'єктів забезпечення кібернетичної безпеки України, зокрема, у частині розвитку державно-приватного партнерства. Таке положення дисертаційної роботи вбачається актуальним та назрілим з позицій удосконалення механізму забезпечення кібербезпеки України. Разом з тим, потребує конкретизації під час публічного захисту позиція дисертанта щодо визначення суб'єктного складу механізму державно-приватного партнерства у сфері забезпечення кібербезпеки України, характеристики нормативних вимог, яким повинен відповідати приватний партнер для можливості виконання юридичних обов'язків у цій сфері.

3. На сторінках 33 – 34 дисертаційної роботи Тараканюк А. В. формулює наукову позицію відповідно до якої, у пріоритеті рівнів кібербезпеки (безпека людини, суспільства й держави, в основу якого покладені конституційні принципи захисту життєво важливих інтересів зазначених суб'єктів) запропоновано надати пріоритет інтересам держави, оскільки від цього безпосередньо залежатиме й реалізація інтересів особи й суспільства. Така

авторська позиція вбачається досить дискусійною та такою, яка вимагає додаткової аргументації з огляну на дію проголошених у статті 3 Конституції України принципи відповідальності держави перед людиною за свою діяльність, визначальне значення прав і свобод людини для визначення змісту і спрямованості діяльності держави.

4. На думку дисертанта, з метою кіберзахисту усіх суб'єктів – від окремої особи до суспільства й держави в цілому – слід сформувати комплексну систему (доктрину, політику) їхньої безпеки, підґрунтам якої маєстати кібербезпека, (с. 98 дисертаційної роботи). Така позиція здобувача вбачається актуальною та nauовообґрунтованою, проте потребує конкретизації під час прилюдного захисту в частині характеристики нормативно-правових актів, в яких можуть знайти свій розвиток відповідні пропозиції дисертанта.

5. На сторінці 219 дисертаційної роботи, дисерtant зазначає, що на його думку для досягнення мети дослідження, оптимальним при визначенні та удосконаленні термінологічного апарату механізму правового забезпечення кібербезпеки є більш широкий підхід, який ґрунтуються не лише на власне правовому регулюванні, а й на питаннях правового забезпечення. Водночас, Таракюк А. В. не наводить в роботі авторський підхід щодо характеру співвідношення понять «правове забезпечення» та «правове регулювання» у контексті реалізації мети і завдань дослідження. Висловлення авторської позиції щодо окресленого питання під час прилюдного захисту могла б істотно посилити наукову цінність проведеного дослідження.

6. На сторінці 300 дисертаційної роботи Таракюк А. В. наголошує на необхідності застосування комплексного підходу до визначення системи гарантій та засобів протидії кіберзагрозам, водночас, серед них не згадує про кіберстрахування. Зважаючи на світові тенденції активного використання цього правового та економічного засобу протидії наслідкам кіберзагроз, потребує висвітлення під час публічного захисту позиція здобувача щодо напрямів та перспектив застосування кіберстрахування, як засобу забезпечення

кібербезпеки та гарантії відновлення інтересів осіб, проти яких спрямована діяльність кіберзагроз.

Відповідність дисертації встановленим вимогам. Докторська дисертація А. В. Тарасюка є завершеною науковою працею, в якій отримано нові науково обґрунтовані результати, що є суттєвими для вирішення конкретних наукових задач - формування механізму правового забезпечення кібербезпеки України, розроблення теоретичних зasad механізму здійснення нагляду та контролю у цій сфері правового регулювання.

Результати дослідження можуть бути використані у законотворчій та практичній роботі суб'єктів забезпечення кібернетичної безпеки України для удосконалення охорони національного інформаційного суверенітету, найважливіших соціальних цінностей, пов'язаних з інформаційною діяльністю.

Таким чином, дисертація Тарасюка Анатолія Васильовича на тему «Теоретико-правові основи забезпечення кібербезпеки України» відповідає вимогам п. п. 9, 10, 11, 12 Порядку присудження наукових ступенів, затвердженого постановою Кабінету Міністрів України від 24 липня 2013 р. № 567 з наступними змінами та доповненнями і надає підстави стверджувати, що її автор заслуговує на присудження наукового ступеня доктора юридичних наук за спеціальністю 12.00.07 – адміністративне право і процес; фінансове право; інформаційне право.

### **Офіційний опонент:**

**доктор юридичних наук, доцент,  
професор кафедри інтелектуальної власності  
та інформаційного права**

**Інституту права Київського національного  
університету імені Тараса Шевченка**

*Сур.*

**О.А. Заярний**

