ВІДГУК

офіційного опонента – доктора юридичних наук, доцента Ткачука Тараса Юрійовича про 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 дисертаційної роботи. Конституція України визначає, що захист суверенітету і територіальної цілісності України є найважливішими функціями держави, справою всього Українського народу. Зовнішньополітична діяльність України спрямована на забезпечення її національних інтересів і безпеки шляхом підтримання мирного і взаємовигідного співробітництва з членами міжнародного співтовариства за загальновизнаними принципами і нормами міжнародного права.

В останні роки спостерігаються докорінні зміни у зовнішньому та внутрішньому безпековому середовищі України, що і зумовлює потребу перегляду існуючих та розробки нових підходів до безпекової сфери. Важливим аспектом у цій площині є правничий чинник.

У свою чергу кібербезпека посідає особливе місце в умовах євроінтеграції України, адже впровадження новітніх технологій в усі сфери життєдіяльності, з одного боку, дає можливість забезпечити усім право на свободу інформації, оптимізувати різні технологічні процеси, інтегрувати задачі та рішення в глобальні інформаційно-телекомунікаційні системи, а з іншого – створює високі ризики протиправного використання інформації.

Чинне правове забезпечення кібербезпеки України має серйозні недоліки, які підтверджуються навіть у реалізації Закону України «Про санкції» ряду Рішень РНБО щодо застосування санкцій уведених в дію Указами Президента України, до прикладу систему блокування доступу до IP санаційних інтернет ресурсів успішно проходять засобами VPN зв'язку або самі споживачі, або

особи під санкції впроваджують VPN у сам програмний продукт та ряд інших прикладів останніх років

Сьогодення постає перед Україною з новими викликами та надскладними завданнями будівництва інформаційного суспільства, адже вже сформовано усвідомлення важливості не тільки нарощування технологічних можливостей здійснення інформаційного обміну, але й глибоке розуміння усіма суб'єктами інформаційних відносин необхідності здійснення максимально доступних заходів захисту щодо інформаційних ресурсів та забезпечення кібербезпеки, що неможливо без чіткого усвідомлення сутності останньої та правового забезпечення.

У цьому контексті варто підтримати позицію А. Тарасюка, що 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.

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).

Ступінь обґрунтованості наукових положень, висновків і рекомендацій, сформульованих у дисертації. Зазначене дослідження базується на комплексному, системному підході, характеризується належним рівнем наукових узагальнень, що значною мірою обумовлено й характером дослідницької бази. Поряд із працями з інформаційного права, Анатолій Тарасюк широко використав наукові розробки із загальної теорії держави і права, конституційного права, філософії права та інших галузевих правових наук. Детальному аналізу дисертантом піддано законодавчі та інші нормативні акти України, НАТО, більшості європейських країн, які визначають правові засади забезпечення кібербезпеки.

Безсумнівною перевагою роботи є використання та аналіз значного обсягу загальнотеоретичних наукових праць українських та зарубіжних вчених. Дисертаційна робота Тарасюка А.В. характеризується системним підходом до предмету дослідження. Структура дисертації повністю відповідає меті й завданням дослідження, що дозволяє послідовно розглянути всі проблемні аспекти, визначені автором.

Глибина та достовірність результатів дисертаційного дослідження базуються на досконалому володінні автором методами наукового пошуку. Зокрема, теоретико-методологічною основою дослідження стали 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).

У дисертації наведено теоретичне узагальнення і нове вирішення актуальної 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.

Достовірність та наукова новизна наукових положень, висновків і рекомендацій, сформульованих у дисертації. Результати проведеного дослідження є доказом того, що автору притаманні здібності до самостійних наукових пошуків, до плідного аналізу складних теоретико-правових процесів і явищ, вміння раціонально відбирати, кваліфіковано узагальнювати та аналізувати різнобічні джерела, формулювати на цій підставі практичні висновки й рекомендації. Значення одержаних результатів в теоретичній і практичній сферах обумовлюється тим, що сформульовані і обґрунтовані в дисертації висновки та пропозиції розширюють і поглиблюють існуючі знання про правове забезпечення інформаційної безпеки України.

Повнота викладення наукових положень, висновків і рекомендацій, сформульованих у дисертації в опублікованих працях. 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. Дублювання дисертаційних матеріалів за статтями та порушення вимог МОН України щодо публікацій не виявлено.

Також під час вивчення матеріалів дисертації, аналізу наукових публікацій автора не було виявлено ознак порушення академічної доброчесності, а саме академічного плагіату, самоплагіату, фабрикації та фальсифікації результатів дослідження. Таким чином, дисертаційна робота Анатолія Тарасюка визначається самостійною оригінальною працею та не містить порушень академічної доброчесності.

Автореферат дисертації та публікації автора відповідають змісту дисертації, в свою чергу, зміст автореферату та основних положень дисертації ідентичні. Таким чином, можна зробити висновок, що основні положення та висновки дисертації автором оприлюднені повною мірою.

Наукова і практична цінність дисертації. Дисертаційна робота є одним з перших у вітчизняній правничій науці комплексним дослідженням теоретико-правових основ забезпечення кібернетичної безпеки людини, суспільства, держави. У результаті проведеного дослідження сформовано теоретико-методологічні основи правового забезпечення кібербезпеки України шляхом розвитку теоретичних засад інформаційного права та формування пропозицій щодо вдосконалення інформаційного законодавства. Визначено шляхи розвитку правового забезпечення кібербезпеки України в сучасних умовах, сформульовано низку нових наукових положень та висновків, спрямованих на досягнення поставленої мети. Використовуючи значний масив емпіричних

даних та наукових джерел, автор зробив досить цікаві й обґрунтовані узагальнюючі висновки. Зокрема:

– *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.

Варто також погодитись із дисертантом, що досвід зміни парадигми забезпечення національної безпеки з реактивної на проактивну для України у контексті її євроатлантичних спрямувань є надзвичайно важливим, адже дозволяє правильно визначати стратегічні пріоритети та оптимізувати зусилля

щодо забезпечення кібербезпеки, а також сприятиме плідному співробітництву з усіма європейськими країнами у розбудові систем регіональної та міжнародної кібербезпеки. Не менш важливим є цей досвід і для подальшої розбудови теорії національної безпеки та наукових засад забезпечення кібербезпеки. Зокрема, до перспективних напрямів подальшого наукового пошуку належить передусім дослідження у сфері оцінювання загроз кібербезпеці України та методів управління ризиками в інформаційній сфері.

Вивчення змісту дисертації, автореферату дисертації та наукових праць дає підстави зробити висновок про достатній ступінь обґрунтованості та достовірності наукових положень та висновків, що виносяться на захист, їх наукову новизну та практичну значущість, а також про глибокий аналіз питань, пов'язаних із правовим забезпеченням кібербезпеки України.

Дискусійні положення та зауваження щодо змісту дисертації. Визнаючи загалом високий теоретичний рівень роботи, її практичне значення, слід відзначити, що це не виключає можливостей критичного підходу до окремих позицій здобувача, висловити деякі міркування та зауваження, які мають бути обговорені під час захисту і враховані автором в його подальших наукових дослідженнях.

1. Автором значна увага в роботі приділена попередженню та протидії зовнішнім загрозам інформаційної безпеки України. Зокрема даному питанню фактично присвячено окремий параграфи 2.4., 3.3., 5.2.. Проте, значні проблеми ефективності забезпечення кібербезпеки України, а особливо безпеки громадян у кіберпросторі, зосереджені в площині внутрішніх загроз. Хотілося б почути думку автора які пріоритетні напрями доцільно впроваджувати в Україні саме для попередження внутрішніх загроз.

3. У дисертації спеціальний розділ 3 присвячено загрозам кібербезпеціи людини під час використання кіберпростору. Як уявляється, дисертантові більше уваги варто було приділити кібербезпеці людини, особливо в умовах екстериторіального принципу дії, у тому числі в Україні, Регламенту (ЄС) 2016/679 про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних (Загальний Регламент про

захист даних GDPR), який почав діяти з травня 2018 року, а правовим забезпеченням України так і не було імплементовано GDPR до сьогоднішнього дня включно.

4. Не зрозумілою залишилась думка автора щодо співвідношення кібербезпеки України та національної безпеки. Зі змісту дисертації, де автором проводяться певні роздуми щодо цього зауваження власне авторська позиція відсутня. Тобто доцільно було обґрунтувати таку думку більш детально.

5. Робота ще більше виграла б від наявності запропонованої автором певною стратегії чи концепції забезпечення кібербезпеки людини в умовах використання кіберпростору. Жодним чином не применшуючи науковий доробок автора, вважаємо, що бажаним би було у змісті дисертації або в додатках до неї відобразити положення концептуального характеру, спрямовані на реформування відповідного блоку питань.

Водночас висловлені зауваження характеризують складність досліджених проблем, мають дискусійний характер, а тому у цілому не впливають на загальну позитивну оцінку наукового дослідження. Виконана Анатолієм Тарасюком наукова праця сприяє розв'язанню ряду теоретичних і практичних питань, що мають важливе значення для розвитку науки інформаційного права, адже робота спрямована на розроблення концептуальних правових засад забезпечення кібербезпеки нашої держави та практичних рекомендацій щодо вдосконалення механізмів її реалізації, а також вдосконалення чинного інформаційного законодавства. Положення дисертації знайшли належне відображення в опублікованих дисертантом наукових публікаціях. Зміст автореферату дисертації відображає основні положення дисертації, її структуру та отримані результати. Дисертація оформлена відповідно до вимог МОН України, що ставляться до докторських дисертацій. Тема і зміст дисертації відповідають спеціальності 12.00.07- адміністративне право і процес; фінансове право; інформаційне право.

Викладене дозволяє зробити висновок, що дисертація «Теоретико-правові основи забезпечення кібербезпеки України» є завершеною працею, в якій отримано нові науково обґрунтовані результати, що розв’язують наукову

проблему, яка має важливе значення для науки інформаційного права, тобто за своєю актуальністю, новизною постановки та вирішенням досліджених проблем, теоретичним рівнем і практичною корисністю, достовірністю і обґрунтованістю одержаних результатів повністю відповідає вимогам Порядку присудження наукових ступенів, затвердженого постановою Кабінету Міністрів України від 24.07.2013 р. № 567 (зі змінами), а її автор – **Тарасюк Анатолій Васильович** – заслуговує на присудження наукового ступеня доктора юридичних наук за спеціальністю 12.00.07 – адміністративне право і процес; фінансове право; інформаційне право.

Офіційний опонент:
Заступник завідувача кафедри
організації захисту інформації з обмеженим доступом
Навчально-наукового інституту інформаційної безпеки
НА СБ України
доктор юридичних наук, доцент Тарас ТКАЧУК

«22» червня 2021 року

Підпис засвідчую:
Учений секретар Національної академії
СБ України
кандидат юридичних наук Андрій ПРОЗОРОВ

«22» червня 2021 року