

*До разової спеціалізованої
вченої ради ДФ 08.051.177
Дніпровського національного
університету імені
Олеся Гончара*

РЕЦЕНЗІЯ

рецензента Сачка Олександра Васильовича, професора, доктора юридичних наук, професора кафедри адміністративного і кримінального права, декана юридичного факультету Дніпровського національного університету імені Олеся Гончара Міністерства освіти і науки України на дисертацію Олійника Артема Андрійовича за темою «Кримінологічні засади забезпечення інформаційної безпеки: міжнародний, національний та зарубіжний досвід», представлену до захисту у разову спеціалізовану вчену раду Дніпровського національного університету імені Олеся Гончара на здобуття ступеня доктора філософії галузі знань 08 Право зі спеціальності 081 «Право»

Стан розробки проблеми. Сучасний світ переживає зміни, зумовлені переходом від індустріального до інформаційного суспільства, що реально чи потенційно несе нові загрози національній безпеці держави. Динамічна діджиталізація та стрімке поширення комунікаційних платформ (зокрема, соціальних мереж) створили не лише нові можливості для реформування публічного управління, а й стали потужним інструментом для реалізації злочинних намірів та ведення масштабних інформаційних війн. Усвідомлення цього безпекового виклику на міждержавному рівні прийшло наприкінці XX століття, що актуалізувало необхідність спільного міжнародного реагування на загрози локального і глобального характеру.

Дисертація Олійника Артема Андрійовича є завершеним самостійним дослідженням актуальної науково - практичної проблеми кримінологічних засад забезпечення інформаційної безпеки в міжнародному, національному та зарубіжному досвіді.

Актуальність теми дослідження зумовлена тим, що сучасна кіберзлочинність вийшла за межі класичних ізольованих фактів несанкціонованого доступу. Сьогодні вона становить собою системну індустрію правопорушень, що охоплює цифрові шахрайства нового покоління, поширення деструктивного програмного забезпечення та скоординовані атаки на критичну інфраструктуру. Особливу суспільну небезпеку становлять цілеспрямовані кібердиверсії проти державних баз даних, енергетичних мереж та систем управління, що здатні паралізувати інституційну спроможність цілих галузей економіки і створити плацдарм для масштабних інформаційно-психологічних операцій.

Наукові пошуки дисертанта зумовлені також фрагментарністю та відсутністю комплексного підходу до висвітлення означеної проблеми у вітчизняній юридичній науці.

Автор цілком вірно визначив об'єкт та предмет дослідження. Структура роботи є логічною і послідовною та обумовлена поставленими метою і завданнями дослідження. Комплекс філософських, загальнонаукових і спеціальних методів, що їх використовує автор, дозволяє якнайповніше розкрити і вирішити ряд проблемних аспектів нормативного та організаційного забезпечення ефективної діяльності правоохоронних органів.

Слід підкреслити, що у дослідженні належної уваги приділено вивченню джерельної бази з проблеми. Аналізуються роботи не лише вітчизняних представників науки кримінального права, але і праці спеціалістів в галузі міжнародного кримінального права та фахівців у сфері державного управління. Крім того критично розглянуто праці європейських фахівців, присвячені проблемам кримінологічного запобігання загрозам інформаційній безпеці.

Окремий корпус джерел становлять нормативно - правові акти України та

акти первинного і вторинного права країн Європи, що становлять протидію міжнародній кіберзлочинності з боку держави. Тож можна упевнено казати, що в дисертації наведено теоретичне узагальнення і запропоновано шляхи вирішення важливої наукової проблеми з використанням найновітніших досягнень української науки кримінального права, робіт зарубіжних криміналістів, чинного законодавства України, з урахуванням норм міжнародного кримінального права..

У результаті проведеного дослідження сформульовано низку нових концептуальних наукових положень та висновків, запропонованих особисто автором.

Так, на підставі ґрунтовного теоретичного аналізу автор обґрунтовує комплексну трирівневу модель інформаційної безпеки як об'єкта кримінологічного захисту, який базується на розширеній міжнародній матриці безпеки (Тріада CIA (конфіденційність, цілісність, доступність) доповнена процесуальними елементами автентичності, неспростовності) та структурно розподіляється на інфраструктурний, правовий режим та підзвітність (інформаційно-регуляторний) і соціально-психологічний (когнітивний) рівні. Такий підхід дозволив виділити наскрізний характер сучасних кіберзагроз та визначити специфічні вектори проактивної превенції для кожного з рівнів;

При цьому у роботі достатньо повно - обґрунтовано дворівневий розподіл поняття «кіберстійкість» у контексті забезпечення інформаційної безпеки на державний (публічно-правовий) та особистісний (людиноцентричний) рівні. Зокрема, «кіберстійкість держави» визначено як стратегічну спроможність національної системи інформаційної безпеки підтримувати критичні функції, адаптуватися до гібридних загроз та відновлювати цифрову інфраструктуру на основі інституційної координації сектору безпеки (МВС, Нацполіція, ЦПД), ефективному управлінні ризиками ланцюгів постачання та впровадженні метрик «кіберзрілості» за міжнародними стандартами; «кіберстійкість особи» визначено як сукупність когнітивних навичок, правової обізнаності та кібергігієни індивіда, що формують його когнітивний імунітет до дезінформації та здатність захищати

приватність у цифровому середовищі; обґрунтовано концепцію «когнітивного імунітету» нації як невід'ємного елемента виміру інформаційної безпеки, що базується на зарубіжному досвіді розбудови потенціалу (capacity building) та передбачає перехід від захисту технічного периметра до формування стійкості людського капіталу.

Не можна не відмітити як позитивний факт дослідження у дисертації особливостей та тенденцій забезпечення інформаційної безпеки в умовах воєнного стану в Україні; законодавчих та інституційних засад забезпечення інформаційної безпеки України; кримінологічної превенції у сфері інформаційної безпеки від державного суверенітету до захисту прав людини.

Цікавою є пропозиція вдосконалення віктимологічного підходу до запобігання кіберзлочинності через обґрунтування змісту «техногенної віктимності» організацій, на основі аналізу міжнародного досвіду використання хмарних сервісів. Так, в умовах розмиття меж цифрової інфраструктури провідним чинником злочинних посягань є організаційна недбалість, яка виявляється у помилках налаштування конфігурації, поширенні неконтрольованого програмного забезпечення та відсутності чіткої договірної підзвітності, саме ці вразливості нівелюють систему захисту об'єкта та перетворюють легітимних працівників на носіїв кіберзагроз;

Слушним є - визначення засад реалізації принципу невідворотності кримінальної відповідальності у цифровому середовищі, шляхом інтеграції техніко - юридичного елемента «неспростовності» до системи доказування, що дозволяє нейтралізувати наслідки використання злочинцями систем анонімізації та транскордонної маршрутизації трафіку в умовах глобальної кризи доведення джерела кібератак та причетності конкретної особи до кіберзлочинів;

Слід погодитися з підходом до класифікації моделей забезпечення кіберстійкості шляхом виокремлення чотирьох взаємозалежних вимірів (стратегічного, нормативного, інституційного та екосистемного), що дозволяє комплексно оцінювати рівень «кіберзрілості» держави і суспільства;

Проведене дослідження є доказом того, що автор застосовує в своїй

науковій роботі різноманітні методи, вміло і вітчизняної та іноземної правової науки, з якими ознайомлена в належній мірі.

Дисертація написана академічно вірно і достатньо лаконічно, чіткою і ясною мовою з використанням загальноприйнятої наукової термінології. На використані джерела і результати інших авторів зроблені коректні посилання. Бібліографічний опис цитувань в дисертаційній роботі складено у відповідному вигляді.

Результати дослідження мають теоретичну і практичну цінність та можуть стати базою подальшого розроблення проблем кіберзагрозам в міжнародному та національному вимірах.

Наукові положення, висновки і рекомендації, сформульовані в роботі, у повній мірі відображені в наукових статтях, що опубліковані у фахових виданнях. Дисертація пройшла достатньо серйозну апробацію на міжнародних, науково-методичних та науково-практичних конференціях.

Зауваження та дискусійні аспекти дисертаційного дослідження.

Віддаючи належне обґрунтованості положень, що відображають наукову новизну одержаних результатів та виносяться на захист, вважаю, що окремі положення дисертації мають дискусійний характер та потребують уточнення або додаткової аргументації під час наукової дискусії на захисті. Дізнаючи високий науковий рівень виконаної роботи, доцільно висловити деякі зауваження та дискусійні міркування: пропонуючи концепцію «когнітивного імунітету нації», автор акцентує увагу на протидії дезінформації та ІПСО. Однак залишається не до кінця з'ясованим: через які саме юридичні та кримінологічні механізми має здійснюватися розмежування між протидією деструктивним когнітивним впливам ворога та дотриманням конституційних гарантій свободи слова і думки в умовах мирного часу (після закінчення воєнного стану)?

Запропоноване автором створення Національного Інституту безпеки штучного інтелекту є вельми прогресивною ідеєю. Водночас виникає запитання: в системі якого саме органу виконавчої влади (наприклад, Мінцифри, СБУ, РНБО) бачить здобувач цей Інститут, та які безпосередньо кримінологічно-

превентивні (а не лише контролюючі чи консультативні) функції він повинен виконувати?

Автор слушно вводить категорію «техногенна віктимність» організацій. Проте у роботі бажано було б ширше розкрити конкретні заходи кримінологічної профілактики щодо керівників суб'єктів критичної інфраструктури за недотримання вимог кібергігієни та халатне ставлення до захисту цифрових контурів.

Аналіз додержання академічної доброчесності. Аналіз дисертаційної роботи та наукових публікацій Олійника А. А. дає підстави для висновку про дотримання здобувачкою принципів академічної доброчесності. Дисертація має самостійний характер, використані наукові джерела, нормативні матеріали та судова практика належним чином оформлені з відповідними посиланнями. *Ознак академічного плагіату, фабрикації або фальсифікації результатів дослідження не виявлено.*

ВИСНОВОК

Дисертаційне дослідження **Олійника А. А.** на тему «**Кримінологічні засади забезпечення інформаційної безпеки: міжнародний, національний та зарубіжний досвід**» є самостійною, завершеною та комплексною науковою працею, що характеризується належним рівнем наукової новизни, теоретичної та практичної значущості.

За своїм змістом робота відповідає галузі знань 08 «Право» спеціальності 081 «Право» та відповідає вимогам Порядку підготовки здобувачів вищої освіти ступеня доктора філософії та доктора наук у вищих навчальних закладах (наукових установах), що затверджений постановою Кабінету Міністрів України від 23 березня 2016 року № 261, а також вимогам постанови Кабінету Міністрів України від 12 січня 2022 року №44 «Про затвердження Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої

освіти, наукової установи про присудження ступеня доктора філософії» та Вимогам до оформлення дисертації, затверджених наказом МОН України від 12.01.2017 р. № 40, і заслуговує представлення до захисту в разовій спеціалізованій раді для присудження ступеня доктора філософії за спеціальністю 081 – Право.

Рецензент:

Професор кафедри адміністративного і кримінального права, декан юридичного факультету Дніпровського національного університету імені Олеся Гончара доктор юридичних наук, професор



Олександр САЧКО

Підпис д.ю.н, професора Сачко О.В.

«ЗАСВІДЧУЮ»

Проректор з наукової роботи
Дніпровського національного
університету імені Олеся Гончара

« 14 » 08 2026 р.



Олег МАРЕНКОВ