

*До разової спеціалізованої
вченої ради ДФ 08.051.179
Дніпровського національного
університету імені
Олеся Гончара*

РЕЦЕНЗІЯ

Рецензента Мудриєвської Людмили Михайлівни, доцента, кандидата юридичних наук, завідувачки кафедри теорії держави і права, конституційного права та державного управління юридичного факультету Дніпровського національного університету імені Олеся Гончара Міністерства освіти і науки України на дисертацію Олійника Артема Андрійовича на тему «Кримінологічні засади забезпечення інформаційної безпеки: міжнародний, національний та зарубіжний виміри», 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»

Аналіз актуальності теми дослідження.

Питання побудови інформаційного суспільства в Україні в межах глобального інформаційного простору почали вирішуватися ще на початку 2000-х років, закінчення цього процесу планувалось до 2015 року. Дійсно, значні досягнення до цього моменту вже були зроблені. Але разом з розвитком інформаційно-комунікаційних відносин формувалась і система правопорушень в цій сфері. Актуальність теми дослідження зумовлена тим, що кіберзлочинність як соціально-правове явище на сучасному етапі трансформувалася з сукупності одиничних деліктів у сфері несанкціонованого доступу до комп'ютерної інформації у структурно організовану транснаціональну індустрію протиправної діяльності. Об'єктивна сторона відповідних посягань нині охоплює якісно нові способи вчинення шахрайства з використанням інформаційно-комунікаційних технологій, створення та розповсюдження шкідливого програмного забезпечення, а також скоординовані кібератаки, спрямовані на об'єкти критичної інфраструктури. Підвищений ступінь суспільної небезпеки становлять цілеспрямовані кібердиверсійні операції проти державних інформаційних

ресурсів, об'єктів паливно-енергетичного комплексу, оскільки їх реалізація здатна спричинити деструктивні наслідки у вигляді порушення функціональної спроможності цілих секторів національної економіки та слугувати інструментальною основою для проведення гібридних інформаційно-психологічних операцій.

Для України дослідження зазначеної проблематики набуває підвищеної актуальності з огляду на те, що в умовах повномасштабної збройної агресії та гібридної війни кіберпростір *de facto* набув статусу самостійного театру воєнних дій, що зумовлює необхідність адаптації національного законодавства до реалій ведення кібервійни. За таких обставин формування та вдосконалення новітнього нормативно-правового інструментарію протидії кіберзагрозам виходить за межі суто галузевого (кримінально-правового чи інформаційно-безпекового) завдання, набуваючи характеру одного з визначальних чинників забезпечення державного суверенітету, національної безпеки та гарантування сталого демократичного розвитку Української держави.

Автором поставлено на меті розробку кримінологічних механізмів не тільки запобігання цифровим загрозам, але формування системи національної кіберстійкості.

Аналіз зв'язку роботи з науковими програмами, планами, темами.

Тематика дисертації відповідає сучасним науковим програмам, спрямованим на дослідження головних засад боротьби з кіберзлочинністю. Отримані результати сприяють систематизація знань про кіберзлочини, інформаційні атаки та їхні характеристики, аналізу нових форм кримінальної діяльності в цифровому середовищі, прогнозуванню розвитку загроз.

Дисертаційне дослідження співвідноситься з Переліком пріоритетних тематичних напрямів наукових досліджень і науково-технічних розробок на період до 31 грудня року, наступного після припинення або скасування воєнного стану в Україні, затверджених постановою Кабміну України № 476 від 30 квітня 2024 року; Пріоритетними напрямами розвитку науки і техніки та інноваційної діяльності (відповідно до Закону України від 12 січня 2023 року №2859-IX зі змінами). Положення дисертації корелюють із Цілями сталого розвитку України

на період до 2030 року, затвердженими Указом Президента України від 30 вересня 2019 року № 722/2019; Стратегією національної безпеки України; Стратегією кібербезпеки України; Комплексним стратегічним планом реформування органів правопорядку як частини сектору безпеки і оборони України на 2023 - 2027 роки, затвердженого Указом Президента України від 11 травня 2023 року № 273/2023; Рішенням Ради національної безпеки і оборони України «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації», затвердженому Указом Президента України від 13 лютого 2017 року № 32/2017.

Дисертація відповідає дослідницькій темі кафедри адміністративного і кримінального права Дніпровського національного університету імені Олеся Гончара «Забезпечення реалізації та захист основних свобод, прав людини, національних інтересів держави в умовах гібридних загроз і безпекових викликів» (затвердженої рішенням ради юридичного факультету, протокол № 7 від 08.01.25 р., номер держреєстрації 0125U002352)..

Тему дисертації затверджено рішенням Вченої ради Дніпровського національного університету імені Олеся Гончара від 1 грудня 2022 року (протокол № 4).

Таким чином, дисертаційне дослідження є складовою передових наукових розробок у галузі права, відповідає актуальним науковим програмам і планам протидії кіберпродукції та інформаційним операціям проти держави, захисту критичної інформаційної інфраструктури в період військової загрози.

Аналіз обґрунтованості теми дисертації, її мети, завдань, об'єкта та предмета дослідження.

Обґрунтованість теми дисертаційного дослідження і визначення відповідно до теми об'єкта, предмета, мети і завдань логічно узгодженні, відображають актуальність та нагальність дослідження визначеної проблематики. Мета дослідження відображає комплексність, ієрархічність, детермінізм проблеми кібербезпеки, особливо в умовах воєнного стану. Відзначено, що для правильного розуміння інформаційної безпеки як предмета кримінологічного захисту та юридичної профілактики необхідно розробити відповідну теоретичну

модель. В основі цієї моделі лежить розширена міжнародна система безпеки — класична Тріада CIA (конфіденційність, цілісність та доступність), до якої додаються елементи автентичності та невідкличності.

За своєю структурою інформаційна безпека охоплює три взаємопов'язаних виміри: матеріально-технічний (інфраструктурний), нормативно-правовий та людський (соціально-психологічний та когнітивний). Такий багаторівневий аналіз дозволяє глибше зрозуміти, як сучасні кібератаки впливають одночасно на технічні системи, законодавчі режими та психіку людей.

Особливий наголос зроблено на антропоцентричний підхід — пріоритетно захищати громадську свідомість, процес формування громадської думки, цифрові права й свободи громадян від незаконних маніпуляцій, пропаганди та шкідливих інформаційно-технологічних впливів.

Аналіз методологічної основи дослідження.

Завдяки застосуванню розгалуженої системи філософських, загальнонаукових та спеціально-наукових методів автору вдалось зробити періодизацію наукового обґрунтування та дослідження безпеки і показано еволюцію цього процесу, починаючи з дослідження безпеки як технічного захисту даних (I етап: 1991–1996 рр.), через правову основу базових інститутів (II етап: 1997–2000 рр.) та міжнародну гармонізацію вітчизняних нормативних стандартів (III етап: 2001–2013 рр.) до обґрунтованого нами IV етапу (з 2014 року до сьогодні). Четвертий етап розвитку інформаційної безпеки має якісно нову природу, яка формується під впливом військово-політичних викликів. На відміну від попередніх періодів, цей етап характеризується принципіальною зміною підходу: замість локального технічного захисту окремих інформаційних систем, розвивається комплексна державна політика та національна кібероборона.

У межах цього нового періоду вдалося уточнити термінологічну базу дослідження через розмежування кількох взаємопов'язаних, але різних понять. «Інформаційна безпека» розглядається як найширше поняття, яке включає захист громадської свідомості та нецифрових даних. На відміну від цього, «кібербезпека» та «цифрова безпека» — це вужчі, технологічно спрямовані

категорії. Таке уточнення термінології дозволило чітко окреслити, що саме становить предмет кримінологічного захисту та юридичної відповідальності.

Аналіз повноти викладу в опублікованих працях наукових положень, висновків і рекомендацій, сформульованих у дисертації.

Аналіз наукових публікацій здобувача свідчить про належний рівень апробації результатів дисертаційного дослідження. Основні наукові положення, висновки та рекомендації, сформульовані у дисертації Олійника Артема Андрійовича, знайшли своє відображення у 10 публікаціях: 5 – у фахових наукових виданнях, 5 – у матеріалах науково-практичних конференцій міжнародного і республіканського рівня. Тематика опублікованих праць охоплює найсуттєвіші моменти визначеної тематики, як-то: сутність інформаційної безпеки як правового явища у національному та міжнародному просторі, значення формування інформаційної стійкості суспільства в умовах воєнного стану, ролі інформаційної безпеки і боротьби з кіберзлочинністю для функціонування публічної влади і збереження суверенітету країни.

Кількість і якість публікацій відповідають встановленим вимогам, що дає підстави стверджувати про достатній рівень оприлюднення результатів дослідження та їх наукову апробацію.

Аналіз наукової новизни одержаних результатів.

Наукова новизна результатів дослідження Олійника Артема Андрійовича полягає в розробці та обґрунтовані комплексної трирівневої моделі інформаційної безпеки як об'єкта кримінологічного захисту, яка інтегрує розширену матрицю безпеки СІА з процесуальними елементами автентичності і неспростовності, структурно об'єднуючи інфраструктурний, правовий та соціально-психологічний виміри. Це дозволило виділити наскрізний характер сучасних кіберзагроз та визначити специфічні вектори їх превенції.

Автором запропоновано дворівневий концепт «кіберстійкості» — на державному (публічно-правовому) та особистісному (людиноцентричному) рівнях, — що враховує як стратегічні спроможності національної системи безпеки, так і когнітивні навички й кібергігієну індивіда.

Сформульована оригінальна концепція «когнітивного імунітету нації» як невід'ємної складової інформаційної безпеки, яка передбачає захист людського капіталу від дезінформації та маніпуляцій, а також виділена «когнітивна імунність суспільства» як самостійна кримінологічна категорія мікрорівня кіберстійкості. Запропонована класифікація моделей кіберстійкості за чотирма взаємозалежними вимірами (стратегічний, нормативний, інституційний, екосистемний), що дозволяє комплексно оцінювати кіберзрілість держави.

Удосконалено віктимологічний підхід через введення категорії «техногенна віктимність» організацій, що враховує організаційну недбалість як криміногенний фактор.

Автором розширена кримінологічна характеристика кіберзлочинності в умовах воєнного стану з урахуванням загроз штучного інтелекту та Інтернету речей, обґрунтована криміналізація нових цифрових загроз (синтетичний контент експлуатації дітей), а також визначена і практична модель використання наданих пропозицій в сфері публічного управління: доцільність заснування національного Інституту безпеки штучного інтелекту як координаційного центру впровадження міжнародних стандартів у запобіганні кіберзлочинам.

Аналіз практичного значення отриманих результатів.

Практичне значення отриманих результатів полягає в тому, що викладені у дослідженні висновки і пропозиції можуть бути використані у:

- *науково-дослідній діяльності* – як основа для подальших наукових досліджень кримінологічних, кримінально-правових та процесуальних аспектів запобігання кіберзлочинності в Україні, зокрема у сфері впливу Генеративного ШІ та міжнародної співпраці;

- *правотворчій діяльності* – під час розробки змін і доповнень до чинного законодавства, що регулює питання кібербезпеки, захисту персональних даних та протидії дезінформації, а також гармонізації національного законодавства з актами ЄС та стандартами верховенства права;

- *правозастосовній сфері* – як науково обґрунтовані заходи щодо підвищення ефективності діяльності правоохоронних органів (Національної поліції, Кіберполіції, Прокуратури) із виявлення, розслідування та запобігання

транскордонним кіберзлочинам, а також для забезпечення дотримання гарантій прав людини відповідно до прецедентної практики ЄСПЛ під час цифрових розслідувань;

- навчальному процесі під час підготовки відповідних наукових, навчально-методичних видань та проведенні занять із навчальних дисциплін «Кримінологія», «Запобігання злочинності у контексті глобалізації», «Кримінальне право України»

Аналіз структури та змісту дисертаційної роботи.

В розділі 1 «Теоретико-методологічні основи кримінологічного забезпечення інформаційної безпеки» визначено, що сучасна трансформація цифрового середовища вимагає фундаментального перегляду підходів до розуміння кібербезпеки, а саме — здійснення науково обґрунтованого переходу від вузькотехнологічного інтерпретування до комплексної трирівневої моделі інформаційної безпеки як самостійного об'єкта кримінологічної охорони та правової превенції.

В основі сутності цього об'єкта лежить адаптована міжнародна Тріада CIA (*Confidentiality, Integrity, Availability* — конфіденційність, цілісність, доступність), яка була розширена та доповнена кримінально-процесуально значущими елементами: автентичністю та неспростовністю.

Забезпечення комплексного захисту зазначених елементів зумовлює необхідність градації об'єкта охорони на три взаємопов'язані рівні: техніко-технологічний, інформаційно-регуляторний та антропоцентричний.

В результаті компаративістського аналізу виявлено специфічні особливості та обмеження зарубіжної доктрини інформаційної безпеки. Якщо українська школа традиційно орієнтована на правову кодифікацію та стратегічне планування, то західна доктрина відзначається високим рівнем математизації та техноцентризму.

Головним недоліком суто математичних західних моделей є ігнорування динамічної поведінки правопорушника та «людського фактора», що обмежує їх застосування для повноцінної кримінологічної превенції. Зазначене обґрунтовує необхідність застосування мультидисциплінарного підходу.

Водночас новітні зарубіжні концепції (зокрема стандарти GDPR та концепція когнітивної безпеки COGSEC) відображають позитивний глобальний тренд — перехід до пріоритетного захисту індивідуальної свідомості та фундаментальних прав людини.

В розділі 2 «Національний вимір кримінологічного запобігання загрозам інформаційній безпеці України» обґрунтовано необхідність переходу України від технічної моделі захисту інформації до людиноцентричної моделі когнітивної стійкості в умовах війни. Основна логіка розгортається у трьох взаємопов'язаних площинах: стратегічна трансформація, інституційна діагностика та людиноцентричний підхід.

Воєнний стан змінив саму парадигму інформаційної безпеки — держава мусить не просто захищатися, а випереджально реагувати на нові загрози. Ефективна протидія гібридній агресії можлива лише через одночасне поєднання наступних напрямів: правового визнання цифрових доказів для міжнародних трибуналів, інституційного зміцнення Кіберсил ЗСУ, переходу критичної інфраструктури на принцип «нульової довіри» та збереження балансу між повноваженнями спецслужб і правами людини (за стандартами ЄСПЛ).

Чинна система є розгалуженою, але страждає на дублювання функцій і переважно оборонний, цивільно-правоохоронний характер — це заважає державі проводити наступальні кібероперації. Як вихід з визначеної проблеми автором пропонується розділ поняття «кіберстійкості» на дві рівноважних складових: державну (спроможність інституцій) і особистісну (кібергігієна та правова обізнаність громадянина).

Головна теза розділу — безпека держави похідна від стійкості кожної людини. Вводиться категорія «когнітивного імунітету нації» — здатності громадян самотійно протистояти маніпуляціям та ІПСО.

Розділ 3 «Зарубіжний досвід та вдосконалення національної системи кримінологічного реагування» присвячено порівняльно-правовому аналізу передового зарубіжного досвіду забезпечення інформаційної безпеки та формування кіберстійкості, а також визначенню основних напрямів вдосконалення кримінологічного забезпечення інформаційної безпеки та

формування національної кіберстійкості в Україні, виходячи з міжнародного досвіду в цій сфері. Зазначено, що для України механічне копіювання якоїсь однієї парадигми є недоцільним, прийнятним є синтез найкращих елементів: імплементація мілітаризованої проактивної доктрини за зразком США та Ізраїлю (активне кіберстримування); суворе гармонізація законодавства з Директивою ЄС NIS2 та актом CRA (персональна відповідальність керівництва критичної інфраструктури); запозичення британського досвіду створення єдиного міжвідомчого координаційного центру, а також адаптація досвіду країн Балтії та Польщі щодо захисту когнітивного суверенітету.

Висновки характеризуються високим рівнем обґрунтованості, базуються на комплексному теоретичному та порівняльно-правовому аналізі, проведеному у відповідних розділах дисертації, та підкріплюються застосуванням широкого методологічного інструментарію. Цінність дослідження розкривається у трьох взаємопов'язаних вимірах: теоретико-методологічному, безпековому та прикладному. В межах першого виміру розроблено нову трирівневу модель інформаційної безпеки (інфраструктурний, правовий, соціально-психологічний рівні), яка розширює класичну тріаду CIA процесуальними елементами автентичності й неспростовності. Уточнено періодизацію розвитку вітчизняної доктрини (виокремлено четвертий, «воєнний» етап з 2014 р.) та розмежовано поняття «інформаційна безпека», «кібербезпека» і «цифрова безпека», що усуває термінологічну плутанину в науці. Запропоновано авторські категорії — «когнітивний імунітет нації» та дворівневу «кіберстійкість» (державну і особистісну) — які збагачують кримінологію новим, людиноцентричним інструментарієм аналізу. В рамках другого підходу обґрунтовано чотирирівневий механізм притягнення агресора до відповідальності за кібератаки, що дає практичний алгоритм для міжнародних трибуналів. Дослідження синхронізує національне законодавство зі свіжими міжнародними інструментами (Конвенція ООН 2025 р., NIS2, FISMA) і фіксує зміну статусу України — від об'єкта захисту до активного суб'єкта європейської кібербезпеки (інтеграція з Європолем, SIENA). Щодо практичної цінності проведеного дисертаційного дослідження, то треба констатувати, що результати одразу конвертуються у готові до

впровадження продукти: пропозиції з криміналізації нових загроз (дипфейки сексуального характеру щодо дітей), концепція національного Інституту безпеки ІІІ як координаційного хабу, а також авторський спецкурс «Правові засади кіберстійкості та цифрова держава» для підготовки фахівців. Це надає дослідженню виражений впроваджувальний характер — воно не обмежується констатацією проблем, а пропонує конкретні інституційні, законодавчі та освітні рішення.

Сукупно це дозволяє говорити про дослідження як про цілісну доктринальну основу переходу України від реактивного технічного захисту до проактивної, людиноцентричної стратегії кіберстійкості в умовах війни.

Загальна оцінка дисертації. Загалом зміст дисертації справляє враження структурованого, комплексного і концептуального дослідження, у якому автор поєднав теоретичний, правовий та практичний аналіз однієї з найбільш динамічних та актуальних проблем вдосконалення інформаційної безпеки України в умовах швидкого розвитку ІІІ і використання його досягнень в правовому полі.

Зауваження та дискусійні аспекти дисертаційного дослідження.

1. Автор доречно зауважує, що баланс між свободою та безпекою є ключовим викликом сучасної інформаційної політики. Але в світовій практиці ми стикаємося з тим, що цей баланс, внаслідок свого неконкретного формулювання, постійно порушується. Як саме дисертант пропонує зберігати цей баланс в Україні в умовах воєнного стану і як конкретно бачить кримінологічні превенції у сфері інформаційної безпеки в контексті балансу між захистом державного суверенітету та прав і свобод людини?

2. Дисертантом запропоновано для практичної реалізації європейських безпекових стандартів приєднання до європейської системи кібербезпеки та інтеграції авторської пропозиції стосовно заснування національного Інституту безпеки ІІІ (за прикладом Інституту безпеки штучного інтелекту Великої Британії). Це, безумовно, оптимізує процес імплементації європейських стандартів інформаційної безпеки, в кібербезпеки як її різновиду,

в Україні. Але цей процес тривалий і динамічний. Як вбачає автор сучасні дії України по мінімізації діяльності кіберзлочинців та притягнення їх до юридичної відповідальності?

3. Дещо дискусійним видається недостатньо повне використання дисертантом методу кримінологічного прогнозування — одного з базових інструментів кримінологічної науки, спрямованого на передбачення майбутнього стану злочинності та пов'язаних з нею явищ і факторів (криміногенної ситуації), виявлення основних тенденцій їх розвитку та формулювання науково обґрунтованого висновку щодо поточної динаміки злочинності. Застосування визнаних методів кримінологічного прогнозування (екстраполяції, експертних оцінок, моделювання, сценарного методу) дозволило б не лише констатувати наявні тенденції, а й підкріпити авторську тезу про необхідність переходу від реактивної до випереджальної (проактивної) моделі протидії кіберзагрозам конкретними прогностичними викладками, що суттєво посилило б практичну цінність одержаних результатів для формування державної політики у досліджуваній сфері.

ВИСНОВОК

Дисертаційне дослідження **Олійника Артема Андрійовича** на тему **«Кримінологічні засади забезпечення інформаційної безпеки: міжнародний, національний та зарубіжний виміри»** є комплексним, завершеним науковим дослідженням, що характеризується наявністю наукової новизни та має практичну актуальну значущість. 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 наукового ступеня доктора філософії за спеціальністю 081 – Право.

Рецензент:

Завідувачка кафедри теорії держави і права,
конституційного права та державного
управління юридичного факультету
Дніпровського національного
університету імені Олеся Гончара
кандидат юридичних наук, доцент



Людмила МУДРИЄВСЬКА

Підпис к.ю.н, доцента Мудриєвської Л.М.

«ЗАСВІДЧУЮ»

Проректор з наукової роботи
Дніпровського національного
університету імені Олеся Гончара
«06» ____ 08 ____ 2026 р.



Олег МАРЕНКОВ