ЗАТВЕРДЖУЮ

Проректор з наукової роботи
Дніпровського національного університету імені Олеся Гончара
Олег МАРЕНКОВ

«13» 06 **2026 р.**

ВИСНОВОК

Про наукову новизну, теоретичне та практичне значення результатів дисертації
Олійника Артема Андрійовича
«Кримінологічні засади забезпечення інформаційної безпеки: міжнародний, національний та зарубіжні виміри»,
представленої на здобуття ступеня доктора філософії
за спеціальністю 081 Право.

ВИТЯГ

з протоколу № 5 міжкафедрального семінару юридичного факультету Дніпровського національного університету імені Олеся Гончара від 03 червня 2026 року

ПРИСУТНІ: 17 з 17 членів наукового семінару.

ГОЛОВУЮЧА: д-р юрид. наук, проф. **К.В. Бережна** (12.00.07 – адміністративне право і процес), завідувачка кафедри європейського та міжнародного права Дніпропетровського національного університету імені Олеся Гончара.

СЕКРЕТАР: канд. юрид. наук, доц., каф цивільного, трудового та господарського права Дніпровського національного університету імені Олеся Гончара **О.А. Грабильнікова** (12.00.02 – конституційне право, муніципальне право).

ПРИСУТНІ: д-р юрид. наук, проф. **О. Л. Соколенко** (12.00.07 – адміністративне право і процес); д-р. юрид. наук, проф. **Т. В. Корнякова** (12.00.08 – кримінальне право і процес); д-р. юрид. наук, проф. **Н. С. Юзікова** (12.00.08 – кримінальне право і процес); канд. юрид. наук, доц. **О. П. Литвин** (12.00.07 – адміністративне право і процес); д-р. юрид. наук, проф. **Є. А. Кобрусєва** (12.00.07 – адміністративне право і процес); д-р юрид.наук, доц. **Н.П. Капітаненко** (12.00.07 – адміністративне право і процес): д-р. філософії у галузі права **О.О. Дриголь** (081Право); канд. юрид. наук, доц. **О. В. Лахова** (12.00.08 – кримінальне право і процес); д-р юрид. наук, проф. **К. В. Бережна** (12.00.07 – адміністративне право і процес); канд. юрид. наук, доц. **Л. М. Мудриєвська** (12.00.01 – теорія держави і права); канд. юрид. наук, доц. **Т. М. Заворотченко** (12.00.02 – конституційне право, муніципальне право); канд. юрид. наук, проф.

І. Г. Алєксєєнко (12.00.01 – теорія держави і права); д-р. юрид. наук, проф. **І. В. Патерило** (12.00.07 – адміністративне право і процес), д-р. юрид. наук, проф. **О. В. Марченко** (12.00.07 – адміністративне право і процес); д-р юрид. наук, проф. **О.В. Сачко** (12.00.09 – кримінальний процес та криміналістика; судова експертиза); канд. юрид. наук, доц. **Ю. В. Живова** (12.00.08 – кримінальне право і процес); канд. юрид. наук, доц. **О. А. Грабильнікова** (12.00.02 - конституційне право, муніципальне право).

Запрошені: аспірант 4 року навчання А.А. Олійник.

Порядок денний: розгляд і обговорення дисертаційної роботи Олійника Артема Андрійовича на тему: «Кримінологічні засади забезпечення інформаційної безпеки: міжнародний, національний та зарубіжні виміри», представленої на здобуття ступеня доктора філософії за спеціальністю 081.

Тема дисертації затверджена Вченою радою Дніпровського національного університету імені Олеся Гончара (протокол № 4 від 01 грудня 2022 року), науковим керівником призначено доктора юридичних наук, професора Н. С. Юзікову (протокол №4 від 01 грудня 2022 року). Підготовка здобувача третього рівня вищої освіти здійснюється за акредитованою освітньо-науковою програмою «Право» зі спеціальності 081 Право (Сертифікат про акредитацію освітньої програми 8127, дійсний до 01.07.2029 р.).

СЛУХАЛИ:

Обговорення дисертаційної роботи Олійника Артема Андрійовича на тему: «Кримінологічні засади забезпечення інформаційної безпеки: міжнародний, національний та зарубіжні виміри», представленої на здобуття ступеня доктора філософії за спеціальністю 081 Право.

За результатами звіту про оцінку на унікальність тексту наукового дослідження Олійника Артема Андрійовича на тему: «Кримінологічні засади забезпечення інформаційної безпеки: міжнародний, національний та зарубіжні виміри», представленої на здобуття ступеня доктора філософії за спеціальністю 081 Право, здійсненої на плагіат програмою «StrikePlagiarism» виявлено, що унікальність тексту складає 94,4%. Таким чином, на підставі перевірки зроблено висновок: робота Олійника Артема Андрійовича може бути допущена до захисту.

Перевірку на плагіат здійснювала комісія у складі: канд. юрид. наук, доц. кафедри цивільного, трудового та господарського права Грабильнікова О.А.; канд. юрид. наук, доц. кафедри адміністративного і кримінального права Лахова О.В.; канд. юрид. наук, доц. кафедри адміністративного і кримінального права Дриголь О.О.

Робота розглядалась трьома фаховими експертами – д-р. юрид. наук, проф. Т.В. Корнякова, канд. юрид. наук, доц. Ю.В. Живова, д-р. юрид. наук, проф. О.В. Сачко.

Робота виконана на 263 сторінках, з них 194 сторінки основного тексту, робота структурована та складається з анотації, вступу, трьох розділів, що

містять одинадцять підрозділів, висновків, списку використаних джерел, додатків.

Слово надається аспіранту Олійнику Артему Андрійовичу. Будь ласка, регламент виступу - 20 хвилин.

Доповідь А.А. Олійник:

Добрий день, шановна голова міжкафедрального семінару, члени міжкафедрального семінару, шановні присутні! На Ваш розгляд надається дисертаційна робота з теми: «Кримінологічні засади забезпечення інформаційної безпеки: міжнародний, національний та зарубіжні виміри», яка подається на здобуття ступеня доктора філософії за спеціальністю 081 Право. Науковий керівник: доктор юридичний наук, професор Юзікова Наталія Семенівна.

Сьогодні ми є свідками й безпосередніми учасниками першої у світі повномасштабної кібервійни, яка розгортається паралельно із традиційними бойовими діями на виснаження. Інформаційний простір перетворився на повноцінний театр воєнних дій. За даними Ситуаційного центру забезпечення кібербезпеки СБУ та Державної служби спеціального зв'язку та захисту інформації України, інтенсивність ворожих кібератак на українську критичну інфраструктуру з початку повномасштабного вторгнення зросла у декілька разів, сягаючи понад 4 500 масштабних кіберінцидентів на рік. Вражаються енергетичні системи, логістичні вузли, урядові реєстри та бази даних правоохоронних органів.

Проте загроза не обмежується суто технічним периметром. Активний розвиток технологій штучного інтелекту та Інтернету речей породив небачені раніше криміногенні та віктимологічні ризики. Зловмисники та спецслужби агресора використовують ШІ для генерації високоточних фішингових кампаній, автоматизованого пошуку вразливостей у коді програмного забезпечення та створення глибоких фейків (*дипфейків*). Особливу тривогу викликає використання ШІ для продукування синтетичного контенту експлуатації дітей, маніпулювання суспільною свідомістю через когнітивні атаки та проведення транснаціональних інформаційно-психологічних операцій (ІПСО).

У цих умовах традиційні, реактивні методи правової превенції, орієнтовані на фіксацію вже вчинених злочинів, демонструють свою повну неефективність. Виникає гостра, життєво важлива потреба у формуванні проактивної кримінологічної моделі, здатної захистити інформаційний суверенітет держави та цифрові права кожної особи.

У дослідженні пропонується розширити класичну міжнародну безпекову матрицю, відому як Тріада CIA конфіденційність, цілісність, доступність, доповнивши її двома процесуальними техніко-юридичними елементами: *автентичністю* (чистотою джерела інформації) та *неспростовністю* (неможливістю заперечити факт вчинення цифрової дії). На цій основі обґрунтовано комплексну трирівневу модель інформаційної безпеки як об'єкта кримінологічного захисту:

1. *Інфраструктурний рівень* (захист фізичних мереж, серверів, ліній зв'язку та Інтернету речей).

2. *Правовий режим та підзвітність* (інформаційно-регуляторний рівень, що фіксує правила гри, договірні зобов'язання та юридичну відповідальність).

3. *Соціально-психологічний або когнітивний рівень* (захист людського капіталу, мислення, процесу формування волі та суспільної свідомості від деструктивних інформаційних інтервенцій).

Доведено, що сучасні кіберзагрози мають наскрізний характер — вони починаються на інфраструктурному рівні (наприклад, злам сервера), пробивають правовий режим (через прогалини у законодавстві) і досягають когнітивної сфери, дезорієнтуючи суспільство.

Центральне місце у дисертації посідає перегляд понятійно-категоріального апарату. Пропонується авторське визначення дворівневого розподілу поняття «кіберстійкість», яке відрізняється від статичного поняття «захист». Захист передбачає побудову стіни; кіберстійкість - це здатність системи тримати удар, функціонувати в умовах успішної атаки та миттєво відновлюватися.

«Кіберстійкість держави» визначено як стратегічну спроможність національної системи інформаційної безпеки підтримувати критичні функції, адаптуватися до умов гібридної війни та оперативно відновлювати цифрову інфраструктуру на основі жорсткої інституційної координації сектору безпеки (МВС, Кіберполіції, ЦПД), ефективного управління ризиками ланцюгів постачання та регулярного оцінювання за метриками «кіберзрілості».

«Кіберстійкість особи» дефініційовано як сукупність когнітивних навичок, правової обізнаності та усвідомленої кібергігієни індивіда, що формують його стійкість до дезінформації, соціальної інженерії та здатність захищати власну приватність без порушення прав інших користувачів.

Розвиваючи мікрорівень кіберстійкості, запропоновано визначення «когнітивного імунітету суспільства» як самостійної кримінологічної та віктимологічної категорії. Це внутрішній самозахисний бар'єр нації, який дозволяє суспільній свідомості розпізнавати ворожі маніпуляції (ІПСО, фейки, штучно спровоковану паніку) та відсікати їх на рівні індивідуального сприйняття, мінімізуючи віктимність громадян у цифровому середовищі.

На основі узагальнення зарубіжної наукової думки з'ясовано, що західна доктрина відзначається глибокою математизацією (застосування теорії ігор, Байєсівських мереж для прогнозування атак). Однак доведено, що ключовим недоліком західних моделей є ігнорування динамічної поведінки правопорушника та людського фактора, що робить їх недостатніми для повної кримінологічної превенції.

Тому для України обґрунтовано доцільність формування гібридної моделі кіберстійкості, яка б гармонійно поєднала європейську правову стабільність, англосаксонську операційну гнучкість та транзитну швидкість імплементації інновацій.

Визначено, що міжнародні стандарти, такі як американські принципи FISMA та європейська Директива NIS2 (ухвалена задля суттєвого підвищення

загального рівня кібербезпеки в ЄС), мають бути не просто скопійовані, а глибоко інтегровані в національне правове поле. Особливу роль відіграє підписана у жовтні 2025 року в Ханої під егідою УНП ООН перша глобальна Конвенція про запобігання, припинення та боротьбу з кіберзлочинністю (відкрита для підписання до кінця 2026 року).

Проте головною проблемою у міжнародному праві залишається криза процесуальної атрибуції - правопорушники використовують транскордонну маршрутизацію та системи анонімізації, щоб уникнути відповідальності. Для подолання цієї кризи у дисертації обґрунтовано чотирирівневий виконавчий (процесуальний) механізм, що поєднує можливості Будапештської конвенції та норм міжнародного гуманітарного права:

1. Збір комп'ютерних даних (ст. 18, 19 Будапештської конвенції) для встановлення ланцюжка команд від державних органів агресора до конкретної хакерської групи.
2. Забезпечення «процесуальної чистоти» лог-файлів та IP-адрес для їхньої беззаперечної допустимості у Міжнародному кримінальному суді.
3. Використання Другого додаткового протоколу для отримання прямих доказів (змісту комунікацій через глобальних провайдерів) щодо цілеспрямованих ударів по критичній цивільній інфраструктурі (лікарні, водоканали).
4. Накладення технічних параметрів кібератак на матеріальні норми міжнародного гуманітарного права (принципи пропорційності та розрізнення), що дозволяє кваліфікувати ворожі кібератаки як повноцінні воєнні злочини.

Визначено, що формування балансу між свободою та безпекою є наріжним каменем сучасної кримінологічної політики. Надмірний державний контроль під гаслами безпеки неминуче загрожує скочуванням у тоталітаризм та порушенням фундаментальних прав людини. Водночас повна відсутність регулювання створює ідеальне поле для безкарної діяльності кіберзлочинців.

Оптимальне рішення полягає у запровадженні випереджальних превентивних механізмів, які спираються на Конвенцію про захист прав людини і основоположних свобод. Будь-які обмеження у цифровому просторі (блокування ресурсів, вилучення даних) мають бути легітимними, пропорційними та проходити суворий міждисциплінарний аналіз, особливо під час проведення стабілізаційних заходів на деокупованих територіях України. Наш «юридичний щит» проти злочинності повинен діяти в чітких межах поваги до приватності (Стаття 8), свободи вираження поглядів (Стаття 10) та права на власність (Стаття 1 Першого протоколу).

Підсумовуючи, виокремимо головні результати, які виносяться на захист та мають вагоме наукове і практичне значення:

Доведено, що система інформаційної безпеки в умовах воєнного стану вимагає негайного стратегічного переходу від реактивної (пасивної) моделі до проактивної (випереджальної) превенції.

Сформульовано оновлену кримінологічну характеристику кіберзлочинності, куди вперше інтегровано фактори ризику штучного інтелекту, та обґрунтовано необхідність криміналізації створення і поширення

згенерованого за допомогою ШІ синтетичного контенту експлуатації дітей (*дипфейків*).

Впроваджено віктимологічний підхід через обґрунтування концепції «техногенної віктимності організацій» (вразливості хмарних налаштувань та використання «тіньових ІТ»), де головним чинником злочинів визначено організаційну недбалість менеджменту, яка перетворює легітимних працівників на носіїв внутрішніх кіберзагроз.

Обґрунтовано зміну міжнародно-правового статусу України в системі європейської безпеки: завдяки успішній інтеграції правоохоронних органів у транскордонні операції (Європол, мережа SIENA) Україна остаточно перейшла від ролі пасивного реципієнта допомоги до статусу активного донора та творця світових прецедентів колективної безпеки.

За результатами проведеного дослідження запропоновано:

- *По-перше*, створення в Україні національного Інституту безпеки ШІ (за прикладом Офісу штучного інтелекту ЄС та досвіду Великої Британії), який має стати єдиним координаційним хабом для превенції та розслідування високотехнологічних кіберзлочинів.
- *По-друге*, розроблено та впроваджено в освітній процес Олеся Гончара ДНУ авторський спецкурс «Правові засади кіберстійкості та цифрова держава» для підготовки нової генерації фахівців, здатних забезпечувати когнітивний імунітет нації та сталий повоєнний розвиток України.

Дякую за увагу!

Завершивши доповідь, здобувач відповів на **запитання учасників міжкафедрального наукового семінару**.

ЗАПИТАННЯ ТА ВІДПОВІДІ:

Канд. юрид. наук, доц. Живова Ю.В.: Ви пропонуєте криміналізувати створення та поширення дипфейків, згенерованих штучним інтелектом (наприклад, синтетична дитяча порнографія, (ШІ-контент експлуатації дітей); дезінформаційні воєнні дипфейки (фейкові накази та звернення командування); ШІ-шантаж та реванш-порно (підробка інтимного контенту дорослих). Як на практиці Ваша проактивна кримінологічна модель допоможе виявляти такі загрози ще до того, як вони завдадуть реальної шкоди людині чи державі?

А.А. Олійник, здобувач: *Дякую за запитання*! Насправді всі три наведені вами приклади від ШІ-експлуатації дітей до воєнних фейків і шантажу об'єднує те, що вони б'ють по найвразливішому: по людській психіці та довірі.

Наша проактивна модель працює на випередження і допомагає зупинити ці загрози ще «на зльоті» завдяки трьом практичним крокам:

Перший - Технічний рівень. Ми пропонуємо впровадити обов'язкове цифрове маркування (*водяні знаки*) для будь-яких ШІ-програм. Це дозволить спеціальним алгоритмам безпеки автоматично розпізнавати підробку (дипфейк)

під час її завантаження в мережу й блокувати поширення до того, як відео стане вірусним.

Другий - Інституційний крок швидкої реакції через Хаб. Запропонований у дисертації Національний інститут безпеки ШІ (за аналогією з Інститутом штучного інтелекту ЄС та досвіду Великої Британії) має працювати як єдиний аналітичний центр 24/7. Він не чекає, поки жертва прийде з заявою до поліції. Інститут проводить постійний моніторинг і за допомогою автоматизованих систем виявляє аномальні сплески дезінформації чи масові розсилки шантажу, миттєво передаючи дані Кіберполіції чи СБУ.

І, третій крок - Когнітивний рівень. Навіть найкращий софт може пропустити загрозу, тому головний щит - це людина. Запропонований спецкурс у ДНУ та ширші програми кібергігієни вчать розпізнавати маніпуляції ШІ на рівні критичного мислення. Коли студент, військовий чи пересічний громадянин знає, як перевірити автентичність відео за 30 секунд, дипфейк втрачає свою силу і не завдає шкоди. Тому проактивна модель не чекає скоєння злочину, щоб потім його розслідувати. Вона створює умови, за яких згенерувати і поширити небезпечний дипфейк стає технічно складно, юридично карано, а для суспільства - очевидно.

Д-р. юрид. наук, проф. Патерило І.В.: Ваша концепція «когнітивного імунітету суспільства» виглядає перспективно. Які конкретні інструменти, на Вашу думку, повинна використовувати держава, щоб сформувати цей імунітет у пересічних громадян для захисту від ворожих ІПСО та психологічних маніпуляцій?

А.А. Олійник, здобувач: *Дякую за запитання*! Знаєте, якщо звичайний кіберзахист це «маска та антисептик» для комп'ютера, то когнітивний імунітет - це внутрішній біологічний захист самої людини. Навіть якщо ворожа ІПСО пробиває технічні фільтри і з'являється в екранному просторі, громадянин із міцним когнітивним імунітетом просто не дасть цьому вірусу інфікувати свій мозок.

Щоб сформувати таку стійкість у пересічних громадян, держава має використовувати такі інструменти:

1. Масштабування досвіду. Ми не можемо приставити до кожного коментаря в соцмережах офіцера СБУ або ЦПД. Проте ми можемо навчити людей мислити критично. Практичним кроком моєї роботи є впровадження спецкурсу в ДНУ. Держава має масштабувати цей підхід: зробити короткі, обов'язкові модулі з медіаграмотності та кібергігієни для всіх від школярів та студентів до держслужбовців та військових. Людина має автоматично, за 30 секунд, вміти розрізняти емоційний маніпулятивний контент від фактів.
2. Державний інструмент швидкого інформування. Центр протидії дезінформації та Мінцифри мають працювати проактивно. Замість довгих офіційних спростувань через три дні, держава повинна запускати миттєві, лаконічні «сповіщення про небезпеку» в популярних месенджерах чи Дії (наприклад: *"Увага! Зараз мережею шириться ШІ-дипфейк про евакуацію, оригінал заяви тут"*). Це дає людям психологічну опору і руйнує ефект несподіванки, на який розраховують спецслужби ворога.

3. Гейміфікація та інтерактивні симулятори. Сухі пам'ятки та буклети ніхто не читає. Пересічного громадянина треба вчити через гру. Створення державних безкоштовних онлайн-симуляторів (де людина на практиці пробує себе в ролі «мисливця за фейками» або навіть у ролі бота, щоб зрозуміти механізм обману) підвищує віктимологічну безпеку у рази ефективніше, ніж будь-які заборони. Тому когнітивний імунітет не будується заборонами інтернет-ресурсів. Він будується через підвищення інтелектуального капіталу нації. Коли українці навчаться розпізнавати алгоритми соціальної інженерії так само легко, як правила дорожнього руху, будь-яка транснаціональна інформаційна атака просто розіб'ється об наше суспільство

Канд. юрид. наук, доц. Мудриєвська Л.М.: Ви вводите у науковий обіг авторські дефініції «кіберстійкість» і протиставляєте його звичайному поняттю «захисту». Поясніть: чому в умовах воєнного стану державі недостатньо просто мати «кіберзахист» і чому важливо будувати саме «кіберстійкість»?

А.А. Олійник, **здобувач:** *Дякую за запитання*! Воно дозволяє наочно продемонструвати зміну філософії безпеки, яку я запропоновано у роботі.

Найпростіше різницю між цими поняттями можна пояснити через медичну або військову аналогію:

Кіберзахист - це статична фортечна стіна. Головна логіка захисту - побудувати максимально міцний паркан, закрити всі двері й сподіватися, що ворог не пройде. Але в умовах сучасної повномасштабної кібервійна ідеального захисту не існує. Рано чи пізно будь-яку стіну пробивають через новітній штучний інтелект, уразливості систем чи банальну людську помилку (соціальну інженерію). І коли стіну кіберзахисту пробито, система, яка не має стійкості, просто «падає», паралізуючи міністерства, лікарні чи банківську сферу.

Кіберстійкість - це живий організм, який тримає удар. Навіть якщо ворог пробив технічний периметр і заніс вірус у систему, кіберстійкість дозволяє державі не зупинятися. Система продовжує виконувати свої критичні функції в умовах успішної атаки, локалізує загрозу і миттєво відновлюється до первинного стану.

Чому в умовах воєнного стану класичного кіберзахисту державі вже замало?

По-перше, ворог діє безперервно. Зафіксувати понад 4 500 масштабних атак на рік і відбити абсолютно всі фізично неможливо. Держава повинна вміти жити, воювати й надавати цифрові послуги громадянам *безпосередньо під час атак*.

По-друге, це бінарна система. На відміну від суто технічного захисту, авторська модель кіберстійкості поєднує техніку (макрорівень) та людину (мікрорівень). Якщо уражено сервер, але персонал має високу цифрову гігієну та алгоритми швидкого реагування, державний реєстр підніметься за лічені хвилини.

Тому, кіберзахист - це спроба уникнути синяків та ран, що в умовах війни нереально. А кіберстійкість — це здатність піднятися після будь-якого нокдауну,

зберегти цифровий суверенітет і продовжити боротьбу. Саме на розбудову такої проактивної та живучої моделі й спрямовані результати дис. Дослідження.

Д-р. юрид. наук, проф. Бережна К. В.: У своїй доповіді ви характеризували перехід від криміналізації кіберзлочинів до побудови системної кіберстійкості інфраструктури та захисту приватності. Як саме процесуальні інструменти Будапештської конвенції та нової Конвенції ООН Про запобігання, припинення та боротьбу з кіберзлочинністю (2025 року) дозволяють Україні подолати проблему юридичної атрибуції кібератак і кваліфікувати їх як воєнні злочини для майбутніх міжнародних трибуналів?»

А.А. Олійник, здобувач: *Дякую за запитання*! Ви праві, сьогодні це складна проблема. Спіймати хакера за руку в Інтернеті - це одне, а от перетворити цифри, лог-файли чи якісь IP-адреси на реальні, допустимі докази для суду в Гаазі - це величезний виклик»

У своєму дослідженні я виділяю три прості кроки, як Будапештська конвенція та нова Конвенція ООН 2025 року допомагають Україні вирішити цю проблему на практиці:

1. Вони допомагають знайти справжнього винного (проблема атрибуції). Головна хитрість агресора — сховатися за анонімними хакерами. Процесуальні інструменти конвенцій (зокрема, статті про термінове збереження та вилучення комп'ютерних даних) дозволяють нашим правоохоронцям офіційно відстежити весь ланцюжок команд: від комп'ютера хакера до кабінету конкретного військового генерала РФ.
2. Вони дають швидкі та юридично "чисті" докази. Гаазький трибунал має дуже суворі вимоги до доказів. Оскільки ці конвенції визнані світом, зібрані за ними цифрові сліди автоматично вважаються допустимими у суді. Більше того, Другий додатковий протокол дозволяє нам напряму, без довгової бюрократії, брати інформацію у світових IT-гігантів (Google, Microsoft тощо), щоб довести умисел ворога знищити нашу цивільну інфраструктуру.
3. Вони прирівнюють кібератаки до звичайних воєнних злочинів. Завдяки чітким міжнародним визначенням, ми можемо накласти технічні параметри хакерського удару на класичні правила війни. Якщо цифровий удар по електростанції чи лікарні призводить до таких же катастрофічних наслідків, як приліт звичайної ракети, конвенції дозволяють Гаазі кваліфікувати цю кібератаку як повноцінний воєнний злочин.

Вказані міжнародні механізми не дозволять агресору сховатися за анонімністю в Інтернеті. Вони перетворюють віртуальні сліди на реальні кримінальні вироки для воєнних злочинців».

ВИСТУПИЛИ: науковий керівник здобувача д-р. юрид. наук, проф. Н. С. Юзікова, фахівці: канд. юрид. наук, доц. Ю. В. Живова, канд. юрид. наук, доц. Л. М. Мудрієвська, д-р. юрид. наук, проф. Т.В. Корнякова.

Після відповідей на запитання учасників міжкафедрального семінару було озвучено **висновок наукового керівника здобувача,** д-р. юрид. наук, проф . **Юзікової Наталії Семенівни,** з оцінкою роботи здобувача у процесі підготовки

дисертації та виконання індивідуального плану наукової роботи та індивідуального навчального плану.

ВИСТУП НАУКОВОГО КЕРІВНИКА:

Добрий день, шановні члени міжкафедального наукового семінару, шановні присутні! Повідомляю, що відгук з оцінкою роботи аспіранта 4 року навчання Олійника Артема Андрійовича подано до відділу аспірантури та головуючому на засіданні сьогоднішнього міжкафедального наукового семінару.

Олійник Артем Андрійович з 23.09.2022 року по 2026 рік навчався в аспірантурі Дніпровського національного університету імені Олеся Гончара з метою здобуття наукового ступеню «доктор філософії». У 2022 році отримав диплом магістра у Національному юридичному університеті імені Ярослава Мудрого. За період навчання в аспірантурі здобувач Олійник А.А. у повному обсязі та своєчасно виконав навчальний план підготовки доктора філософії, затверджений рішенням Вченої ради Дніпровського національного університету імені Олеся Гончара, протокол № 4 від 01.12.2022 року.

Аспірантом успішно опановані такі передбачені планом дисципліни, як «Філософія та наукова етика», «Іноземна мова», «Інноваційно-дослідницька діяльність», «Методологія педагогічного процесу у вищій школі», «Методологія кримінологічних досліджень», «Адміністративний процес в парадигмі права», «Актуальні проблеми адміністративного права», «Актуальні проблеми кваліфікації злочинів», «Адміністративний процес в парадигмі права», а також успішно пройдено педагогічну практику.

Індивідуальний план наукової роботи Олійником А.А. виконаний своєчасно у повному обсязі. При цьому, ним виконані всі види робіт, пов'язані з проведенням дисертаційного дослідження та оформлення його результатів. При проходженні в аспірантурі викладацької практики аспірант представив головні положення дослідження у контексті захисту інформаційної безпеки.

Під час проведення дослідження Олійником А.А. виявлені глибокі знання у сфері права, загалом, та щодо предмета компаративістського й кримінологічного дослідження інституту інформаційної безпеки, зокрема, здатність до здійснення наукового пошуку, досконале володіння загальними та спеціальними методами дослідницької діяльності та творчого пошуку ефективних новітніх шляхів запобігання високотехнологічній злочинності в Україні в умовах сучасних гібридних викликів.

При виконанні індивідуального плану та дисертаційного дослідження здобувач виявив наполегливість, працьовитість, цілеспрямованість і творчий підхід до розв'язання складних наукових задач, обґрунтування і аналізу отриманих результатів, наполегливість та організованість у процесі наукового пошуку. Основні результати дисертації одержано автором самостійно.

За період навчання в аспірантурі за темою дисертації Олійником А.А. опубліковано 10 наукових праць, з них 5 статей у наукових фахових виданнях України категорії Б. Основні положення, висновки й рекомендації дисертації обговорювалися на засіданнях кафедри. Апробацію одержаних наукових

результатів дисертаційного дослідження здійснено у виступах на міжнародних та всеукраїнських науково-практичних конференціях, форумах, круглих столах: всеукраїнському науково-практичному юридичному форуму «Національна парадигма правового розвитку сучасної України» (м. Дніпро 18.05. 2023 р.); всеукраїнській науково-практичній конференції «Забезпечення принципів поваги, захисту та реалізації прав дитини у цифровому середовищі» (м. Дніпро 23.11.2023 р.); всеукраїнському науково-практичному круглому столі «Інформаційна агресія в сучасному світі: правовий аналіз та протидія» (м. Харків, 21.06. 2024 р.); міжнародній науково-практичній конференції «Актуальні проблеми прав людини: від універсальних стандартів до національної практики» (м. Львів – Торунь 10.12.2025 р.); всеукраїнській науково-практичній конференції «Актуальні проблеми правової науки (м. Запоріжжя 22.12. 2025 р.). Вимоги МОН України щодо кількості публікацій за результатами дисертаційного дослідження та їх рівня повністю виконано.

Сьогодні здобувач отримав низку важливих нових наукових результатів, що належним чином аргументовані, відповідають високому теоретичному рівню, логічно пов'язані між собою, а їх реалізація в комплексі дозволить на якісно новому рівні сформувати проактивну модель протидії гібридним загрозам, модернізувати систему захисту критичної інфраструктури та суттєво вдосконалити загальнодержавний механізм забезпечення національного інформаційного суверенітету.

Серед нових положень, запропонованих дисертантом, на особливу увагу заслуговують:

- обґрунтування комплексної трирівневої моделі інформаційної безпеки як об'єкта кримінологічного захисту, яка базується на розширеній міжнародній матриці (Тріаді CIA, доповненій елементами автентичності й неспростовності) та структурно розподіляється на інфраструктурний, правовий і когнітивний рівні із визначенням специфічних векторів превенції для кожного з них;
- удосконалення періодизації розвитку системи інформаційної безпеки України із виокремленням четвертого етапу (з 2014 року до сьогодення), який характеризується онтологічним переходом від реактивного технічного захисту до стратегічної кіберстійкості держави та захисту суспільної свідомості в умовах воєнного стану;
- розробка чотирирівневого виконавчого (процесуального) механізму, який через синергію Будапештської конвенції та норм міжнародного гуманітарного права забезпечує чіткий алгоритм притягнення агресора до юридичної відповідальності за кібератаки (на рівнях атрибуції, легітимізації доказів для Міжнародного кримінального суду, доведення умислу та кваліфікації як воєнних злочинів);
- Обґрунтування дворівневого розподілу поняття «кіберстійкість» на державний (публічно-правовий) та особистісний (людиноцентричний) рівні із формулюванням їхніх авторських дефініцій;
- запровадження у науковий обіг категорій «когнітивний імунітет суспільства» (як самостійної кримінологічної та віктимологічної категорії) та

«техногенна віктимність організацій» у контексті використання хмарних сервісів;

- класифікація зарубіжних моделей кіберстійкості (континентальної, англосаксонської, транзитної) та обґрунтування доцільності формування в Україні гібридної моделі, що інтегрує правову стабільність, операційну гнучкість та інноваційну динаміку.

Дослідження у цих напрямках представляють глибокий теоретичний і практичний інтерес.

Позиції, які відстоює автор, ґрунтуються на наявних досягненнях світової та вітчизняної кримінологічної доктрини, положеннях суміжних галузей права: кримінального права, кримінального процесуального права, міжнародного гуманітарного права, а також філософії, соціології, психології та політології. Наведений у дослідженні матеріал містить значний особистий доробок дисертанта, який суттєво збагачує уявлення стосовно засад забезпечення інформаційної безпеки в Україні, включаючи вдосконалення превентивних механізмів, гармонізацію національного законодавства з європейськими стандартами верховенства права та формування національної кіберстійкості в умовах локальних і глобальних викликів, воєнного стану та повоєнного відновлення держави. Олійник А.А. продемонстрував вміння самостійно узагальнювати та аналізувати національні нормативно-правові акти, практику ЄСПЛ, міжнародні стандарти (FISMA, Директива NIS2, нова Конвенція ООН 2025 року), зарубіжну практику й спеціальну літературу, чітко визначати наукові завдання й формулювати обґрунтовані пропозиції щодо їх розв'язання.

Отримані висновки і рекомендації зумовили обґрунтування необхідності і доцільності запровадження низки змін і уточнень до чинного законодавства України щодо загальнодержавної інформаційної безпекової політики, формування випереджальних превентивних механізмів, ефективної координації інституцій влади (МВС, Нацполіція, ЦПД), а також реалізації авторської пропозиції стосовно заснування національного Інституту безпеки ШІ як головного координаційного хабу (за прикладом провідних світових інституцій, таких як Інститут безпеки ШІ Великої Британії та Офіс штучного інтелекту Європейського Союзу).

Отже, дисертаційне дослідження Олійника А.А. побудоване на комплексному, системному підході, характеризується високим рівнем наукових узагальнень. Автор використав достатній обсяг фундаментальних робіт з філософії, конституційного, міжнародного, кримінального права, кримінології, а також логіки, соціології та політології.

Результати дисертаційного дослідження Олійником А.А. впроваджено у практичну, наукову та освітню діяльність. Зокрема, отримано акти впровадження результатів дослідження у наукову діяльність та освітній процес Дніпровського національного університету імені Олеся Гончара щодо можливості та доцільності використання наукових доробок здобувача при проведенні занять із навчальних дисциплін «Кримінологія», «Запобігання злочинності у контексті глобалізації», «Кримінальне право України», а також запровадження авторського міждисциплінарного спецкурсу «Правові засади кіберстійкості та

цифрова держава». Дисципліна спрямована на підготовку нової генерації фахівців (правників, політологів, соціологів), які володітимуть крос-функциональними компетентностями для ефективної протидії гібридним загрозам, захисту критичної інфраструктури та формування когнітивного імунітету суспільства в умовах сталого повоєнного розвитку України

Таким чином, за результатами навчання в аспірантурі та проведеним дисертаційним дослідженням здобувачем підтверджено високий рівень теоретичних знань, умінь, навичок та інших здібностей, достатніх для реалізації нових ідей, розв'язання комплексних проблем у галузі професійної та дослідницької діяльності, а також проведення власного монографічного дослідження, результати якого мають наукову новизну, глибоке теоретичне та практичне значення для забезпечення інформаційної безпеки в міжнародному, національному та зарубіжному вимірах в умовах воєнного стану, гібридної війни та активного розвитку технологій штучного інтелекту.

Висновок: дисертація **Олійника Артема Андрійовича на** тему «Кримінологічні засади забезпечення інформаційної безпеки: міжнародний, національний та зарубіжний виміри» яка підготовлена на кафедрі адміністративного і кримінального права Дніпровського національного університету імені Олеся Гончара, за своїм змістом, науковою новизною та методологічним підходом є самостійною, завершеною кваліфікаційною науковою працею. У дисертаційному дослідженні отримано нові, належним чином аргументовані результати, які в сукупності вирішують актуальне наукове завдання щодо формування цілісних кримінологічних засад превенції сучасних кіберзагроз та розбудови національної кіберстійкості.

Автор дисертації Олійник Артем Андрійович за всіма набутими компетентностями заслуговує на присудження ступеня доктора філософії зі спеціальності 081 Право, а робота може бути рекомендована до захисту у разовій спеціалізованій вченій раді.

Дякую за увагу!

ВИСНОВКИ ФАХІВЦІВ-ЕКСПЕРТІВ:

Д-р. юрид. наук, проф. Т.В. Корнякова: Представлена дисертаційна робота Олійника Артема Андрійовича, присвячена формуванню та реалізації кримінологічних засад інформаційної безпеки, відзначається своєю чіткою прагматичною спрямованістю та критичним значенням для правозастосування в сучасних реаліях. В умовах воєнного стану та активізації гібридних загроз автор зміг вийти за межі суто кабінетної теорії та сфокусувався на розробці реальних механізмів захисту інформаційного простору України.

Практична цінність дослідження полягає у глибокому аналізі чинників, що зумовлюють кіберзлочинність, та розробці конкретних кримінологічних рекомендацій щодо протидії деструктивним когнітивним впливам на суспільство. Автор детально проаналізував зарубіжні інструменти мінімізації безпекових ризиків в інтернеті та адаптував їх до національних правових реалій. Сформульовані висновки мають високу прикладну якість і можуть

безпосередньо використовуватися суб'єктами правозастосовної діяльності для оптимізації стратегій захисту прав особи та держави.

Робота виконана на належній емпіричній та статистичній базі, є глибокою та практично значущою. Без сумніву, дисертація Олійника Артема Андрійовича відповідає всім критеріям самостійного наукового пошуку, та може бути рекомендована до публічного захисту у разовій раді за спеціальності 081 Право.

канд. юрид. наук, доц. Ю. В. Живова: Дисертація Олійника Артема Андрійовича є сміливою та комплексною працею, яка заповнює суттєві прогалини у вітчизняній кримінологічній доктрині безпеки. Автор виявив високу наукову зрілість, обравши предметом аналізу складне перехрестя міжнародного, зарубіжного та національного рівнів правового регулювання інформаційних відносин в умовах кризи та воєнного стану.

Цікавою та науково обґрунтованою виглядає позиція автора щодо імплементації міжнародно-правових стандартів безпеки в українське законодавство крізь призму цифрової трансформації суспільства. Особливу увагу привертає здійснений автором аналіз детермінації кіберзлочинності, що дозволило виокремити найбільш ефективні зарубіжні практики кримінологічного запобігання цим явищам. Запропоновані дисертантом дефініції, класифікації загроз та когнітивних впливів свідчать про формування його як зрілого науковця, здатного до генерації нових юридичних ідей. Робота написана грамотною науковою мовою, а її висновки є переконливими.

Загалом, дисертаційне дослідження Олійника Артема Андрійовича є вагомим науковим здобутком. Робота повністю відповідає встановленим вимогам, і я можу рекомендувати дисертацію до захисту у разовій спеціалізованій раді щодо присудження ступеня доктора філософії за спеціальністю 081 «Право».

Канд. юрид. наук, доц. Л. М. Мудриєвська: Дисертаційне дослідження Олійника Артема Андрійовича на тему «Кримінологічні засади забезпечення інформаційної безпеки: міжнародний, національний та зарубіжний виміри» є актуальним та своєчасним науковим оглядом, що безпосередньо відповідає глобальним викликам сучасності. Обізнаність автора проявилась у глибокому аналізі теоретико-методологічних засад запобігання злочинності в інформаційному просторі.

Особливу наукову цінність роботі надає комплексний підхід до вивчення закономірностей детермінації кіберзлочинності та когнітивних впливів в умовах глобалізації й стрімкої цифрової трансформації суспільства. Автор продемонстрував високий рівень наукового мислення, вдало поєднавши міжнародні стандарти, специфіку національного законодавства та передовий досвід зарубіжних країн. Порівняльно-правовий аспект є ключовим елементом, що дозволив дисертанту не лише констатувати проблеми, але й запропонувати цілісні моделі правового реагування на новітні інформаційні загрози. Структура дисертації логічна, виклад матеріалу послідовний та науково обґрунтований.

На мою думку, виконана робота має достатньо високий науковий рівень і демонструє вагомий внесок у розвиток теорії інформаційної безпеки, кримінального права та кримінологічної науки в цілому. Вважаю цю дисертацію цілісним, глибоким та практично значущим науковим дослідженням та можу рекомендувати до захисту роботи Олійника Артема Андрійовича на разовій спеціалізованій вченій раді для здобуття ступеня доктора філософії за спеціальністю 081 Право.

Голова міжкафедрального семінару юридичного факультету д-р юрид. наук, проф. К.В. Бережна:

Чи є ще бажаючі виступити? Якщо бажаючих немає, то давайте перейдемо до обговорення висновку.

ВИСНОВОК

Актуальність теми дисертації. 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.

Для України ця проблема набуває важливого значення, тому що в умовах повномасштабної збройної та гібридної агресії кіберпростір перетворився на повноцінний простір воєнних дій. За таких умов формування новітніх правових механізмів протидії кіберзагрозам перестає бути суто галузевим юридичним завданням і стає ключовим фактором збереження державного суверенітету, забезпечення національної безпеки та захисту демократичного розвитку України.

Затвердження теми та плану дисертації. Тема дисертації «Кримінологічні засади забезпечення інформаційної безпеки: міжнародний, національний та зарубіжні виміри» затверджена Вченою радою Дніпровського національного університету імені Олеся Гончара відповідно до встановленого порядку підготовки здобувачів третього (освітньо-наукового) рівня вищої освіти за спеціальністю 081 «Право».

Зв'язок роботи з науковими програмами, планами, темами. Дисертаційне дослідження виконано відповідно до пріоритетних напрямів розвитку юридичної науки України, Стратегії інтеграції України до Європейського Союзу, положень Угоди про асоціацію між Україною та ЄС, а також у межах науково-дослідної роботи кафедри кримінального права та кримінології Дніпровського національного університету імені Олеся Гончара, пов'язаної з дослідженням сучасних проблем кримінального права, кримінальної

політики та адаптації кримінального законодавства України до європейських стандартів.

Публікації та особистий внесок здобувача. Основні положення, висновки та рекомендації дисертаційного дослідження доповідалися та обговорювалися на засіданнях кафедри кримінального права та кримінології Дніпровського національного університету імені Олеся Гончара, а також на міжнародних і всеукраїнських науково-практичних конференціях.

Результати дослідження відображено у наукових публікаціях здобувача, зокрема у фахових наукових статтях з юридичних наук та тезах доповідей на науково-практичних конференціях. Усі наукові результати, висновки та пропозиції, викладені в дисертації, отримані автором самостійно.

Наукова новизна одержаних результатів. Наукова новизна дисертаційного дослідження полягає в тому, що дисертація є першим в Україні комплексним монографічним дослідженням, в якому реалізовано кримінологічно-інтегративний підхід до формування засад забезпечення інформаційної безпеки, гармонізованих із європейськими стандартами верховенства права, з визначенням шляхів розв'язання низки фундаментальних і прикладних проблем національної кіберстійкості.

Найсуттєвішими вважаються такі положення:

Вперше:

- обґрунтовано 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;
- обґрунтовано дворівневий розподіл поняття «кіберстійкість» у контексті забезпечення інформаційної безпеки на державний (публічно-правовий) та особистісний (людиноцентричний) рівні, й запропоновано авторське визначення. 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;

- підхід до забезпечення інформаційної безпеки України в умовах розвитку технологій штучного інтелекту шляхом приєднання до європейської системи кібербезпеки та інтеграції авторської пропозиції заснування національного Інституту безпеки ШІ (за прикладом Інституту безпеки штучного інтелекту Великої Британії) як координаційного хабу для впровадження міжнародних стандартів у практику запобігання, виявлення і розслідування високотехнологічних кіберзлочинів;
- запропоновано визначення «когнітивного імунітету суспільства» як самостійної кримінологічної та віктимологічної категорії, що становить мікрорівень національної кіберстійкості і визначає здатність суспільства виступати самозахисним бар'єром проти транснаціональних інформаційно-психологічних операцій та шахрайства у цифровому середовищі.

вдосконалено:

- віктимологічний підхід 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;
- періодизацію розвитку системи забезпечення інформаційної безпеки України шляхом виокремлення IV (з 2014 року до сьогодення), який зумовлений воєнними викликами і характеризується переходом від технічного захисту до формування стратегічної кіберстійкості держави;
- 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;
- кримінологічну характеристику кіберзлочинності в умовах воєнного стану, шляхом включення до неї нових факторів криміногенного ризику штучного інтелекту та Інтернету речей та обґрунтовано доцільність криміналізації нових цифрових загроз, зокрема, створення та поширення згенерованого за допомогою ШІ синтетичного контенту експлуатації дітей;
- підхід до класифікації моделей забезпечення кіберстійкості шляхом виокремлення чотирьох взаємозалежних вимірів (стратегічного, нормативного, інституційного та екосистемного), що дозволяє комплексно оцінювати рівень «кіберзрілості» держави і суспільства;

набуло подальшого розвитку:

- науковий підхід до розуміння сутності інформаційної безпеки держави, що ґрунтується на інтеграції правових, соціальних та етичних аспектів у єдину систему захисту; забезпеченні справедливої рівноваги між свободою слова та межами державного контролю задля превенції кіберзлочинності; гармонізації міжнародних стандартів (зокрема, Будапештської конвенції та GDPR) із національними правовими традиціями, а також на впровадженні випереджальних превентивних механізмів, які враховують поведінкові ризики та соціальні фактори протиправності у цифровому середовищі;
- антропоцентричний підхід до забезпечення інформаційної безпеки, де найвищим пріоритетом (соціально-психологічним рівнем) визнається захист суспільної свідомості, процесу формування волі та цифрових прав людини;
- положення щодо зміни міжнародно-правового статусу України в системі європейської кібербезпеки шляхом успішній інтеграції правоохоронних органів України у спільні транскордонні поліцейські операції та системи обміну розвідувальними даними (Європол. SIENA), для остаточного національного переходу від ролі реципієнта (об'єкта захисту) до статусу активного учасника колективної безпеки.

Практичне значення одержаних результатів. Практичне значення результатів дослідження 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 (акт впровадження в наукову діяльність Дніпровського національного університету імені Олеся Гончара від 9 вересня 2025 р.);
- 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 ьа запобігання транскордонних кіберзлочинів, 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» (акт впровадження у навчальний процес Дніпровського національного університету імені Олеся Гончара від 07.10. жовтня 2025 р.).

Список публікацій здобувача за темою дисертації,
в яких опубліковані основні наукові результати дисертації:

1. Олійник А. А. Сутність інформаційної безпеки як правового явища у національному та міжнародному просторі. *Актуальні проблеми вітчизняної юриспруденції* № 6. 2023. С.293-299. DOI https://doi.org/10.32782/2408-9257-2023-6-45.
2. Олійник А. А. Формування стійкого цифрового суспільства: превентивна роль інформаційної безпеки та кримінально-правової політики у запобіганні злочинності . *Актуальні проблеми вітчизняної юриспруденції* № 2. 2025. С. 177-182. DOI https://doi.org/10.32782/2408-9257-2025-2-27
3. Олійник А. А. Запобігання правопорушенням у сфері інформаційної безпеки: від захисту державного суверенітету до гарантування прав людини. *Актуальні проблеми вітчизняної юриспруденції* № 6. 2025. С.129-134. DOI https://doi.org/10.32782/2408-9257-2025-6-19
4. Олійник А.А. Кіберстійкість та права людини: імплементація міжнародних превентивних моделей у цифровий простір в Україні. *Аналітичне порівняльне правознавство* № 6. Ч. 3. 2025. С. 84-90. DOI https://doi.org/10.24144/2788-6018.2025.06.3.12
5. Юзікова Н.С., Олійник А. А. Напрями забезпечення правопорядку на звільнених територіях: інституційні підходи, довіра та практики взаємодії поліції й громади. *Науковий вісник УжНУ. Серія "Право"* № 93. Частина 4. 2026. С.247-255. DOI https://doi.org/10.24144/2307-3322.2026.93.4.35

Які засвідчують апробацію матеріалів дисертації:

6. Олійник А.А. Організація безпеки інформаційного суверенітету для України як об'єкта глобальних інформаційних впливів Збірник тез Всеукраїнського науково-практичного юридичного форуму «Національна парадигма правового розвитку сучасної України» (Дніпровський національний університет імені Олеся Гончара, м. Дніпро, 18 травня 2023 року). Дніпро: Ліра, 2023. С. 334-340. URL:https://www.dnu.dp.ua/docs/ndc/2023/materiali%20konf/new_NACIONALNA%20PARADIGMA.pdf
7. Олійник А.А. Модель забезпечення цифрової безпеки в мережі internet крізь призму досвіду зарубіжних країн. Збірник тез Всеукраїнської науково-практичної конференції "Забезпечення принципів поваги, захисту та реалізації прав дитини у цифровому середовищі». (м. Дніпро 23.листопада 2023) Дніпровський національний університет імені Олеся Гончара, Дніпро, Ліра, 2023. С.349-352 URL: https://www.dnu.dp.ua/docs/ndc/2023/ materiali%20konf/new_Zbirnyk_Konf_Zahyst%20prav_dytyny_v_cifrovomu_sviti.pdf
8. Олійник А.А. Окремі форми інформаційної агресії матеріали всеукраїнського науково-практичного круглого столу. Інформаційна агресія в сучасному світі: правовий аналіз та протидія Харків, 21 червня 2024 р. : електрон. наук. вид. / редкол.: В. С. Батиргареєва та ін. – Харків : Майдан, 2024. С. 56-58. https://ivpz.kh.ua/wp-content/uploads/2024/11/%D0%86%D0%BD%D1%84%D0%BE%D0%B0%D0%B3%D1%80%D

0%B5%D1%81%D1%96%D1%8F_21.06-%D0%B7%D0%B1%D1%96%D1%80%D0%BD%D0%B8%D0%BA_compressed.pdf

9. Олійник А. А. Міжнародне запобігання злочинності у сфері цифрових технологій у контексті захисту прав людини. Матеріали міжнародної науково-практичної конференції. Актуальні проблеми прав людини: від універсальних стандартів до національної практики : Київський університет права Національної академії наук України, 11 грудня 2025 р. Львів – Торунь : Liha-Pres, 2025. С. 100-104.
DOI https://doi.org/10.36059/978-966-397-557-3-27
10. Олійник А.А. Методологічний потенціал генетичного підходу Б. О. Кістяківського у дослідженні генези прав людини. Матеріали Всеукраїнської науково-практичної конференції «Актуальні проблеми правової науки. Запоріжжя. 22.12. 2025. С.79-82. URL: https://www.znu.edu.ua/faculty/law/nauka/2025/_vseukrayins__koyi_naukovo-praktichnoyi_konferents__yi_aktual__n___problemi_pravovoyi_nauki_ta_pravookhoronnoyi_d__yal__nost__.pdf

На підставі заслуховування та обговорення доповіді Олійника А.А.. про основні положення дисертаційної роботи, питань та відповідей на них

УХВАЛИЛИ:

1. Дисертаційна робота Олійника Артема Андрійовича на тему: «Кримінологічні засади забезпечення інформаційної безпеки: міжнародний, національний та зарубіжний виміри», подана на здобуття ступеня доктора філософії з галузі 08 Право за спеціальністю 081 Право є завершеним, самостійним дослідженням, в якому отримані нові науково обґрунтовані результати, що розв'язують конкретне наукове завдання і відповідає вимогам «Порядку присудження ступеня доктора філософії та скасування рішення разової спеціалізованої вченої ради закладу вищої освіти, наукової установи про присудження ступеня доктора філософії» (Постанова Кабінету Міністрів України від 12.01.2022 р. № 44) та може бути винесена на розгляд Вченої ради Дніпровського національного університету імені Олеся Гончара для розгляду питання про утворення спеціалізованої вченої ради для разового публічного захисту дисертації на здобуття ступеня доктора філософії за спеціальності 081 Право.

2. Рекомендувати дисертаційну роботу Олійника Артема Андрійовича на тему: «Кримінологічні засади забезпечення інформаційної безпеки: міжнародний, національний та зарубіжний виміри», до захисту у разовій спеціалізованій вченій раді для присудження Олійнику А.А. ступеня доктора філософії з галузі знань 08 Право за спеціальністю 081 Право.

3. Клопотати перед Вченою радою університету розглянути питання про створення спеціалізованої вченої ради для проведення разового захисту дисертації на здобуття ступеня доктора філософії зі спеціальності 081 Право Олійника Артема Андрійовича у такому складі:

№ з/п	Прізвище, ім'я, по батькові	Місце основної роботи, підпорядкування, посада	Науковий ступінь, шифр, назва спеціальності, за якою захищена дисертація, рік присудження	Вчене звання (за спеціальністю, кафедрою), рік присвоєння	Наукові публікації, опубліковані за останні п'ять років, за науковим напрямом, за яким підготовлено дисертацію здобувача
1	2	3	4	5	6
1.	Корнякова Тетяна Всеволодівна (голова)	Дніпровський національний університет імені Олеся Гончара Міністерства освіти і науки України, завідувач кафедри адміністративного і кримінального права Дніпровського національного університету імені Олеся Гончара	Доктор юридичних наук 12.00.08 – кримінальне право та кримінологія; кримінально-виконавче право, 2012 р., Україна	професор кафедри адміністративного і кримінального права, 2021 р., Україна	Yevhen Leheza, Volodymyr Shablystyi, Irina V. Aristova, Ivan O. Kravchenko and Tatiana Korniakova Foreign Experience in Legal Regulation of Combating Crime in the Sphere of Trafficking of Narcotic Drugs, Psychotropic Substances, their Analogues and Precursors: Administrative and Criminal Aspect. *Journal of Drug and Alcohol Research* Volume 12 (2023). Issue 4, Article number 236240 **(Scopus)** Режим доступу до ресурсу: https://www.ashdin.com/articles/foreign-experience-in-legal-regulation-of-combating-crime-in-the-sphere-of-trafficking-of-narcotic-drugs-psychotropic-su.pdf DOI: https://doi.org/10.4303/JDAR/236240 Ключові слова: Foreign experience; Illegal trafficking; Narcotic drugs and psychotropic substances; Precursors; Countermeasures; Legal regulation Закордонний досвід; Незаконний обіг; Наркотичні засоби та психотропні речовини; прекурсори; Протидія; Правове регулювання

					Корнякова Т.В. Прогнозування ефективності спеціальної конфіскації як кримінально-правової санкції у запобіганні злочинності/ Predicting the effectiveness of special confiscation as a criminal penalty in preventing crime. Актуальні проблеми вітчизняної юриспруденції № 4. 2023. С 180-185 http://apnl.dnu.in.ua/4_2023/27.pdf DOI https://doi.org/10.32782/39221536 Ключові слова превентивна політика, запобігання злочинності, незаконне збагачення, спеціальна конфіскація, кримінальні правопорушення, справедлива рівновага. Корнякова Т.В. Правове регулювання реагування на правопорушення та події в контексті діяльності Національної поліції України. Наукові праці Міжрегіональної Академії управління персоналом. Юридичні науки. 2023. № 5 С. 31-35(68). https://journals.maup.com.ua/index.php/law/article/view/2967/3416 DOI https://doi.org/10.32689/2522-4603.2023.5.5 Ключові слова: правове регулювання, правопорушення, Національна поліція України, громадський порядок, законодавство, захист прав громадян

2.	Сачко Олександр васильович (рецензент)	Дніпровський національний університет імені Олеся Гончара Міністерства освіти і науки України, професор кафедри адміністративного і кримінального права	Доктор юридичних наук 12.00.09 – кримінальний процес; криміналістика; оперативно-розшукова діяльність; судова медицина та психіатрія, 2019 р., Україна	професор кафедри адміністративного і кримінального права 2022 р., Україна	Сачко О.В. Правосуб'єктність міжнародних неурядових організацій: стан і перспективи розвитку Актуальні проблеми вітчизняної юриспруденції № 4. 2022 рік С. 230-236 Режим доступу до ресурсу: http://apnl.dnu.in.ua/4_2022/35.pdf DOI: https://doi.org/10.32782/39221345 **(Фахове видання, категорія «Б»)** Ключові слова: міжнародна неурядова громадська організація; міжнародна правосуб'єктність; суб'єкт міжнародного права; суб'єкт міжнародних правовідносин; глобалізація; цифровізація; цифрові права. Сачко О.В. Вплив воєнного стану на адміністративно-правове регулювання правопорушень та подій при забезпеченні публічної безпеки та порядку органами поліції. Наукові праці Міжрегіональної Академії управління персоналом. Юридичні науки. 2023. № 5-6(68-69). https://journals.maup.com.ua/index.php/law/article/view/2971/3420 DOI https://doi.org/10.32689/2522-4603.2023.5.9 Ключові слова: Національна поліція України, воєнний стан, адміністративно-правове регулювання, правопорушення, публічна

					безпека, міжнародні стандарти прав людини Сачко О.В. Забезпечення публічної безпеки органами Національної поліції та органами Служби безпеки України під час воєнного стану. Актуальні проблеми вітчизняної юриспруденції. 2023. № 6. С. 128-133. https://apnl.dnu.in.ua/6_2023/23.pdf DOI https://doi.org/10.32782/2408-9257-2023-6-21 Ключові слова: Національна поліція України, Служба безпеки, тероризм, воєнний стан, військова агресія, Антитерористичний центр, публічна безпека.
3	Мудриєвська Людмила Михайлівна (рецензент)	Дніпровський національний університет імені Олеся Гончара Міністерства освіти і науки України, завідувачка кафедри теорії держави і права, конституційного права та державного управління	Кандидат юридичних наук, 12.00.01 - теорія та історія держави і права; історія політичних і правових учень, 2011 р., Україна	Доцент кафедри теорії держави і права, 2004 р. Україна	Мудриєвська Л.М., Тороп М.О. Покарання, як вид юридичної відповідальності в науковій спадщині українських науковців - прихильників позитивістської парадигми середини XIX – початку XX сторіччя. *Аналітично-порівняльне правознавство.* 2024. № 6. С.48- 52. DOI https://doi.org/10.24144/2788-6018.2024.06.6 Ключові слова: покарання, смертна кара, кримінальна відповідальність, поліцейська відповідальність, юридична відповідальність, юридичний позитивізм, каральна система, проступки.

					Капітаненко Н.П., Мудриєвська Л.М. Юридичні гарантії забезпечення інформаційних прав в умовах воєнного стану. *Науковий вісник публічного та приватного права.* 2025. № 1. С. 9-15. DOI https://doi.org/10.32844/2618-1258.2025.1.2. Ключові слова: інформаційні права та свободи, гарантії забезпечення інформаційних прав, юридичні гарантії, обмеження прав і свобод, воєнний стан, кримінальна відповідальність, конституційні права та свободи. Мудриєвська Л.М., Чукаєва В.О. Конституційно-правова відповідальність як гарантія забезпечення прав і свобод людини і громадянина. *Правові новели.* 2025.№ 25. С.7-14. DOI https://doi.org/10.32782/ln.2025.25.01. https://legalnovels.in.ua/journal/25_2025/3.pdf Ключові слова: реальність права, постсоціалістична правова система, права людини і громадянина, конституційно-правова відповідальність, механізм реалізації права.
4.	Бабенко Андрій Миколайович	Одеський державний університет внутрішніх справ. кафедра кримінально-правових	Доктор юридичних наук 12.00.08. – кримінальне право та кримінологія; кримінально-	Професор кафедра кримінального права та кримінології. 2020 р.	Бабенко А.М., Резніченко Г.С., Теслюк І.О. Безпека малолітніх та неповнолітніх осіб в соціальних Інтернет-мережах: сучасні підходи до запобігання правопорушенням.

		дисциплін інституту права та безпеки, завідувач кафедри	виконавче право 2015 р.		Юридичний науковий електронний журнал. 2025. № 10. С.415-417. URL:http://lsej.org.ua/10_2025/96.pdf DOI https://doi.org/10.32782/2524-0374/2025-10/94 Ключові слова: неповнолітні, мережа Інтернет, соціальні Інтернет-мережі, інформаційні технології, злочинність, запобігання Бабенко А.М., Підгородинський В.М., Позігун І.О. Кримінологічний аналіз окремих показників кримінальних правопорушень проти основ національної безпеки України. Актуальні проблеми вітчизняної юриспруденції. 2024. № 5. С.85-92. URL: http://apnl.dnu.in.ua/5_2024/15.pdf DOI https://doi.org/10.32782/2408-9257-2024-5-13 Ключові слова: національна безпека, кримінальні правопорушення, кримінальні правопорушення проти основ національної безпеки, рівень, динаміка, структура, питома вага. Бабенко А.М., Підгородинськнй В.М. Позігун І.О.Будяченко О.М. Міжнародно-правові заходи запобігання відмиванню грошей. *Юридичний науковий електронний журнал*. 2024.

					№ 12. С, 300-302 URL: http://www.lsej.org.ua/12_2024/69.pdf DOI https://doi.org/10.32782/2524-0374/2024-12/67 Ключові слова: запобігання злочинності, відмивання грошей, легалізація доходів, одержаних злочинним шляхом, міжнародноправові заходи, міжнародно-правові угоди, фінансовий моніторинг, кримінальна відповідальність, протидія.
5.	Ричка Денис Олегович (опонент)	ННІ Придніпровська державна академія будівництва та архітектури Українського державного університету науки та технології Доцент кафедри публічного управління та права	Кандидат юридичних наук 12.00.08 – кримінальне право та кримінологія; кримінально-виконавче право, 2019 р., Україна		Ричка Д.О. Кіберінциденти у 2025 році в Україні: державна реакція, кримінально-правові наслідки та динаміка проваджень (порівняння з 2023–2024 роками // Юридичний науковий електронний журнал № 2/2026.- Запоріжжя: С.263-266. DOI https://doi.org/10.32782/2524-0374/2026-2/59 Ключові слова: кібербезпека, кіберзлочинність, міжнародне співробітництво, кримінальна відповідальність, CERT-UA, Держспецзв'язку, кіберінцидент, ЄРДР, цифрове середовище, підслідність, фішинг, шкідливе ПЗ. Ричка Д.О. Кіберсили збройних сил України: науково-практичний аналіз проєкту Закону України «Про кіберсили Збройних сил України» у порівнянні з моделями НАТО// Київський часопис права.

					2025. No 4 – Київ. С139-143. DOI https://doi.org/10.32782/klj/2025.4.20 Ключові слова: кібероборона, Кіберсили, ЗСУ, НАТО, СуОС, NICC, AJP-3.20, права людини, кіберрезерв, NCI Agency, CCDCOE Ричка Д.О. Електронні довірчі послуги, як інструмент зниження криміногенних ризиків у цифровому документообігу// Актуальні проблеми вітчизняної юриспруденції № 6. 2025. – Дніпро. С.141-146. DOI https://doi.org/10.32782/2408-9257-2025-6-21 Ключові слова: цифрове середовище, інформаційна безпека, кримінальне правопорушення, кваліфікований електронний підпис, кваліфікована електронна печатка, кваліфікована електронна позначка часу, довірчий список, запобігання злочинності, кіберзлочинність, підроблення документів, шахрайство, доказування

Результати відкритого голосування:
«За» – 17 осіб.
«Проти» – немає.
«Утрималися» – немає.

Рішення прийнято одноголосно.

Голова
міжкафедрального семінару **Катерина БЕРЕЖНА**

Секретар **Олена ГРАБИЛЬНІКОВА**