До спеціалізованої вченої ради Д 08.727.02
в Дніпропетровському державному
університеті внутрішніх справ

ВІДГУК

офіційного опонента – доктора юридичних наук Тихонової Олени Вікторівни – на дисертаційне дослідження Думчикова Михайла Олександровича «Концептуальні засади кримінально-правової охорони кіберпростору в Україні», подане на здобуття наукового ступеня доктора юридичних наук за спеціальністю 12.00.08 – кримінальне право та кримінологія; кримінально-виконавче право.

Актуальність теми дисертаційної роботи

Активне застосування цифрових технологій у всіх значних сферах життя суспільства є невід'ємною характеристикою сучасності. В даний час цей вектор розвитку суспільного життя об'єктивно обумовлює і суттєве зростання кількості вчинених кримінальних правопорушень із використанням електронно обчислюваної техніки.

Згідно з доповіддю Cybersecurity Ventures, збитки від кримінальних правопорушень у 2023 році сягнули приголомшливих 8 трильйонів доларів США, що на 2 трильйони більше, ніж у 2021 році. Це свідчить про величезний економічний вплив та зростаючу потребу у захисті від подібних інцидентів.

Динаміка злочинності у кіберпросторі в Україні слідує глобальному тренду. Враховуючи військовий стан та збільшення напруги у сфері інформаційної безпеки, стає важливим вжиття заходів для зміцнення кіберпростору. Звіт IBM «Cost of a Data Breach Report 2023» вказує, що 41% аналізованих кримінальних правопорушень у кіберпросторі становив фішинг, з основною метою – збір конфіденційної інформації. Це підкреслює необхідність розвитку антифрауд систем та інтеграції штучного інтелекту у механізми кібербезпеки, що може значно знижувати витрати на витоки даних.

Україна стикається з викликами адаптації національного законодавства до змінюваних умов забезпечення кібербезпеки, що зумовлені стрімкими технологічними змінами та посиленням рівня кіберзагроз. Розробка концептуальних засад кримінально-правової охорони кіберпростору дозволить уніфікувати практику застосування норм кримінального права, забезпечити адаптацію кращих міжнародних практик до українських реалій і, врешті-решт, підвищити ефективність боротьби зі злочинністю у кіберпросторі. Актуальні дані та аналіз трендів не тільки в Україні, але й у світі, демонструють критичну потребу в дієвих правових та технологічних рішеннях для захисту кіберпростору, забезпечення економічної стабільності та захисту прав і свобод громадян в цифрову епоху.

Без сумніву, кримінальні правопорушення, здійснені за допомогою передових інформаційно-телекомунікаційних технологій, мають свої унікальні особливості. Зловживання технічними новинками для здійснення протиправних дій відкриває злочинцям можливості атакувати основоположні суспільні відносини, охороняються законом, включаючи права та інтереси індивідуальності, громадськість та державну безпеку. Складність у виявленні та переслідуванні комп'ютерних злочинців, особливо в кіберпросторі, який не має фізичних кордонів, значно збільшує рівень суспільної загрози таких дій.

Враховуючи зазначене ми цілком переконані, що дисертаційна робота Думчикова Михайла Олександровича, на тему «Концептуальні засади кримінально-правової охорони кіберпростору в Україні» є актуальним та своєчасним, а також відповідає потребам подальшого розвитку України як незалежної, самостійної держави та економічно вільної держави.

Зв'язок роботи із державними та науковими програмами планами та темами

Дисертаційна робота відповідає Цілям сталого розвитку на період до 2030 року та виконана у відповідності до пріоритетних напрямів розвитку науки і техніки в Україні на період до 2024 року. Тематика роботи повністю

відповідає тематичному плану виконання науково дослідних робіт Сумського державного університету, а її основні положення були відображені: 1) проєкт Міністерства освіти і науки України «Концептуальні засади реформування системи правоохоронних органів в сучасних умовах трансформації нагляду і контролю щодо забезпечення економічної безпеки України» (номер державної реєстрації 0120U100474); 2) проєкт Міністерства освіти і науки України «Корупція в умовах воєнного стану та післявоєнної відбудови: оптимальна модель протидії» (номер державної реєстрації 0124U000556); 3) проєкт Міністерства освіти і науки України «Кібербезпекові та цифрові трансформації економіки країни воєнного часу: боротьба із кіберзлочинами, корупцією та тіньовим сектором» (номер державної реєстрації 0124U000544); 4) проєкт Міністерства освіти і науки України «Національна безпека України через запобігання фінансовим шахрайствам та легалізації брудних грошей: воєнні та післявоєнні виклики» (номер державної реєстрації 0123U101945); 5) проєкт Міністерства освіти і науки України «Засади діяльності правоохоронних органів у сфері контролю за системою залучення і використання МТД: глобалізаційний вимір» (номер державної реєстрації 0124U000635); 6) програма ERASMUS+ Модуль Жана Моне «Досвід ЄС щодо захисту персональних даних у кіберпросторі» (2023-2026 – EUEPPDC – 101125350 – ERASMUS-JMO-2023-MODULE); 7) в межах договору № БФ/24-2021 щодо «Виконання завдань перспективного плану розвитку наукового напряму «Суспільні науки» у Сумському державному університеті».

Науково-практична значимість одержаних результатів дослідження

Подана до захисту дисертаційна робота виступає ґрунтовним комплексним науковим дослідженням, що відповідає меті та завданням. Так, мета дослідження полягає в розробленні на основі аналізування наявних наукових підходів, чинного вітчизняного та зарубіжного законодавств і

практики їх реалізації комплексних науково й практично обґрунтованих концептуальних засад кримінально-правової охорони кіберпростору в Україні. Поставлена мета зумовлює вирішення наступних завдань:

– охарактеризувати становлення та генезу кримінальної відповідальності за кримінальні правопорушення в кіберпросторі в Україні;

– охарактеризувати методологічні засади дослідження кримінально-правової охорони кіберпростору в Україні;

– проаналізувати теоретико-правові підходи до тлумачення поняття «кіберпростір;

– сформувати поняття та ознаки кримінальних правопорушень у кіберпросторі;

– здійснити теоретико-прикладну типологізацію кримінальних правопорушень у кіберпросторі;

– надати кримінально-правову характеристику кіберзалежних та кіберутворювальних кримінальних правопорушень;

– визначити особливості кримінально-правової кваліфікації кримінальних правопорушень у кіберпросторі, предметом та засобом учинення яких є віртуальні активи;

– визначити особливості призначення покарання за вчинення кримінальних правопорушень у кіберпросторі;

– здійснити кримінально-правову характеристику обставин, що обтяжують покарання за кримінальні правопорушення в кіберпросторі;

– охарактеризувати особливості застосування норм і принципів міжнародного права у сфері кіберпростору в Україні;

– здійснити порівняльно-правовий аналіз кримінальної відповідальності за вчинення кримінальних правопорушень у кіберпросторі;

– запропонувати напрями вдосконалення Кримінального кодексу України

Обрана Михайлом Думчиковим методологія відповідає стану сучасних наукових досліджень, а їх застосування характерезується системним підходом, що дає можливість досліджувати проблеми в єдності їх соціального змісту та юридичної форми. Дисертантом було опрацьовано значну кількість наукових джерел, здійснено ґрунтовний аналіз законодавчого підґрунтя питань пов'язаних з охороною кіберпростору в Україні.

Інформаційною базою дослідження виступили законодавчі та нормативно-правові документи з питань кримінально-правової охорони кіберпростору в Україні, статистичні дані Департаменту кіберполіції Національної поліції України, Офісу Генерального прокурора України, дані міжнародних громадських та урядових організацій у сфері кібербезпеки й кіберзахисту та результати анкетування 300 громадян України для з'ясування їх думки з питань кримінально-правової охорони кібернетичного простору в Україні.

Новизна наукових положень і висновків, сформованих у дисертації

Особливу увагу в дисертаційному дослідженні заслуговує саме наукова новизна, що говорить про дійсно ґрунтовний підхід в досліджені.

Наукова новизна результатів дисертаційного дослідження виражається у тому, що воно становить одну з перших спроб на основі використання комплексного й системного підходів розробити галузево-профільовані та ефективні концептуальні засади кримінально-правової охорони кіберпростору в Україні з урахуванням останніх наукових досягнень, положень міжнародно-правових актів, що визначають кримінальну відповідальність за кримінальні правопорушення в кіберпросторі, положень національного законодавства та позитивних рис зарубіжного досвіду. Найбільш вагомі результати дослідження, які характеризуються науковою новизною, отримані особисто і виносяться на захист, полягають у наступному:

вперше:

– сформовано концепцію кримінально-правової охорони кіберпростору в Україні, яка передбачає криміналізацію та пеналізацію окремих діянь: крадіжку віртуальних активів, кібершпигунство, атаки на критичну інфраструктуру, та використання штучного інтелекту у злочинній діяльності;

– виділено етапи становлення кримінальної відповідальності за кримінальні правопорушення в кіберпросторі на теренах України: початковий (із 24 серпня 1991 до 5 квітня 2001 р.), зародження (з 5 квітня 2001 до 7 вересня 2005 р.), імплементаційний (із 7 вересня 2005 до 1 січня 2009 р.), економічний (з 1 січня 2009 до 5 жовтня 2015 р.), нормотворчий (із 5 жовтня 2015 до 12 вересня 2020 р.), сучасний (із 12 вересня 2020 р. до сьогодні);

– запропоновано виділити принципи, що забезпечують функціонування кіберпростору: дисципліну, відповідальність, додержання прав і свобод людини та громадянина й своєчасне втручання;

– обґрунтовано невідповідність термінології сучасному стану науки і техніки та доцільність розгляду інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронно-комунікаційних мереж у сукупності як інформаційно-телекомунікаційні технології, системи та мережі;

– запропоновано на законодавчому рівні в статті 1 Закону України «Про основні засади забезпечення кібербезпеки України» закріпити поняття «несанкціоноване втручання» – одержання можливості для ознайомлення та (або) використання цифрової інформації, що міститься в інформаційно-телекомунікаційній технології, системі або мережі, за допомогою проникнення особи, яка не має права доступу до інформаційно-телекомунікаційної технології, системи або мережі та (або) поза дозволом власника інформаційно-телекомунікаційної технології, системи або мережі;

– запропоновано авторську типологізацію шкідливих технічних засобів, зокрема, за процесом створення: 1) шкідливі технічні засоби, що створені

спеціально для вчинення певної категорії кримінальних правопорушень і не можуть бути застосовані для іншої роботи; 2) традиційні технічні засоби, які внаслідок модифікації застосовують для вчинення кримінальних правопорушень; 3) традиційні технічні засоби, які можна використовувати для вчинення кримінальних правопорушень;

– з'ясовано, що залежно від фінансового інструменту варто виділяти такі способи таємного викрадення безготівкових, електронних грошей або віртуальних активів: 1) за допомогою оплати покупок із використанням персональних даних володільця карти або електронного гаманця в інформаційно-телекомунікаційних мережах; 2) одержанням доступу до системи дистанційного банківського обслуговування; 3) за допомогою зняття коштів у банкоматі;

– запропоновано виділення в межах кваліфікуючої ознаки статті 189 Особливої частини Кримінального кодексу України нового способу вимагання – «погрози блокування, видалення, знищення, модифікації або погрози іншого несанкціонованого втручання в роботу інформаційно-телекомунікаційних технологій, систем і мереж, що може завдати шкоди правам та інтересам потерпілої особи»;

– обґрунтовано доцільність уведення в Кримінальний кодекс України спеціалізованого складу крадіжки – «Крадіжка у сфері обігу безготівкових або електронних грошей і віртуальних активів» і виокремлено два способи вчинення такого суспільно небезпечного діяння: 1) введенням цифрової інформації в інформаційно-телекомунікаційні технології, системи і мережі; 2) унаслідок іншого втручання в роботу інформаційно-телекомунікаційних технологій, систем і мереж;

удосконалено:

– пропозицію в доктринальному підході щодо визначення сутності поняття «кіберпростір» виокремлення таких аспектів: інформаційного, віртуального та соціального;

– авторське визначення дефініції поняття «віртуальний-простір», під яким варто розуміти створене комп'ютерними технологіями глобальне комунікативне середовище, основою якого є створення, збереження, впорядкування та обмін інформацією за допомогою електронних мереж;

– підстави типологізації кримінальних правопорушень у кіберпросторі, зокрема, їх перелік доповнено такими підставами: 1) сутністю кримінальних правопорушень у кіберпросторі; 2) правовим режимом, інформацією, що є предметом кримінального правопорушення в кіберпросторі; 3) метою використання електронно-обчислювальних машин інформаційно-телекомунікаційних мереж;

– поняття віртуального активу для потреб Закону України «Про віртуальні активи», під яким пропонується розуміти цифрову валюту (віртуальну, без фізичної форми), створення й контроль за якою базуються на криптографічних методах, щодо якої встановлена повна децентралізація, що гарантує коректність операцій у системі, зокрема, відсутність можливості впливати на транзакції учасників криптосистеми;

набули подальшого розвитку:

– характеристика теоретико-прикладних підходів до типологізації кримінальних правопорушень у кіберпросторі;

– підстави розмежування понять «кримінальне правопорушення в кіберпросторі», «кримінальне правопорушення у сфері комп'ютерної інформації» та «комп'ютерне кримінальне правопорушення»;

– модель вчинення кримінального правопорушення в кіберпросторі;

– види обставин, що обтяжують покарання за вчинення суспільно небезпечних діянь у кіберпросторі.

При цьому на особливу увагу заслуговують наступні положення:

В підрозділі 1.4 дисертант визначає основні характеристики кримінальних правопорушень у кіберпросторі та розкриває їх сутність, особливу увагу серед яких заслуговує: 1) інтелектуальний характер, що

означає наявності певного набору навичок та знань технологічного та комунікативного характеру. Як приклад дисертант наводить, що особа яка здійснює кібершахрайство, повинна гарно володіти навичками соціальної інженерії, а особа яка створює та розповсюджує віруси, навичками програмування для створення небезпечного програмного забезпечення й навичками маркетингу для його збуту; 2) використання навичок соціальної інженерії; 3) доступність матеріалів, необхідних для скоєння кримінального правопорушення в кіберпросторі, що полягає у повній відкритості схем, методів та способів вчинення цих суспільно небезпечних діянь.

В підрозділі 2.1 дисертації, на основі аналізу існуючих доктринальних підходів до типологізації видів кримінальних правопорушень в кіберпросторі дисертант запропонував вдосконалений розширений авторський підхід. По-перше, типологізувати кримінальні правопорушення в кіберпросторі за родовим об'єктом. По-друге, відповідно до кваліфікації суб'єктів вчинення кримінальних правопорушень у кіберпросторі. По-третє, залежно від кількості об'єктів посягання. По-четверте, залежно від спрямованості кримінальних правопорушень у кіберпросторі. По-п'яте, залежно від чисельності суб'єктів вчинення кримінального правопорушення. По-шосте, залежно від цілі використання електронно-обчислювальних машин інформаційно-телекомунікаційних мереж. По-сьоме, залежно від мети вчинення кримінальних правопорушень в кіберпросторі. По-восьме, залежно від повноти ознак кримінальних правопорушень в кіберпросторі. По-дев'яте, залежно від правового режиму інформації, яка є предметом кримінальних правопорушень в кіберпросторі. По-десяте, залежно від сутності кримінальних правопорушень в кіберпросторі. По-одинадцяте, залежно від кількості суб'єктів вчинення кримінальних правопорушень в кіберпросторі. По-дванадцяте, відповідно до видів кримінальних правопорушень в кіберпросторі передбачених Конвенцією Ради Європи «Про кіберзлочинність». По-тринадцяте, відповідно до статті 12 Кримінального кодексу України на кримінальні проступки та злочини.

В підрозділі 2.2 дисертантом обґрунтовано, що суттєвим недоліком, чинного кримінального законодавства є невідповідність термінології сучасному стану науки та техніки, зокрема запропоновано замінити термін «електронно-обчислювальні машини» на термін «цифровий пристрій», який об'єднує на багато більшу кількість інформаційно-телекомунікаційних технологій. Одночасно з цим дисертант пропонує розглядати інформаційні (автоматизовані), електронні комунікаційні, інформаційно-комунікаційні системи, електронні комунікаційні мережі у сукупності як інформаційно-телекомунікаційні технології, системи та мережі.

В підрозділі 2.3 дисертаційної роботи виділено основні особливості, які характеризують кіберутворювальні кримінальні правопорушення, зокрема: 1) об'єктом таких кримінальних правопорушень виступають різнорідні суспільні відносини, які передбачені різними розділами Особливої Частини кримінального кодексу України; 2) засобом вчинення кримінального правопорушення завжди будуть виступати елементи інформаційно – телекомунікаційних технологій, систем та мереж; 3) в окремих кримінальних правопорушеннях цього типу кіберпростір виступає, як місце вчинення суспільно – небезпечного діяння; 4) закріплені в законі України, шляхом введення в окремі статті Особливої частини Кримінального кодексу України, або визначені в рамках кваліфікуючих ознак передбачаючих кримінальну відповідальність за конкретні суспільно небезпечні діяння.

В підрозділі 2.3 дисертант визначає основні способи легалізації майна в кіберпросторі отриманого злочинним шляхом: 1) легалізація майна, отриманого злочинним шляхом за допомогою вже існуючої інтернет-інфраструктури (маркетплейсів, сайтів оголошень, соціальних мереж, інтернет-аукціонів, краудфандінгу); 2) легалізація майна, отриманого злочинним шляхом, у результаті створення нової вебінфраструктури (інтернет-магазин); 3) легалізація майна, отриманого злочинним шляхом, завдяки використанню обмінників і цифрових (електронних) валют; 4) легалізація майна, отриманого злочинним шляхом за допомогою

віртуальних активів. На нашу думку аналіз способів легалізації майна, отриманого злочинним шляхом у кіберпросторі, дозволить ідентифікувати основні методи, які використовуються кіберзлочинцями для відмивання грошей або інших активів. Кожен із цих методів має свої особливості та вимагає відповідних правових та технічних заходів протидії.

В підрозділі 3.1 дисертант аналізує практичну складову вчинення крадіжки віртуальних активів у кіберпросторі та акцентує увагу саме на ролі інформаційно-телекомунікаційних технологій, систем і мереж, які є ключовими елементами у цьому процесі. Автор зазначає, що вони не тільки слугують засобом для вчинення кримінальних правопорушень, але й виступають як місце, де ці діяння реалізуються. На нашу думку, такий підхід важливий для розуміння особливостей кіберзлочинів і розробки ефективних методів їх протидії.

В розділі 4.2 дисертантом було проаналізовано законодавство зарубіжних держав в частині встановлення кримінальної відповідальності за кримінальні правопорушення у кіберпросторі, і як результат сформовано можливості запровадження позитивного досвіду зарубіжних країн, щодо установлення кримінальної відповідальності за кримінальні правопорушення у кіберпросторі, зокрема Естонії та Данії: 1) підвищена кримінально правова охорона об'єктів та суспільних відносин у рамках державної діяльності в кіберпросторі; 2) визначення складу кримінального правопорушення «комп'ютерне шахрайство», як незаконна зміна, доповнення або видалення цифрової інформації або програмного коду, яка використовується для цифрової автоматизованої оброблення даних з метою отримання для себе або третіх осіб незаконної вигоди.

Зазначу, що ціла низка й інших положень заслуговує на увагу та позитивне схвалення наукових пошуків дисертанта.

Практичне значення наукових результатів дисертації

Справжнім надбанням дисертації є можливість її використання в освітній, науковій та практичній сферах, що підтверджено відповідними актами впровадження та показує багатовекторний підхід до дослідження. Так, до дисертації додано: акт про впровадження результатів дисертаційного дослідження в науковій діяльності Сумського державного університету; акт про впровадження результатів дисертаційного дослідження в освітньому процесу Сумського державного університету; акт провадження Державної служби спеціального зв'язку та захисту інформації України в Сумській області; акт провадження Департаменту кіберполіції Головного управління Національної поліції України в Сумській області.

Повнота відображення наукових положень дисертації в опублікованих дисертантом працях

Наукові положення та результати дослідження висвітлені у 48 наукових працях, з яких 2 монографії (1 одноосібна), 6 статей у періодичних наукових виданнях, що індексуються БД Scopus та Web of Science (при цьому 2 статті опубліковані в журналах Q2), 17 наукових статей у фахових виданнях України та 5 у закордонних виданнях, 18 тез доповідей на конференціях та семінарах. У зазначених працях повністю розкривається зміст та сутність положень, задекларованих Думчиковим Михайлом як такі, що мають елементи наукової новизни.

Дискусійні положення та зауваження по дисертації

Враховуючи високу позитивну оцінку дисертації Думчикова Михайла Олександровича, вважаю за доцільне висловити наявні зауваження та певні дискусійні положення й недоліки, серед яких можна визначити наступні:

1. Аналізуючи сучасний стан кримінально противоправних діянь у кіберпросторі автор зазначає, що вони характеризуються високою динамікою росту, небезпечністю й збільшенням кількості осіб, які вчиняють кримінальні

правопорушення зокрема, неповнолітніх. Так наприклад, дисертант зазначає, що актуальні тренди породили нові види кримінальних правопорушень у кіберпросторі та сприяли вдосконаленню вже наявних. Водночас автор не вказує, про спектр яких трендів мається на увазі. На мою думку, конкретні приклади дозволили б збагатити дослідження.

2. В підрозділі 1.3 «Теоретико-правові підходи тлумачення поняття «кіберпростір»» автор аналізуючи співвідношення понять «кіберпростір» та «Інтернет простір», зазначає на тому, що Інтернет-мережа на противагу загальній думці не є єдиною з існуючих інформаційно-телекомунікаційних мереж. На мою думку така теза потребує додаткової аргументації та наведення відповідних прикладі.

3. В своєму дисертаційному дослідженні автор наголошує, що норми статті 363 Особливої частини кримінального кодексу України є бланкетними, оскільки не містить у собі конкретних технічних вимог. Для визначення, чи є дії особи порушенням правил експлуатації інформаційно-телекомунікаційних технологій чи правил захисту інформації, стаття відсилає до певних інструкцій або правил, що обумовлюють порядок роботи з інформаційно-телекомунікаційними технологіями, системами та мережами, що встановлюються правоможною особою та доводяться до користувачів. Водночас автором не наведено конкретних прикладів нормативно-правових актів щодо регулювання зазначених суспільних відносин в сфері внутрішньої безпеки засобів зберігання, оброблення й передавання цифрової інформації яка міститься в інформаційно-телекомунікаційних технологіях, системах і мережах.

4. В підрозділі 2.3 «Кримінально-правова характеристика кіберутворювальних кримінальних правопорушень» автор наголошує, на відсутності соціальної обумовленості криміналізації норми частини 4 статті 190 Кримінального кодексу України через невідповідність змісту норми й категорії діянь, вчинюваних у кіберпросторі шляхом обману чи зловживання довірою. На мою думку позиція автора потребує додаткової аргументації з

зазначенням практичних кейсів неправильного застосування норм аналізованої статті.

5. В підрозділі 2.3 «Кримінально-правова характеристика кіберутворювальних кримінальних правопорушень» аналізуючи кримінальне правопорушення, передбачене статтею 194 Кримінального кодексу України, автор пропонує викласти диспозицію частини 1 зазначеної статті у такій редакції: «умисне знищення або пошкодження чужого майна, що заподіяло шкоду у великих розмірах, або таке, що вчинене шляхом несанкціонованого втручання в роботу інформаційно-телекомунікаційних технологій, систем і мереж». Позиція автора вбачається у спробі перевести зазначені суспільно небезпечні діяння у призму кіберпростору. Однак на мою думку залишається досить спірною соціальна обумовленість таких нововведень. Вважаю, що позиція автора потребує додаткової аргументації та висвітлення статистичних даних, щодо такої суспільно небезпечної дії у кіберпросторі.

6. Автором запропоновано можливості запровадження позитивного досвіду зарубіжних країн, щодо установлення кримінальної відповідальності за кримінальні правопорушення у кіберпросторі. А чи є позитивний досвід в рамках кримінально-правової охорони кіберпростору України, який би змогли запозичити зарубіжні країни?

Разом з тим, наведені положення та висловлені зауваження носять характер рекомендацій та здебільшого доповнюють зміст роботи та не впливають на загальне позитивне враження від роботи, яке має наукову новизну та практичну цінність.

Загальний висновок

Дисертаційна робота Михайла Думчикова на тему «Концептуальні засади кримінально-правової охорони кіберпростору в Україні» містить положення та напрацювання, які дійсно мають наукову новизну та практичне значення. Дисертаційна робота є завершеною працею, в якій отримано нові науково обґрунтовані результати, що вирішують конкретну наукову

проблему – проблему кримінально правової охорони кіберпростору в Україні. Дисертаційна робота має суттєве значення для науки кримінального права та кримінології, тобто за своєю актуальністю новизною постановки та вирішення досліджуваних проблем та практичною значущістю, відповідає п.п. 7, 8, 9 «Порядку присудження та позбавлення наукового ступеня доктора наук», затвердженого постановою Кабінету Міністрів України від 17 листопада 2021 року № 1197.

На основі вищезначеного можна зробити висновок про те, що її автор – Думчиков Михайло Олександрович – заслуговує на присудження наукового ступеня доктора юридичних наук зі спеціальності 12.00.08 – кримінальне право та кримінологія; кримінально-виконавче право.

Офіційний опонент:

Доктор юридичних наук, професор,
професор кафедри економічної безпеки та
фінансових розслідувань
Національної академії внутрішніх справ **Олена ТИХОНОВА**