

До спеціалізованої вченої ради Д 08.727.02

в Дніпропетровському державному

університеті внутрішніх справ

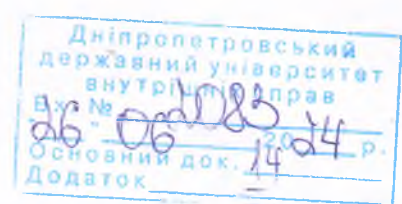
ВІДГУК

офіційного опонента – доктора юридичних наук Ключко Альони Миколаївни – 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 криминологія; кримінально-виконавче право.

Актуальність теми дисертаційного дослідження обумовлене кількома ключовими аспектами. В умовах військового конфлікту значно зростає кількість кібератак на інформаційну інфраструктуру держави, що ставить під загрозу безпеку критичних об'єктів, таких як електростанції, водопостачання, транспортні системи фінансовий та банківський сектори. Водночас, кіберпростір використовується для проведення інформаційних операцій, що впливають на громадську думку та моральний стан населення. У контексті глобалізації та поширення цифрових комунікацій кіберпростір стає ареною нових форм злочинності, які вимагають відповідної правової реакції.

Цифрова революція спричинила швидкі технологічні зміни, які стали каталізатором виникнення нових форми злочинності в кіберпросторі, що в свою чергу вимагає адекватної правової реакції. Водночас, розширення меж кіберпростору, зростання кількості цифрових платформ та пристроїв, підключених до Інтернету, збільшують потенціал для осіб, що вчиняють кримінальні правопорушення у кіберпросторі. Використання штучного інтелекту також має двоякий вплив: з одного боку, такі системи можуть допомогти в захисті від суспільно небезпечних діянь у кіберпросторі, а з іншого – стати їх об'єктом або інструментом вчинення.

Діджиталізація, яка передбачає інтеграцію інформаційно-телекомунікаційних технологій у всі сфери життєдіяльності людини, збільшує



вразливість до кримінальних правопорушень у кіберпросторі. Зростання обсягів зберігання та обробки персональних даних вимагає ефективного захисту для запобігання їх несанкціонованому доступу та використанню. Крім того, збільшення кількості електронних послуг і фінансових транзакцій підвищує ризик кібершахрайства та інших кримінальних правопорушень цього типу.

Україна, як і багато інших країн, зіштовхується з викликами адаптації національного законодавства до сучасних вимог забезпечення кібербезпеки, що включає необхідність розробки нових підходів до кримінально-правової охорони кіберпростору.

Розробка концепції кримінально-правової охорони кіберпростору сприятиме уніфікації практики застосування норм кримінального права і, як наслідок, підвищенню ефективності боротьби зі злочинністю у кіберпросторі.

Водночас, аналіз міжнародного досвіду та принципів міжнародного права дозволить адаптувати кращі практики до українських реалій і забезпечити комплексний підхід до кримінально-правової охорони кіберпростору. Оновлення Кримінального кодексу України з урахуванням сьогоденних викликів кібербезпеки є критично важливим для забезпечення сталого розвитку в цифрову епоху.

Комплексний підхід до кримінально-правової охорони кіберпростору в Україні є необхідним для забезпечення безпеки в умовах військових загроз, стрімкої цифровізації та технологічних змін. Дослідження Думчикова Михайла Олександровича спрямоване на розробку теоретичних і практичних засад ефективного захисту кіберпростору, що є критично важливим для національної безпеки, економічної стабільності та захисту прав громадян.

Тематика дисертації Думчикова Михайла Олександровича має зв'язок із державними та науковими програмами, планами та темами, зокрема повністю відповідає Цілям сталого розвитку України на період до 2030 року й виконана відповідно до пріоритетних напрямів розвитку науки і техніки в Україні на період до 2023 року з розділу «Фундаментальні наукові дослідження з найбільш важливих проблем розвитку науково-технічного,

соціально-економічного, суспільно-політичного, людського потенціалу для забезпечення конкурентоспроможності України у світі та сталого розвитку суспільства і держав» і Стратегії розвитку наукових досліджень Національної академії правових наук України на 2021–2025 роки.

Дисертацію виконано в Сумському державному університеті. З урахуванням тематики дослідження дисертант приймав участь у виконанні таких науково-дослідних робіт, зокрема:

- 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);

- проєкт Міністерства освіти і науки України «Корупція в умовах воєнного стану та післявоєнної відбудови: оптимальна модель протидії» (номер державної реєстрації 0124U000556);

- 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);

- 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);

- 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);

- Програма ERASMUS+ Модуль Жана Моне «Досвід ЄС щодо захисту персональних даних у кіберпросторі» (2023-2026 – EUEPPDC – 101125350 – ERASMUS-JMO-2023-MODULE).

Робота є складовою частиною в межах договору № БФ/24-2021 щодо «Виконання завдань перспективного плану розвитку наукового напрямку «Суспільні науки» у Сумському державному університеті».

Науково-практична значущість проведеного дослідження полягає у тому, що основні його положення дають можливість сформувати цілісну правову базу, яка відповідає сучасним потребам та загрозам в сфері забезпечення кібербезпеки. Результати дослідження можуть бути використані для вдосконалення законодавства України, зокрема, в частині кримінальної відповідальності за вчинення суспільно небезпечних діянь у кіберпросторі, що дозволить створити ефективні правові механізми для запобігання, виявлення та розслідування кримінальних правопорушень у кіберпросторі, а також забезпечити належний захист прав та інтересів держави й громадян. Основні результати дисертаційного дослідження можуть бути використані в діяльності правоохоронних органів, судової системи та інших суб'єктів залучених до боротьби із злочинністю у кіберпросторі, зокрема, розробка методичних рекомендацій, навчальних програм та тренінгів для підвищення кваліфікації працівників, які займаються розслідуванням кримінальних правопорушень у кіберпросторі.

Висновки та пропозиції Михайла Думчикова можуть бути використані в процесі викладання навчальних дисциплін правничого характеру в закладах вищої освіти. Так, базові положення дисертації використано Сумським державним університетом у навчальному процесі при викладанні дисциплін «Основи кримінального права», «Порівняльне кримінальне право», «Основи запобігання кіберзлочинності», «Сучасні проблеми кримінального права та процесу», «Міжнародне кримінальне право» (акт впровадження Сумського державного університету від 31.05.2023 р.). Особливої уваги заслуговує практична цінність дисертаційної роботи, адже одержані результати підтверджені актами апробації Державної служби спеціального зв'язку та захисту інформації України в Сумській області, Департаменту кіберполіції Головного управління Національної поліції України в Сумській області.

Надане на рецензування дисертаційне дослідження є комплексною роботою присвяченою створенню та побудові концепції кримінально-правової охорони кіберпростору в Україні.

Високий ступінь обґрунтованості й достовірності наукових положень, висновків, рекомендацій, результатів дослідження зумовлений раціональною та внутрішньо узгодженою структурою дисертаційної роботи. Науково-теоретичне підґрунтя для виконання дисертаційної роботи становлять наукові праці фахівців у галузі права (кримінальне право, криміналістика, фінансове право, інформаційне право, цивільне право й інших правничих наук), соціальних і поведінкових наук (економіка), гуманітарних наук (філософія й соціологія). Нормативно-правовою базою дисертаційного дослідження були Конституція України, міжнародні законодавчі акти, європейські рекомендації, законодавчі акти в системі вітчизняного законодавства і проекти законодавчих актів різних рівнів, що врегульовують сферу забезпечення кібербезпеки.

Інформаційною та емпіричною основою дослідження були: 1) статистичні дані Департаменту кіберполіції Національної поліції України, Офісу Генерального прокурора України; 2) статистичні дані міжнародних громадських та урядових організацій у сфері кібербезпеки й кіберзахисту; 3) результати анкетування 300 громадян України для з'ясування їх думки з питань кримінально-правової охорони кібернетичного простору в Україні.

Результати дослідження відображені в 48 наукових працях, перелік яких наведено в рефераті та дисертації. У зазначених наукових працях розкрито сутність та зміст тих наукових положень, які заявлені дисертантом як наукова новизна. Характер видань та зміст наукових праць Михайла Думчикова відповідають вимогам щодо повноти висвітлення одержаних результатів дисертації на здобуття наукового ступеня доктора юридичних наук за спеціальністю 12.00.08 – кримінальне право та криминологія; кримінально-виконавче право.

Узагальнений в роботі теоретичний та нормативний матеріал аналізується з використанням ретельно підібраного методологічного апарату.

який включає як загальнонаукові, так і спеціальні наукові методи дослідження. Обґрунтоване застосування цих методів сприяло успішному вирішенню завдань, поставлених Михайлом Думчиковим.

Наукова новизна одержаних результатів полягає розробці й обґрунтуванні концептуальних засад кримінально-правової охорони кіберпростору в Україні. Найбільш вагомими результатами 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) з поза дозволу 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.

На особливу увагу заслуговують наступні положення, висновки, рекомендації та пропозиції, що викладені в дисертаційній роботі, найбільш наочно демонструють її новизну, теоретичну та практичну значимість:

1) у підрозділі 1.1. дисертант досить вдало визначено основні етапи становлення кримінальної відповідальності за кримінальні правопорушення у кіберпросторі на теренах України: 1) початковий (1991–2001 рр.) який характеризується правовим вакуумом у регулюванні кримінально правової охорони кіберпростору та безкарністю кримінальних правопорушень в кіберпросторі; 2) зародження (2001–2005 рр) прийняття Кримінального кодексу України, який визначав три види кримінально караних діянь у кіберпросторі; 3) імплементаційний (2005–2009 рр) ознаменувався ратифікацією Україною Конвенції «Про кіберзлочинність», яка окреслила 23 кримінальних правопорушення в кіберпросторі, та фактичною імплементацією частини цих норм в українське законодавство; 4) економічний (2009–2015 рр) характеризується появою віртуальних валют та розвитком економічних кримінальних правопорушень в кіберпросторі; 5) нормотворчий (2015–2020 рр) створення спеціалізованого правоохоронного органу Департаменту кіберполіції Національної Поліції України, ухвалення Закону України «Про основні засади забезпечення кібербезпеки України»; 6) сучасний (2020 рік – сьогодні) характеризується карантинними обмеженнями, які спричинила пандемія COVID – 19 та збройна агресія Російської Федерації дала новий поштовх у розвитку кримінально протиправних діянь в кіберпросторі;

2) у підрозділі 1.3 дисертантом визначені основні принципи, що забезпечують стабільність функціонування кіберпростору, зокрема: 1) принцип своєчасного втручання, який встановлює основні вимоги для забезпечення неперервності та стабільності діяльності у кіберпросторі, а також

ефективної взаємодії між його учасниками. Його застосування передбачає запобігання свідомому посиленню напруженості або дестабілізації серед акторів кіберпростору; 2) принцип дотримання прав і свобод людини і громадянина, який закладає фундаментальні засади для захисту прав і свобод людини та громадянина в контексті зростаючого впливу інформаційно-телекомунікаційних технологій; 3) принцип дисципліни, наголошує на необхідності держав вести себе відповідально у сфері інформаційно-комунікаційних технологій для підтримки міжнародного миру та безпеки; 4) принцип відповідальності, який насамперед, пов'язаний із децентралізованим характером кіберпростору, він підтверджує необхідність багатостороннього підходу до забезпечення його стабільності;

3) у підрозділі 2.2 дисертантом сформовано авторське визначення «несанкціоноване втручання» під яким пропонується розуміти, отримання можливості для ознайомлення та (або) використання цифрової інформації, які містяться в інформаційно-телекомунікаційній технології, системі або мережі шляхом проникнення, особою яка не має права доступу до інформаційно-телекомунікаційної технології, системи або мережі та (або) по за дозволом власника інформаційно-телекомунікаційної технології, системи або мережі;

4) визначена в підрозділі 2.1 класифікація шкідливих технічних засобів за процесом створення, зокрема: : 1) шкідливі технічні засоби, створені спеціально для вчинення певної категорії кримінальних правопорушень, що не можуть бути використані для іншої роботи; 2) традиційні технічні засоби, які після модифікації застосовують для вчинення кримінальних правопорушень; 3) традиційні технічні засоби, що можуть використовуватися для вчинення кримінальних правопорушень;

5) сформоване в підрозділі 3.1 визначення віртуального активу, як цифрової валюти (віртуальної, без фізичної форми), створення і контроль за якою базується на криптографічних методах, щодо якої встановлена повна децентралізація, що гарантує коректність операцій в системі в тому числі відсутності можливості впливати на транзакції учасників криптосистеми;

б) в підрозділі 4.2 Дисертант досліджуючи міжнародний досвід у сфері правового регулювання встановлення кримінальної відповідальності за правопорушення, вчинені за допомогою інформаційно-телекомунікаційних технологій, наголошує на значних відмінностях у підходах, які застосовуються в різних правових системах. Зокрема, в країнах англо-саксонської правової сім'ї, таких як Сполучені Штати Америки, правове регулювання злочинності в кіберпросторі має і загальнодержавний, і штатний рівні, де нормативні акти доповнюються судовою практикою за допомогою системи прецедентів. Це відображає більш гнучкий підхід до адаптації законодавства під швидкі зміни в технологічному секторі. Водночас, країни романо-германської правової сім'ї демонструють більшу уніфікацію у своїх правових рамках щодо кримінальної відповідальності за кримінальні правопорушення у кіберпросторі, що відображає їх схильність до більш централізованого та систематичного підходу. Проте, навіть серед цих країн існують значні відмінності. Так, дисертант акцентує уваги, що, у країнах західної та центральної Європи кримінальна відповідальність за суспільно небезпечні діяння в кіберпросторі не виділяється в окремі розділи кримінальних кодексів, а інтегрується в загальні положення. У той же час у північноєвропейських країнах можна спостерігати виділення таких норм в спеціалізовані розділи їхніх кримінальних кодексів, що свідчить про вищий рівень правової спеціалізації у цій сфері.

Відзначаючи в цілому високий рівень виконання дисертаційної роботи Думчиковим Михайлом на тему «Концептуальні засади кримінально-правової охорони кіберпростору в Україні», її наукове та практичне значення, цілісність та послідовність викладення матеріалу, необхідно зазначити, що в цьому дослідженні присутні **дискусійні положення, зауваження**, які можуть стати підґрунтям наукової дискусії і напрямами подальшої розробки проблеми кримінально-правової охорони кіберпростору в Україні. Зокрема:

1) В підрозділі 1.1 «Становлення та генеза кримінальної відповідальності за кримінальні правопорушення у кіберпросторі в Україні»

дисертант визначає основні причини виникнення та розвитку кримінальних правопорушень у кіберпросторі, серед яких прибутковість, простота вчинення та розвиток інформаційних технологій. Поза тим, на мою думку, змістовність зазначених причин виникнення та розвитку цих суспільно небезпечних діянь у кіберпросторі розкрита автором в неповній мірі. Зокрема, дисертант вказує на прогресуючу статистику збитків від кримінальних правопорушень у кіберпросторі, спираючись на цьому на статистику в усьому світі, оминаючи при цьому окремо статистичні дані по Україні. Тому, вважаю, що позиція автора потребує додаткової аргументації під час публічного заходу;

2) На сторінці 62-63 дисертаційного дослідження автор зазначає, що сучасний стан кримінально протиправних діянь у кіберпросторі характеризується високою динамікою росту, небезпечністю й збільшенням кількості осіб, які вчиняють кримінальні правопорушення зокрема, неповнолітніх та наголошує, що каталізатором такого росту виступає пандемія Covid-19, оминаючи при цьому причини, які пов'язані з збройною агресією Російської Федерації. На мою думку наведена статистика щодо збільшення/зменшення тих чи інших видів суспільно небезпечних діянь у кіберпросторі дозволило б більш якісно розкрити стан злочинності у кіберпросторі у зазначений період;

3) В підрозділі 2.2 «Кримінально-правова характеристика кіберзалежних кримінальних правопорушень» дисертаційного дослідження автор вказує, що відповідно до частини першої статті 361 Особливої частини Кримінального кодексу України «Несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж», що кримінальна відповідальність за скоєне суспільно небезпечне діяння настає саме внаслідок несанкціонованого втручання, тобто доступу до інформаційно-телекомунікаційних систем по за дозволом власника інформаційно-телекомунікаційної системи, мережі чи цифрового пристрою. Водночас автор наголошує, що такі дії повинні бути пов'язані зі зміною нормального режиму

роботи інформаційно-телекомунікаційних технологій, але без передбачених наслідків які зазначені в частині третій цієї статті. На мою думку висловлена теза потребує додаткового обґрунтування та наведення конкретних прикладів:

4) В підрозділі 3.2 «Особливості призначення покарання, за вчинення кримінальних правопорушень в кіберпросторі» дисертантом наведена статистика вироків за вчинення кримінальних правопорушень передбачених XVI розділом Особливої частини Кримінального кодексу України, однак залишається поза увагою статистика призначення судом покарання за кіберутворювальні кримінальні правопорушення, зокрема кіберкрадіжки та кібершахрайства;

5) В підрозділі 4.1 «Теоретико-правові аспекти застосування норм і принципів міжнародного права стосовно регулювання відносин в кіберпросторі в Україні» автор аналізує принципи міжнародного права через призму їх реалізації в кіберпросторі. При цьому автор, виділяє лише ті принципи, які закріплені в міжнародних нормативних актах. На мою думку авторська позиція відносно визначення та характеристики принципів міжнародного права, щодо регулювання відносин в кіберпросторі, значно б збагатило дослідження;

6) На сторінці 378 дисертаційного дослідження автор наводить результати імплементації норм Конвенції «Про кіберзлочинність» у законодавство України зазначивши, що підробка пов'язана з комп'ютером не знайшла свого закріплення в рамках чинного Кримінального кодексу України. Вважаю, що автору необхідно було навести приклади можливого внесення цього складу кримінального правопорушення в законодавство.

Водночас висловлені зауваження носять характер побажань та не можуть суттєво вплинути на загальну високу наукову цінність рецензованої роботи та позитивну оцінку проведеного Михайлом Думчиковим дослідження.

Загальний висновок щодо дисертації Думчикова Михайла Олександровича на тему «Концептуальні засади кримінально-правової охорони кіберпростору в Україні»:

Дисертаційна робота Думчикова Михайла Олександровича на тему «Концептуальні засади кримінально-правової охорони кіберпростору в Україні» містить положення та напрацювання, які включають наукову новизну та мають практичну цінність. Усе викладене дає підставу для висновку про те, що дисертаційне дослідження виконане на належному науково-теоретичному рівні, є завершеною працею, в якій отримано нові науково обґрунтовані результати, що вирішують конкретну наукову проблему, тобто має суттєве значення для науки кримінального права та кримінології. Тема і зміст дисертації відповідає спеціальності 12.00.08 – кримінальне право та кримінологія; кримінально-виконавче право та профільно спеціалізованої вченої ради Д 08.727.02 у Дніпропетровському державному університеті внутрішніх справ.

Таким чином, за своєю актуальністю, новизною постановки та вирішенням досліджених проблем, теоретичним рівнем та практичною значущістю дисертаційна робота Думчикова Михайла Олександровича виконана на рівні вимог до докторських дисертацій відповідно до п.п. 7, 8, 9 «Порядку присудження та позбавлення наукового ступеня доктора наук», а її автор 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 міжнародних відносин
Сумського національного
аграрного університету

Альона К. ІОЧКО

