МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
ДНІПРОВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ВНУТРІШНІХ СПРАВ

ДУМЧИКОВ МИХАЙЛО ОЛЕКСАНДРОВИЧ

УДК 343.3:004.056:007(477)

КОНЦЕПТУАЛЬНІ ЗАСАДИ КРИМІНАЛЬНО-ПРАВОВОЇ ОХОРОНИ КІБЕРПРОСТОРУ В УКРАЇНІ

12.00.08 – кримінальне право та кримінологія;
кримінально-виконавче право

Реферат дисертації на здобуття наукового ступеня
доктора юридичних наук

Дніпро – 2024

Дисертацією є рукопис.

Робота виконана в Сумському державному університеті Міністерства освіти і науки України.

Науковий консультант:

доктор юридичних наук, доцент
Бондаренко Ольга Сергіївна,
Сумський державний університет,
завідувач кафедри кримінально-правових
дисциплін та судочинства Навчально-наукового інституту права.

Опоненти:

доктор юридичних наук, професор
Тихонова Олена Вікторівна,
Національна академія внутрішніх справ,
професор кафедри забезпечення фінансової безпеки
та фінансового розслідування;

доктор юридичних наук, професор
Клочко Альона Миколаївна,
Сумський національний аграрний університет,
професор кафедри міжнародних відносин;

доктор юридичних наук, доцент
Кирбят'єв Олег Олександрович,
управління протидії кіберзлочинам в Запорізькій області
Департаменту кіберполіції Національної поліції України,
старший інспектор з оперативного пошуку та партнерства
у сфері інформаційних технологій.

Захист відбудеться 13 липня 2024 року о 09-00 годині на засіданні спеціалізованої вченої ради Д 08.727.02 Дніпровського державного університету внутрішніх справ за адресою: 49005, м. Дніпро, просп. Науки, 26.

З дисертацією можна ознайомитись у загальній бібліотеці Дніпровського державного університету внутрішніх справ (м. Дніпро, просп. Науки, 26).

Учений секретар
спеціалізованої вченої ради **В. С. Березняк**

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Обґрунтування вибору теми дослідження. Актуальність дослідження кримінальних правопорушень у кіберпросторі в сучасному світі істотна. Зростання використання інформаційно-телекомунікаційних технологій та цифровізація різних сфер життєдіяльності призводять до збільшення кількості й складності кримінальних правопорушень у кіберпросторі.

Кіберпростір дає злочинцям нові можливості для здійснення широкого спектра кримінальних правопорушень, таких як крадіжка конфіденційної інформації, фінансові махінації, атаки на критичну інфраструктуру, поширення шкідливих програм та багато іншого. Кібертероризм також стає все більш небезпечним явищем, здатним спричинити серйозні наслідки для безпеки держави та громадян.

Дослідження кримінальних правопорушень у кіберпросторі має на меті розкриття нових форм злочинної діяльності, аналізування причин і механізмів здійснення суспільно небезпечних діянь у кіберпросторі, розроблення ефективних методів протидії та розслідування таких кримінальних правопорушень. Ці дослідження важливі для забезпечення безпеки й захисту інформації, виявлення та припинення кібератак, забезпечення кібербезпеки держави і громадян.

Ураховуючи швидкий темп розвитку технологій, постійну зміну методів та прийомів осіб, які вчиняють кримінальні правопорушення в кіберпросторі, дослідження кримінальних правопорушень у цій сфері є невід’ємною частиною стратегічних зусиль для забезпечення кібербезпеки та протидії кіберзлочинності. Такі дослідження сприяють розробленню ефективних політик, законодавчих актів і технологічних рішень для запобігання та протидії кіберзагрозам, а також забезпечення судового переслідування й покарання винних осіб.

В умовах повномасштабного вторгнення кіберпростір став однією з ключових арен для здійснення агресії та військових дій проти України. Кримінально-правова охорона кіберпростору в умовах воєнного стану в Україні має на меті забезпечення безпеки, розкриття та запобігання кіберзлочинам, захист критично важливої інфраструктури й сприяння міжнародному співробітництву у цій сфері. Це необхідний елемент стратегії для забезпечення національної безпеки та захисту інтересів держави.

Суспільна небезпека зазначених кримінальних правопорушень обумовлена багатьма факторами, серед яких основними, на нашу думку, є транснаціональність, латентність та власне масштаби таких суспільно небезпечних діянь. Згідно з даними офісу Генерального прокурора України в період із 2015 до 2023 року було обліковано приблизно 20 822 кримінальних правопорушень, передбачених XVI розділом Особливої частини Кримінального кодексу України. За цей самий період винесено всього 426 обвинувальні вироки суду.

Вищезазначене засвідчує необхідність здійснення глибокого та

змістовного наукового вивчення суспільно небезпечних діянь, вчинюваних у кіберпросторі для з'ясування основних проблемних аспектів установлення кримінальної відповідальності за їх учинення, і розроблення основних заходів, необхідних для їх усунення.

З огляду на те, що поняття «кіберпростір» та проблема його охорони й установлення кримінальної відповідальності за вчинення в ньому суспільно небезпечних діянь становлять науковий інтерес для фахівців різних галузей, зазначені питання вивчали фахівці в галузі права, економіки, державного управління, політології тощо.

Зокрема, це такі вчені, як Д. Азаров, О. Алексєєва, О. Амелін, Ю. Батурин, Ю. Бельський, П. Біленчук, Л. Біловус, О. Богач, В. Болгов, А. Боровик, О. Тихонова В. Бохенко, А. Булатов, М. Буряк, В. Бурячок, А. Василенко, І. Васильковський, І. Верес, Б. Войтко, В. Гавловський, Ю. Гаркуша, С. Гахов, С. Гнатюк, В. Голубєв, Ю. Градова, І. Грекова, А. Гринчак, Б. Дердюк, А. Клочко М. Дмитрук, О. Довженко, О. Дубас, К. Дубняк, В. Дуленко, Д. Казначева, А. Калініна, М. Карчевський, Л. Клапків, О. Колодюк, Д. Кондратов, О. Користін, О. Корченко, М. Кравцова, Г. Крайник, А. Кріпак, Я. Крупіна, В. Кундеус, В. Курушин, О. Кушнерьов, Н. Лазаренко, О. Литвинова, О. Манжай, І. Коптун, К. Марисюк, В. Марков, В. Матвійчук, В. Міщук, Н. Міщук, М. Мягка, А. Овчаренко, О. Омельчук, М. Панов, О. Пащенко, Ю. Піцик, М. Плугатир, Л. Прудка, П. Пушкаренко, О. Кирбят'єв Н. Ржевська, В. Русецький, Н. Савчук, О. Самойленко, А. Селюк, А. Семенов, В. Сідак, О. Сіренко, Є. Скулиш, А. Соломко, А. Ставер, О. Столяр, К. Тарасюк, О. Терешкун, М. Туранський, Ю. Філей, Т. Філіпенко, В. Фурашев, В. Хахановський, І. Чекунов, Ю. Чокас, С. Шапочка, Г. Швиданенко, В. Шемчук, Г. Шинкарецька, М. Яцишин.

Що ж до конкретних вітчизняних наукових доробок, присвячених сутності, видам та правовій природі кіберпростору й кіберзагроз, а також кримінальним правопорушенням у кіберпросторі, окремим їх видам, то хотілося б акцентувати на основних із них. Одним із найбільш фундаментальних вважаємо дисертаційне дослідження на здобуття наукового ступеня доктора юридичних наук І. Діордиці «Адміністративно-правове регулювання кібербезпеки в Україні» (2018 р.), де з'ясовано концептуальні засади кібербезпеки, правову природу загроз кібербезпеці України, надано класифікацію кіберзагроз та їх легітимізацію в нормативних актах України, запропоновано напрями оптимізації адміністративно-правового регулювання кібербезпеки в Україні.

На особливу увагу заслуговує й докторська дисертація Є. Котух «Теоретико-методологічні засади забезпечення кібербезпеки в публічному секторі» (2022 р.). Учений окреслив особливості інформаційного суспільства, що впливають на кібербезпеку, розглянув проблемні аспекти електронного врядування в контексті забезпечення кібербезпеки. Автор пропонує комплексний підхід до формування та реалізації державної політики у сфері кібербезпеки й упровадження моделі інституційної кібербезпеки, наголошує

на розвитку публічно-приватного партнерства у галузі кібербезпеки.

Серед наукових праць, дотичних до дисертаційного дослідження, необхідно назвати й дисертацію Ю. Піцик «Кіберзлочини проти власності: кримінально-правова та кримінологічна характеристика» (2019 р.). Особливістю цієї праці є формування комплексної кримінально-правової та вдосконалення кримінологічної характеристики кіберзлочинів проти власності та вироблення практичних рекомендацій щодо запобігання цим суспільно небезпечним діянням. Автор здійснив типологізацію кримінальних правопорушень у кіберпросторі на основі їх родового об'єкта та способу вчинення.

Не можемо не звернути увагу й на працю О. Довженка «Основи методики розслідування кіберзлочинів» (2020 р.). Автор запропонував типологізацію кіберзлочинів, що ґрунтується на методі групофікації та полягає в поєднанні типологізацій, які базуються на особливій природі кіберзлочинів та чинному підході Кримінально-процесуального кодексу України, що полягає в класифікації залежно від предмета та об'єкта таких кримінальних правопорушень.

Водночас, незважаючи на значну кількість наукових праць із зазначених питань, концептуальні засади кримінально-правової охорони кіберпростору в Україні на рівні комплексного дослідження є маловивченими, особливо ураховуючи швидку цифровізацію та диджиталізацію суспільства і, як наслідок, появу нових й удосконалення наявних кримінальних правопорушень у кіберпросторі.

Таким чином, необхідність підвищення рівня нормативно-правового регулювання в контексті кримінально-правової охорони кіберпростору та встановлення кримінальної відповідальності за вчинення кримінальних правопорушень у кіберпросторі зумовили актуальність дослідження концептуальних засад кримінально-правової охорони кіберпростору в Україні.

Ця наукова праця є спробою запропонувати оновлений підхід до кримінально-правової охорони кіберпростору в Україні та встановлення кримінальної відповідальності за вчинення кримінальних правопорушень у кіберпросторі.

Зв'язок роботи з науковими програмами, планами, темами, грантами. Дисертація виконана відповідно до Стратегії розвитку наукових досліджень Національної академії правових наук України на 2021–2025 роки, а також у межах науково-дослідних тем Навчально-наукового інституту права Сумського державного університету «Концептуальні засади реформування системи правоохоронних органів в сучасних умовах трансформації нагляду і контролю щодо забезпечення економічної безпеки України» (номер державної реєстрації 0120U100474), «Корупція в умовах воєнного стану та післявоєнної відбудови: оптимальна модель протидії» (номер державної реєстрації 0124U000556), «Національна безпека України через запобігання фінансовим шахрайствам та легалізації брудних грошей: воєнні та післявоєнні виклики» (номер державної реєстрації 0123U101945),

«Кібербезпекові та цифрові трансформації економіки країни воєнного часу: боротьба із кіберзлочинами, корупцією та тіньовим сектором» (номер державної реєстрації 0124U000544), «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).

Мета та завдання дослідження. Мета дисертаційного 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.

Для досягнення зазначеної мети були вирішені такі завдання:

− 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.

Об'єктом дослідження є суспільні відносини, що виникають у процесі кримінально-правової охорони кіберпростору.

Предметом дослідження є концептуальні засади кримінально-правової охорони кіберпростору в Україні.

Методи дослідження. Методологічною основою дослідження стала сукупність методів наукового пізнання. З філософських методів ми

використали *метод концептуального аналізу* під час аналізування понятійно-категоріального апарату, зокрема, понять «кримінальне правопорушення в кіберпросторі», «віртуальний актив», «комп'ютерне кримінальне правопорушення», «кіберпростір», «віртуальний простір», «інтернет-простір», «інформаційний простір» (підрозділи 1.1, 1.3, 1.4). За допомогою *емпіричного методу* ми проаналізували статистику вчинення кіберзалежних кримінальних правопорушень (підрозділи 3.2, 3.3). *Метод аналізу* було використано під час дослідження міжнародних нормативних актів, нормативних актів національного й зарубіжного законодавств, що регулюють кримінальну відповідальність за вчинення суспільно небезпечних діянь у кіберпросторі. За допомогою цього методу було проаналізовано Кримінальний кодекс України, акти кримінального законодавства зарубіжних держав та міжнародні конвенції, зокрема Конвенцію «Про кіберзлочинність» (підрозділи 2.2, 2.3, 4.1, 4.2). За допомогою *методу контент-аналізу* було проведено системний аналіз вебконтенту, що стосується вчинення кримінальних правопорушень у кіберпросторі (підрозділи 2.1, 2.2, 2.3, 3.2). *Порівняльно-правовий метод* дав можливість порівняти законодавство зарубіжних країн щодо встановлення кримінальної відповідальності за кримінальні правопорушення в кіберпросторі та політику впровадження покарання за їх учинення (підрозділи 1.1, 4.2). *Метод анкетування* було використано для проведення опитування громадян України з метою з'ясування їх думки з питань кримінально-правової охорони кіберпростору в Україні (підрозділи 3.2, 3.3).

Науково-теоретичне підґрунтя для написання дисертації становили наукові праці з кримінального права, криміналістики, кримінології, філософії, економіки, політології, соціології та психології, а також інших правових наук, зокрема, й зарубіжних учених. *Нормативною основою* дисертаційного дослідження були Конституція України, міжнародні договори України, нормативно-правові акти національного законодавства сучасного періоду, проєкти законів, законодавства низки зарубіжних країн.

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.

Наукова новизна одержаних результатів полягає в тому, що подане дисертаційне дослідження є однією з перших спроб комплексно на монографічному рівні 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. На підставі проведеного дослідження сформульовано

низку нових концептуальних наукових положень та висновків, запропонованих особисто здобувачем.

уперше:

− 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.

Особистий внесок здобувача в одержання наукових результатів, що містяться в дисертації. Дисертаційне дослідження здобувач виконав

самостійно, всі сформульовані в ньому положення та висновки обґрунтував на основі особистих досліджень. Нові наукові результати дисертації автор одержав особисто. У монографії «Peculiarities of criminal legal protection of cyberspace and combating cybercrimes», у співавторстві з О. Бондаренко особистий внесок здобувача полягає у всебічному аналізі нових форм вчинення кримінальних правопорушень у кіберпросторі, зокрема, крадіжку з платіжних карт – « кардинг», повереннння оплати за отриманий товар «рефандинг», та основні форми вчинення суспільно небезпечних діянь у кіберпросторі, предметом яких є віртуальні активи.

У науковій статті «Становлення та генеза кримінальної відповідальності за кримінальні правопорушення в кіберпросторі на теренах України», підготовленій разом із І. Каріхом, особисто здійснений аналіз основних етапів становлення злочинності в кіберпросторі на теренах України. У науковій статті «Загальна характеристика та види розкрадань шляхом використання інформаційних технологій як одного з найпоширеніших видів кримінальних правопорушень у кіберпросторі» в співавторстві з Д. Малетовим дисертант дослідив можливості комп'ютерно-технічної експертизи як важливої допомоги в розкритті та розслідуванні кримінальних правопорушень, пов'язаних із розкраданнями коштів із банківських карт, розкрив сутність «кардингу» як найпопулярнішого кримінального правопорушення, пов'язаного з викраденням безготівкових коштів.

У науковій статті «Кримінологічні аспекти протидії легалізації корупційних доходів у кіберпросторі», підготовленій разом з О. Бондаренко, дисертант провів аналіз криміналістичної характеристики легалізації відмивання злочинних доходів у кіберпросторі, зазначив основні способи легалізації майна, отриманого злочинним шляхом за допомогою віртуальних активів.

У науковій статті «Легалізація доходів, отриманих злочинним шляхом за допомогою використання віртуальної валюти (криптовалюти): кримінологічний та кримінально-правовий аспект» у співавторстві з Д. Репіним особистий внесок здобувача полягає у всебічному дослідженні поняття «віртуальний актив» та наданні його авторського визначення, окресленні та аналізуванні основних ознак віртуальних активів, визначенні, що саме підпадає під визначення категорії віртуальних активів. У науковій статті «Криміналістичні проблемні аспекти боротьби зі злочинами у кіберсфері» в співавторстві з В. Пахомовим та О. Бондаренко дисертант надав рекомендації щодо вдосконалення нормативно- правової бази з питань забезпечення кібербезпеки, здійснив розмежування понять «комп'ютерний злочин» і «кіберзлочин», а також криміналістичну типологізацію кримінальних правопорушень у кіберпросторі. У науковій статті «Зарубіжний досвід протидії кримінальним правопорушенням проти власності, вчиненим із використанням інформаційно-телекомунікаційних технологій» у співавторстві з І. Каріхом особистий внесок здобувача полягає в окресленні та аналізуванні основних підходів до встановлення кримінальної

відповідальності за вчинення кримінальних правопорушень у кіберпросторі проти власності за законодавством зарубіжних держав, виокремленні позитивного досвіду кримінально-правової охорони кіберпростору зарубіжних держав від зовнішніх та внутрішніх посягань. У науковій статті «Неправомірний вплив на інформаційну інфраструктуру України» в співавторстві з І. Каріхом здобувач визначив основні фактори та загрози державній інформаційній інфраструктурі, яка може бути об'єктом учинення суспільно небезпечного діяння, запропонував підходи до вдосконалення нормативно-правової системи кримінально-правової охорони державної інфраструктури України. У науковій статті «До проблем визначення поняття та ознак кіберзлочинів» у співавторстві з Я. Шевцовим дисертант визначив специфічні ознаки кримінальних правопорушень у кіберпросторі, зокрема, детально проаналізовані такі ознаки, як анонімність та територіальна складова.

У науковій статті «Кіберзлочинність як новітній феномен та джерело високого рівня суспільної небезпеки» в співавторстві з В. Пахомовим дисертант проаналізував кримінальні правопорушення, регламентовані XVI розділом Особливої частини Кримінального кодексу України, визначив їх специфічні характеристики, запропонував криміналізувати нові види кримінальних правопорушень у кіберпросторі. У науковій статті «Criminal legal characteristic of social engineering as a way of committing fraud» у співавторстві з В. Пахомовим та О. Бондаренко дисертант визначив значення соціальної інженерії під час учинення кримінальних правопорушень у кіберпросторі, проаналізував основні суспільно небезпечні діяння, вчинювані в кіберпросторі за допомогою методів соціальної інженерії. У науковій статті «Cybercrime as a threat to the national security of the Baltic States and Ukraine: The comparative analysis» у співавторстві з О. Бондаренко та М. Уткіною особистий внесок дисертанта полягає у визначенні основних загроз для України й країн Балтії у сфері забезпечення кібербезпеки, запропонуванні варіантів протидії наявним кіберзагрозам; проаналізувавши позитивний досвід країн Балтії, автор запропонував удосконалення системи кримінально-правової охорони кіберпростору.

У науковій статті «The essence and classification of cybercrime in the field of computer information» у співавторстві з В. Пахомовим дисертант здійснив класифікацію кримінальних правопорушень у кіберпросторі, проаналізував найбільш суспільно небезпечні кримінальні правопорушення, які вчиняються у світі, на основі позитивного зарубіжного досвіду запропонував зміни до низки статей Особливої частини Кримінального кодексу України. У науковій статті «Digital Currency as a Subject of Economic Criminal Offenses» у співавторстві з Н. Горобець і Р. Дегтяр здобувач окреслив поняття «віртуальний актив», проаналізував кримінальні правопорушення, де віртуальні активи можуть бути предметом кримінального посягання, виокремив та проаналізував окремі способи легалізації майна, отриманого злочинним шляхом за допомогою цифрової валюти. У науковій статті «Peculiarities of countering legalization of criminal income with the help of virtual

assets: legislative regulation and practical implementation» у співавторстві з О. Рєзніком та О. Бондаренко особистий внесок здобувача полягає у визначенні основних способів легалізації злочинних доходів за допомогою віртуальних активів та наданні їх характеристики, а також проаналізовано нормативні підходи щодо вдосконалення системи протидії легалізації майна, отриманого злочинним шляхом за допомогою віртуальних активів.

У науковій статті «Criminological and forensic characteristics of forms of embezzlement committed through the use of information technology» у співавторстві з О. Юніним, Н. Нестор, А. Борко, О. Єрменчук дисертант визначив та проаналізував кримінальні правопорушення, що можуть вчинятися за допомогою інформаційних технологій, як засіб учинення кримінального правопорушення, порівняв системи кримінально-правової охорони кіберпростору України та зарубіжних держав, зокрема, країн Європейського Союзу та Сполучених Штатів Америки. У науковій статті «Issues of regulating cryptocurrency and control over its turnover: international experience» у співавторстві з Н. Кононенко, Л. Басенко, Р. Халеніним та Н. Глущенко особистий внесок дисертанта полягає в наданні авторського визначення поняття «криптовалюта», визначенні основних схем використання криптовалюти в протиправній діяльності, окресленні й охарактеризуванні основних ознак «криптовалюти», аналізуванні зарубіжних підходів щодо регулювання «криптовалют» у зарубіжних державах.

Практичне значення одержаних результатів полягає в тому, що викладені в дисертації висновки та пропозиції можуть бути використані в:

– науковій діяльності як основа для подальших досліджень кримінально-правової охорони кіберпростору в Україні (акт впровадження Сумського державного університету від 2.05.2023 р.);

– практичній діяльності з метою підвищення ефективності діяльності Державної служби спеціального зв’язку та захисту інформації України в Сумській області, Департаменту кіберполіції Головного управління Національної поліції України в Сумській області (акт впровадження Державної служби спеціального зв’язку та захисту інформації України в Сумській області від 12.05.2023 р., акт впровадження відділу протидії кіберзлочинам в Сумській області Департаменту кіберполіції Національної поліції України);

– освітньому процесі – під час проведення лекційних, семінарських і практичних занять із дисциплін «Кримінальне право», «Кримінологія», «Основи запобігання кіберзлочинності», «Сучасні проблеми кримінального права та процесу», «Міжнародне кримінальне право» (акт впровадження Сумського державного університету від 31.05.2023 р.).

Апробація результатів дисертації. Основні положення та результати проведеного дослідження були обговорені і дістали позитивну оцінку на 18 міжнародних та всеукраїнських науково-практичних конференціях. Останні результати дослідження оприлюднені на: 1) міжнародних науково-практичних конференціях, зокрема, «Реформування правової системи в контексті євроінтеграційних процесів» (Суми, 2022 р.), «Trends and directions of

development of scientific approaches and prospects of integration of internet technologies into society» (Швеція, 2021 р.), «Die wichtigsten Vektoren für die Entwicklung der Wissenschaft im Jahr» (Люксембург, 2020 р.) 2) всеукраїнських науково-практичних конференціях: «Травневі правові читання» (Черкаси, 2020 р.), «Актуальні питання та перспективи розвитку кримінального права, кримінології та судочинства» (Київ, 2021 р.), «Актуальні питання та перспективи розвитку кримінального права, кримінології та судочинства (Київ, 2022 р.).

Публікації. Основні теоретичні положення, висновки та рекомендації дослідження автор висвітлив у 48 публікаціях, зокрема, 2 монографіях, 17 наукових статтях у фахових виданнях України, 6 періодичних наукових виданнях, що індексуються БД Scopus та Web of Science, 5 закордонних виданнях, 18 тезах доповідей на конференціях і семінарах.

Структура та обсяг дисертації. Дисертація складається з основної частини (вступу, чотирьох розділів, що вміщують дванадцять підрозділів, висновків), списку використаних джерел і додатків. Загальний обсяг дисертації становить 501 сторінку, з яких 386 сторінок основного тексту. Список використаних джерел налічує 517 найменувань і займає 47 сторінок, додатки викладено на 42-х сторінках.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У **вступі** обґрунтовано актуальність теми дисертації; визначено її зв’язок із науковими програмами, планами, темами; розкрито мету, завдання, об’єкт, предмет і методи дослідження, його емпіричну базу, а також окреслено наукову новизну та практичне значення одержаних результатів, наведено відомості щодо апробації результатів дослідження, публікацій.

Розділ 1 «Історичні та теоретико-методологічні засади дослідження кримінальних правопорушень у кіберпросторі» складається з чотирьох підрозділів, присвячених становленню та генезі кримінальної відповідальності за кримінальні правопорушення в кіберпросторі в Україні; методологічним засадам дослідження кримінальних правопорушень у кіберпросторі; теоретико-правовим підходам до тлумачення поняття кіберпростору, поняття та ознак кримінальних правопорушень у кіберпросторі.

У *підрозділі 1.1 «Становлення та генеза кримінальної відповідальності за кримінальні правопорушення в кіберпросторі в Україні»* висвітлено генезис розвитку феномену кримінальних правопорушень у кіберпросторі у світі з 70-х років XX століття до сьогодення. Запропоновано авторський підхід до ретроспективного розвитку кримінальної відповідальності за правопорушення в кіберпросторі на теренах України, зокрема, виділено шість етапів: 1) початковий (1991–2001 рр.) – зазначений період характеризується правовим вакуумом у регулюванні відносин у кіберпросторі як загалом, так і в межах правової охорони кіберпростору зокрема; 2) зародження

(2001–2005 рр.) – основною характеристикою цього етапу є набрання 5 квітня 2001 року чинності Кримінальним кодексом України, водночас спостерігається перша спроба врегулювання кримінальних правопорушень у кіберпросторі в законодавстві; 3) імплементаційний (2005–2009 рр.) – найбільшим досягненням цього періоду є ратифікація Україною Конвенції «Про кіберзлочинність», що стала основою для встановлення кримінальної відповідальності за суспільно небезпечні діяння, вчинювані в кіберпросторі; 4) економічний (2009–2015 рр.) – цей період відзначається появою віртуальних активів та перенесенням спектра вчинюваних діянь у кіберпросторі в економічний ракурс; 5) нормотворчий (2015–2020 рр.) – зазначений період характеризується створенням спеціального правоохоронного Департаменту кіберполіції Національної поліції України та прийняттям низки законодавчих актів із питань охорони кіберпростору; 6)сучасний (2020 рік – до сьогодні) – характеризується високою динамікою зростання, небезпечністю й збільшенням кількості осіб, які вчиняють кримінальні правопорушення.

З'ясовані основні причини виникнення та розвитку кримінальних правопорушень у кіберпросторі на сучасному етапі: по-перше, прибутковість кримінальних правопорушень, вчинених у кіберпросторі; по-друге, простота вчинення кримінальних правопорушень; по-третє, розвиток інформаційних технологій – одна з основних причин швидкого поширення кіберзлочинності в XXI столітті; по-четверте, недостатнє розуміння на державному рівні й рівні суспільства можливої небезпеки та настання непередбачуваних наслідків злочинності в кіберпросторі. Доведено, що сучасний стан кіберзлочинності становить великі загрози для суспільства, і з кожним роком кількість кримінальних правопорушень у кіберпросторі зростає, що поглинають усе більше коштів, по-перше на їх розслідування та по-друге, завдані збитки від їх учинення.

У підрозділі 1.2 «Методологічні засади дослідження кримінальних правопорушень у кіберпросторі» зазначено, що підбір правильної методології є одним із важливих елементів успіху під час проведення наукового дослідження. Комбінування різних методів дозволяє застосовувати комплексний підхід до аналізування проблеми кримінально-правової охорони кіберпростору. Наприклад, соціологічні методи можуть доповнювати правовий аналіз, а технічні методи можуть допомогти виявити технічні вразливості кіберпростору. Отже, компонування різних методів у науковому дослідженні кримінально-правової охорони кіберпростору є важливим для розширення обсягу дослідження, забезпечення достовірності результатів, застосування комплексного підходу й одержання глибшого розуміння проблеми.

З філософських методів використовували метод концептуального аналізу під час аналізування понятійно-категоріального апарату, зокрема, понять «кримінальне правопорушення в кіберпросторі», «віртуальний актив», «комп'ютерне кримінальне правопорушення», «кіберпростір», «віртуальний простір», «інтернет-простір», «інформаційний простір». За допомогою

емпіричного методу ми проаналізували статистику вчинення кіберзалежних кримінальних правопорушень. Метод формального аналізу було використано під час дослідження міжнародних нормативних актів, нормативних актів національного й зарубіжного законодавств, що регулюють кримінальну відповідальність за вчинення суспільно небезпечних діянь у кіберпросторі. За допомогою цього методу було проаналізовано Кримінальний кодекс України, акти кримінального законодавства зарубіжних держав та міжнародні конвенції, зокрема Конвенцію «Про кіберзлочинність». За допомогою методу контент-аналізу було проведено системний аналіз вебконтенту, що стосується вчинення кримінальних правопорушень у кіберпросторі. Порівняльно-правовий метод дав можливість порівняти законодавство зарубіжних країн щодо встановлення кримінальної відповідальності за кримінальні правопорушення в кіберпросторі та політику впровадження покарання за їх учинення. Метод анкетування було використано для проведення опитування громадян України з метою з'ясування їх думки з питань кримінально-правової охорони кіберпростору в Україні.

У підрозділі 1.3 «Теоретико-правові підходи до тлумачення поняття «кіберпростір» досліджено поняття «інформаційний простір», «віртуальний простір», «кіберпростір» та «інтернет-простір». Установлено, що поняття «кіберпростір» ширше за поняття «інтернет-простір», проте вужче від «інформаційного» та «віртуального просторів» і фактично є їх частиною. Виділено основні аспекти щодо формування поняття «кіберпростір»: по-перше, філософський, відповідно до якого поняття «кіберпростір» охоплює не лише певні блоки інформаційної залежності, а й людей, репрезентованих власними проєкціями в ньому, зокрема, створеними текстовими аргументаціями, зображеннями та повідомленнями; по-друге, легальний – це штучно створене середовище, існування якого обмежене інформаційно-телекомунікаційною мережею, користувачі якої можуть вільно вступати в адміністративні, цивільні, кримінальні та інші правовідносини; по-третє, доктринальний, відповідно до якого кіберпростір – це віртуальне місце, створене мережею взаємозалежних комп'ютерів, за допомогою яких взаємодіють звичайні користувачі.

На підставі аналізування в межах доктринального аспекту запропоновано розглядати кіберпростір в інформаційному, віртуальному та соціальному ракурсах. Доведено, що найбільш правильно розглядати кіберпростір саме з позиції віртуалістики. З погляду віртуального сприйняття кіберпростору обов'язковим є використання різноманітних гаджетів (комп'ютерів, телефонів, засобів віртуальної реальності), за допомогою яких власне створюється та функціонує кіберпростір. Кіберпростір – це віртуальне місце, створене мережею взаємозалежних комп'ютерів, за допомогою яких взаємодіють звичайні користувачі. Критично проаналізувавши позиції вчених щодо характеристик кіберпростору, автор виділив та проаналізував такі: віртуальність, мережеву належність, середовище взаємодії, динамічність, комунікативність і поєднання територіалізації та детериторіалізації. Наголошено, що в забезпеченні стабільності функціонування кіберпростору

вагому роль відіграють принципи. Виділено такі принципи забезпечення стабільності в межах кіберпростору: дисципліну, відповідальність, додержання прав і свобод людини та громадянина й своєчасне втручання.

У підрозділі 1.4 «*Поняття та ознаки кримінальних правопорушень у кіберпросторі»* наголошено на доцільності узгодження термінології нормативно-правових актів, зокрема Закону України «Про основні засади забезпечення кібербезпеки України», з нормами Кримінального кодексу України – замість поняття «кіберзлочин» потрібно використовувати поняття «кримінальне правопорушення в кіберпросторі». Визначено та проаналізовано основні характеристики кримінальних правопорушень у кіберпросторі: 1) інтелектуальний характер; 2) транснаціональний характер; 3) латентність; 4) використання навиків соціальної інженерії; 5) суб'єктна складова; 6) дистанційність; 7) доступність матеріалів, необхідних для скоєння кримінального правопорушення в кіберпросторі; 8) анонімність.

Проаналізовано такі підходи до розуміння специфіки поняття «кримінальне правопорушення в кіберпросторі»: по-перше, поняття «кримінальне правопорушення в кіберпросторі» вужче за поняття «комп'ютерне кримінальне правопорушення» та поняття «кримінальне правопорушення у сфері комп'ютерної інформації»; по-друге, поняття «кримінальне правопорушення в кіберпросторі», «комп'ютерне кримінальне правопорушення» та «кримінальне правопорушення у сфері комп'ютерної інформації» є тотожними; по-третє, поняття «кримінальне правопорушення в кіберпросторі» ширше за поняття «комп'ютерне кримінальне правопорушення» та «кримінальне правопорушення у сфері комп'ютерної інформації»; по-четверте, поняття «кримінальне правопорушення в кіберпросторі» з погляду криміналістичної позиції.

На основі розмежування понять «кримінальні правопорушення в кіберпросторі», «комп'ютерні кримінальні правопорушення» та «кримінальні правопорушення у сфері комп'ютерної інформації» з'ясовано, що кримінальні правопорушення в кіберпросторі можуть бути: 1) скоєні з використанням кіберпростору, проте не є «комп'ютерними кримінальними правопорушеннями» та «кримінальними правопорушеннями у сфері комп'ютерної інформації», наприклад, скоєні з використанням засобів високих технологій; 2) скоєні з використанням кіберпростору, що є «кримінальними правопорушеннями у сфері комп'ютерної інформації» та «комп'ютерними кримінальними правопорушеннями»; 3) скоєні з використанням кіберпростору, що є «кримінальними правопорушеннями у сфері комп'ютерної інформації», але не є «комп'ютерними кримінальними правопорушеннями»; 4) скоєні з використанням кіберпростору, що є «комп'ютерними кримінальними правопорушеннями», проте не є «кримінальними правопорушеннями у сфері комп'ютерної інформації».

Надане авторське визначення поняття «кримінальне правопорушення в кіберпросторі» – суспільно небезпечне, протиправне, винне, каране діяння, що посягає й заподіює шкоду різним суспільним відносинам за допомогою використання інформаційно-телекомунікаційних технологій,

інформаційно-телекомунікаційних систем і мереж та створюваного ними кіберпростору.

Розділ 2 «Кримінально-правова характеристика кримінальних правопорушень у кіберпросторі» складається з трьох підрозділів, у яких детально висвітлено питання теоретико-прикладних аспектів типологізації кримінальних правопорушень у кіберпросторі, кримінально-правової характеристики кіберзалежних та кіберутворювальних кримінальних правопорушень.

У *підрозділі 2.1 «Теоретико-прикладні аспекти типологізації кримінальних правопорушень в кіберпросторі»* здійснено типологізацію кримінальних правопорушень в кіберпросторі за низкою підстав: по-перше, запропоновано типологізувати кримінальні правопорушення в кіберпросторі за родовим об'єктом; по-друге, відповідно до кваліфікації суб'єктів учинення кримінальних правопорушень в кіберпросторі; по-третє, залежно від кількості об'єктів посягання комп'ютерної інформації як складної багаторівневої системи операцій (характеристика елементів комп'ютерної інформації); по-четверте, залежно від спрямованості кримінальних правопорушень у кіберпросторі; по-п'яте, залежно від кількості суб'єктів учинення кримінального правопорушення; по-шосте, залежно від мети 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, що є предметом кримінальних правопорушень в кіберпросторі; по-десяте, залежно від сутності кримінальних правопорушень в кіберпросторі; по-одинадцяте, залежно від кількості суб'єктів учинення 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.

Залежно від кваліфікації суб'єктів учинення кримінальних правопорушень у кіберпросторі було виділено, по-перше, ті, що вчиненні «звичайними» користувачами, по-друге, ті, що вчинені досвідченими користувачами та по-трете, ті, що вчинені «користувачами спеціалістами». В залежності від кількості об'єктів посягання автор виділив однооб'єктні й багатооб'єктні. За кількістю суб'єктів вчинення було виділено кримінальні правопорушення, вчинені одним суб'єктом та групою осіб (злочинною організацією, організованою групою). Залежно від повноти ознак - безумовно та умовно кіберорієнтовані.

За видом родового об'єкта складу кримінального правопорушення було виділено кримінальні правопорушення в кіберпросторі проти основ національної безпеки України, проти власності, проти громадської безпеки, у сфері господарської діяльності, у сфері обігу наркотичних засобів, психотропних речовин, їх аналогів або прекурсорів, у сфері використання

електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.

Залежно від об'єкту посягання комп'ютерної інформації як складної багаторівневої системи операцій (характеристика елементів комп'ютерної інформації): 1) знищення інформації, оброблюваної в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах чи комп'ютерних мережах; 2) модифікація інформації, оброблюваної в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах чи комп'ютерних мережах; 3) блокування інформації, оброблюваної в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах чи комп'ютерних мережах; 4) неправомірне розповсюдження інформації, оброблюваної в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах чи комп'ютерних мережах; 5) викрадення інформації, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах чи комп'ютерних мережах.

Залежно від мети використання електронно-обчислювальних машин інформаційно-телекомунікаційних мереж було виділено такі кримінальні правопорушення в кіберпросторі: по-перше, в яких комп'ютерна інформація, електронно-обчислювальні машини, інформаційно-комунікаційні мережі – основна мета посягання, зокрема, це такі кримінальні правопорушення, як знищення, блокування, зміна інформації, що міститься в електронно-обчислювальних машинах, а також порушення порядку роботи електронно-обчислювальних машин, інформаційних та електронних комунікаційних мереж; по-друге, в яких комп'ютерна інформація, електронно-обчислювальні машини, інформаційно-комунікаційні мережі – проміжна мета, а саме в межах використання електронно-обчислювальних машин, інформаційно-комунікаційних мереж, мереж електрозв'язку досягають іншої мети, зокрема, здійснення шахрайства у кіберпросторі, незаконне одержання конфіденційної інформації; по-третє, в яких електронно-обчислювальні машини, інформаційно-комунікаційні мережі є засобами забезпечення злочинної діяльності: незаконне збирання та систематизація інформації, ведення «чорної» бухгалтерії, баз даних щодо поширення предметів, які перебувають в обмеженому обігу: наркотиків, зброї, листування електронною поштою.

Залежно від сутності кримінальних правопорушень у кіберпросторі було виділено кіберзалежні й кіберутворювальні кримінальні правопорушення. Визначено, що кіберзалежні кримінальні правопорушення – це ті кримінальні правопорушення, які вчиняють безпосередньо з використанням електронно-обчислювальних машин, комп'ютерних мереж, мережі «Інтернет» та інших телекомунікаційних мереж, тобто фактично з використанням тієї чи іншої форми прояву кіберпростору. Кіберутворювальні кримінальні правопорушення – це традиційні кримінальні правопорушення, що стали кіберзлочинами чи кіберпроступками внаслідок використання електронно-обчислювальних машин та інформаційно-телекомунікаційних

мереж як основного засобу вчинення кримінального правопорушення.

У *підрозділі 2.2 «Кримінально-правова характеристика кіберзалежних кримінальних правопорушень в кіберпросторі»* наголошено, що основним предметом кіберзалежних кримінальних правопорушень є цифрова інформація у сфері цифрових технологій, інформаційно-телекомунікаційних систем та мереж. Акцентовано на недоліках чинного кримінального законодавства щодо невідповідності термінології сучасному стану науки й техніки, зокрема, автор запропонував замінити термін «електронно-обчислювальні машини» на термін «цифровий пристрій», який об'єднує набагато більшу кількість інформаційно-телекомунікаційних технологій. Автор вважає за доцільне розглядати інформаційні (автоматизовані), електронні комунікаційні, інформаційно-комунікаційні системи, електронні комунікаційні мережі в сукупності як інформаційно-телекомунікаційні технології, системи та мережі. Автор пропонує нову назву XVI розділу Особливої частини Кримінального кодексу України – «Кримінальні правопорушення у сфері функціонування цифрових пристроїв оброблення інформації, в інформаційно-комунікаційних системах та телекомунікаційних мережах».

На основі аналізування статті 361 Особливої частини Кримінального кодексу України автор пропонує встановлення градації кримінальної відповідальності за настання суспільно небезпечних наслідків, де перехоплення, витік та копіювання цифрової інформації – найм'якші, а блокування й знищення – найтяжчі. Автор наголошує на необхідності законодавчого закріплення поняття несанкціонованого втручання, під яким пропонує розуміти одержання можливості для ознайомлення та (або) використання цифрової інформації за допомогою проникнення в інформаційно-телекомунікаційні системи та мережі з використанням спеціальних технічних засобів і (або) спеціального програмного забезпечення особи, яка не має права доступу до такої інформації та (або) роботи з нею. Акцентовано на тому, що в Законі про кримінальну відповідальність не приділено уваги кримінально-правовій відповідальності за перехоплення цифрової інформації. Одночасно з цим запропоновано під перехопленням цифрової інформації розуміти створення додаткової лінії її маршруту, внаслідок якого цифрова інформація потрапляє до осіб, які не мають права доступу до неї, якщо під час цього не було спотворено процесу її оброблення.

Виділено основні особливості шкідливого програмного забезпечення, зокрема: швидке самопоширення й приєднання його копій до інших програм або носіїв, що спочатку не були уражені шкідливою програмою, та виконання різних деструктивних дій, які порушують нормальну роботу цифрового пристрою, зокрема: 1) блокування цифрової інформації, наявної в цифровому пристрої; 2) примусового перезавантаження операційної системи цифрового пристрою; 3) знищення цифрової інформації, розміщеної на цифровому пристрої; 4) внесення змін до файлової системи цифрового пристрою; 5) сповільнення режиму роботи цифрового пристрою або її повне припинення.

Автор зауважує, що дії у формі перехоплення цифрової інформації не кваліфікуються за частиною 2 статті 362 Кримінального кодексу України, оскільки в диспозиції цієї статті чітко зазначено, що така особа має право доступу до інформації. У разі суспільно небезпечних діянь у формі перехоплення цифрової інформації особа, навпаки, не має права доступу до цифрової інформації й лише за допомогою шкідливих технічних засобів шляхом несанкціонованого втручання може перехопити її, продублювавши модуль передавання. Копіювання інформації в цьому разі автор вважає формою її витоку. Дисертант пропонує таку редакцію частини 2 статті 362 Особливої частини Кримінального кодексу України: «Несанкціоноване копіювання цифрової інформації, що обробляється в інформаційно-телекомунікаційних технологіях, системах і мережах, якщо це призвело до її витоку, вчинене особою, яка має право доступу до такої інформації».

Досліджено особливості об’єктивної сторони кримінального правопорушення, передбаченого статтею 363 Кримінального кодексу України, та встановлено його бланкетний характер, тобто воно містить терміни, визначення й роз’яснення яких необхідно шукати в інших нормативно-правових актах, зокрема: 1) правилах експлуатації; 2) порядку захисту цифрової інформації; 3) правилах захисту цифрової інформації.

Обґрунтовано, що, незважаючи на начебто однакове трактування дій у формі порушення порядку захисту цифрової інформації й порушення правил захисту цифрової інформації, вони не є ідентичними за змістом. Під порушеннями правил захисту цифрової інформації автор пропонує розуміти недодержання вимог до реалізації системи захисту цифрової інформації певного інформаційного ресурсу. Одночасно з цим порушення порядку захисту цифрової інформації – це визначені нормативно-правовими актами вимоги щодо створення та організації роботи системи захисту цифрової інформації, що полягають у забезпеченні запобігання несанкціонованим діям стосовно інформації, оброблюваної в інформаційно-телекомунікаційній системі.

Підкреслюється нагальність уведення додаткової кваліфікаційної ознаки до статті 363-1 Кримінального кодексу України, а саме якщо такі дії вчинені з корисливих мотивів (ч. 3) або вчинені проти інформаційної інфраструктури держави (ч. 4).

У *підрозділі 2.3 «Кримінально-правова характеристика кіберутворювальних кримінальних правопорушень в кіберпросторі»* визначено, що кримінальні правопорушення, основним засобом яких є інформаційно-телекомунікаційні технології, системи й мережі, якщо водночас їх родовим об’єктом не є суспільні відносини, регламентовані розділом XVI Особливої частини Кримінального кодексу України, прийнято називати кіберутворювальними кримінальними правопорушеннями.

Виділено основні ознаки кіберутворювальних кримінальних правопорушень: 1) об’єктом є різні суспільні відносини, передбачені різними розділами Особливої частини Кримінального кодексу України; 2) засобом

учинення завжди будуть елементи інформаційно-телекомунікаційних технологій, систем та мереж; 3) в окремих кримінальних правопорушеннях цього типу кіберпростір є місцем учинення суспільно небезпечного діяння; 4) закріплені в законі України за допомогою введення в окремі статті Особливої частини Кримінального кодексу України або визначені в межах кваліфікуючих ознак, що передбачають кримінальну відповідальність за конкретні суспільно небезпечні діяння.

Автор виділив основні сфери вчинення шахрайства у кіберпросторі: 1) шахрайство у сфері електронної комерції; 2) шахрайство на інтернет-аукціонах; 3) традиційне шахрайство з використанням інформаційно-телекомунікаційних технологій; 4) шахрайство у сфері надання фінансових послуг. Акцентується на недоцільності змісту частини 3 статті 190, зокрема, через невідповідність змісту норми й категорії діянь, вчинюваних у кіберпросторі обманом чи зловживанням довірою. Водночас дисертант підкреслює, що операцію з використанням електронно-обчислювальної техніки можна вважати незаконною лише в разі несанкціонованого проникнення в інформаційно-телекомунікаційні технології, системи та мережі.

Зазначено, що основна сутність фішингу полягає в одержанні цифрової інформації про логіни, паролі до акаунтів, інтернет-банкінгу або електронних гаманців та інших цифрових даних особи, збережених в інформаційно-телекомунікаційних технологіях, мережах і системах. Автор підкреслює недоцільність кваліфікації діянь у формі фішингу за статтею 190 Особливої частини Кримінального кодексу України, сам обман у цьому разі є лише способом одержання персональних даних у вигляді цифрової інформації, а предметом фішингу є цифрова інформація. Одночасно з цим пропонується діяння у формі фішингу кваліфікувати за частиною 3 статті 361 Особливої частини Кримінального кодексу України так: «несанкціоноване втручання в роботу інформаційно-телекомунікаційних технологій, мереж і систем, що призвело до витоку інформації у формі копіювання».

Доведено нагальність уведення спеціалізованого складу кримінального правопорушення, зазначеного статтею 185 (крадіжка), яка б передбачала кримінальну відповідальність за крадіжку у сфері обігу безготівкових або електронних грошей і віртуальних активів. Залежно від фінансового інструменту було виділено такі способи таємного викрадення безготівкових, електронних грошей або віртуальних активів: 1) за допомогою оплати покупок із використанням персональних даних володільця картки або електронного гаманця в інформаційно-телекомунікаційних мережах; 2) одержанням доступу до системи дистанційного банківського обслуговування; 3) за допомогою зняття коштів у банкоматі. Водночас наголошується, що крадіжка безготівкових коштів або електронних грошей за допомогою оплати покупок із використанням персональних даних володільця картки або електронного гаманця в інформаційно-телекомунікаційних мережах може виражатися двома різними формами: 1) уведенням персональних даних володільця картки або електронного гаманця у вигляді

цифрової інформації; 2) за допомогою іншого втручання в роботу інформаційно-телекомунікаційних технологій.

Проаналізовано один із способів незаконного впливу на потерпілу особу, що полягає в погрозі незаконного знищення чи пошкодження цифрової інформації її блокуванням, модифікацією або видаленням. Підкреслено, що наразі така законодавча ініціатива не набула свого розвитку. Одночасно з цим автор запропонував кваліфікуючу ознаку до статті 189: «погроза блокування, видалення, знищення, модифікації або погроза іншого несанкціонованого втручання в роботу інформаційно-телекомунікаційних технологій, систем і мереж, що може завдати шкоди правам та інтересам потерпілої особи».

Обґрунтовано необхідність криміналізації суспільно небезпечних діянь у формі умисного знищення або пошкодження майна, вчиненого несанкціонованим втручанням у роботу інформаційно-телекомунікаційних технологій, систем і мереж, зокрема, за допомогою викладення диспозиції частини 1 статті 194 Особливої частини Кримінального кодексу України в такій редакції: «умисне знищення чи пошкодження чужого майна, що заподіяло шкоду у великих розмірах або вчинене способом несанкціонованого втручання у роботу інформаційно-телекомунікаційних технологій, систем і мереж».

Визначені та проаналізовані основні способи легалізації майна в кіберпросторі: 1) легалізація майна, отриманого злочинним шляхом, за допомогою вже наявної інтернет-інфраструктури; 2) легалізація майна, отриманого злочинним шляхом, унаслідок створення нової вебінфраструктури; 3) легалізація майна, отриманого злочинним шляхом, завдяки використанню обмінників і цифрових (електронних) валют; 4) легалізація майна, отриманого злочинним шляхом, за допомогою віртуальних активів.

Розділ 3 «Особливості кваліфікації кримінальних правопорушень в кіберпросторі» складається з трьох підрозділів, присвячених характеристиці особливостей кримінально-правової кваліфікації кримінальних правопорушень у кіберпросторі, предметом та засобом учинення яких є віртуальні активи, особливостей призначення покарання за вчинення кримінальних правопорушень у кіберпросторі та обставин, що обтяжують покарання за вчинення кримінальних правопорушень у кіберпросторі.

У *підрозділі 3.1 «Особливості кримінально-правової кваліфікації кримінальних правопорушень у кіберпросторі, предметом та засобом учинення яких є віртуальні активи»* визначені поняття, сутність та характеристики віртуальних активів, зокрема, під віртуальним активом варто 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, неможливість впливати на транзакції учасників криптосистеми. З огляду на специфіку віртуальних активів пропонується розглядати їх у трьох «формах»: як інформацію, як валюту та як інші нематеріальні блага.

Охарактеризовано кримінальні правопорушення, у яких віртуальні активи можуть бути предметом або засобом учинення суспільно небезпечного діяння. З'ясовано, що, незважаючи на фактичну відсутність правового регулювання віртуальних активів в Україні, поширеність їх використання серед українського суспільства лише зростає. Водночас зростає кількість суспільно небезпечних діянь, спрямованих на використання віртуальних активів як предмета або засобу вчинення кримінального правопорушення. Завдяки специфічним особливостям віртуального активу виникає багато запитань щодо кримінальної кваліфікації суспільно небезпечних діянь, спрямованих на їх протиправне заволодіння, зокрема, в межах учинення шахрайських дій або таємного викрадення віртуальних активів.

Автор, аналізуючи практичну складову вчинення крадіжки віртуальних активів у кіберпросторі, зазначає, що інформаційно-телекомунікаційні технології, системи та мережі завжди будуть засобом учинення кримінального правопорушення. Водночас інформаційно-телекомунікаційні мережі можуть розглядатися як місце його вчинення, оскільки всі віртуальні активи передаються, зберігаються та обертаються лише в межах певних криптографічних мереж – блокчейнів.

Запропоновано розширити предмет крадіжки, включивши до нього цифровий інформаційний продукт, тобто сукупність унікальних інформаційно-телекомунікаційних даних, об'єднаних у матеріальний чи віртуальний носій, що мають усі ознаки товару, власну вартість і належать за правом власності іншій особі. У разі крадіжки продукту порушуються не стільки відносини у сфері обігу цифрової інформації або авторські права, скільки відносини власності, оскільки правомірний власник більше не може здійснювати права користування, володіння й розпорядження викраденим продуктом. Прикладом такого продукту є саме віртуальний актив.

Визначені та проаналізовані основні способи легалізації злочинних доходів за допомогою віртуальних активів: 1) сервіси для конвертації віртуальних активів; 2) P2P-обмін; 3) сайти азартних ігор; 4) міксери віртуальних активів; 5) використання фіктивних інтернет-сайтів із продажу цифрових товарів.

У *підрозділі 3.2 «Особливості призначення покарання за вчинення кримінальних правопорушень в кіберпросторі»* зазначено, що проблематика призначення судом покарання за вчинення суспільно небезпечних діянь у кіберпросторі сьогодні посідає одне з основних місць як у науці кримінального права, так і в правозастосовній практиці. Сьогодні питання призначення покарання за кримінальні правопорушення в кіберпросторі є одними з найскладніших та найбільш неоднозначних серед проблем, що характеризують сучасний стан розвитку кримінальної юстиції в Україні.

На підставі аналізування слідчо-судової практики з'ясовано, що основними покараннями, застосовуваними за вчинення кримінальних правопорушень, передбачених XVI розділом Особливої частини Кримінального кодексу України, є штраф, обмеження волі й позбавлення волі.

На основі аналізування судової практики, зокрема, за період із 1 січня

2015 року до 1 січня 2023 року, було визначено, що фактично в 39 % усіх розглядуваних справ було призначено покарання у вигляді штрафу й у 61 % – у вигляді позбавлення волі. Водночас 98 % осіб, які вчинили кримінальні правопорушення за відповідними статтями Особливої частини Кримінального кодексу України і яким призначили покарання у вигляді позбавлення волі на певний строк, було звільнено від відбування основного покарання з випробуванням. У 2 % випадків особам було заборонено займатися певними видами діяльності.

Обґрунтовано, що з огляду на індивідуалізацію покарання за кримінальні правопорушення, регламентовані Особливою частиною Кримінального кодексу України, варто брати до уваги, що такі суспільно небезпечні діяння завжди вчиняються з використанням інформаційно-телекомунікаційних технологій, представлених у формі цифрових пристроїв. Зважаючи на це, пропонується розглядати спеціальну конфіскацію як можливість покарання.

Акцентується на основних проблемах призначення покарання, відповідальність за вчинення яких передбачена XVI розділом Особливої частини Кримінального кодексу України, зокрема: 1) вчинення декількох суспільно небезпечних діянь, передбачених Особливою частиною Кримінального кодексу України, для досягнення одного злочинного результату та власне призначення покарання за сукупністю кримінальних правопорушень; 2) вчинення кіберзалежних кримінальних правопорушень неповнолітніми особами.

У *підрозділі 3.3 «Кримінально-правова характеристика обставин, що обтяжують покарання за кримінальні правопорушення в кіберпросторі*» розкрито обставини, що обтяжують покарання за кримінальні правопорушення, враховуючи їх специфіку реалізації в межах кіберпростору. Здійснено типологізацію обставин, що обтяжують покарання за кримінальні правопорушення в кіберпросторі: 1) обставини, що обтяжують покарання, які суд за їх наявності у справі враховує під час призначення покарання; 2) обставини, які суд залежно від характеру вчиненого кримінального правопорушення має право не визнати такими, що обтяжують покарання.

У межах обставини, що обтяжує покарання за кримінальне правопорушення в кіберпросторі, зокрема, вчинення кримінального правопорушення щодо особи, яка перебуває в матеріальній, службовій чи іншій залежності від винного, виокремлено приклади таких суспільно небезпечних діянь: по-перше, шантаж у кіберпросторі, тобто вимагання коштів, послуг або інформації від особи, яка перебуває в службовій залежності від них; по-друге, вимагання або викрадення ідентифікаційних чи інших персональних даних для їх подальшого використання в злочинних діяннях; по-третє, відстеження й постійний контроль особи за допомогою програмного забезпечення віддаленого доступу до комп’ютера або мобільного телефону особи, яка перебуває в залежності від них, що порушує недоторканність приватного життя особи; по-четверте, «кібернасильство», що полягає в завданні шкоди за допомогою електронних форм спілкування й

контакту та може виявлятися в поширенні неправдивої інформації, чуток, пліток, образ, погроз щодо особи, залякуванні з метою контролювання її дій та поведінки або без такої.

Доведено нагальність доповнення статті 67 Кримінального кодексу України обставинами, що обтяжують кримінальне покарання, з урахуванням інформаційно-телекомунікаційного буму, з одного боку, й збройної агресії російської федерації та умов гібридної війни, з іншого, такими обставинами: 1) якщо кримінально протиправне діяння спрямоване на заподіяння шкоди державному комп'ютеру; 2) якщо предметом учинення кримінального правопорушення є цифрова інформація, що має ознаки державної таємниці.

Розділ 4 «Міжнародно-правові заходи та зарубіжний досвід кримінально-правової охорони кіберпростору» складається з двох підрозділів, що розкривають питання теоретико-правових аспектів застосування норм і принципів міжнародного права стосовно регулювання суспільних відносин у кіберпросторі в Україні, а також порівняльно-правового аналізу кримінальної відповідальності за вчинення кримінальних правопорушень у кіберпросторі.

У *підрозділі 4.1 «Теоретико-правові аспекти застосування норм і принципів міжнародного права стосовно регулювання відносин у кіберпросторі в Україні»* визначено, що основні принципи міжнародного права закріплені в декількох документах: 1) Статуті Організації Об'єднаних Націй; 2) Підсумковому акті Організації з безпеки і співробітництва в Європі; 3) Декларації про міжнародні принципи відповідно до Статуту Організації Об'єднаних Націй.

Проаналізовано основні принципи щодо регулювання міжнародних відносин у межах кіберпростору: 1) принцип суверенної рівності, поважання прав, властивих суверенітету; 2) принцип незастосування сили або погрози силою; 3) принцип співробітництва між державами; 4) принцип невтручання у внутрішні справи; 5) принцип рівноправ'я та право народів розпоряджатися своєю долею; 6) принцип мирного врегулювання суперечок; 7) принцип поважання прав людини та основних свобод, включаючи свободу совісті, релігії та переконань; 8) принцип невтручання у внутрішні справи; 9) принцип непорушності кордонів.

Доведено, що, незважаючи на закріплення в законодавствах більшості держав стратегії кібербезпеки та встановлення основних кіберзагроз, на міжнародному рівні залишається неврегульованим питання визнання кібератак агресією. Така неврегульованість ставить під сумнів і фактично нівелює можливості міжнародно-правового захисту держав від учинення кібератак із боку інших держав або окремих осіб за сприяння конкретних держав. З'ясовано, що застосування сили в кіберпросторі – це суспільно небезпечні діяння щодо використання спеціального шкідливого програмного забезпечення, яке модифікує, видаляє, блокує, копіює цифрову інформацію, що призводить до часткового або повного руйнування інформаційно-телекомунікаційної інфраструктури держави.

Обґрунтовано що кримінально-правова охорона кіберпростору є

глобальною проблемою людства та властива усім світовим державам. Тому створення якісної системи нормативного регулювання кримінально-правової охорони кіберпростору є не лише внутрішньодержавною, а й міжнародною проблемою. Доведено, що основна акумуляція зусиль щодо кримінально-правової охорони кіберпростору відбувається саме в межах прийняття міжнародних нормативних актів, які регулюють питання віднесення того чи іншого суспільно небезпечного діяння до кримінального правопорушення в кіберпросторі. З'ясовано що міжнародне співробітництво у сфері кримінально-правової охорони кіберпростору Україна реалізує за допомогою укладення й ратифікації конвенцій та угод, а також положень, які містять рекомендації щодо встановлення кримінальної відповідальності за суспільно небезпечні діяння, вчинювані в кіберпросторі. Насамперед Конвенція «Про кіберзлочинність», що була прийнята в межах діяльності Ради Європи.

Зазначено, що норми Конвенції містили спробу нормативного регулювання трьох основних блоків питань, зокрема: 1) уніфікації нормативно-правового закріплення кримінальних правопорушень у кіберпросторі в національних законодавствах держав-учасниць; 2) зближення національних кримінально-правових норм держав-учасниць; 3) регламентації та закріплення міжнародного співробітництва із запобігання, протидії, профілактики й розслідування кримінальних правопорушень у кіберпросторі.

На підставі аналізування основних норм Конвенції «Про кіберзлочинність» доведено, що, незважаючи на різноманітність закріплених у ній норм, Конвенція містить лише загальні положення регламентації відповідальності за кримінальні правопорушення з використанням інформаційно-телекомунікаційних технологій, систем і мереж. Акцентовано на необхідності доповнення й уточнення норм Конвенції «Про кіберзлочинність» у межах національних законодавств держав-учасниць.

Проаналізовано норми Конвенції «Про кіберзлочинність» на предмет імплементації в кримінальне законодавство України в розрізі співвідношення норм Конвенції та норм Кримінального кодексу України, одночасно визначаючи їх позитивні й негативні моменти.

У *підрозділі 4.2 «Порівняльно-правовий аналіз кримінальної відповідальності за вчинення кримінальних правопорушень в кіберпросторі за законодавством зарубіжних держав»* проаналізовані заходи щодо встановлення кримінальної відповідальності за кримінальні правопорушення в кіберпросторі в країнах англо-саксонської та романо-германської правових сімей. Правова регламентація установлення кримінальної відповідальності за кримінальні правопорушення в кіберпросторі переважно розміщена в окремих нормативних актах; водночас така країна, як Сполучені Штати Америки, крім загального регулювання відносин щодо встановлення кримінальної відповідальності за кримінальні правопорушення в кіберпросторі, застосовує регулювання на рівні окремих штатів, що значно відрізняється в кожному з них. Навпаки, країни романо-германської правової сім'ї характеризуються уніфікацією своєї правової регламентації щодо

кримінальної відповідальності за кримінальні правопорушення в кіберпросторі. Проте, незважаючи на належність до однієї правової сім'ї, кримінальні законодавства цих країн значно відрізняються між собою. Зокрема, країни Західної та Центральної Європи не виділяють як окремий розділ кримінальні правопорушення в кіберпросторі, а кримінальна відповідальність за них передбачена різними розділами їх Кримінальних кодексів. Так само в країнах Північної Європи кримінальна відповідальність за суспільно небезпечні діяння, вчинені за допомогою використання інформаційно-телекомунікаційних технологій, систем та мереж, виділена в окремий розділ.

Серед проаналізованих заходів виокремлено ті, які можуть буди запозичені у вітчизняне правозастосування: 1) на основі досвіду Естонії запропоновано підвищену кримінально-правову охорону об'єктів та суспільних відносин у межах державної діяльності в кіберпросторі, зокрема державної інформаційно-телекомунікаційної інфраструктури; 2) з огляду на позитивний досвід Данії запропоновано визначення складу кримінального правопорушення «комп'ютерне шахрайство» як незаконної зміни, доповнення чи видалення програмного коду або цифрової інформації, використовуваної для цифрового автоматизованого оброблення даних із метою отримання для себе або третіх осіб незаконної вигоди; 3) на основі досвіду Сполучених Штатів Америки запропоновано в межах статті 361 Особливої частини Кримінального кодексу України додати наслідки у вигляді «несанкціонованого одержання цифрової інформації»; 4) на основі досвіду Сполучених Штатів Америки ввести в національне законодавство «цифрові збитки» – будь-яке пошкодження цілісності та доступності цифрових даних, програм, систем або цифрової інформації. На думку автора, такий підхід на законодавчому рівні дав би можливість вносити рішення про розмір та характер збитків у кожному випадку індивідуально, враховуючи всі обставини справи; 5) досвід Великобританії щодо введення й трактування поняття «кібертероризм» – неправомірний доступ до цифрової інформації, що зберігається в інформаційно-телекомунікаційних технологіях, системах і мережах, розцінюється як терористичний акт і тягне за собою підвищену кримінальну відповідальність, якщо одержана таким чином інформація завдала значної шкоди або використовувалася для організації масових заворушень.

ВИСНОВКИ

У дисертації наведене теоретичне узагальнення й запропоноване нове вирішення наукової проблеми – розроблення концептуальних засад кримінально-правової охорони кіберпростору в Україні, що стала основою для формулювання пропозицій щодо вдосконалення законодавства у цьому контексті. У результаті проведеного дослідження сформульовано низку нових наукових положень і висновків, спрямованих на досягнення поставленої

мети, основні з яких викладено нижче.

1. Етапами становлення кримінальної відповідальності за кримінальні правопорушення в кіберпросторі на теренах України є: 1) початковий етап, що характеризується правовим вакуумом у регулюванні кримінально-правової охорони кіберпростору та безкарністю кримінальних правопорушень у кіберпросторі; 2) етап зародження, особливостями якого є прийняття Кримінального кодексу України, що визначав три види кримінально караних діянь у кіберпросторі та активне використання зловмисників у своїй кримінально-протиправній діяльності, різноманітних IRC-клієнтів для вчинення шахрайств у кіберпросторі; 3) імплементаційний етап, що полягає в ратифікації Україною Конвенції «Про кіберзлочинність», яка визначала 23 кримінальні правопорушення в кіберпросторі та фактичну імплементацію частини норм Конвенції про кіберзлочинність у законодавство України; 4) економічний етап, який характеризується появою віртуальних валют та розвитком економічних кримінальних правопорушень у кіберпросторі; 5) нормотворчий етап, що полягає у створенні спеціалізованого правоохоронного органу – Департаменту кіберполіції Національної поліції України, прийнятті Закону України «Про основні засади забезпечення кібербезпеки України»; 6) сучасний етап, що характеризується карантинними обмеженнями, які спричинила пандемія COVID-19, та збройною агресією російської федерації, що дала новий поштовх у розвитку кримінально-протиправних діянь у кіберпросторі, зокрема, з’явилися нові види кримінальних правопорушень у кіберпросторі, а їх кількість стрімко збільшується.

2. Проєктування методології дослідження є важливим кроком для забезпечення ефективного, надійного та відповідного юридичного розслідування кіберзлочинів. Вона сприяє покращанню кібербезпеки, забезпеченню справедливості та захисту прав потерпілих сторін. Методологія є загальним підходом до дослідження кіберзлочинів та може варіюватися залежно від конкретного випадку й доступності ресурсів. У контексті цього дослідження було використано такі наукові методи: метод аналізу, емпіричний метод, метод контент-аналізу, метод кейс-студії, порівняльно-правовий метод, метод системного аналізу.

3. Визначено основні характеристики та принципи кіберпростору. Зокрема, серед основних характеристик було виділено віртуальність, мережеву належність, середовище взаємодії, динамічність, комунікативність та поєднання територіалізації й детериторіалізації. Серед принципів, що забезпечують стабільність функціонування кіберпростору, ми виділили такі: дисципліну, відповідальність, додержання прав і свобод людини та громадянина й своєчасне втручання.

4. Кримінальне правопорушення в кіберпросторі – суспільно небезпечне, протиправне, винне, каране діяння, що посягає та заподіює шкоду різнорідним суспільним відносинам за допомогою використання інформаційно-телекомунікаційних технологій, інформаційно-телекомунікаційних систем та мереж і створюваного ними

кіберпростору.

5. Ознаками кримінальних правопорушень у кіберпросторі є: 1) інтелектуальний характер; 2) анонімність; 3) транснаціональний характер; 4) латентність; 5) використання навиків соціальної інженерії; 6) суб'єктна складова; 7) дистанційність; 8) доступність матеріалів, необхідних для скоєння кримінального правопорушення в кіберпросторі.

6. На основі аналізування наявних доктринальних підходів до типологізації видів кримінальних правопорушень у кіберпросторі запропоновано вдосконалений розширений авторський підхід. По-перше, типологізувати кримінальні правопорушення в кіберпросторі за родовим об'єктом; по-друге, відповідно до кваліфікації суб'єктів учинення 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 кількості суб'єктів учинення кримінального правопорушення; по-шосте, залежно від мети використання електронно-обчислювальних машин інформаційно-телекомунікаційних мереж; по-сьоме, залежно від мети вчинення кримінальних правопорушень у кіберпросторі; по-восьме, залежно від повноти ознак кримінальних правопорушень у кіберпросторі; по-дев'яте, залежно від правового режиму інформації, що є предметом кримінальних правопорушень у кіберпросторі; по-десяте, залежно від сутності кримінальних правопорушень у кіберпросторі; по-одинадцяте, залежно від кількості суб'єктів учинення кримінальних правопорушень у кіберпросторі; по-дванадцяте, відповідно до видів кримінальних правопорушень у кіберпросторі, передбачених Конвенцією Ради Європи «Про кіберзлочинність»; по-тринадцяте, відповідно до статті 12 Кримінального кодексу України на кримінальні проступки та злочини.

7. Наголошено, що основним предметом кіберзалежних кримінальних правопорушень є цифрова інформація у сфері цифрових технологій, в інформаційно-телекомунікаційних системах та мережах. Кіберутворювальні кримінальні правопорушення є класичними кримінальними правопорушеннями, які внаслідок використання інформаційно-телекомунікаційних технологій перейшли в кіберпростір.

8. Основними особливостями, що характеризують кіберутворювальні кримінальні правопорушення, є: 1) об'єкт таких кримінальних правопорушень – різнорідні суспільні відносини, передбачені різними розділами Особливої частини Кримінального кодексу України; 2) засіб учинення кримінального правопорушення завжди будуть елементи інформаційно-телекомунікаційних технологій, систем та мереж; 3) місце учинення (в окремих випадках є кіберпростір; 4) кваліфікуючі ознаки, що передбачають кримінальну відповідальність за конкретні суспільно небезпечні діяння.

9. Кіберзалежні кримінальні правопорушення характеризуються вчиненням декількох суспільно небезпечних діянь, передбачених Особливою частиною Кримінального кодексу України, для досягнення одного злочинного

результату та власне призначенням покарання за сукупністю кримінальних правопорушень.

10. Найбільш часто застосовуваним покараннями за кіберутворювальні кримінальні правопорушення є штраф і позбавлення волі. Водночас штраф як основне покарання становить 61 % серед усіх інших. Установлено, що в 93 % випадків призначення покарання у вигляді позбавлення волі замінюють на звільнення від відбування покарання з випробуванням.

11. Основними способами легалізації майна, отриманого злочинним шляхом, є: 1) легалізація майна, отриманого злочинним шляхом, за допомогою вже наявної інтернет-інфраструктури (маркетплейси, сайти оголошень, соціальні мережі, інтернет-аукціони, краудфандинг); 2) легалізація майна, отриманого злочинним шляхом, створенням нової вебінфраструктури (інтернет-магазин); 3) легалізація майна, отриманого злочинним шляхом, використанням обмінників та цифрової (електронної) валюти; 4) легалізація майна, отриманого злочинним шляхом, за допомогою віртуальних активів.

12. Основними ознаками віртуальних активів є: 1) децентралізованість; 2) транснаціональність; 3) конфіденційність операцій; 4) цифровізація; 5) майновий характер; 6) анонімність. Акцентовано на співвідношенні понять «віртуальний актив» та «криптовалюта», доведено неідентичність зазначених понять.

13. Наголошено на необхідності введення додаткової обставини, що обтяжує кримінальні правопорушення в кіберпросторі: 1) заподіяння шкоди інформаційно-телекомунікаційній технології, системі або мережі державного значення, які мають ознаки критичної інфраструктури; 2) предметом кримінального правопорушення є цифрова інформація, що має ознаки державної таємниці.

14. На підставі аналізування Статуту Організації Об’єднаних Націй, Підсумкового акта Організації з безпеки і співробітництва в Європі та Декларації про міжнародні принципи відповідно до статуту Організації Об’єднаних Націй визначені основні принципи міжнародного права та надано їх характеристику через призму регулювання міжнародних відносин у межах кіберпростору.

15. Стратегія кібербезпеки закріплена в законодавствах більшості держав. Незважаючи на окреслення основних кіберзагроз на рівні національних законодавств, на міжнародному рівні залишається неврегульованим питання визнання кібератак агресією. Така неврегульованість ставить під сумнів та фактично унеможливлює міжнародно-правовий захист держав від учинення кібератак із боку інших держав або окремих осіб за сприяння конкретних держав.

16. Співробітництво держав у межах регулювання відносин, що виникають у кіберпросторі, та прийняття декількох міжнародних нормативних актів, жоден із зазначених документів повністю не врегульовує питань ані кіберпростору, ані кібербезпеки. Зазначені міжнародні нормативні акти здебільшого зосереджують увагу саме на формах учинення суспільно

небезпечних діянь у кіберпросторі. Сьогодні виникає нагальна потреба в уніфікованому міжнародному нормативному акті, де б визначалися поняття «кримінальне правопорушення в кіберпросторі», «кіберпростір», «кібертероризм», «кіберзагроза», «кібератака», «кіберзброя». Одночасно з цим у такому акті повинно бути врегульоване питання щодо притягнення до відповідальності за кібератаки, превентивні кібератаки та кібератаки у відповідь.

17. Узагальнено та систематизовано зарубіжний досвід правового регулювання відповідальності за вчинення кримінальних правопорушень за допомогою використання інформаційно-телекомунікаційних технологій. З'ясовано, що країни, які належать до англосаксонської правової сім'ї, крім нормативного регулювання, широко використовують систему судових прецедентів, у цьому разі правова регламентація встановлення кримінальної відповідальності за кримінальні правопорушення в кіберпросторі переважно розміщена в окремих нормативних актах. Наприклад, така країна, як Сполучені Штати Америки, крім загального регулювання відносин щодо встановлення кримінальної відповідальності за кримінальні правопорушення в кіберпросторі, застосовує регулювання на рівні окремих штатів, які дуже різняться між собою. Навпаки, країни романо-германської правової сім'ї характеризуються уніфікацією своєї правової регламентації щодо кримінальної відповідальності за кримінальні правопорушення в кіберпросторі. Проте, незважаючи на належність до однієї правової сім'ї, кримінальні законодавства цих країн істотно відрізняються між собою. Так, країни Західної та Центральної Європи не виділяють як окремий розділ кримінальні правопорушення в кіберпросторі, а кримінальна відповідальність за них передбачена різними розділами їх Кримінальних кодексів, у країнах Північної Європи кримінальна відповідальність за суспільно небезпечні діяння за допомогою використання інформаційно-телекомунікаційних технологій, систем та мереж виділена в окремий розділ.

Запропоновано такі зміни до Кримінального кодексу України:

1. Викласти назву статті 361 та її зміст у такій редакції:

Несанкціоноване втручання в роботу інформаційно-телекомунікаційних технологій, систем та мереж

Несанкціоноване втручання в роботу інформаційно-телекомунікаційних технологій, систем та мереж, тобто одержання можливості для ознайомлення та (або) використання цифрової інформації, яка міститься в інформаційно-телекомунікаційній технології, системі або мережі за допомогою проникнення, особою, яка не має права доступу до інформаційно-телекомунікаційної технології, системи або мережі та (або) за дозволом власника інформаційно-телекомунікаційної технології, системи або мережі, що не призвело до наслідків у вигляді витоку, копіювання, модифікації, спотворення процесу оброблення, перехоплення, блокування і (або) знищення цифрової інформації, –

Ті самі дії, вчинені повторно або за попередньою змовою групою осіб, –

Дії, передбачені частиною першою або другою цієї статті, якщо вони призвели до витоку, перехоплення, копіювання, спотворення процесу оброблення та (або) модифікації цифрової інформації, –

Дії передбачені частиною першою або другою цієї статті, якщо вони призвели до блокування та (або) знищення цифрової інформації, –

Дії, передбачені частинами першою – четвертою цієї статті, якщо вони заподіяли значну шкоду чи створили небезпеку тяжких технологічних аварій або екологічних катастроф, загибелі або масового захворювання населення чи інших тяжких наслідків, –

Дії, передбачені частинами першою – третьою та четвертою цієї статті, якщо вони вчинені організованою групою або злочинною організацією, –

Дії, передбачені частинами третьою – четвертою цієї статті, якщо вони вчинені під час дії воєнного стану, –

Дії, передбачені частинами першою – четвертою цієї статті, не вважаються несанкціонованим втручанням в інформаційно-телекомунікаційні технології, системи та мережі, якщо вони були вчинені відповідно до порядку пошуку та виявлення потенційних вразливостей таких систем чи мереж.

2. Викласти частину другу статті 362 у такій редакції: Несанкціоноване копіювання цифрової інформації, яка оброблюється в інформаційно-телекомунікаційних технологіях, системах та мережах, якщо це призвело до її витоку, вчинене особою, яка має право доступу до такої інформації.

3. Викласти назву статті 363 та її зміст у такій редакції:

Порушення правил експлуатації інформаційно-телекомунікаційних технологій, систем та мереж або порядку чи правил захисту цифрової інформації, яка в них оброблюється

Порушення правил експлуатації інформаційно-телекомунікаційних технологій, систем та мереж або порядку чи правил захисту цифрової інформації, яка в них оброблюється, якщо це заподіяло значну шкоду, вчинені особою, яка відповідає за їх експлуатацію.

4. Викласти статтю 363-1 у такій редакції:

Перешкоджання роботі інформаційно-телекомунікаційних технологій, систем та мереж шляхом масового розповсюдження повідомлень електрозв’язку

Умисне масове розповсюдження повідомлень електрозв’язку, здійснене без попередньої згоди адресатів, що призвело до порушення або припинення роботи інформаційно-телекомунікаційних технологій, систем та мереж, –

Ті самі дії, вчинені повторно або за попередньою змовою групою осіб, якщо вони заподіяли значну шкоду, –

Дії, передбачені частиною першою або другою цієї статті, якщо вони вчинені з корисливих мотивів, –

Дії, передбачені частиною першою або другою цієї статті, якщо вони спричинили тяжкі наслідки або вчинені проти інформаційної інфраструктури держави.

5. Виключити з частини третьої статті 190 такий текст: …або шляхом незаконних операцій із використанням електронно-обчислювальної техніки.

6. Доповнити частину другу статті 190 таким змістом: Шахрайство, вчинене повторно або за попередньою змовою групою осіб, або таке, що завдало значної шкоди потерпілому, або шляхом операцій із використанням інформаційно-телекомунікаційних технологій, систем та мереж.

7. Доповнити розділ VI «Кримінальні правопорушення проти власності» нормами такого змісту:

185-1. Крадіжка у сфері обігу безготівкових або електронних грошей та віртуальних активів.

1. Крадіжка у сфері обігу безготівкових або електронних грошей і віртуальних активів, учинена введенням цифрової інформації в інформаційно-телекомунікаційні технології, системи та мережі.

2. Крадіжка у сфері обігу безготівкових або електронних грошей та віртуальних активів чи інше втручання в роботу інформаційно-телекомунікаційних технологій, систем та мереж.

3. Дії, передбачені частинами першою – другою цієї статті, вчинені повторно або за попередньою змовою групою осіб, або такі, що завдали значної шкоди потерпілому.

4. Дії, передбачені частинами першою – третьою цієї статті, якщо вони вчинені за допомогою модифікації цифрової інформації.

5. Крадіжки, передбачені частинами першою – другою цієї статті, вчинені у великих розмірах або організованою групою.

6. Дії, передбачені частинами першою – другою цієї статті, вчинені в умовах воєнного або надзвичайного стану.

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Наукові праці, у яких опубліковані основні наукові результати дисертації:

Монографії

1. Dumchikov M., Bondarenko O., Peculiarities of criminal legal protection of cyberspace and combating cybercrimes : monograph. Germany : AP Lambert Academic Publishing GmbH & Co. KG, 2023. 73 p.

2. Концептуальні засади кримінально-правової охорони кіберпросторів Україні : монографія / М. О. Думчиков. Суми : Сумський державний університет, 2023. 416 с.

Статті у фахових виданнях України категорії «Б»

3. Думчиков М. О. Процеси диджиталізації і криміналістика: ретроспективний аналіз. *Збірник «Криміналістика і судова експертиза».* 2020. Вип. 65. С. 100–108. DOI: https://doi.org/10.33994/kndise.2020.65.10

4. Думчиков М. О., Рєпін Д. А. Легалізація доходів, отриманих злочинним шляхом, за допомогою використання віртуальної валюти (криптовалюти): кримінологічний та кримінально-правовий аспект. *Журнал*

східноєвропейського права. 2020. № 82. С. 32–37.

5. Думчиков М. О., Пахомов В. В., Бондаренко О. С. Криміналістичні проблемні аспекти боротьби зі злочинами у кіберсфері. *Збірник «Криміналістика і судова експертиза»*. 2020. № 1. С. 18–22.

6. Думчиков М. О., Бондаренко О. С. Кримінологічні аспекти протидії легалізації корупційних доходів у кіберпросторі. *Правові горизонти*. 2021. № 14. С. 105–110.

7. Думчиков М. О. Порівняльний аналіз кримінально-правової охорони кіберпростору країн Балтії та України. *Південноукраїнський правничий часопис*. 2022. № 4. С. 73–80. DOI: https://doi.org/10.32850/sulj.2022.4.1.12.

8. Думчиков М. О., Шевцов Я. А. До проблеми визначення поняття та ознак кіберзлочинів. *Журнал східноєвропейського права*. 2022. № 104. С. 12–22.

9. Думчиков М. О. Особливості кваліфікації шахрайства в кіберпросторі, засобом вчинення якого є віртуальні активи. *Науково-інформаційний вісник Івано-Франківського університету права імені Короля Данила Галицького. Серія Право.* 2022. № 14 (26). С. 159–165. DOI: 10.33098/2078-6670.2022.14.26.149-155.

10. Думчиков М. О. Способи легалізації (відмивання) майна, одержаного злочинним шляхом у кіберпросторі. *Аналітично-порівняльне правознавство*. 2022. № 5. С. 330–334. DOI: https://doi.org/10.24144/2788-6018.2022.05.61.

11. Думчиков М. О. Особливості протидії легалізації злочинних доходів за допомогою віртуальних активів у кіберпросторі: практичний вимір. *Law. State. Technology*. 2022. № 1. С. 133–145.

12. Думчиков М. О., Каріх І. В. Становлення та генеза кримінальної відповідальності за кримінальні правопорушення у кіберпросторі на теренах України. *Юридичний науковий електронний журнал*. 2022. № 5. С. 476–478. DOI: https://doi.org/10.32782/2524-0374/2022-5/113.

13. Думчиков М. О., Малетов Д. В. Загальна характеристика та види розкрадань шляхом використання інформаційних технологій як одного з найпоширеніших видів кримінальних правопорушень у кіберпросторі. *Юридичний науковий електронний журнал*. 2022. № 7. С. 278–28. DOI: https://doi.org/10.32782/2524-0374/2022-8/60.

14. Думчиков М. О. Кримінальні правопорушення в сфері комп’ютерної інформації: ретроспективний аналіз. *Науковий вісник Міжнародного гуманітарного університету.* 2022. № 57. С. 86–90. DOI: https://doi.org/10.32841/2307-1745.2022.57.18.

15. Думчиков М. О. Кримінально-правова характеристика поняття та видів кіберзлочинів. *Науковий вісник Міжнародного гуманітарного університету*. 2022. № 55. С. 65–68. DOI: https://doi.org/10.32841/2307-1745.2022.55.14.

16. Думчиков М. О. Поняття та ознаки кіберпростору, які роблять його привабливим для вчинення кримінальних правопорушень в сфері

комп'ютерної інформації. *Юридичний науковий електронний журнал*. 2022. № 3. С. 195–197. DOI: https://doi.org/10.32782/2524-0374/2022-3/44.

17. Думчиков М. О., Каріх І. В. Зарубіжний досвід протидії кримінальним правопорушенням проти власності, вчиненим із використанням інформаційно-телекомунікаційних технологій. *Прикарпатський юридичний вісник*. 2023. № 2. С. 55-61.

18. Думчиков М. О., Каріх І. В. Неправомірний вплив на інформаційну інфраструктуру України. *Юридичний науковий електронний журнал*. 2023. № 5. С. 111–116.

19. Думчиков М. О. Аналіз міжнародних нормативних актів в сфері встановлення кримінальної відповідальності за суспільно небезпечні діяння, вчинені в кіберпросторі. *Актуальні проблеми політики*. 2023. № 71. С. 158–163. DOI: https://doi.org/10.32782/app.v71.2023.21.

Статті в зарубіжних періодичних наукових виданнях юридичного напряму

20. Pakhomov V., Bondarenko O., Dumchikov M. Criminal legal characteristic of social engineering as a way of committing fraud. *Legea si Viata*. 2019. № 4/2. P. 149–153.

21. Думчиков М. О., Пахомов В. В. Кіберзлочинність як новітній феномен та джерело високого рівня суспільної небезпеки. *Visegrad Journal on Human Rights*. 2021. № 2. С. 333–340.

22. Dumchykov M. O. Doctrinal approaches to defining the concept of cybercrime and its main features. *European Socio-Legal and Humanitarian Studies*. 2022. № 2. P. 111–116.

23. Dumchykov M. O. International legal standards for combating fraud in the field of computer information. *European Socio-Legal and Humanitarian Studies*. 2022. № 2. P. 121–129.

24. Dumchykov M. O. The main reasons for committing economic criminal offenses in cyberspace. *European Socio-Legal and Humanitarian Studies*. 2023. № 1. P. 59–65.

Статті в періодичних наукових виданнях, що індексуються БД Scopus та Web of Science

25. Dumchikov M., Kononenko N., Batsenko L., Halenin R., Hlushchenko N. Issues of regulating cryptocurrency and control over its turnover: international experience. 2020, 10–20 July. Vol. 9. Issue 31. DOI: https://doi.org/10.34069/AI/2020.31.07.1. (**WoS**).

26. Dumchikov M., Yunin O., Nestor N., Borko A., Yermenchuk O. Criminological and forensic characteristics of forms of embezzlement committed through the use of information technology. *Amazonia Investiga*. 2021. № 10. P. 131–140. DOI: https://doi.org/10.34069/AI/2021.41.05.13. (**WoS**).

27. Dumchikov Mykhailo, Bondarenko Olga, Utkina Maryna. Cybercrime as a Threat to the National Security of the Baltic States and Ukraine: The Comparative Analysis. *International Journal of Safety and Security Engineering*.

2022. № 4. P. 10. DOI: https://doi.org/10.18280/ijsse.120409. (**Scopus**).

28. Dumchikov M., Fomenko O., Pakhomov V., & Kabenok Y. The essence and classification of cybercrime in the field of computer information. *Amazonia Investiga.* 2022. № 11 (51). P. 291–299. DOI: https://doi.org/10.34069/AI/2022.51.03.29. (**WoS**).

29. Dumchikov M., Horobets N., Honcharuk V., Dehtiar R. Digital Currency as a Subject of Economic Criminal Offenses. *Law, State and Telecommunications Review* [S. l]. 2022. Vol. 14, No. 1. P. 20–30. DOI: 10.26512/lstr.v14i1.38676. (**Scopus**).

30. Dumchikov M. Reznik O. Bondarenko O. Peculiarities of countering legalization of criminal income with the help of virtual assets: legislative regulation and practical implementation. *Journal of Money Laundering Control*. 2022. DOI: 10.1108/JMLC-12-2021-0135. **(Scopus та WoS).**

Наукові праці, що засвідчують апробацію матеріалів дисертації:

31. Думчиков М. О. Topical issues of the current state of carding as the most common type of cybercrime. *Реформування правової системи в контексті євроінтеграційних процесів : матеріали III Міжнародної науково-практичної конференції* : тези доповідей. Суми : Сумський державний університет, 2019. № 2. С. 242-244.

32. Думчиков М. О. Проблеми використання електронних доказів в цивільному процесі. *Травневі правові читання : матеріали І Всеукраїнської науково-практичної конференції здобувачів та викладачів закладів вищої освіти* : тези доповідей. Черкаси, 2020. С. 95-97.

33. Думчиков М. О. Кримінально-правова характеристика телефонного скамінгу як одного з видів соціальної інженерії. *Die wichtigsten Vektoren für die Entwicklung der Wissenschaft im Jahr 2020: der Sammlung wissenschaftlicher Arbeiten «ΛΌГОΣ» zu den Materialien der internationalen wissenschaftlich-praktischen Konferenz* : тези доповідей. Europäische : Duchy of Luxembourg, 2020. С. 68-70.

34. Думчиков М. О. Кіберзлочинність як нова світова кримінальна загроза: ретроспективний аналіз. *Міжвідомчий науково-практичний круглий стіл «Кримінологічна теорія і практика: досвід та проблеми сьогодення та шляхи їх вирішення* : тези доповідей. Київ, 2020. С. 20-22.

35. Думчиков М. О. Кібератаки як новітня загроза інформаційній безпеці. *Реформування правової системи в контексті євроінтеграційних процесів : матеріали IV Міжнародної науково-практичної конференції* : тези доповідей. Суми : Сумський державний університет, 2020. № 2. С. 67-69.

36. Думчиков М. О. Сучасні аспекти кібербезпеки в контексті глобальних загроз. *Реформування правової системи в контексті євроінтеграційних процесів : матеріали IV Міжнародної науково-практичної конференції* : тези доповідей. Суми : Сумський державний університет, 2020. С. 338–341.

37. Думчиков М. О. Інтернет-шахрайство у сфері комп’ютерної

інформації як об’єкт криміналістичного аналізу. *Актуальні питання судової експертології, криміналістики та кримінального процесу* : тези доповідей. Київ : Ліра-К, 2021. С. 108–111.

38. Думчиков М. О. Поняття кіберзлочину в криміналістиці і його значення для розслідування. *Актуальні питання судової експертології, криміналістики та кримінального процесу* : тези доповідей. Київ : Ліра-К, 2021. С. 107–109.

39. Думчиков М. О. General issues of criminal characteristics of legalization of corrupted income. *Реформування правової системи в контексті євроінтеграційних процесів : матеріали V Міжнародної науково-практичної конференції* : тези доповідей. Суми : Сумський державний університет, 2021. С. 275–277.

40. Думчиков М. О. Загальні питання криміналістичної характеристики легалізації корупційних доходів. *Матеріали Всеукраїнської науково-практичної конференції «Актуальні питання та перспективи розвитку кримінального права, кримінології та судочинства»* : тези доповідей. Київ, 2021. С. 112–115.

41. Думчиков М. О. Кіберзлочинність та дистанційне шахрайство як одна із загроз сучасному суспільству. *VI Міжнародна наукова конференція з фундаментальних наук, мистецтва, бізнесу та освіти, інтернет-технологій і суспільства «Trends and directions of development of scientific approaches and prospects of integration of internet technologies into society».* (Стокгольм. Швеція, 23–26 лютого 2021 р.). С. 199–201.

42. Думчиков М. О. Злочини у сфері використання платіжних систем та шахрайство у кіберпросторі як одні з видів кіберзлочинів. *Матеріали Всеукраїнської науково-практичної конференції «Актуальні питання та перспективи розвитку кримінального права, кримінології та судочинства», присвяченої 200-й річниці з дня народження Френсіса Гальтона* : тези доповідей. Київ, 2022. С. 221-225.

43. Думчиков М. О. Відмивання грошей за допомогою криптовалюти. *Реформування правової системи в контексті євроінтеграційних процесів : Матеріали VI Міжнародної науково-практичної конференції* : тези доповідей. Суми : Сумський державний університет, 2022. С. 416-418.

44. Думчиков М. О. Computer – technical expertise in the investigation of computer criminal offenses. *Реформування правової системи в контексті євроінтеграційних процесів : матеріали VI Міжнародної науково-практичної конференції* : тези доповідей. Суми : Сумський державний університет, 2022. С. 574-576.

45. Думчиков М. О. Напрями протидії легалізації злочинних доходів за допомогою віртуальних активів. Реформування правової системи в контексті євроінтеграційних процесів. *Матеріали VI Міжнародної науково-практичної конференції* : тези доповідей. Суми : Сумський державний університет, 2022. С. 257-260.

46. Думчиков М. О. Кіберзлочини в сфері комп’ютерної інформації: поняття та види. *Актуальні питання юридичної науки та практики : зб. наук.*

праць студ. та молодих вчених : тези доповідей. Хмельницький : Вид-во МАУП, 2022. С. 73-77.

47. Думчиков М. О. Криміналістична типологізація кримінальних правопорушень у кіберпросторі. *Реформування правової системи в контексті євроінтеграційних процесів* : тези доповідей. Суми : Сумський державний університет, 2023. С. 330–333.

48. Dumchikov M. O. The main reasons for committing economic criminal offenses in cyberspace. *Реформування правової системи в контексті євроінтеграційних процесів* : тези доповідей. Суми : Сумський державний університет, 2023. С. 263–265.

АНОТАЦІЯ

Думчиков М. О. Концептуальні засади кримінально-правової охорони кіберпростору в Україні. – *Кваліфікаційна наукова праця на правах рукопису.*

Дисертація на здобуття наукового ступеня доктора юридичних наук за спеціальністю 12.00.08 «Кримінальне право та кримінологія; кримінально-виконавче право». – Дніпровський державний університет внутрішніх справ, Дніпро, 2024.

У дисертації наведене теоретичне узагальнення й запропоноване нове вирішення наукової проблеми, що полягало в розробленні на основі аналізування наявних наукових підходів, чинного вітчизняного та зарубіжного законодавств і практики їх реалізації комплексних науково та практично обґрунтованих концептуальних засад кримінально-правової охорони кіберпростору в Україні.

Об’єктом дослідження є суспільні відносини, що виникають у процесі кримінально-правової охорони кіберпростору та встановлення кримінальної відповідальності за вчинення кримінальних правопорушень у кіберпросторі. Предметом дослідження є концептуальні засади кримінально-правової охорони кіберпростору в Україні. Ретроспективно узагальнено й систематизовано наукові дослідження, присвячені кримінально-правовій охороні кіберпростору. Визначено та охарактеризовано шість етапів становлення кримінальної відповідальності за кримінальні правопорушення в кіберпросторі на теренах України. Сформульовано основні характеристики та принципи організації кіберпростору. Визначено й удосконалено основні характеристики кримінальних правопорушень у кіберпросторі. Виділено підстави для типологізації кримінальних правопорушень у кіберпросторі. Визначено та надано характеристику основних ознак віртуальних активів (децентралізованість, транснаціональність, конфіденційність операцій, цифровізація, майновий характер, анонімність). Наведено визначення поняття «віртуальний актив», 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. Визначені та проаналізовані основні обставини, що обтяжують покарання за кримінальні правопорушення в кіберпросторі з урахуванням специфічних особливостей учинення таких суспільно небезпечних діянь. Узагальнено зарубіжний досвід установлення кримінальної відповідальності за вчинення суспільно небезпечних діянь у кіберпросторі та визначено роль для України міжнародного співробітництва у сфері кримінально-правової охорони кіберпростору.

Ключові слова: *кримінальні правопорушення в кіберпросторі, кіберпростір, інформаційно-телекомунікаційні технології, віртуальний простір, інтернет-мережа, кіберзлочини, комп'ютерні кримінальні правопорушення, цифрова інформація, шкідливе програмне забезпечення.*

SUMMARY

Dumchykov M. O. Conceptual principles of criminal law protection of cyberspace in Ukraine. – Qualification scientific work printed as manuscript.

The dissertation for obtaining the scientific degree the Doctor of Law on a specialty 12.00.08 – Criminal Law and Criminology; Criminal Executive Law. – Dnipro State University of Internal Affairs, Dnipro, 2024.

The dissertation presents a theoretical overview and proposes a novel solution to the scientific issue, which involved the development of well-founded conceptual underpinnings for the criminal-law safeguarding of cyberspace in Ukraine. This was achieved through an examination of existing scientific approaches, current domestic and foreign legislation, as well as the practical implementation of these approaches.

The focus of this study is on the societal relations that arise during the enforcement of criminal law for the protection of cyberspace and the establishment of criminal liability for offenses committed in cyberspace. The study specifically explores the conceptual foundation of criminal law protection for cyberspace in Ukraine.

Previous research in the realm of criminal law protection of cyberspace is retrospectively summarized and organized systematically. It is highlighted that a crucial element in successful scientific research lies in employing the correct methodology. This ensures the systematic and comprehensive nature of the research, while also enabling the development of conclusions and recommendations that hold significant value for both academic and practical pursuits. The methods employed include analysis, empirical research, content analysis, case study, comparative legal analysis, and system analysis. These methods were applied in a manner that maintains their interrelatedness and interdependence, thereby contributing to the thoroughness and objectivity of the research.

The study identifies six stages of criminal liability for offenses committed in cyberspace within the borders of Ukraine: 1) initial stage; 2) formation stage;

3) implementation stage; 4) economic stage; 5) legislative stage; 6) contemporary stage.

The relationship between the terms «cyberspace», «information space», «virtual space», and «internet space» is examined. It is determined that the concept of «cyberspace» holds a narrower meaning compared to «information» and «virtual» space, but encompasses a broader scope than the concept of «internet space».

It has been ascertained that three distinct approaches to defining the concept of «cyberspace» are conventionally recognized: legal, doctrinal, and philosophical. Drawing from the analysis of these approaches, particularly the doctrinal one, it is suggested to view cyberspace from an informational, virtual, and societal standpoint.

The primary characteristics and organizational principles of cyberspace have been outlined. Notably, key attributes such as virtual nature, network connectivity, interactive environment, dynamism, communicability, and the interplay of territorial and non-territorial elements have been underscored. Among the principles that ensure the stable functioning of cyberspace, the following have been highlighted: the principle of discipline, the principle of accountability, the principle of upholding individual rights and freedoms, and the principle of timely intervention. Distinctions are made between the terms «cybercriminal offense», «computer information-related offense», and «computer-related criminal offense».

The fundamental attributes of criminal offenses in cyberspace have been identified and refined: 1) intellectual nature; 2) transnational character; 3) latency; 4) utilization of social engineering skills; 5) subjective component; 6) remoteness; 7) availability of necessary materials for committing a cybercrime; 8) anonymity.

Emphasis is placed on the desirability of aligning the terminology outlined in the «Law of Ukraine on the Fundamental Principles of Ensuring Cyber security in Ukraine» with the provisions and norms of the existing Criminal Code of Ukraine. This pertains specifically to the incorporation and utilization of the term «criminal offense in cyberspace», which is proposed to encompass socially perilous, illicit, blameworthy acts that infringe upon and disrupt various social relationships through the use of information and telecommunication technologies, information and telecommunication systems, and the corresponding cyberspace they engender.

Several criteria have been established for categorizing criminal offenses within cyberspace: based on the general target, the quantity of infringements, the direction, the intent behind the use of information and communication technologies, systems, and networks, and in accordance with the types of criminal offenses defined in the «Convention on Cybercrime».

It has been emphasized that criminal acts occurring in cyberspace represent a socially perilous and illicit phenomenon that jeopardizes not only national interests but also international ones. Addressing these offenses is a fundamental objective of law enforcement agencies at both national and international levels.

The distinction is made between criminal offenses committed in cyberspace and those in the realm of digital information circulation and the functioning of

information and communication technologies. The former are labeled as cyber-dependent offenses, where digital information in the realm of digital technologies, information, and telecommunication systems and networks is the primary subject of such offenses. The latter are designated as cyber-formative criminal offenses, representing conventional criminal offenses that have transitioned into cyberspace through the use of information and communication technologies.

The existing criminal legislation is criticized for its failure to align with current scientific and technological advancements. Specifically, the suggestion is made to replace the term «electronic computing machines» with «digital devices», encompassing a broader array of information and communication technologies. Additionally, it is proposed to collectively regard information (automated), electronic communication, information and communication systems, and electronic communication networks as information and communication technologies, systems, and networks.

Attention is drawn to the necessity of introducing legislation for the concept of «unauthorized interference», which encompasses gaining access to and/or using digital information by infiltrating information and communication systems and networks using specialized technical means and/or software, without the lawful right to access or manipulate such data. The author presents a typology of harmful technical means based on their creation process: 1) specific harmful technical means crafted for the commission of particular criminal offense categories, unsuitable for other purposes; 2) conventional technical means adapted for criminal offenses; 3) conventional technical means with potential for criminal usage.

The prevalent understanding of fraudulent activities involving information and communication technologies is linked to «phishing». However, it is argued that «phishing» cannot be classified under the specified Article 190 of the Criminal Code of Ukraine. Instead, it is suggested that «phishing» should fall under Part 3 of Article 361 of the Special Part of the Criminal Code due to its distinct subject matter, namely digital information. In the case of «phishing», deception serves merely as a method for acquiring personal data in the form of digital information.

The primary methods for legitimizing criminally obtained assets in cyberspace are outlined: 1) using existing internet infrastructure (marketplaces, classifieds, social networks, internet auctions, crowdfunding); 2) establishing new web infrastructure (online stores); 3) using exchanges and digital currency for asset laundering; 4) employing virtual assets for laundering obtained property.

The principal attributes of virtual assets are outlined and defined as follows: 1) decentralization; 2) transnational nature; 3) confidentiality of transactions; 4) digitization; 5) property essence; 6) anonymity. The concept of a "virtual asset" is elucidated, referring to digital currency without a physical form, whose creation and control hinge on cryptographic techniques. It operates on a fully decentralized basis, ensuring accurate system operations and precluding the capacity to manipulate transactions by participants in the cryptographic system.

A summary and categorization of foreign practices concerning the legal

regulation of virtual assets are provided. Drawing from these practices and considering the distinct attributes of virtual assets, it is emphasized that virtual assets should be viewed through three dimensions: 1) as information; 2) as currency; 3) as another intangible asset. Presently, virtual assets can only serve as an element of digital information in terms of criminal offenses under Ukrainian legislation. Thereby, it is proposed to broaden the scope of theft to encompass digital information products.

Attention is directed towards the nature of cyber-dependent criminal offenses, characterized by the execution of multiple socially perilous actions, as outlined in the Special Part of the Criminal Code of Ukraine, to achieve a single criminal outcome, leading to the imposition of penalties for an ensemble of criminal acts.

The primary aggravating factors for criminal offenses committed in cyberspace are identified and evaluated, considering the distinct characteristics of such socially perilous activities. It is stressed that an additional aggravating circumstance should be introduced, encompassing: 1) causing damage to an information and communication technology, system, or network of state significance, exhibiting signs of critical infrastructure; 2) employing digital information characterized as a state secret in the commission of the criminal offense.

Despite the adoption of cyber security strategies in the legislation of numerous states, and the identification of key cyber threats, the global recognition of cyber attacks as acts of aggression remains unsettled. This uncertainty jeopardizes the potential for international legal protection against cyber attacks by other states or individuals with the involvement of specific states.

The predominant focus of international normative acts centers on the modes of committing socially perilous acts in cyberspace. The foreign practices in legal regulations pertaining to liability for committing criminal offenses through the utilization of information and communication technologies are summarized and categorized. Countries belonging to the Anglo-Saxon legal tradition widely employ both normative regulations and a system of legal precedents. In contrast, the establishment of criminal liability for offenses in cyberspace is primarily relegated to separate normative enactments. The United States, for instance, applies both general and state-specific regulations. In the Romano-Germanic legal tradition, countries display unified regulations for criminal liability concerning offenses in cyberspace. However, even within this legal framework, substantial differences exist among these countries. For instance, countries in Western and Central Europe do not isolate offenses in cyberspace into a distinct section, incorporating their liability into various sections of their Criminal Codes. Conversely, Northern European countries segregate criminal liability for socially perilous actions using information and communication technologies, systems, and networks into a separate section.

Keywords: *criminal offenses in cyberspace, cyberspace, information and telecommunication technologies, virtual space, Internet network, cybercrimes, computer criminal offenses, digital information, malicious software.*