Міністерство освіти і науки України
Сумський державний університет

Думчиков М. О.

КОНЦЕПТУАЛЬНІ ЗАСАДИ КРИМІНАЛЬНО-ПРАВОВОЇ ОХОРОНИ КІБЕРПРОСТОРУ В УКРАЇНІ

Монографія

Рекомендовано вченою радою Сумського державного університету

Суми
Сумський державний університет
2023

УДК 343.7
Д 82

Рецензенти:

А. М. Куліш – заслужений юрист України, доктор юридичних наук, професор, директор Навчально-наукового інституту права Сумського державного університету;
В. В. Шаблистий – доктор юридичних наук, професор, професор кафедри кримінального права та кримінології факультету підготовки фахівців для органів досудового розслідування Дніпропетровського державного університету внутрішніх справ;
А. М. Клочко – доктор юридичних наук, професор, професор кафедри міжнародного права Сумського національного аграрного університету

Рекомендовано до видання
вченою радою Сумського державного університету
як монографія
(протокол № 11 від 13 квітня 2023 року)

Думчиков М. О.

Д 82 Концептуальні засади кримінально-правової охорони кіберпростору в Україні : монографія / М. О. Думчиков. – Суми : Сумський державний університет, 2023. – 413 с.

ISBN 978-966-657-945-7

У монографії досліджено питання сутності й різновидів кримінальних правопорушень у кіберпросторі та запропоновано науково й теоретично обгрунтовані підходи до вдосконалення кримінального законодавства щодо встановлення кримінальної відповідальності за кримінальні правопорушення в кіберпросторі. Особливу увагу приділено кваліфікації кримінальних правопорушень, передбачених XVI розділом Особливої частини Кримінального кодексу України. Типологізовано кримінальні правопорушення в кіберпросторі. Акцентовано увагу на аналізі міжнародних конвенцій, що визначають відповідальність за суспільно небезпечні діяння, вчинені в кіберпросторі, та проаналізовано стан імплементації норм Конвенції «Про кіберзлочинність» у національне законодавство України.

Для науковців, науково-педагогічних працівників, здобувачів юридичних спеціальностей закладів вищої освіти, працівників правоохоронних органів, уповноважених кваліфікувати кримінальні правопорушення в кіберпросторі, та всіх тих, хто цікавиться проблемами кримінально-правової охорони кіберпростору.

УДК 343.7

ISBN 978-966-657-945-7

ЗМІСТ

С.

ПЕРЕДМОВА

Активне застосування інформаційно-телекомунікаційних технологій в усіх сферах життєдіяльності людини – це невід'ємна частина сучасності.

Цифровізація різноманітних процесів діяльності суспільства є каталізатором вчинення суспільно небезпечних діянь дистанційно й уникнення відповідальності. Викрадення інформації, створення нових схем із легалізації злочинних доходів, зокрема з використання віртуальних активів, порушення приватного життя несанкціонованим втручанням у цифрові пристрої стають нормою сьогодення.

Останніми роками з'явився феномен кібертероризму зі здатністю впливати на об'єкти життєзабезпечення та оборони держави, спричинивши колосальні людські жертви, і фактично набув практичного значення. Президент України Володимир Зеленський у своєму виступі зазначив: «Ця війна стала першою у світі, де кіберпростір перетворився на повноцінну арену бойових дій – таку саму, як на суходолі, в повітрі чи морі. Ворог цинічно використовує кібератаки, як і кулі та ракети, для втілення своїх злочинних планів. Російський агресор посилив кібератаки на сайти державних органів влади й важливі інфраструктурні об'єкти». Крім того, в Стратегії національної безпеки визначено одним з основних пріоритетів посилення спроможностей національної системи кібербезпеки для ефективної протидії кіберзагрозам у сучасному безпековому середовищі. У 2021 році було ухвалено Стратегію кібербезпеки, у якій було визначено основні засади розбудови безпеки держави в кіберпросторі та конкретизовано основні загрози.

Незважаючи на збройну агресію Російської Федерації, спрямованість кримінальних правопорушень у кіберпросторі не обмежується об'єктами державної цифрової інфраструктури.

Кримінальні правопорушення в кіберпросторі різноманітні, а їх види породжені розвитком науки й техніки, а також винахідливістю осіб, які їх вчиняють. На нашу думку, не допустити негативних наслідків диджиталізації суспільства одночасно з діяльністю щодо регулювання процесів цифровізації є одним з основних завдань нашої держави в цьому столітті.

Незважаючи на той факт, що питання відповідальності за кримінальні правопорушення, вчинені в кіберпросторі, вже декілька років розробляють як у нашій державі, так і в низці зарубіжних країн, питання якісної протидії такому негативному явищу залишається відкритим. Суспільна небезпечність зазначених кримінальних правопорушень обумовлена багатьма факторами, серед яких основними, на нашу думку, є транснаціональність, латентність і власне масштаби таких суспільно небезпечних діянь. Згідно з даними офісу Генерального прокурора України в період із 2015 до 2020 року було обліковано приблизно 10 256 кримінальних правопорушень, передбачених XVI розділом Особливої частини Кримінального кодексу України. За цей самий період винесено всього 162 обвинувальні вироки суду.

Вищезазначене свідчить про необхідність та актуальність комплексного вивчення поняття й видів кримінальних правопорушень у кіберпросторі.

РОЗДІЛ 1.
ІСТОРИЧНІ ТА ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ У КІБЕРПРОСТОРІ

1.1. Становлення та генеза кримінальної відповідальності за кримінальні правопорушення в кіберпросторі на теренах України

Характеризуючи генезу кримінальної відповідальності за правопорушення в кіберпросторі, доцільно почати з ретроспективного розвитку злочинності як явища. Варто зазначити, що більшість кримінально-протиправних діянь виникла досить давно й із часом просто набула нових рис, способів учинення, з'явилися нові знаряддя й засоби їх вчинення. Проте кримінальні правопорушення в кіберпросторі є цілком новим видом протиправних діянь. Зокрема, на відміну від традиційних видів кримінальних правопорушень, історія яких охоплює століття, явище кримінальних правопорушень у кіберпросторі є новим, адже виникло майже одночасно з появою мережі Інтернет.

Перші згадки про кримінальні правопорушення в кіберпросторі припадають на початок 1970-х років, такі кримінальні правопорушення тоді називали «хакерами». Складно конкретизувати, хто конкретно вчинив перше кримінальне правопорушення в кіберпросторі, але в більшості джерел, що спеціалізуються на захисті інформаційних технологій, визначають Д. Дрейпера, якого вважають першою професійною особою, яка вчинила правопорушення в кіберпросторі. Основним родом занять Д. Дрейпера був фрикінг. Тобто від появи фрикінгу бере свій початок розвиток кримінальних правопорушень у кіберпросторі, а сам фрикінг визначається як певний набір технологій, що дає змогу проникнути у

вуличні телефони з подальшим одержанням доступу до управління телефонними мережами за допомогою навичок соціальної інженерії [1].

Зазвичай фрикінг здійснюється для безкоштовних дзвінків, поповнення особистого мобільного рахунку. Водночас фрикінгом займалися й такі визначні постаті, як Стів Джобс та Стів Возняк, які пізніше заснували компанію «Apple Computers» [2].

В інших джерелах зародження фрикінгу, а отже, феномену кримінальних правопорушень у кіберпросторі, пов'язують із Д. Енгрессі, який почав дуже точно відтворювати звукові сигнали телефонної лінії за допомогою звичайного свисту. Він поєднував цю навичку з умілим маніпулюванням технічним персоналом, який обслуговував лінію, але не зміг використати телефонні мережі, щоб здійснювати безкоштовні дзвінки по всьому світу. Спочатку фрикінг потрапив у спільноту неповнолітніх хакерів, потім його почали застосовувати молоді техніки, які використовували саморобні електронні схеми для генерування телефонних сигналів [3].

Отже, початок 70-х років XX ст. можна назвати певною відправною точкою в історії кримінальних правопорушень у кіберпросторі. З цього моменту почали активно розвиватися мережа Інтернет та інформаційні технології загалом, стаючи все більш доступними для широкого кола користувачів, а самі можливості в кіберпросторі постійно вдосконалювали, що, звісно, могло зацікавити осіб, які вчиняють кримінальні правопорушення в кіберпросторі.

У 1983 році було винесено перший вирок за кримінальне правопорушення, скоєне в інтернет-просторі. Неповнолітні особи з Мілуокі (Сполучених Штатів Америки) здійснили перше зафіксоване інтернет-проникнення. Ці підлітки зламали 60 комп'ютерів за дев'ять днів, зокрема комп'ютери в лабораторії штату Лос-Аламос. Для учасників цієї групи все закінчилося умовним терміном після того, як затриманий підліток дав

проти них свідчення. У 1984 році Ф. Коен опублікував інформацію про шкідливі комп'ютерні програми, здатні розмножуватися. Так увійшов в обіг термін «комп'ютерний вірус» [4].

У 1986 році Сполучені Штати Америки ухвалили перший закон про злочини у сфері інформаційних технологій – «Закон про комп'ютерне шахрайство та зловживання», що забороняв несанкціонований доступ до комп'ютерних систем та одержання секретної військової інформації. Крім того, цей закон захищав такі види інформації: 1) інформацію, що належить фінансовим установам, а саме: інформацію про кредитні картки й рахунки, дані, що належать державним установам; 2) інформацію від міжнародних та урядових організацій. Отже, це можна назвати першим заходом проти кримінальних правопорушень у кіберпросторі [5].

За цей час хакери вже виробили певну ідеологію й культуру. З'являється велика кількість злочинних угруповань, які діють винятково в кіберпросторі. У роботі хакерів усе частіше переважають не комерційні, а політичні мотиви. З розвитком технологій з'являються нові кримінальні правопорушення в кіберпросторі, після чого особи, які вчиняють кримінальні правопорушення в мережі, починають ділитися вміннями та навичками, навіть серед хакерів формується певна ієрархія, у якій активні як аматори, так і професіонали, що діють у міжнародному масштабі. В історії відома навіть випадкова конкуренція між групами осіб, які вчиняли кримінальні правопорушення в кіберпросторі [2].

Водночас кримінальні правопорушення в кіберпросторі перестають бути рідкісним явищем. Низка хакерів один за одним з'являється в основних засобах масової інформації. Усього за 15 років кримінальні правопорушення в кіберпросторі перестали бути унікальним явищем, але все ще залишаються незвичними, зокрема через їх масштаби та транснаціональну спрямованість.

Рівень суспільної небезпеки досліджуваних кримінальних правопорушень почав зростати одночасно з кількістю вчинюваних кримінальних правопорушень у кіберпросторі. Одним із прикладів можна виділити випадок, коли малолітня особа дванадцяти років одержала доступ до комп'ютеризованої системи контролю води на греблі Теодора Рузвельта в Арізоні. Це дало їй змогу вільно відкрити шлюзи й затопити все місто Темпе, населення якого на той час становило близько одного мільйона жителів. Сам факт такого злому пізніше сприяв появі термінів «інтернет-тероризм», «комп'ютерний тероризм», «кібертероризм» [6].

Наприкінці XX століття кібератаки все більше набували масовості й транснаціонального характеру.

Масовий характер кримінальних правопорушень у кіберпросторі супроводжувався розвитком інформаційних технологій державних структур, що здійснювали свою діяльність. Одним із напрямком такої діяльності був кібернетичний простір. Зокрема, створювали різноманітні державні сайти та сервіси, що були розпорядниками великого обсягу інформації та мали доступ до інтерент-мережі, вебресурси з новинами, вебресурси національних закладів освіти й міжнародні сервіси онлайн-торгівлі. Велика кількість і різноманітність вебресурсів у мережі Інтернет породила нові види кримінальних правопорушень у кіберпросторі й привернула увагу зловмисників у цій сфері, породивши цим так званий хактивізм. Зазначимо, що хактивізм проявлявся у двох основних напрямках діяльності: розповсюдженні інформації шляхом її незаконного поширення на різних вебресурсах у мережі Інтернет і перешкоджанні роботі таких ресурсів загалом [7].

Наприклад, перша така акція для протесту проти політики французького уряду була вчинена 21 грудня 1995 року групою «Strano Network». Ці активісти кілька годин атакували сайти урядових агентств. Сутність цієї атаки полягала в тому, що велика кількість людей із різних

частин світу одночасно підключалася до одного із сайтів, унаслідок чого система перевантажувалася. Таким чином було виведено з ладу відразу кілька сайтів. Шляхом завдання різних збитків планувалося привернути увагу до позиції противників такої політики уряду [8].

Прикладом незаконного поширення інформації може бути перша інтернет-війна, пов'язана з конфліктом у Косово. Різні групи хактивістів, використовуючи Інтернет, порушували роботу урядових комп'ютерів і здобували контроль над різними сайтами з метою заміни розміщеної на них інформації, тобто встановлювали «дефейс». Усі ці дії були спрямовані на засудження військових дій Югославії й НАТО. Крім того, також законними шляхами було поширено багато інформації щодо небезпеки війни. Такі акції мали багато суспільно-політичних наслідків [9].

Проте не всі хакери керуються політичними ідеями, дуже велика кількість має саме комерційні інтереси у своїй діяльності. Зокрема, у 1994 році на весь світ стала відома «справа Володимира Леонідовича Левіна». Група з 12 осіб намагалася за допомогою Інтернету через нелегальний доступ до мережі «Спринт / Теленет» здійснити 40 грошових переказів на суму більше ніж 10 мільйонів доларів із чужих банківських рахунків по всьому світу. Міжнародна кримінальна поліція визнала ці дії «транснаціональним мережевим комп'ютерним кримінальним правопорушенням». Крім того, це було перше велике фінансове кримінальне правопорушення, вчинене за допомогою Інтернету [2].

Отже, до початку XXI століття сформувалися всі основні тенденції, напрямки та форми діяльності кримінальних правопорушень у кіберпросторі. З часу ухвалення першого комп'ютерного закону нормативна база всіх країн світу з цього питання значно розширилася.

Варто виділити етапи розвитку світової кіберзлочинності: 1) вчинення першого кримінального правопорушення в кіберпросторі й власне поява кібернетичних правопорушень; 2) розвиток

кримінально-протиправної діяльності в кіберпросторі та поява субкультури хактивізму; 3) набуття кримінальною-протиправною діяльністю в кіберпросторі транснаціонального й дистанційного характеру; 4) поява нових видів кримінальних правопорушень у кіберпросторі (кардингу, кібертероризму, кібервійни, фішингу тощо).

Сучасні кримінальні правопорушення в кіберпросторі відрізняються від тих, що були в минулому столітті, лише своїми масштабами та наслідками. Варто виділити той факт, що технологічні інновації лише допомагають знаходити нові способи вчинення вже відомих традиційних кримінальних правопорушень.

Також необхідно зазначити, що методи боротьби з кримінальними правопорушеннями в кіберпросторі постійно розвиваються й приносять позитивні результати, і з часом цей простір поступово стає більш урегульованим та безпечним. Хоча кримінально-протиправна діяльність у кіберпросторі як кримінальна категорія також продовжує активно розвиватися й «множиться», і процес цей неймовірно швидкий, адже відбувається в міжнародних масштабах, загальна статистика з цього питання залишається невтішною.

Зараз жертвами зловмисників, які діють у віртуальному просторі (кіберсередовищі), можуть стати не лише окремі громадяни, а й цілі держави. Водночас безпека десятків тисяч користувачів може залежати лише від кількох зловмисників. Примітно, що кількість кримінальних правопорушень у кіберпросторі зростає пропорційно кількості користувачів Інтернету та кількості телекомунікаційних систем.

Наразі кіберзлочинність є, напевно, однією з найбільших глобальних загроз як для України, так і для всього світу. За даними всесвітнього огляду економічних кримінальних правопорушень Pricewater house Coopers (PWC) за 2021 рік, кримінальні правопорушення в кіберпрострі показали найвищий рівень за весь період публікаційних оглядів. Зокрема, рівень

злочинності збільшився з 24 % у 2014 році до 39 % у 2021 році, посівши друге місце серед економічних кримінальних правопорушень у світі й залишивши позаду кримінальні правопорушення, пов'язані з легалізацією грошових коштів, отриманих незаконним шляхом, та різні корупційні кримінальні правопорушення [10].

Статистика свідчить про щорічне зростання кількості кримінальних правопорушень у кіберпросторі. Наприклад, в Україні в 2009 році було офіційно зареєстровано 217 кіберзлочинів, у 2017 році цифра збільшилася до 598, а в 2020 році їх кількість уже становила 1 885. Важливо, що це лише статистика щодо зафіксованих кримінальних правопорушень у кіберпросторі, а об'єктивно оцінюючи ситуацію, можна впевнено стверджувати, що їх значно більше [11].

Станом на 2022 рік майже з будь-якої точки світу будь-хто має доступ до «Даркнету» – окремої мережі в Інтернеті, що згідно з різними даними стала місцем опосередкування осіб, які вчиняють кримінальні правопорушення в кіберпросторі. Саме в цій частині Інтернету відбувається велика кількість правопорушень, у ній є торгові платформи з нелегальними товарами й послугами, з протиправними намірами створюють закриті канали зв'язку, а велика кількість користувачів завдяки використанню спеціальних засобів є анонімами. Найбільша проблема полягає саме в доступності такої мережі, що часто сприяє поширенню кіберзлочинності [12].

Проте зазначена статистика не повністю відповідає дійсності, адже кримінальні правопорушення в кіберпросторі є одними з найлатентніших видів кримінальних правопорушень, а отже, реальна картина й статистичні дані значно більші. Передусім це зумовлено відсутністю чітких методів і прийомів збирання даних про вчинення власне кримінальних правопорушень у кіберпросторі та їх специфікою.

Перше кримінальне правопорушення, здійснене з використанням комп'ютера в колишньому Союзі Радянських Соціалістичних Республік, було зареєстроване в 1979 році у Вільнюсі. Ним стало розкрадання, збитки від якого становили 78 584 карбованців. Цей факт був занесений у міжнародний реєстр подібних правопорушень і став своєрідним початком розвитку нового виду кримінальних правопорушень у колишньому СРСР.

Проаналізувавши наукові джерела, ми пропонуємо власний авторський підхід ретроспективного розвитку кримінальної відповідальності за правопорушення в кіберпросторі на теренах України. На нашу думку, варто виділити п'ять етапів:

1) початковий (1991–2001 рр.);

2) зародження (2001–2005 рр.);

3) імплементаційний (2005–2009 рр.);

4) економічний (2009–2015 рр.);

5) нормотворчий (2015–2020 рр.);

6) сучасний (2020 р. – сьогодні).

Пропонуємо почати з першого етапу становлення й генези кримінальної відповідальності на теренах України, визначений нами як початковий, основний період якого припав на початок незалежності України. Парадокс розвитку людства полягає в тому, що впродовж усього етапу еволюції людина використовувала, накопичувала, передавала інформацію. Безперервний процес інформатизації суспільства охоплює всі сфери діяльності людини й держави: від вирішення проблем національної безпеки, охорони здоров'я та управління транспортом до освіти, фінансів і навіть просто міжособистісного спілкування. З розвитком технологій електронних платежів, «безпаперового» документообігу, серйозний збій локальних мереж може паралізувати роботу цілих корпорацій та банків, призвівши до значних матеріальних збитків [13, с. 34].

Зазначений період характеризується правовим вакуумом у регулюванні відносин у кіберпросторі як загалом, так і в рамках правової охорони кіберпростору зокрема. Технологічна складова як одна з основних ознак кримінальних правопорушень у кіберпросторі фактично відсутня, феномен соціальної інженерії лише починає свій розвиток, а самі кримінальні правопорушення в кіберпросторі є фактично безкарними внаслідок наявності в Кримінальному кодексі України складу кримінального правопорушення за зазначені діяння. Якщо в 2000 році «фактів, де комп'ютерна техніка виступала як об'єкт скоєння кримінального правопорушення, зокрема фактів несанкціонованого проникнення до локальних відомчих комп'ютерних мереж та банків зареєстровано не було», то вже в 2001 році відповідно до статистики Міністерства Внутрішніх Справ України було зареєстровано п'ять таких кримінальних правопорушень. Крім того, якщо кримінальних правопорушень у кіберпросторі в їх класичному вигляді до 2001 року фактично не було, то різні шахрайства в мережах електрозв'язку стають відправною точкою історії кримінальних правопорушень у кіберпросторі на теренах нашої держави.

Основною характеристикою другого етапу, який припадає на 2001 рік, є набрання чинності Кримінальним кодексом України 5 квітня 2001 року. Водночас спостерігається перша спроба врегулювання кримінальних правопорушень у кіберпросторі в законодавстві. Зокрема, в XVI розділі Особливої частини кримінального кодексу України визначено «Злочини у сфері використання електронно-обчислювальних машин, систем та комп'ютерних мереж». Виділено три види кримінальних правопорушень у кіберпросторі: 1) незаконне втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж (стаття 361 Кримінального кодексу України); 2) викрадення, привласнення, вимагання комп'ютерної інформації або

заволодіння нею шляхом шахрайства чи зловживання службовим становищем (стаття 362 Кримінального кодексу України);
3) порушення правил експлуатації автоматизованих електронно-обчислювальних систем (стаття 363 Кримінального кодексу України) [14].

Крім Кримінального кодексу України, питання забезпечення охорони кіберпростору розглянуто в Законі України «Про інформацію», але в ньому не була визначена безпекова інформаційна політика держави.

Варто зауважити, що на цьому етапі законодавство не визначає поняття ані кримінального правопорушення в кіберпросторі, ані кіберпростору. Водночас певні науковці трактують доктринальне поняття кримінального правопорушення, вчиненого у кіберпросторі. Зокрема, Ю. Батурін [16, с. 160] вважає, що кримінальне правопорушення в кіберпросторі – це правопорушення, предметом якого є комп'ютер. Зауважимо, що ми не підтримуємо бачення науковця щодо цієї позиції, насамперед через те, що основним предметом кримінальних правопорушень у кіберпросторі є суспільні відносини у сфері цифрової інформації, а комп'ютер може бути предметом таких кримінальних правопорушень лише в складі, передбаченому статтею 363-1 Особливої частини Кримінального кодексу України. П. Біленчук визначає кримінальне правопорушення в кіберпросторі як суспільно небезпечне діяння, здійснюване з використанням сучасних технологій і засобів комп'ютерної техніки, з метою завдання шкоди майновим або суспільним інтересам держави, підприємств, відомств, організацій, кооперативів, громадським організаціям і громадянам, а також правам особи [15].

Крім того, в частині 4 статті 190 Кримінального кодексу України визначено покарання за шахрайство, вчинене за допомогою електронно-обчислюваної техніки. Судова практика розгляду справ про кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), автоматизованих систем і

комп’ютерних мереж та мереж електрозв’язку трактувала електронно-обчислювальну техніку як комплекс електронних технічних засобів, побудованих на основі мікропроцесорів і призначених для автоматичного оброблення інформації під час виконання обчислювальних та інформаційних завдань [17].

У цей період кібершахраї активно використовували у своїй кримінально-протиправній діяльності MIRC – безкоштовний IRC-клієнт для Microsoft Windows. MIRC являла собою певну соціальну мережу у вигляді чатів і груп. Саме за допомогою неї були зафіксовані перші випадки шахрайства в кіберпросторі, але через брак спеціальних знань в органів внутрішніх справ такі посягання залишалися не викритими. Також через MIRC активно розвивалася сфера інтернет-продажу заборонених наркотичних речовин, адже така торгівля була цілком анонімною.

Аналізуючи третій етап, варто наголосити, що Держави – члени Ради Європи, усвідомлюючи зміни, спричинені цифровою трансформацією, динамічний розвиток комп’ютерних мереж загалом і мережі Інтернет зокрема, стурбовані ризиком, що діяльність у кіберпросторі можуть використовувати для здійснення кримінальних правопорушень, 23 листопада 2001 підписали Конвенцію про кіберзлочинність.

У конвенції визначено необхідність співпраці між Державними й приватними підприємствами для боротьби з кримінальними правопорушеннями в кіберпросторі, а також способи захисту інформаційних і цифрових технологій. Наголошено на більш ефективному й швидкому співробітництві в кримінальних питаннях.

Основною ціллю Конвенції члени Ради Європи вбачали: 1) зупинення кримінально противоправних дій, спрямованих проти цілісності, конфіденційності й доступності комп’ютерних технологій, комп’ютерних мереж і комп’ютерних даних; 2) попередження зловживання комп’ютерними системами, комп’ютерними даними й комп’ютерною

мережею; 3) установлення кримінальної відповідальності за порушення за кримінально противоправні дії в кіберпросторі; 4) надання повноважень спеціалізованим правоохоронним органам для ефективної боротьби з кримінальними правопорушеннями в кіберпросторі; 5) ефективну міжнародну співпрацю та міжнародне співробітництво у сфері забезпечення охорони кіберпростору.

У 2005 році Україна ратифікувала Конвенцію про кіберзлочинність, але навіть у ній не було визначено поняття кримінального правопорушення в кіберпросторі та власне поняття кіберпростору. У Конвенції виділено такі види кримінальних правопорушень у кіберпросторі: 1) правопорушення проти конфіденційності; 2) правопорушення, пов'язані з комп'ютером; 3) правопорушення, пов'язані зі змістом; 4) порушення, пов'язані з порушенням авторських та суміжних прав [18].

Зокрема, правопорушення проти конфіденційності охоплювали: незаконний доступ, нелегальне перехоплення, втручання в дані, втручання в систему й зловживання пристроями. Фактично правопорушення проти конфіденційності, закріплені в Конвенції, відображено в главі XVI Особливої частини Кримінального кодексу України. До таких кримінальних правопорушень належали різні проникнення в комп'ютерну або телекомунікаційну мережу, протизаконне перенаправлення інтернет-трафіку, створення, використання й розповсюдження шкідливого програмного забезпечення, збут інформації з обмеженим доступом і несанкціоновані дії з інформацією, що зберігається в ЕОМ.

Правопорушення, пов'язані з комп'ютером, поділено на підробку, пов'язану з комп'ютером, та шахрайство, пов'язане з комп'ютером. Такі правопорушення відображено в Кримінальному кодексі України в статтях 200, 358 та 190. Зокрема, до них належать будь-які види віртуального шахрайства, «скам», «фішинг», підробка електронних

документів для отримання кредитів, підробка документів для відкриття рахунків в електронних платіжних система тощо.

Стаття 9 Конвенції про кіберзлочинність визначає як правопорушення вироблення, пропонування, розповсюдження, здобуття й володіння дитячою порнографією. Зокрема, стаття 301 Конвенції про кіберзлочинність установлює відповідальність за одержання доступу до дитячої порнографії, її придбання, зберігання, увезення, перевезення чи інше переміщення, виготовлення, збут і розповсюдження. Так само зазначено, що одержання доступу до дитячої порнографії з використанням інформаційно-телекомунікаційних систем або технологій варто вважати умисним, якщо доведено, що особа усвідомлювала, що в такий спосіб вона одержить доступ до дитячої порнографії [14].

Водночас перелік кримінальних правопорушень, передбачених XVI розділом Особливої частини Кримінального кодексу України, розширено й змінено назву розділу. Зокрема, до кримінальних правопорушень у сфері використання електронно-обчислюваних машин, систем та комп'ютерних мереж і мереж електрозв'язку належать такі:

1) несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку. Ця стаття передбачає втручання, що призвело до витоку, втрати, підробки, блокування інформації, спотворення процесу її оброблення або порушення її маршрутизації (стаття 361 Кримінального кодексу України);

2) створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут. Кримінальні правопорушення, передбачені цією статтею, стосуються нелегальних дій, пов'язаних зі шкідливими програмами або технічними засобами. Щодо шкідливих програм – це комп'ютерні віруси (стаття 362^1 Кримінального кодексу України);

3) несанкціонований збут або розповсюдження інформації з обмеженим доступом, що зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації. Зазначені несанкціоновані дії з інформацією передбачають, що вони вчинені особою, яка не мала на це права, а також що доступ до неї одержано нелегальним шляхом (стаття 361^2 Кримінального кодексу України);

4) несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї (стаття 362 Кримінального кодексу України). Ця стаття є дуже неоднозначною, адже передбачає значну кількість можливих дій і наслідків, а особливо велике значення має форма вини;

5) порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється (стаття 363 Кримінального кодексу України). Ця стаття передбачає дії, пов'язані з нелегальним використанням комп'ютерної електроніки, систем та мереж;

6) перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку (стаття 363^1). Як і в статті 363, усі дії пов'язані з порушенням правил експлуатації, але стаття 363-1 окремо виділяє конкретні дії, спрямовані на перешкоджання функціонуванню інших комп'ютерних приладів, їх систем і мереж.

Статтею 176 Кримінального кодексу України встановлено відповідальність за порушення авторського права та суміжних прав.

Аналогічну статтю містить «Конвенція про кіберзлочинність», проте основною відмінністю є використання комп'ютера як предмета кримінального правопорушення.

Головною ознакою третього етапу є фактичне розширення переліку кримінальних правопорушень, що вчиняють у кіберпросторі, але водночас спостерігається реальна неврегульованість як кіберпростору загалом, так і окремих видів кримінальних правопорушень у ньому. Велику кількість кримінальних правопорушень, передбачених Кримінальним кодексом України, що фактично вчиняють у кіберпросторі, кваліфікують без зазначення конкретного знаряддя, виду вчинення й предмета кримінального правопорушення. На нашу думку, під час кваліфікації кримінальних правопорушень, вчинених у кіберпросторі, необхідно акцентувати увагу на визначенні наведених факультативних ознак.

Розглядаючи четвертий етап, який припадає на 2009–2015 роки, варто наголосити, що в цей період спостерігалася динаміка збільшення економічних кримінальних правопорушень у кіберпросторі. Поява криптовалютних активів, динамічний розвиток електронних платіжних систем, соціальних мереж, систем електронної комерції поставили нові виклики перед охороною кіберпростору. Якщо попереднім етапам було властиве вчинення кримінальних правопорушень, пов'язаних із проникненням у системи ЕОМ і телекомунікаційні системи, а також створенням, розповсюдженням та збутом шкідливого програмного забезпечення, то третій етап характеризується кримінальними правопорушеннями економічного спрямування.

Аналізуючи кримінальні правопорушення в кіберпросторі в контексті тіньової економіки, надзвичайно складно переоцінити їх значення у фінансовій системі. Економічний аспект кримінальних правопорушень у кіберпросторі стосується не лише фінансових збитків, завданих ними, а й мотивів і причин таких правопорушень. Ураховуючи той факт, що певні

кримінальні правопорушеня в кіберпросторі мають безпосередньо та опосередковано економічний характер, їх значна кількість спрямована на отримання неправомірного прибутку шляхом викрадення грошових коштів або інформаційних даних фінансового характеру з метою їх продажу. Інші кримінальні правопорушення, що вчиняють з економічних і комерційних мотивів, стосуються надання неправомірних послуг, пов'язаних із кіберпростором, наприклад налагодження нелегальних фінансових структур в інтернет-мережі та псування серверів конкурентів за допомогою DDos-атак.

У цей період кіберзлочинність відіграє досить впливову роль у тіньовій економіці й стає одним із найнебезпечніших суспільно-економічних явищ глобального характеру. Кіберпростір перетворюється на одну з головних ланок в усій системі тіньової економіки, як наслідок – можливість анонімно здійснювати різноманітні операції економічного характеру, що не можуть бути контрольовані державою. Поступово інтернет-мережа починає бути каналом фінансування тероризму [19].

Кіберпростір дає змогу не лише отримувати прибуток, а й відмивати фінанси, отримуючи на виході «чистий» прибуток із мережі. Способів відмивання (легалізації) грошей за допомогою Інтернету дуже багато, з цією метою створюють різні проєкти, онлайн-фонди, інтернет-компанії та інші мережеві фінансові структури, через які проводять незаконні кошти, тим самим перетворюючи їх на легальний прибуток [20].

Стають популярними такі кримінальні правопорушення, як кардинг, скамінг, фішинг і чорний рефаундинг. Кардинг – це використання в операціях реквізитів платіжних карт, одержаних зі зламаних серверів інтернет-магазинів, платіжних і розрахункових систем, а також із персональних комп'ютерів (безпосередньо або через програми віддаленого доступу, «трояни», «боти») [21, с. 75].

Фішинг (англ. phishing) – це вид шахрайства, метою якого є отримання конфіденційної інформації довірливих чи неуважних користувачів мережі персональних даних клієнтів онлайнових аукціонів, сервісів із переказу або обміну валюти, інтернет-магазинів тощо [22].

Скамінг – це різновид шахрайства, здійснюваний переважно в онлайн-середовищі, що полягає в розсиланні через імейл-адреси й соціальні мережі повідомлень із заздалегідь неправдивою інформацією. Наприклад, одержувачеві листа повідомляють, що він став переможцем лотереї і для отримання виграшу йому необхідно переказати невелику суму на зазначений рахунок. Також часто користувачам пропонують інвестувати в офшорні підприємства й нерухомість.

Чорний рефаундинг – це система повернення частини або повної суми коштів продавцем покупцеві, якщо той незадоволений якістю товару та надав докази його браку.

Упродовж розвитку для запобігання шахрайству платіжні картки набувають усе більшого рівня захисту. Але коли створюють нові види захисту, з'являються й нові схеми їх обходу. За даними VISA CEMEA, найпопулярнішими видами шахрайства з кредитними картками є використання викрадених карток (35 % від загальної кількості таких шахрайств), використання підробленої картки (30 %), використання реквізитів картки (28 %), інші види шахрайств (7 %).

Щодо вітчизняного досвіду, то можна навести такий приклад. У 2010 році співробітники Міністерства внутрішніх справ затримали групу білорусів, які викрадали гроші з іноземних карткових рахунків. Для переведення в готівку вони купували через Інтернет дорогі турпутівки в країни Азії та інші країни й перепродавали їх за півціни. У 2012 році більшість зловмисників відпустили, оскільки вони відшкодували збитки розміром понад 330 тис. доларів [23].

П’ятий етап характеризується чотирма визначальними факторами: створенням спеціалізованого правоохоронного органу – Департаменту кіберполіції Національної поліції України 5 жовтня 2015 року; ухваленням Закону України «Про основні засади забезпечення кібербезпеки України»; ухваленням рішення «Про Стратегію кібербезпеки України»; стрімким розвитком криптоактивів.

Законом України «Про основні засади забезпечення кібербезпеки України» установлено основні поняття, такі як кіберпростір, кібербезпека, кіберзлочин, кібератака, кіберзагроза та ін. Зокрема, під кіберпростором варто розуміти середовище (віртуальний простір), що надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з’єднаних) комунікаційних систем і забезпечення електронних комунікацій із використанням мережі Інтернет та/або інших глобальних мереж передавання даних. Відповідно до законодавчого визначення кіберпростору можемо виділити певні характерні йому ознаки: 1) віртуальний характер; 2) є комунікативним середовищем; 3) утворюється за допомогою електронних комунікацій та мережі Інтернет [24].

Кримінальне правопорушення в кіберпросторі (комп’ютерне кримінальне правопорушення) законодавець визначає як суспільно небезпечне винне діяння в кіберпросторі та/або з його використанням, відповідальність за яке передбачена Законом України «Про кримінальну відповідальність» та/або яке визнано злочином міжнародними договорами України.

У Стратегії кібербезпеки України визначено національну систему кібербезпеки, що насамперед повинна забезпечити взаємодію з питань кібербезпеки державних органів, органів місцевого самоврядування, військових формувань, правоохоронних органів, наукових установ, навчальних закладів, громадських об’єднань, а також підприємств, установ

та організацій незалежно від форми власності, що провадять діяльність у сфері електронних комунікацій, захисту інформації та/або є власниками (розпорядниками) об'єктів критичної інформаційної інфраструктури. Водночас виділені основні суб'єкти забезпечення кібербезпеки в державі, зокрема такі: 1) Міністерство оборони України; 2) Державна служба спеціального зв'язку та захисту інформації України; 3) Служба безпеки України; 4) Національна поліція України; 5) Національний банк України; 6) Органи розвідки України.

У цей період криптовалюта стає особливо значущим і суміжним феноменом у рамках кіберпростору. Вона є різновидом електронних грошових коштів, алгоритм діяльності яких базується та функціонує на основі механізму асиметричного шифрування [25, с. 327].

Криптовалюта стає популярною і як засіб розрахунку, і як фінансовий інструмент, але має як багато переваг, так і багато недоліків.

Таблиця 1 – Переваги та недоліки криптовалюти

Перевага	**Недолік**
Простота користування гаманцем	Держави можуть заборонити криптоплатежі на своїй території (а певні вже заборонили: деякі райони Китаю, Ісландія, Тайланд, Киргизія, Болівія та ін.)
Доступність. Дає змогу добувати криптовалюту кожному	Невелика кількість магазинів і банків, що приймають до оплати цю валюту
Швидкість переказів	Неможливість відкликання транзакцій
Захищеність: криптовалюту неможливо скопіювати або підробити	Втрата даних до криптогаманця або його функціональна нездатність призводять до незворотної втрати всієї накопиченої валюти

Продовження таблиці 1

Перевага	**Недолік**
Децентралізований характер, відсутність єдиного цифрового банку	Ненадійність (криптовалюта може як упасти, так і піднятися в ціні за короткий період)
Анонімність – відсутність детальної інформації про власника криптогаманця	У разі неможливості регулювати, контролювати криптовалюту виникає загроза для економічного й фінансового життя держави та суспільства (через відсутність або недостатність відповідного законодавства, спеціалістів і технологій)
Поширеність (серед людей)	Використання для вчинення незаконних дій

Для осіб, які вчиняють кримінальні правопорушення в кіберпросторі, безсумнівною перевагою використання криптовалюти є можливість анонімного відкриття й поповнення електронних гаманців, а також цілодобова доступність і швидкісні проведення транзакцій (упродовж декількох секунд). Криптогаманець фізичної особи найчастіше має прив’язку до електронної пошти або номера мобільного телефону.

Отже, економічне значення кіберзлочинності, а також кіберпростору є дуже високим. Сукупність технічних, економічних та правових особливостей роблять Інтернет майже ідеальним місцем і фактично центром тіньової економіки всього світу.

Сучасний стан кримінально протиправних діянь у кіберпросторі характеризується високою динамікою росту, небезпечністю й збільшенням кількості осіб, які вчиняють кримінальні правопорушення, зокрема неповнолітніх. Стрімкий розвиток інтернет-суспільства, поява нових сервісів онлайн-платежів, перехід підприємств від традиційних способів

ведення бізнесу до електронної комерції, упровадження віртуальних валют у світову економіку шляхом їх законодавчого регулювання поставили перед світовою спільнотою нові виклики. Суспільство швидкими темпами трансформується в інформаційне. Така динаміка зумовлена багатьма факторами, передусім пандемією COVID – 19. Тоді, коли використання комп'ютерів, мобільних пристроїв, Інтернету для купівлі, спілкування, обміну інформацією пом'якшує соціальне дистанціювання, особи, які вчиняють кримінальні правопорушення в кіберпросторі, почали використовувати цю вразливість у своїх інтересах. Усе більше як державних, так і приватних послуг почали надавати онлайн, почало створюватися електронне державне урядування. Спостерігається поступове відтиснення традиційних банківських переказів електронними платіжними системами й віртуальними валютами.

Варто визначити основні причини виникнення та розвитку кримінальних правопорушень у кіберпросторі на цьому етапі.

1. Прибутковість кримінальних правопорушень, вчинених у кіберпросторі. Дохід варіюється залежно від масштабу схеми кримінального правопорушення. Кримінальні правопорушення в кіберпросторі вчиняють щохвилини, завдаючи величезних збитків як окремому громадянинові, так і державі загалом. У 2020 році міністр внутрішніх справ Арсен Аваков зазначив, що до 2021 року глобальні збитки від кримінальних правопорушень у кіберпросторі сягнуть майже 6 трлн доларів США на рік. У світі кількість кримінальних правопорушень у кіберпросторі зростає на 30–40 % на рік [26].

2. Простота вчинення кримінальних правопорушень. Безліч доступних форумів і чатів, на яких можна знайти способи й методи вчинення того чи іншого правопорушення: від «кардингу» до методів ведення інформаційної війни та кібертероризму .

3. Розвиток інформаційних технологій – одна з головних причин швидкого поширення кіберзлочинності в XXI ст. Цей чинник можна пояснити так: комп'ютерні технології відіграють велику роль у житті суспільства, тому для врегулювання таких відносини необхідна відповідна законодавча база.

4. Недостатнє розуміння на державному рівні й рівні суспільства можливої небезпеки та настання непередбачуваних наслідків злочинності в кіберпросторі.

Не можна не звернути уваги на фактори, що відіграють значну роль у розвитку й функціонуванні кримінальних правопорушень у кіберпросторі. Зокрема, соціальні мережі та Інтернет неоднозначно впливають на їх користувачів, оскільки вже зараз звичайний користувач може знайти багато інформації майже про кожну особу у відкритому доступі. Легкий доступ до інформації на форумах, що ведуть особи, які вчиняють кримінальні правопорушення в кіберпросторі, сприяє вчиненню останніх. Наприклад, такі форуми містять інформацію про поетапні дії для вчинення кримінальних правопорушень, а також заходи безпеки для осіб, які вчиняють кримінальні правопорушення в кіберпросторі.

Актуальні тренди сприяли появі нових видів кримінальних правопорушень у кіберпросторі та вдосконаленню вже наявних. Зокрема, такий вид кримінального правопорушення, як скамінг, набуває все більш масового характеру й становить 40 % від усіх кримінальних правопорушень у кіберпросторі, а самі кримінальні правопорушення в цій сфері стають усе латентнішими. Лише за 2018 рік працівники Департаменту кіберполіції були залучені до розслідування більше ніж 11 тисяч кримінальних проваджень.

Таблиця 2 – Статистика кримінальних правопорушень, вчинених у кіберпросторі, за даними Офісу Генерального прокурора:

Рік	**Кількість облікованих кримінальних правопорушеннь**	**Кількість осіб, яким вручено повідомлення про підозру**
2014	450	200
2015	600	267
2016	835	472
2017	2 573	1 272
2018	2 301	1 608
2019	2 204	1 481
2020	2 498	1 675
2021	2 790	2 031

Варто зауважити, що статистична інформація обмежена лише XVI розділом Особливої частини Кримінального кодексу України й не містить даних про інші «традиційні» види кримінальних правопорушень у кіберпросторі, наведених в інших розділах особливої частини Кримінального кодексу України [27, с. 400].

Така невтішна статистика свідчить про стрімкі темпи розвитку кіберзлочинності. На нашу думку, в епоху цифровізації суспільства потрібно більше уваги приділяти безпеці в кіберпросторі. Насамперед це пов’язано з тим, що все більше сфер суспільного життя спільнота переносить у кіберпростір, що відкриває перед особами, які вчиняють кримінальні правопорушення в ньому, усе більше можливостей для реалізації своїх незаконних намірів. З огляду на це ми вважаємо необхідним побудувати нову національну модель забезпечення кібербезпеки держави загалом і кожного громадянина, компанії й організації зокрема. Така модель

повинна ґрунтуватися на чіткій координації між правоохоронними органами, органами фінансового нагляду та судовими системами, а також на їх задовільній кадровій та матеріально-технічній підтримці.

Сучасний стан кіберзлочинності становить велику загрозу для суспільства, і з кожним роком зростає кількість кримінальних правопорушень у кіберпросторі, що поглинають усе більше коштів. Злочинність у кіберпросторі глобально небезпечна для економіки кожної країни світу. У процесі свого функціонування цей вид злочину йде в ногу з науково-технічним прогресом, що так само ускладнює попередження та протидію незаконним діям і дає йому змогу існувати впродовж такого тривалого періоду.

Підсумовуючи вищевикладене, зазначаємо, що початок розвитку кримінальної відповідальності за кримінальні правопорушення в кіберпросторі датують початком 70-х років XX ст. Пропонуємо виділяти шість етапів становлення кримінальної відповідальності за кримінальні правопорушення в кіберпросторі на теренах України: 1) початковий (характеризується правовим вакуумом у регулюванні кримінально правової охорони кіберпростору й безкарністю кримінальних правопорушень у кіберпросторі); 2) зародження (ухвалення Кримінального кодексу України, який визначав три види кримінально караних діянь у кіберпросторі та активне використання зловмисниками у своїй кримінально протиправній діяльності різноманітних IRC-клієнтів для вчинення шахрайств у кіберпросторі); 3) імплементаційний (ратифікація Україною Конвенції про кіберзлочинність, яка визначала 23 кримінальні правопорушення в кіберпросторі й фактичну імплементацію частини норм Конвенції про кіберзлочинність у законодавство України); 4) економічний (характеризується появою віртуальних валют і розвитком економічних кримінальних правопорушень у кіберпросторі); 5) нормотворчий (створення спеціалізованого правоохоронного органу – Департаменту

кіберполіції Національної Поліції України, ухвалення Закону України «Про основні засади забезпечення кібербезпеки України»); 6) сучасний (карантинні обмеження, спричинені пандемією COVID – 19, та збройна агресія Російської Федерації дали новий поштовх у розвитку кримінально протиправних діянь у кіберпросторі, зокрема з'явилися нові види кримінальних правопорушень, а їх кількість стрімко збільшується).

1.2. Теоретико-правові підходи до тлумачення поняття «кіберпростір»

Сьогодні життя сучасної людини майже неможливо уявити без технологій. За всю історію існування людина завжди намагалася створити собі комфортні умови. Завдяки такому прагненню вона змогла оточити себе всіма досягненнями сучасної цивілізації.

Розуміння наслідків інформаційно-комунікаційної революції привело сучасних мислителів до висновку, що людське суспільство зазнало справді серйозних якісних змін. Характер цих змін дає змогу констатувати початок нової ери в розвитку історії людства – ери мережевого панування.

Як писав у середині XX ст. М. Маклюен, «головна особливість електричної ери полягає в тому, що вона створює глобальну мережу, багато в чому подібну до нашої центральної нервової системи», яка формує «єдине поле досвіду». «Інформаційний вибух» у другій половині минулого століття привів до появи мережевого суспільства, що характеризується складністю та структурним дисбалансом [27, с. 400].

Інформаційне середовище наразі є однією з найдинамічніших сфер суспільних відносин, що потребують правового врегулювання. Інтернет-мережа стала невід'ємною частиною життя сучасного суспільства, одержавши власну інфраструктуру й форму вираження, мову, мережеву

культуру, інтернет-магазини, платформи онлайн-навчання, публічні та непублічні форуми.

Унаслідок стрімкого зростання різних інцидентів у галузі інформаційної безпеки та їх загрозливого характеру як для окремих держав, так і для пересічних громадян кримінальні правопорушення в кіберпросторі набувають усе більшого поширення. Такі загрози шкодять значному колу приватних, державних і корпоративних інтересів.

Інтеграція держави у всесвітній інформаційний простір, розвиток інформаційного суспільства й глобальна диджиталізація привели до виникнення нових загроз національним інтересам України в кіберпросторі.

Основними тенденціями розвитку загроз є такі: 1) збільшення кількості атак, багато з яких призводять до великих збитків; 2) підвищення складності атак, що охоплюють кілька етапів і можуть передбачати спеціальні методи захисту від можливих контрзаходів; 3) впливають на всі електронні (цифрові) пристрої, серед яких останнім часом набувають усе більшого значення та найбільше піддаються ризикам у сфері інформаційної безпеки мобільні пристрої; 4) дедалі частіші атаки на інформаційну інфраструктуру великих корпорацій, великих промислових підприємств і навіть державних установ; 5) використання найбільш передових країн у сфері засобів комп'ютерної техніки й застосування найсучасніших методів кібератак на інші країни.

Наразі поняття «кіберпростір», «інтернет-простір», «віртуальний простір» та «інформаційний простір» є загальновживаними як на побутовому, так і на законодавчому рівні. Проте варто зауважити, що вони відрізняються між собою за своєю сутністю й природою, а їх неправильне трактування може створити багато термінологічних проблем. Тому, на нашу думку, першочергово потрібно проаналізувати сутність цих понять.

Серед усіх запропонованих визначень поняття «інформаційного простору» найбільш широке за своєю природою й охоплює всі сфери життя

суспільства, у яких наявна інформація: засоби масової інформації, телебачення, книги, іншу друковану продукцію, телефонію, Інтернет.

Розглядаючи поняття «інформаційного простору» з точки зору інформаційної безпеки, згідно зі словником термінів і визначень у галузі інформаційної безпеки інформаційний простір – це сукупність інформації та інформаційної інфраструктури; сфера діяльності, пов'язана зі створенням, перетворенням і використанням інформації, зокрема індивідуальне й суспільне створення, інформаційно-телекомунікаційна інфраструктура та власне інформація [28].

У доктринальній характеристиці виділяють два підходи до формування поняття інформаційного простору: технічний і гуманітарний.

Згідно з технічним підходом інформаційний простір репрезентований у технічному аспекті як система, що обробляє, зберігає, використовує й передає інформацію за допомогою різнотипних технічних засобів та інших технологічних рішень. За такого підходу інформаційному простору властива обмеженість і прихильність до каналів поширення даних.

Щодо гуманітарного підходу, то варто зазначити, що з точки зору гуманітарних наук інформаційний простір є сукупністю знань та інформації, що формується й постійно змінюється разом з еволюцією суспільства. Гуманітарний підхід передбачає повну відсутність кордонів і прив'язаності до конкретної місцевості інформаційного простору, а об'єкти інформаційного простору так само мають «людську природу – люди та їх спільноти».

Дослідник Й. Дзялошинский наводить аналіз трьох основних підходів до визначення поняття інформаційного простору.

К. Дубняк у своїй праці «Інформаційний простір: структура та функціональні параметри» дає таке визначення: «інформаційний простір – це простір, у якому створюється, переміщується та споживається

інформація». Очевидно, вчений має на увазі певне обмежене середовище, з яким пов’язані інформаційні потоки [29, с. 23].

О. Дубас розглядає це поняття з точки зору сучасної медіасистеми й говорить, що «світовий інформаційний простір інтегрується за допомогою комунікаційних систем і методів передавання інформації, які були вдосконалені в ході національної інформаційної революції та транскордонних інформаційних потоків» [30, с. 277].

А. Семенова визначає інформаційний простір як територію поширення інформації за допомогою конкретних компонентів системи інформації та зв’язку, діяльність якої має гарантоване правове забезпечення. Спеціальними вимірами інформаційного простору можуть стати такі: загальна кількість засобів масової комунікації; загальний обсяг її продукування, що поширюється й приймається на певній території; опосередкована фіксація тих або інших результатів контакту з продукцією засобів масової комунікації реципієнтів [31, с 117].

Л. Білоусов так само зазначає, що створення, передавання, накопичення та зберігання інформації відбуваються за допомогою певних суб’єктів інформаційного середовища, а сам інформаційний простір визначає як коло інтересів інформаційної взаємодії чи впливу: інформацію, призначену для використання суб’єктами інформаційної сфери; інформаційну інфраструктуру, що забезпечує можливість обміну між суб’єктами; соціальні відносини, створювані через формування, передавання, розподіл і зберігання інформації, обмін нею всередині суспільства [32].

Отже, систематизувавши всі вищерозглянуті підходи, вважаємо, що інформаційний простір фактично позбувся всіх обмежень, властивих фізичному простору, але він має певні обмеження, пов’язані з державною таємницею й недоторканністю приватного життя, та конвенціональні межі.

Інформаційний простір є ширшим за кіберпростір, тобто останній є його частиною.

Поняття «віртуальний простір» також значно ширше за «кіберпростір», оскільки «віртуальний» як синонім слова «уявний» охоплює більше коло відносин, ніж обмежені комп'ютерними технологіями [33].

М. Носов пропонує авторський підхід до визначення статусу віртуального простору, під яким розглядає власне віртуальну реальність як базисне поняття віртуалістики. В основі віртуалістики він убачав покладені ідеї поліонтичності, допущення існування незведених одна до одної, тобто онтологічно самостійних, реальностей [34, с. 192].

О. Алексеєва так само вважає, що віртуальний простір може додатково характеризуватися такими особливостями, як: 1) поєднання віртуальної складової з об'єктивною реальністю, структурування майже всіх форм життєдіяльності людини (соціально-політичної, соціокультурної, виробничої, освітньої тощо); 2) віртуальний простір є засобом соціального програмування, реалізації соціоінженерних проєктів; незахищеність людини перед негативною інформацією, яка міститься у віртуальному просторі; 3) стрімкий розвиток технологій маніпулювання свідомістю за допомогою сучасних медіазасобів (поширення фейкових новин, новин з умонтованою точкою зору, технології спіндокторингу (управління новинами й медіаподіями) тощо); 4) ілюзія включеності в соціальний простір, комунікацію; подолання межі між реальним і віртуальним (фальсифікація новин, реаліті-шоу тощо), що зумовлює суперечливе відчуття залученості до насиченого соціального буття, привчає жити серед віртуальних образів, віртуальних цінностей, забезпечує компенсацію реальних почуттів та переживань, створює умови для романтизації насильницьких стереотипів поведінки [35, с. 8].

Віртуальний простір можна розглядати як середовище, створене комп'ютерними технологіями, що породжує аудіовізуальну реальність публічного простору, дає змогу людям взаємодіяти одна з одною й із репрезентованими в ньому об'єктами, організаційно-методологічні умови та сукупність технічних умов, містить програмне забезпечення для зберігання, оброблення та передавання інформації [36, с. 92].

С. Лукін вважає, що сьогодні основними особливостями функціонування віртуального простору є такі: 1) медіатизація, що характеризується сукупністю масових явищ інформаційного впливу й взаємодії; 2) масова комунікація – найважливіший інструмент проєктування та самопостановки віртуального простору; 3) використання практики електронної демократії; 4) застосування smart-технологій.

На нашу думку, «віртуальний простір» – це створене комп'ютерними технологіями глобальне комунікативне середовище, в основі якого лежить створення, збереження, упорядкування та обмін інформацією за допомогою електронних мереж.

Розвиток віртуального простору породжує формування різноманітних форм і методів спілкування між користувачами. Він є більш досконалим та ефективним інструментом взаємодії й взаємовпливу. Водночас Інтернет сприяє інтенсифікації комунікаційних процесів, що є результатом стрімкого прогресу комп'ютерних технологій в усіх сферах суспільного життя. Так створюється віртуальний публічний простір, що формує нові можливості та реалії спілкування, стає найбільш динамічною, технологічною й культурною економікою сучасності, соціальним і політичним явищем нашого часу.

На противагу «інформаційному простору» та «віртуальному простору», «інтернет-простір», навпаки, є надто вузьким поняттям, тому що на відміну від інтернет-мережі є інші менші інформаційно-телекомунікаційні мережі, такі як «FidoNet», «Cren», «Top», «Freenet»,

«Ants P2P» та ін. Крім того, ураховуючи структурні елементи Інтернету, можливо, у майбутньому його замінять міжнародною інформаційно-телекомунікаційною мережєю під іншою назвою, а сам кіберпростір залишиться її складовою.

Пізнавальна діяльність сучасної людини завжди супроводжується активним використанням інформації та інформаційних технологій. Вони слугують для одержання, обміну й зберігання інформації та забезпечують доступ до неї значної кількості людей одночасно.

На сучасному етапі розвитку українського суспільства процеси комунікації в інтернет-просторі відбуваються під впливом різноспрямованих чинників: 1) частково через ускладнення та глобалізацію комунікаційних зв'язків; 2) через відображення різноманітності конфігурацій комунікаційного процесу; 3) через відображення багатогранності й рівня духовного розвитку внутрішнього світу користувачів Інтернету. Загальновідомі факти надмірного захоплення інтернет-простором можна пояснити, з одного боку, своєрідним бажанням людини замінити реальний світ образами віртуальних супутників життя, а з іншого – недостатнім рівнем розвитку сучасного інтернет-гуманізму [37, с. 88].

На думку Л. Лазаренко, екоорієнтована модель існування людини в інтернет-просторі охоплює чотири компоненти: особистісні ціннісні орієнтації суб'єктів спілкування; підвищення попиту на екологічно орієнтоване життя в інтернет-просторі; підтримку екологічно орієнтованих інтернет-ініціатив щодо гуманного поводження з людьми в Інтернеті, що можуть не відразу окупитися; проєктування технологічних інтернет-інновацій та інтернет-комунікації у сфері гармонізації процесу розвитку сучасної особистості з новими соціальними інфраструктурами, що виникають в інтернет-середовищі [38].

З появою інтернет-мережі майже кожна людина одержала можливість швидкого та оперативного доступу до інформації. Саме з огляду на інтенсивний розвиток інтернет-мережі стало можливо говорити про такий феномен, як кіберпростір.

Загалом прийнято розглядати кіберпростір як частину ноосфери й абстракцію, що об'єднує всі інформаційні процеси, які відбуваються як усередені окремних комп'ютерів, так і всередині комп'ютерних мереж. У повсякденній промові термін «кіберпростір» закріпився як один із широко використовуваних синонімів для мережі Інтернет, але варто пам'ятати, що поняття «кіберпростір» та «Інтернет» не є тотожними [39].

Кіберпростір як один із сучасних суспільних продуктів надав необхідні можливості людству для вирішення на якісно новому рівні актуальних проблем, проте він також не позбавлений відповідного набору соціальних і психологічних недоліків. Структурна й інтелектуальна розмитість зазначеного феномену обумовлюють його недостатню вивченість, проте вже існують загальні, принципові положення, одержані в результаті сучасних напрацювань [40, с. 160].

Щоб повноправно оперувати терміном «кіберпростір», необхідно визначити, що це. Є декілька підходів, що пояснюють природу кіберпростору та намагаються дати йому як доктринальне, так і легальне визначення, але більшість розглядають його як щось закрите, «поле», у якому розгортаються інформаційні процеси. З цього підходу випливає уявлення про кіберпростір як щось видиме, уявне.

Термін «кіберпростір» використовують у зарубіжному й вітчизняному законодавствах і доктринальних джерелах. Поняття кіберпростір (англ. cyberspace) можна розглядати як греко-латинську комбінацію, що складається з двох частин: «кібер-» (cyber-) і «простір» (space). В Оксфордському словнику англійської мови зазначено, що префікс «cyber-» походить від грецького слова κυβερνήτες, що буквально

перекладається як «правителі». Стародавні греки використовували слово «кібернетика» в сенсі «мистецтво рульового», тобто «мистецтво управління». На початку XIX ст. французький математик і фізик А. М. Ампер, який запропонував власну класифікацію наук, назвав науку про управління державою «кібернетикою» (cybernetique), помістивши її між дипломатією та теорією влади [41].

У сучасному вживанні «кібернетика» належить до науки про управління, передавання інформації та комунікаційні процеси в складних динамічних системах (технічних, обчислювальних, біологічних, нейронних, соціальних). Теоретичною основою кібернетики є досягнення багатьох наукових дисциплін, серед яких особливе місце посідають математичні науки й логіка, науки про життя, розроблення засобів автоматизованого управління та ін. Основні ідеї кібернетики були сформульовані в 1948 році Норбертом Вінером у праці «Кібернетика, або управління і зв'язок у тварин і машин».

Енциклопедичне визначення поняття «простір» має два значення: 1) простір (математ.) – множина об'єктів, між якими встановлені відношення, подібні за своєю структурою до звичайних просторових відношень типу околу, відстані та ін; 2) простір – форма співіснування матеріальних об'єктів процесів (характеризує структурність і протяжність матеріальних систем). Загальні властивості простору: протяжність, єдність, дискретність і неперервність [42].

Еволюція кібердискурсу сприяла появі цілого нового набору термінів, що позначають появу нового світу, створеного поширенням комп'ютерно-опосередкованої комунікації (СМС). На сьогодні префікс «кібер-» використовують у словах, що позначають зв'язок з електронними мережами зв'язку й віртуальною реальністю [43].

Для формування конкретної дефініції поняття кіберпростір, а також визначення його сутності спробуємо виокремити його специфічні ознаки.

На думку А. Льюїса, кіберпростір має такі ознаки: 1) об'єднує глобальні комп'ютерні мережі та інформаційні ресурси, що не мають чітко визначеного власника й забезпечують інтерактивну комунікацію фізичних і юридичних осіб; 2) взагалі не обмежений жодними кордонами; 3) має децентралізований статус, яким повністю не володіє та не управляє жодна держава, об'єднання держав, жодна міжнародна організація, а також жодний оператор зв'язку; 4) є простором, у якому будь-яка особа може вільно діяти, висловлюватися й навіть працювати [44].

Варто зауважити, що, попри поширеність терміна кіберпростір у повсякденному житті, його сутність і специфіка не є чітко визначеними. У широкому розумінні кіберпростір ототожнюють зі сферою використання комп'ютерної техніки, автоматизованих систем, комп'ютерних мереж та мереж електрозв'язку, а у вузькому – з віртуальним простором, що невілює його матеріальну складову.

Вивчивши генезу й методологічні засади кримінальної відповідальності в кіберпросторі, пропонуємо перейти до характеристики поняття кіберпростору. На нашу думку, його необхідно розглядати в трьох аспектах: філософському, легальному, доктринальному. Так само в доктринальному аспекті кіберпростір можна розглядати в інформаційному, віртуальному та соціальному аспектах.

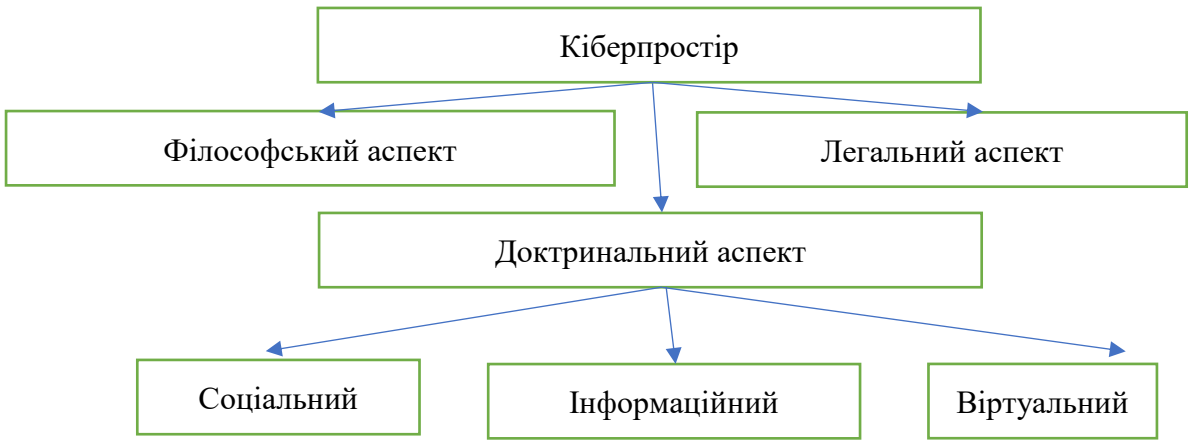

Рисунок 1 – Аспекти кіберпростору

З філософської точки зору (методологічний аспект) сутність об'єкта дослідження полягає в його внутрішньому змісті, який виражається «в єдності всіх різноманітних і суперечливих форм буття», тобто кіберпростір визначають як соціотехнічну систему. За допомогою кіберпростору можна опинитися там, де у фізичному розумінні нас немає, взяти участь у комунікації чи конференції, а сама людина, віртуального тіла якої насправді не існує, може діяти в рамках кібернетичного контексту (біографія, твори, дописи в соціальних мережах).

З філософського аспекту визначення поняття кіберпростору охоплює не лише блоки інформаційної належності, а й людей, репрезентованих своїми проєкціями, тобто створеними ними текстовими аргументаціями, зображеннями та повідомленнями. Самі суб'єкти, репрезентовані в кіберпросторі, постають безтілесними створіннями.

Канадський письменник-фантаст В. Гібсон уперше написав про кіберпростір у «пророчому» оповідані «Burning Chrome», опублікованому в липневому номері журналу «Omni» за 1982 рік, так: «штучний інтелект», «віртуальна реальність», «транснаціональні корпорації», «матриця» [45].

Роман В. Гібсона 1984 року «Нейромант», у якому автор визначає кіберпростір як середовище «сенсорних галюцинацій», які щодня відчувають мільярди операторів з усіх націй, зокрема діти, набув особливої популярності в цьому контексті [46].

Графічне репрезентування комп'ютерних даних осіб. Неймовірна складність. Потоки світла, кластери й сузір'я інформації, упорядковані людським розумом. Зокрема, завдяки працям В. Гібсона поняття кіберпростору міцно закріпилося в масовій свідомості та багато в чому визначило сучасну культуру сприйняття простору й часу.

З поширенням на початку 1990-х рр. Всесвітньої павутини (WWW) термін «кіберпростір» знайшов практичне застосування для опису онлайн-світу, в якому взаємодія окремих осіб і груп здійснюється за допомогою

електронних мереж, пов’язаних інформаційно-комунікаційними технологіями. Дж. Барлоу – один із активних захисників свободи в Інтернеті – у відповідь на Закон «Про пристойність у телекомунікаціях» опублікував Декларацію незалежності кіберпростору, у якій зазначив, що «кіберпростір складається з транзакцій, відносин і самих думок, які утворюють подібність хвильового візерунка в мережі нашого спілкування. Наш світ скрізь і ніде, і це не місце, де живуть наші тіла» [47].

Аналізуючи легальний аспект кіберпростору, варто звернутися до нормативних актів, що надають поняття «кіберпростору». Зокрема, у Національній військовій стратегії для операцій у кіберпросторі Сполучених штатів Америки 2006 року кіберпростір визначений як галузь, що характеризується можливістю зберігання, модифікації й обміну даними за допомогою електронних та електромагнітних засобів через мережеві системи й пов’язану з ними фізичну інфраструктуру [48].

Варто зауважити, що це визначення згодом було покладено в основу розроблення документів про стратегічне бачення, кіберкомандування повітряних сил 2008 року та Стратегії національної безпеки Сполучених Штатів Америки 2010 року. У зазначених документах наголошується, що військові повинні й надалі мати можливості захищати інтереси Сполучених Штатів Америки в кіберпросторі, космосі, повітрі воді та на землі [49].

Отже, в офіційному дискурсі безпеки Сполучених Штатів Америки кіберпростір розглядають саме як фізичний простір. Директор Національного центру біотехнологічної інформації Дж. Лімпан наголошував, що визначення такого підходу характерне саме для фахівців із Міністерства оборони Сполучених Штатів Америки, одночасно відбувається поступове зміщення точки зору в бік розуміння кіберпростору з власне фізичного до віртуального простору [50].

Комплексний документ з оцінювання стану безпеки кіберпростору Сполучених Штатів Америки «Кібербезковий огляд» від 2009 року

визначає кіберпростір як інформаційну сферу, сукупність інформації, інформаційних систем, суб'єктів та об'єктів інформації, сайтів в інформаційно-телекомунікаційних мережах, мереж зв'язку, інформаційних технологій.

Відповідно до визначення, запропонованого в Президентській Директиві з національної безпеки, кіберпростір – це місце (точка) з'єднання між комп'ютерами, що перетворилося на глобальне віртуальне співтовариство, а мережу Інтернет визначено переважно з функціональних позицій. Водночас директива характеризує Інтернет не лише як об'єднання мереж та сукупність різноманітних сервісів, а і як спеціальну структуру, що поєднує різних індивідуумів з усього світу: користувачів мережі, поширювачів інформації, сервіс-провайдерів та інших зацікавлених осіб [51].

Президентська директива з внутрішньої безпеки 23 (NSPD-54 / HSPD23) визначає кіберпростір через технічну базу, на основі якої він функціонує. До складу цієї бази входить сукупність програмних засобів, за допомогою яких здійснюються оброблення й передавання інформації. Крім технічної та технологічної складових, директива визначає інформаційну базу, що складається з потоків інформації, які люди передають одна одній за допомогою мережевих засобів зв'язку. Згідно із зазначеною директивою кіберпростір – це сукупність суспільних відносин, що виникають у процесі використання функціонуючої електронної комп'ютерної мережі й складаються в інформаційному просторі за допомогою електронно-обчислювальних машин та послуг інформаційного характеру, що надають за їх допомогою. Водночас можна бути користувачем таких послуг лише за допомогою електронно-обчислювальних машин та засобів зв'язку комп'ютерної мережі [52]. Як і директива з національної безпеки 54, директива з внутрішньої безпеки наголошує, що Інтернет є лише одним із видів комп'ютерних мереж. Як висновок, поняття кіберпростору ширше за

поняття Інтернет, оскільки кібернетичний простір так само створюють і звичайні комп'ютерні мережі всередині підприємства («інтранет»), а також віртуальні мережі, призначені для з'єднання приватних мереж різних компаній між собою («екстранет») [53].

Закон Сполучених Штатів Америки «Про безпеку комп'ютерних систем» від 1987 року тлумачить кіберпростір як дещо більше, ніж просто мережу Інтернет: він охоплює всі мережеві форми та цифрову активність, є формою співіснування й сукупності матеріальних і нематеріальних об'єктів та процесів, спрямованих на генерування, сприйняття, зберігання, оброблення та обмін інформацією [54].

Кіберпростір – це штучно створене середовище, існування якого обмежене інформаційно-телекомунікаційною мережею, користувачі якої можуть вільно вступати в адміністративні, цивільні, кримінальні та інші правовідносини. Кіберпростір може виникнути в будь-якій інформаційно-телекомунікаційній мережі. Наприклад, можна говорити про інтернет-простір у контексті мережі Інтернет. Отже, Інтернет – це не сам по собі кіберпростір, а просто стан, у якому він може існувати.

Згідно з рішенням Верховного Суду Сполучених Штатів Америки під кіберпростором розуміють «унікальне середовище, не розміщене в географічному просторі, але доступне кожному в будь-якій точці світу за допомогою доступу до мережі Інтернет» [55].

Верховний Суд США визначає Інтернет як «глобальне об'єднання комп'ютерних мереж та інформаційних ресурсів, що не має чітко визначеного власника й служить для інтерактивної комунікації фізичних та юридичних осіб».

У національному законодавстві України поняття кіберпростору визначено в Законі України «Про основні засади забезпечення кібербезпеки України»: середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в

результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій із використанням мережі Інтернет та/або інших глобальних мереж передавання даних [56].

На наш погляд, визначення поняття кіберпростору надане в Законі України «Про основні засади забезпечення кібербезпеки України», найбільш повно розкриває сутність і природу кіберпростору. У ньому відображене відношення віртуального простору до кіберпростору як загальне до особливого. Підкреслено унікальність кіберпростору як сфери комунікації та людської активності, а також те, що Інтернет не є єдиною інформаційно-телекомунікаційною мережею.

З точки зору доктринального аспекту визначення поняття «кіберпростір» можна розглядати в соціальній, інформаційній та віртуальній характеристиках.

Соціальний аспект аналізу кіберпростору передбачає вивчення всіх соціальних взаємодій, що відбуваються в цьому цифровому середовищі, зокрема функціонування численних віртуальних спільнот, а також нових способів конструювання особистості.

Дж. Сулер наголошує на такій властивості кіберпростору, як текстуальність, тобто текстова взаємодія між суб'єктами кіберпростору в інтернет-мережі у вигляді чатів, блогів, форумів, електронної пошти, месенджерів і соціальних мереж. На його думку, текстуальність – це потужна сила самовираження й міжособистісних стосунків, що являє собою унікальний спосіб презентування своєї ідентичності та впізнавання один одного в онлайн-середовищі [57].

Н. Чапелеєва зазначає, що основними психологічними механізмами інтерпретування кіберпростору є семіотизація й наративізація. У процесі семіотизації реальність позначається шляхом накладання, структурування та концептуалізації певних когнітивних структур. Семіотизація відбувається на двох рівнях. Перший рівень пасивного відображання

дійсності шляхом накладання вже відомих когнітивних структур. Другий рівень передбачає конструювання реальності через її перетворення. Наративізація являє собою конструювання реальності в наративній формі, зверненій до іншого, зокрема внутрішнього іншого. Під час цього конструюється наративний текст інтерпретації, що може оперувати як продуктивним, так і репродуктивним рівнем семіотизації [58, с. 311].

Розгляд і дослідження кіберпростору в контексті психологічної герменевтики й семіотики можливі через його текстуальну природу. Семіотичний світогляд розглядає все як знак, що кодує щось «позаду», символізує щось приховане за ним або сигналізує про це «щось». Завдяки семіотичному аналізу стає можливим відкривати додаткові значення й конструювати нові. Процес семіотичного моделювання є основою для формування суб'єктивної реальності особистості.

У праці одного з перших дослідників проблем кіберпростору Е. Кетша зазначено, що концептуально це поняття пов'язано з розвиненою електронною культурою, яка дає змогу обробляти й працювати з інформацією в електронній формі з використанням складних комп'ютерів, що зберігають та аналізують дані й забезпечують можливість здійснювати комунікації незалежно від перебування [59, с. 431].

Beer Sijpesteijn розглядає кіберпростір як «соціокультурний феномен, продукт технологічної творчості й перспективну ідею», стверджує, що це новий ризоматичний за своєю типологією вид семіотичного простору, в якому операції зі знаками здійснюються за допомогою сучасних комп'ютерних технологій, що полегшують та істотно прискорюють розумову діяльність людей [60, с. 87].

Вартим уваги також є визначення, запропоноване П. Вуллей з Інституту технологій повітряних сил США, яка пропонує розуміти кіберпростір як створене людиною цифрове довкілля, використовуване для миттєвих, безкордонних, глобальних, безорганізаційних, культурних,

національних чи політичних кордонів збирання, зберігання й передавання даних та інформації між електронним обладнанням [61, с. 310].

За визначенням П. Воллі, кіберпростір – це принципово новий вид проєкційного середовища культури, що з'єднує реальність і сучасну технологічну сферу, полегшуючи й прискорюючи цим інтелектуальну діяльність людини [62].

Ф. Крамер вказує на те, що кіберпростір виконує інтегративну функцію, об'єднує людей відповідно до їхніх інтересів і потреб та таким чином формує основу для зростання солідарності в суспільстві. Будучи частиною кіберпростору, засоби масової інформації залучені до дій інших соціальних інститутів, а самі функціонують як соціальні інститути. Потрібно зазначити, що кіберпростір інтегрує не лише ЗМІ, а й інші джерела інформації. Крім окремих людей і їх груп, в Інтернеті також є електронні помічники (програми штучного інтелекту), яких навчають створювати й поширювати контент самостійно [63].

С. Гаков, аналізуючи кіберпростір із точки зору соціальної діяльності, зазначає, що його зміст становлять соціальні відносини між власниками інформаційних систем, власниками інформації, споживачами (користувачами), спеціально вповноваженими державними органами, роботодавцями, працівниками, юридичними й фізичними особами. Зокрема, до них, на його думку, належать: 1) виробники ІТ-продуктів та ІТ-послуг тощо; 2) правові норми, що регулюють відповідні суспільні відносини, які визначають правові системи інформації, інформаційні системи (її компоненти) і технології, юридичну відповідальність тощо; 3) практична діяльність людини, пов'язана зі створенням кіберпростору, впровадженням інформаційних технологій та підтриманням їх у функціонально здатному стані, забезпеченням кібербезпеки особи, суспільства, держави тощо [64, с. 55].

Отже, кіберпростір – це соціальний феномен, оскільки він наповнений людьми, а точніше – їх образами, здебільшого породженими текстами. Тому кіберпростір можна визначити як об'єкт психологічної герменевтики, а також як тип семіотичного простору, що охоплює опосередковану електронними пристроями віртуальну та реальну складові людської реальності.

Очевидно, що кібер- і реальний простори нерозривно пов'язані й перетинаються в загальному потоці соціальних взаємодій. У цьому контексті варто зазначити, що нові можливості, які відкривають перед людьми інформаційно-комунікаційні технології, фактично привели до стирання межі між реальним світом і кіберпростором. Через призму аналізу інформаційного аспекту кіберпростору вбачають функціонування сукупності безлічі інформаційних потоків, через які інформація, передана в цифровому вигляді, «тече» з неймовірною швидкістю.

К. Дарбік визначав, що кіберпростір є ареною для консолідації комплексних наукових теорій у галузі систем управління комунікаційними процесами, процесами обміну інформацією та їх застосування в практиці функціонування соціальних структур у віртуальному просторі [65].

На думку С. Рибки, кіберпростір – це середовище, утворене організованою сукупністю інформаційних процесів (створення, передавання, використання інформації) за участю людини, зокрема на об'єктах критичної інфраструктури держави із застосуванням ресурсів складових частин національної інформаційно-комунікаційної інфраструктури [66, с. 130].

На нашу думку, позиція С. Рибки щодо визначення поняття кіберпростору з точки зору інформаційного аспекту є дещо обмеженою, оскільки фактично містить у собі лише централізовану складову, за якої насправді кіберпростір є децентралізованим і не належить ані державі, ані конкретній особі.

Д. Дубов наголошує, що кіберпростір – це середовище, створене організованою сукупністю інформаційних процесів на основі інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем, уніфікованих за загальними принципами й правилами незалежно від форми власності [67, с. 112].

Дж. Василевскіх наголошував, що термін кіберпростір вживають для опису глобальної галузі інформаційного середовища, яка складається з взаємозалежних мереж, утворених інфраструктурою інформаційних технологій, а також будь-яких даних, що містяться в ній, охоплюючи Інтернет, телекомунікаційні мережі й комп'ютерні системи, зокрема процесори та контролери [68, с. 227].

Очевидно, що кіберпростір є інформаційним простором. На цьому акцентують увагу В. Гавловський [69, с. 51] і В. О. Голубєв, який у статті «Боротьба з комп'ютерними злочинами – проблема транснаціонального масштабу» описує термін «кіберпростір» як інформаційний простір, створений за допомогою комп'ютера, в якому необхідно позначити об'єкти або символічний прояв інформації, – простір, у якому діють переміщення комп'ютерних програм і даних [70].

На нашу думку, найбільш правильно розглядати кіберпростір саме з позиції віртуалістики. З точки зору 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, у яких взаємодіють звичайні користувачі. Незважаючи на те, що кіберпростір фактично не є вмістилищем реальних матеріальних об'єктів, реальні матеріальні об'єкти створюють віртуальні місця, які не мають просторово-часової межі, але є місцями взаємодії. Вони зберігають величезну кількість інформації та

створюють захисні кордони цієї інформації або обмежують можливість доступу до певних ресурсів у кіберпросторі.

Б. Варф у своєму дисертаційному дослідженні наголошує, що кіберпростір являє собою комп'ютерно-технологічну віртуальну реальність, яка характеризується абсорбцією гіпертексту й гіперреальності, модифікацією просторово-часових меж, просторово-часових потоків та їх багатовимірністю й дискретністю [71].

С. Хілдерт визначає кіберпростір як одну з багатьох форм віртуальної реальності, але наголошує, що, якщо віртуальна реальність означає ширше коло явищ, починаючи від музичного твору й закінчуючи відображенням снів і фантазій, то кіберпростір має чітко визначені кордони взаємодії людини та електронно-обчислюваної техніки. Для С. Хілдера кіберпростір – це метафізична абстракція, використовувана для опису об'єктів, широко поширених у комп'ютерній мережі [72].

В. Фурашев розглядає кіберпростір як форму співіснування сукупності матеріальних і нематеріальних об'єктів та процесів, спрямованих на генерування, сприйняття, зберігання, оброблення й обмін інформацією. Учений наголошує, що кіберпростір – це дуже складне явище, яке поєднує в собі реальність і віртуальність, матеріальне й нематеріальне, абстрактне та реальність і має такі властивості: протяжність, єдність розсуду й безперервність, матеріальність і нематеріальність, абстрактність та реальність, реальність загального впливу [73, с. 163].

В. Бурячок розуміє кіберпростір як віртуальне комунікаційне середовище, утворене системою зав'язків між користувачами та об'єктами інформаційної інфраструктури, такими як IP для передавання інформації, яка циркулює в них, з метою задоволення інформаційних потреб суспільства [74, с. 190].

С. Гнатюк пропонує визначати кіберпростір як віртуальний простір, що виникає в результаті взаємодії користувачів, програмно-апаратних

засобів і мережевих технологій (зокрема, Інтернеу) для підтримки й управління процесами перетворення інформації (електронних інформаційних ресурсів) із метою задоволення інформаційних потреб для охоплення суспільства [75, с. 123].

Наступним етапом аналізу поняття «кіберпростір» є окреслення та детальне характеризування його сутнісних ознак. У наукових джерелах немає сталої позиції щодо переліку таких ознак.

На думку А. Тарговскі, характеристики кіберпростору такі: 1) об'єднує глобальні комп'ютерні мережі й інформаційні ресурси, що не мають чітко визначеного власника та забезпечують інтерактивну комунікацію фізичних і юридичних осіб; 2) взагалі не обмежений жодними кордонами; 3) має децентралізований статус, яким повністю не володіє й не управляє жодна держава, об'єднання держав, жодна міжнародна організація, а також жодний оператор зв'язку; 4) є простором, у якому будь-яка особа може вільно діяти, висловлюватися та навіть працювати [76, с. 335].

К. Дарбік виділяє такі ознаки кіберпростору: 1) випадковість; 2) неістотність; 3) необмежений; 4) універсальність і поширеність; 5) інтерактивність; 6) динамічність; 7) гнучкість; 8) непередбачуваність; 9) ліберальність [65].

На думку А. Манжая, кіберпростір має три основні характеристики: 1) це інформаційний простір; 2) є комунікативним середовищем; 3) утворений за допомогою технічних систем [77].

За С. Гаховим до основних характеристик кіберпростору належать його динамічність, функціональність, інформаційність й визначення його як середовища існування. Динамічність кіберпростору, на думку науковця, означає його постійно мінливий характер, а протяжність та обсяг обумовлені кількістю електронно-телекомунікаційних систем, що функціонують у ньому. Функціональність у цьому разі означає комплекс

вибірково використовуваних компонентів, взаємодія яких набуває сфокусованого корисного результату.

Автор підкреслює, що середовище функціонування процесів інформаційно-телекомунікаційної системи буде визначатися через структурні, функціональні, часові, інформаційні ознаки. Прикладом інформаційних характеристик інформаційної системи може бути об'єм її запам'ятовувальних компонентів тощо [78, с. 55].

Критично проаналізувавши позиції вчених, вважаємо, що серед основних характеристик кіберпростору варто виділити такі: віртуальність, мережеву належність, середовище взаємодії, динамічність, комунікативність і поєднання територіалізації та детериторіалізації. Пропонуємо детально проаналізувати кожну з них.

По-перше, віртуальна складова, сучасне вживання терміна «віртуальність» усе більше виходить за межі сфери інформатики й комп'ютерних технологій. У повсякденне життя ввійшли «нереальні» комбінації, такі як «віртуальна компанія», «віртуальні гроші», «віртуальна демократія», «віртуальна освіта» тощо. Отже, віртуальна реальність є максимально об'єктивованою, надзвичайно конкретною та відчутною. Це означає, що кіберпростір не є суворо обмеженим і не залежить від конкретного просторово-часового розміщення. Розміщення взаємодії в кіберпросторі не вимагає від агентів взаємодії бути в певному місці в певний час, щоб їх зустріч відбулася в кіберпросторі. Безсумнівно, взаємодія в кіберпросторі має фізичний субстрат, але вона може бути синхронною або асинхронною та доступною для агентів майже в будь-якому географічному просторі. Віртуальність у цьому разі не є протилежністю реальності. Проте віртуальність означає, що щось у кіберпросторі може бути не таким, яким здається. Кіберпростір як віртуальне місце не є місцем у звичайному розумінні, за якого місце чи простір взаємодії обмежені просторово-часовими кордонами.

По-друге, мережева належність, тобто зв'язок між кіберпростором і мережею. Кіберпростір не можна ототожнювати з мережею або описувати як сукупність даних, що зберігаються на комп'ютерах та стають доступними через комп'ютерні мережі. Проте кіберпростір значно залежить від функціонування інформаційно-комунікаційних мереж (переважно Інтернету). Більш конкретно кіберпростір – це місце або простір, що контролює існування й роботу взаємозв'язаних комп'ютерних мереж. Отже, будь-яка зміна стану відповідних взаємозв'язаних комп'ютерів, наприклад вимкнення електроенергії, також буде пов'язана зі зміною в тому, як вони взаємодіють у кіберпросторі: наприклад, неможливість взаємодії.

Мережа Інтернет – це матеріальне відображення кіберпростору в реальному світі. Вона складається з окремих комп'ютерів, серверів та інших технічних пристроїв, об'єднаних між собою провідним і бездротовим шляхами по всьому світу (через супутник, мікрохвильові й електромагнітні сигнали, Wi-Fi, 3G, LTE), тобто це всесвітня інформаційно-телекомунікаційна мережа.

В інтерпретації мережевої належності сутності кіберпростору можна виділити такі його основні риси: 1) кіберпростір – це просто Інтернет, його ресурси та послуги, а також користувачі; 2) кіберпростір ототожнюють із віртуальною реальністю, створюваною комп'ютером, мережею й Інтернетом; 3) кіберпростір є соціальною мегамережею – «мережею мереж», у якій індивідуальні учасники та групи (спільноти) користуються глобальними ресурсами, надаваними через Інтернет; 4) кіберпростір – це складна еволюційна динамічна система (system of systems), і з огляду на це його передусім варто розглядати саме так незалежно від того, чи буде він проявляти свої технічні, інформаційні й соціальні аспекти [79].

По-третє, середовище взаємодії. Кіберпростір як простір взаємодії – ще одна його важлива характеристика. Приклади взаємодії в кіберпросторі:

інтернет-банкінг, геймінг, соціальні мережі, електронні торги, новини, онлайн-шопінг, пошукові системи, електронний уряд, краудсорсинг.

Якщо брати до уваги технічну та соціальну складові, то кіберпростір як середовище взаємодії:

1) середовище (ситуація), у якому його окремі елементи (телекомунікаційна мережа, комп'ютерна система тощо) можуть бути використані як інструмент для досягнення протиправної мети – порушення нормального функціонування цього середовища або заволодіння предметами (об'єктами інтелектуальної власності, платіжними продуктами, матеріальними активами);

2) особлива ситуація, за якої внесено зміни діянням (його наслідком), що може слугувати доказом у кримінальному провадженні.

Як середовище взаємодії М. Мягка виділяє таку властиву кіберпростору специфіку:

− на відміну від реального світу не має кордону між країнами;

− не обмежений, кожний має свободу висловлення своєї думки;

− комунікація в ньому здебільшого анонімна, користувачі можуть повідомляти про себе будь-яку інформацію на свій розсуд або взагалі залишитися інкогніто. Варто зауважити, що архіскладно перевірити достовірність інформації, а сам кіберпростір стає певним середовищем безкарності людей, які тим чи іншим чином використовують його з порушенням соціальних норм, норм моралі та нормативно визначених правил поведінки [80, с. 141].

По-четверте, динамічність. Кіберпростір не є чітко визначеним і конкретизованим. Зважаючи на це, його можна розглядати як своєрідну функціональну структуру, що має безліч потоків своєї діяльності, які відкриваються для звичайного користувача лише окремими блоками, а сам конект може здійснюватися з будь-якого місця. Така функціональна структура постійно змінюється, відображаючи мобільність і динамічність

кіберпростору, але водночас довжина інтервалів між інформаційними полями здебільшого залишається невідомою.

По-п’яте, комунікативність. Кіберпростір є соціальним простором, оскільки є багато соціальних взаємовідносин між реальними людьми в реальному житті. Ідеться про побудову мережевої ідентичності, що характеризується гнучкістю, фрагментацією та різноманітністю.

Використовуючи різноманітні аудіовізуальні комп’ютерні технології, особа може реалізувати свою комунікативну функцію, контактувати не лише з іншими людьми, а й зі штучними персонажами, створеними іншими людьми, з метою використання цих образів у подальшому вчиненні злочину.

Суб’єкти комунікацій у кіберпросторі взаємодіють один з одним із певною мотивацією: бізнес (одержання або надання послуг, ведення справ); спілкування (спілкування з однодумцями, участь у спільноті, визначеній спільністю інтересів); когнітивний (здобуття освіти); розваги (інтерактивні ігри, телебачення) тощо. Тому кіберпростір є альтернативою реальному матеріальному світу. Користувачі мережі так само є учасниками соціальних відносин, поширених у сучасному інформаційному суспільстві, і сформували певні соціальні групи за певними критеріями [81, с. 176].

По-шосте, поєднання територіалізації та детериторіалізації. Одним із серйозних інформаційних викликів стало протиріччя між, з одного боку, транскордонним характером кіберпростору, а з іншого – територіальними параметрами, що мають категорії суверенітету та юрисдикції держави, реалізовувані в межах державних кордонів.

Як у вітчизняній, так і в іноземній науковій доктрині впродовж усього інтегрування громадських та державних інститутів у кіберпростір звучали побоювання і щодо неефективності географічної територіальності в міжнародному праві, і щодо відсутності збігів кордонів держав із межами реалізації їх влади [82, с. 177].

У сучасній доктрині сфера суверенітету та юрисдикції також обмежується державною територією, що належить до невід'ємних ознак держави.

Сьогодні одночасно відбуваються, з одного боку, територіалізація кіберпростору, тобто поширення на нього такої конфігурації влади, що діє щодо територіальних просторів, а з іншого – його детериторіалізація, яка полягає у визнанні й розвитку транснаціональних юридичних підходів, обмежених чинним міжнародним правом, але що потребують уточнення з урахуванням специфіки діяльності в кіберпросторі.

Наприклад, К. Айкенсер зазначає, що відповідно до норм міжнародного права правила юрисдикції значно базуються на суверенітеті держав щодо конкретної території та знаходження власності осіб у межах цієї території. Зокрема, визначено, що перебування цих осіб та знаходження власності є цілком відомими. Проте в еру хмарних і комп'ютерних технологій, коли інформація перетинає межі безперешкодно, частини окремих файлів можуть існувати в кількох юрисдикціях, а саме місце зберігання інформації часто залежить від приватних компаній. Породжуються нові та складні питання для держав, що намагаються забезпечити примусову юрисдикцію, компаній, які отримують запити від правоохоронних органів, а також осіб, які хочуть захистити своє приватне життя [83, с. 50].

Отже, можна визначити кіберпростір як частину інформаційного простору, який функціонує на основі інформаційно-комунікаційних технологій, що дає змогу створювати складні інформаційні потоки з метою одержання, обміну, зберігання та управління інформацією, здійснювати комунікації в умовах безлічі різних мереж, має децентралізований і транснаціональний характер.

Варто зауважити, що в забезпеченні стабільності функціонування кіберпростору вагому роль також відіграють принципи. На нашу думку,

доцільно виділити такі принципи забезпечення стабільності в рамках кіберпростору: своєчасного втручання, додержання прав і свобод людини й громадянина, дисципліни, відповідальності.

Принцип своєчасного втручання. Зазначений принцип містить загальні вимоги до підтримки стабільної діяльності кіберпростору й функціонування в ньому його суб'єктів. Реалізація цього принципу передбачає недопущення навмисної ескалації чи наростання нестабільності серед суб'єктів кіберпростору. Водночас варто наголосити, що мова йде не лише про державне регулювання кіберпростору, оскільки дії приватних компаній та загалом окремих осіб можуть бути спрямовані на забезпечення стабільності кіберпростору. Наприклад, окремі державні чи приватні компанії з метою нейтралізації кіберзагроз можуть співпрацювати між собою, а окремі особи повинні дотримуватися інструкцій і рекомендацій щодо експлуатації повіреної ними електронно-обчислювальної техніки, зокрема оновлення програмного забезпечення комп'ютера чи системи управління контентом вебсайту, щоб знизити ризики проникнення в комп'ютерну мережу, і їх подальшого використання для проведення широкомасштабних стабілізаційних заходів із підтримки безпечності кіберпростору.

Принцип додержання прав і свобод людини й громадянина. Одночасно зі збільшенням ролі інформаційно-телекомунікаційних технологій у житті людини розширюються загрози, пов'язані з їх доступністю й захищеністю, а самі інформаційно-телекомунікаційні технології стають усе більш руйнівними для людської діяльності. У процесі відстоювання та реалізації стратегічних національних інтересів у кіберпросторі держава повинна приділяти належну увагу, щоб реалізація таких інтересів не порушувала прав і свобод людини й громадянина. Так само приватні суб'єкти діяльності в кіберпросторі повинні враховувати та мінімізувати ризики порушення прав людини в інтернет-просторі й за його

межами. Кожна держава повинна дотримуватися своїх міжнародно-правових зобов'язань у галузі прав людини. Захист прав і свобод користувачів кіберпростору, з одного боку, та додержання користувачами своїх прав, з іншого, мають вирішальне значення для забезпечення стабільності кіберпростору.

Принцип дисципліни. Резолюція Генеральної Асамблеї Організації Об'єднаних Націй від 2018 року «Про відповідальну поведінку держав у кіберпросторі» передбачає загальну вимогу до користувачів кіберпростору. Відповідно до цілей Статуту Організації Об'єднаних Націй, зокрема щодо міжнародного миру та безпеки, держави повинні співпрацювати в розробленні та здійсненні заходів із попереджання вчинення дій у сфері інформаційно-комунікаційних технологій, визнаних шкідливими або здатних створити загрозу міжнародному миру й безпеці. Проте варто зауважити, що така вимога фактично стосується лише урядових організацій та підприємств. Недержавні суб'єкти також можуть здійснювати атаки у відповідь на зловмисників, і подібні дії також можуть підірвати стабільність кіберпростору [84].

Принцип відповідальності. Цей принцип насамперед пов'язаний із децентралізованим характером кіберпростору. Він підтверджує необхідність багатостороннього підходу до забезпечення його стабільності. Очевидно, що поряд із відповідальністю суб'єктів, які відповідають за кіберполітику держави, приватних підприємств та організацій, що є володільцями й розпорядниками інформації в хмарних сервісах, кожна людина тим чи іншим чином залучена до кіберпростору й повинна робити зусилля для захисту своїх електронно-обчислювальних машин та інших девайсів від можливих атак і зломів. Варто наголосити, що навіть люди, які не використовують усі можливості інтернет-мережі, опосередковано можуть залежати від можливостей кіберпростору (послуг, товарів та їх отримання), і тому зацікавлені в належній політиці щодо його охорони.

Кіберпростір – нове місце існування сучасної людини. Незалежно від волі та свідомості кожний є частиною цього середовища, оскільки більшість соціальних взаємодій у сучасному світі відбувається за допомогою інформаційно-комунікаційних технологій, продуктом яких є ця всеосяжна цифрова реальність.

Ґрунтуючись на вищевикладеному, можна зробити такі висновки: поняття «кіберпростору» ширше за поняття «інтернет-простору», але вужче від «інформаційного» та «віртуального простору» і фактично є його частиною. Варто розглядати кіберпростір у трьох аспектах: філософському, легальному й доктринальному. Крім того, в доктринальному аспекті кіберпростір можна розглядати в інформаційному (кіберпростір – це система функціонування децентралізованих інформаційних потоків, створена на основі інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем, учасники якої створюють, поширюють, зберігають інформацію), віртуальному (кіберпростір – це віртуальний простір, який виникає в результаті взаємодії користувачів мережевих технологій) та соціальному (кіберпростір – це соціальний феномен, наповнений людьми, проєкції яких породжені текстовими символами, які взаємодіють між собою у віртуальному середовищі шляхом спроб конструювання цифрової особистості) аспектах. Основними характеристиками кіберпростору є такі: віртуальна складова, мережева належність, середовище взаємодії, динамічність, комунікативність, поєднання територіалізаії та детериторіалізації. Сереж основних принципів, що забезпечують стабільність функціонування кіберпростору, варто виділити принцип своєчасного втручання, принцип додержання прав і свобод людини й громадянина, принцип дисципліни, принцип відповідальності.

1.3. Поняття та ознаки кримінальних правопорушень у кіберпросторі

Сьогодні ми живемо в епоху інформаційного суспільства, у якому інформаційно-телекомунікаційні системи та електронно-обчислювальні машини охоплюють усі сфери життя як окремої людини, так і держав загалом. Люди завжди були вразливими, але XXI ст. поставило виклики перед загрозами не лише в реальному житті, а й у кіберпросторі.

На початку 2018 року було окреслено основні тенденції диджиталізації, зокрема такі: збільшення обсягів цифрового перетворення, використання смарт-технологій і гаджетів, підвищення рівня персоналізації даних, оптимізація виробничих процесів та перехід на роботизовані системи виробництва, розвиток AR-технологій [85].

Диджиталізація суспільства привела до поширення телекомунікаційних, електронних послуг і глобальних комп'ютерних мереж та інтернет-мережі загалом, водночас не передбачаючи потенціалу зловживань, створюваних високими технологіями.

Сьогодні жертвами кримінальних правопорушників у кіберпросторі можуть стати не лише окремі люди, а й цілі країни. Нові технологічні розробки дають змогу зробити життя людей значно комфортнішим, але одночасно спостерігається зворотний процес, за якого з появою нових технологічних досягнень багато хто починає використовувати їх для полегшення кримінально протиправної діяльності. Кількість кримінальних правопорушень у кіберпросторі зростає пропорційно збільшенню користувачів комп'ютерних мереж та Інтернету, а за даними Інтерполу кримінальні правопорушення в кіберпросторі найдинамічніше зростають серед усіх інших видів кримінальних правопорушень [86].

Спостерігаємо, що в XXI ст. інформація стала певним товаром, який одержав реальну вартість, що зумовило розуміння інформації як предмета

посягання. Варто зауважити, що інформація стає товаром саме в умовах товарного виробництва, у яких продукти виробляють із метою продажу на ринку. Щоб стати товаром, інформація повинна бути результатом специфічної конкретної праці, зокрема юридичної, політичної, наукової тощо, водночас маючи здатність до обміну загалом або конкретної частини на інший товар у його матеріальному вигляді чи на його грошовий еквівалент. У рамках кримінальних правопорушень у кіберпросторі такими інформаційними товарами можуть бути як інсайдерська інформація, так і навчання в закритих та приватних чатах кримінально протиправній діяльності в кіберпросторі. Наголошуємо, що складність виявлення й безпосередньо розслідування кримінальних правопорушень у кіберпросторі роблять цю категорію суспільно небезпечних діянь досить привабливою для осіб, які вчиняють кримінальні правопорушення.

Виникнення кримінальних правопорушень у кіберпросторі є неминучим наслідком глобалізації інформаційних процесів, а тому становить головну загрозу соціогуманітарній, національній, економічним складовим. Зростання кількості кримінальних правопорушень у кіберпросторі, постійне вдосконалення інформаційних технологій та нові способи покращання інструментів їх вчинення створюють економічні загрози для глобальних інформаційних мереж [87, с. 122].

Розвиток кримінальних правопорушень у кіберпросторі одночасно відбувається у двох напрямках. З одного боку, щороку з’являються нові види кримінальних правопорушень у кіберпросторі, а з іншого – правопорушники вдало пристосовують електронно-обчислювальні машини для здійснення кримінальних правопорушень у кіберпросторі, відповідальність за які вже передбачена в статтях Особливої частини Кримінального кодексу України, але що є «некомп’ютерними».

Крім того, використання інформаційно-телекомунікаційних систем дає змогу кримінальним правопорушникам ефективно координувати

діяльність злочинної організації, уникаючи завдяки цьому відповідальності за вчинене. Наприклад, у злочинних організаціях, створених в інтернет-мережі, співвиконавці кримінальних правопорушень у кіберпросторі взагалі можуть не мати інформації один про одного, як результат – зменшення ризиків бути викритими. Водночас використання мережевих протоколів зв'язку дає їм змогу ефективно діяти в співучасті для досягнення умислу злочинної організації й виконання всіх протиправних цілей.

Динамічність розвитку кримінальних правопорушень у кіберпросторі зробила їх предметом наукового інтересу багатьох вітчизняних та зарубіжних науковців і спеціалістів. Кримінальні правопорушення в кіберпросторі вивчають із позицій кримінального права, криміналістики, кримінології, кримінального процесу та інших галузей юридичних наук. Розгляд кримінальних правопорушень у кіберпросторі з ракурсу різних наукових концепцій дає певні істотні відмінності в становленні уніфікованого понятійного апарату.

Під час реформування законодавства України до нього було введено нові інститути «правопорушення» та «кримінальний проступок», що в майбутньому змінили підхід до розуміння поняття «злочину» у вітчизняному кримінальному законодавстві.

На законодавчому рівні поняття «кримінального правопорушення» почали вживати ще з часів затвердження Указом Президента України від 8 квітня 2008 року Концепції реформування кримінальної юстиції в Україні. Крім того, концепція надавала визначення поняття «кримінального проступку» як окремого діяння, що відповідно до законодавства про кримінальну відповідальність належить до злочинів невеликої тяжкості, які згідно з політикою гуманізації кримінального законодавства визначаються законодавцем такими, що не мають значного ступеня суспільної небезпеки [88].

Варто зауважити, що зазначена колізія кримінального законодавства виникла ще під час ухвалення Кримінально процесуального кодексу України у 2012 році, але така проблема вирішувалася фактичною відсутністю норм матеріального права, які б регулювали поняття «кримінального проступку» та «кримінального правопорушення».

Отже, учасники кримінально-правових відносин на практиці не застосовували положення, що стосувалося категорії кримінального проступку, керуючись лише нормативними приписами, які регулювали реально наявну в законодавстві про кримінальну відповідальність України категорію злочинів [89, с. 246].

У міжнародних нормативних актах і безпосередньо практиці Європейського суду також вживають термін «кримінальне правопорушення», зокрема Європейська конвенція «Про захист прав людини та основних свобод» від 4 листопада 1950 року, яку Україна ратифікувала 17 липня 1997 року, зазначає, що нікого не може бути визнано винним у вчиненні кримінального правопорушення на підставі будь-якої дії або бездіяльності, яка на час її вчинення не становила кримінального правопорушення за національним правом або міжнародним законодавством [90].

У статті 36 Кримінальної Конвенції «Про боротьбу з корупцію» також використано термін «кримінального правопорушення», але не надано його визначення.

Також зазначимо, що термін «кримінальне правопорушення» вживають у законодавстві іноземних держав, зокрема Іспанії, Італії, але Кримінальні кодекси цих держав лише визначають його види. Виняток становить Кримінальний кодекс штату Канзас, у якому зазначено, що кримінальне правопорушення – це дія або бездіяльність, передбачена законодавством штату, за яку може бути призначено покарання у вигляді позбавлення волі, смертної кари чи штрафу.

Верховна Рада України ухвалила Закон «Про внесення змін до деяких законодавчих актів України щодо спрощення досудового розслідування окремих категорій злочинів від 20 квітня 2018 року № 7279-д «Про внесення змін до Кримінального кодексу України», зокрема щодо кваліфікації кримінальних правопорушень. Цей закон був підписаний Президентом 19 квітня 2019 року, його положення набрали чинності 1 січня 2020 року.

У статті 8 Конституції України закріплено, що в Україні визнається й діє принцип верховенства права, а нормативно-правові акти ухвалюють на основі Конституції України та повинні відповідати їй [91].

Одночасно спостерігаємо колізію в законодавстві про кримінальну відповідальність, у якій закріплено поняття «кримінального правопорушення» та «кримінального проступку», що взагалі не згадані в Конституції України на відміну від злочину. Так само частина 1 статті 3 Кримінального кодексу України визначає, що законодавство України про кримінальну відповідальність становить Кримінальний кодекс України, який ґрунтується на Конституції України й загальновизнаних принципах і нормах міжнародного права, певним чином порушуючи цим принцип системної узгодженості. Зокрема, в Конституції України надана класифікація правопорушень за видами та зазначено, що вони обумовлені винятково законами України. Конституція України виділяє засади цивільно-правової відповідальності, діяння, що визначають як злочини, адміністративні й дисциплінарні правопорушення, та встановлює відповідальність за них.

Стаття 11 Кримінального кодексу України містить поняття «кримінального правопорушення» і розуміє під ним передбачене Законом України про кримінальну відповідальність суспільно небезпечне винне діяння (дію або бездіяльність), вчинене суб’єктом кримінального правопорушення.

З цього визначення поняття «кримінального правопорушення» можна виділити його основні ознаки: суспільна небезпека, протиправність, винність і караність.

Перша з них – суспільна небезпечка. Загалом суспільна небезпека кримінального правопорушення полягає в тому, що воно завдає або створює загрозу заподіяння шкоди охоронюваним законом про кримінальну відповідальність суспільним відносинам. Саме така ознака кримінального правопорушення, як суспільна небезпека, надає йому матеріального характеру, вона закріплюється в законі й набуває юридичного значення.

Суспільну небезпеку діяння як ознаку кримінального правопорушення оцінють на двох рівнях: 1) законодавчому, на якому законодавець криміналізує конкретне суспільно небезпечне діяння; 2) притягнення до відповідальності, за якого орган дізнання, слідчий, прокурор і суддя оцінюють суспільну небезпеку конкретного вчиненого злочину. Тому суспільна небезпека є ціннісним поняттям. Критеріями оцінювання суспільної небезпеки та її ступеня є об'єктивні й суб'єктивні ознаки кримінального правопорушення. Його предмет, наслідки, характер, форма вини, мотив і мета – одні з основоположних категорій кримінального права, тому суспільна небезпека кримінального правопорушення повинна бути вихідною й кінцевою точкою будь-якого кримінального розслідування [92, с. 310].

Суспільна небезпека кримінального правопорушення характеризується двома показниками, а саме: його характером і масштабом. Характер суспільної небезпеки є її якісним критерієм, який залежить від важливості об'єкта кримінального правопорушення. Отже, лише законом про кримінальну відповідальність охороняються основи національної безпеки України, недоторканності приватного життя, миру, безпеки людини, міжнародного правопорядку тощо. Конкретне кримінальне правопорушення

може бути спрямоване проти одного чи кількох охоронюваних кримінальним законом інтересів. Наприклад, у разі протиправного розповсюдження шкідливих програмних засобів, унаслідок якого правопорушник одержав доступ до даних браузера, об'єктом кримінального правопорушення будуть суспільні відносини у сфері нормального функціонування електронно-обчислювальних машин, а в разі подальшого використання даних, що стали відомі особі, яка вчинила кримінальне правопорушення для «кардингу» (розкрадання шляхом використання засобів комп'ютерної інформації), об'єктом також будуть відносини у сфері власності.

Ступінь суспільної небезпеки є кількісним критерієм і визначається ознаками конкретного кримінального правопорушення, зокрема місцем, способом, обставинами його вчинення, наявністю конкретної зброї, ступенем реалізації. Вирішальну роль в оцінюванні ступеня суспільної небезпеки кримінального правопорушення відіграють його наслідки [93].

На думку Ю. Філея, суспільна небезпека – це соціальне явище, легалізація (формалізація) якого є функцією держави. Водночас протиріччя між суспільною небезпекою та кримінальними правопорушеннями може бути наслідком відставання законодавства від вимог життя. Останню тезу автора підтверджує сучасний стан нормативного опису положень розділу VII Особливої частини КК України, у якому часто завуальована законодавцем «формальна» суспільна небезпека закріплюється у відповідних заборонах, не відповідає «реальній небезпеці».» Суспільна небезпека фактично відсутня в об'єктивній дійсності або, навпаки, значно перевищує передбачену зовнішніми ознаками закону, визначеними у відповідних статтях Особливої частини Кримінального кодексу [94, с. 100].

Іншою невід'ємною ознакою кримінального правопорушення, що виражає його внутрішній психологічний зміст, є вина. Ця ознака відображає головний принцип кримінального права – суб'єктивне ставлення, тобто

відповідальність лише за наявності вини, що випливає зі статті 62 Конституції України [91].

Отже, відповідно до положень Конституції вина неодмінно є обов'язковим елементом будь-якого злочину або кримінального проступку, відсутність якого свідчить про відсутність самого складу кримінального правопорушення.

Можна дійти висновку, що вина розглядається законодавцем як психологічна категорія. Одночасно її трактують як категорію соціальну, тому що особа, яка вчиняє злочин, нехтує вимогами суспільства, посягає на його інтереси, завдає істотної шкоди особі, суспільству, державі [95].

Повністю підтримуємо позицію, відповідно до якої емоційний стан є самостійною ознакою суб'єктивної сторони складу кримінального правопорушення, адже, по-перше, без сумніву, не належить до інших факультативних ознак суб'єктивної сторони (мотив, мета) та такої обов'язкової ознаки, як вина, які ми розглянемо далі, а, по-друге, він об'єктивно властивий деяким складам кримінальних правопорушень (наприклад, злочинам, передбаченим ст. 116, 123 КК України) [96, с. 116].

Вину варто обговорювати у двох аспектах. По-перше, як ознаку кримінального правопорушення. По-друге, як складову його суб'єктивної сторони. Водночас необхідно зазначити, що будь-яке суспільно небезпечне діяння є актом добровільної й свідомої поведінки суб'єкта, а свідомість і воля є суб'єктивними критеріями такої поведінки [97, с. 236].

Вина як істотна ознака кримінального правопорушення характеризує його внутрішній психологічний зміст, виявляє психічне ставлення особи до суспільно небезпечного діяння та його наслідків. Ця ознака відображає найважливіший принцип кримінального права – принцип суб'єктивної вини, тобто відповідальності лише за наявності вини. Кримінальним правопорушенням може бути визнано лише діяння, вчинене винно, тому одним зі складів вини є також здатність особи відчувати провину. Крім того,

певний вплив на вину чинить поведінка потерпілого та обставини, що обтяжують або пом'якшують відповідальність. Тобто вину можна визначити як сукупність об'єктивних і суб'єктивних обставин із точки зору їх відображення у свідомості та волі особи, яка вчинила передбачене кримінальним законом діяння [98, с. 350].

Визначення вини містить ст. 23 КК України, у якій проголошено: «Виною є психічне ставлення особи до вчинюваної дії чи бездіяльності, передбаченої цим Кодексом, та її наслідків, виражене у формі умислу або необережності». Цим законодавець обґрунтовує дві можливі форми вини – умисел і необережність, що так само поділяють на окремі види. Водночас будь-який вид провини розглядають крізь призму двох ознак: інтелектуальної й вольової.

Як справедливо наголосив П. Л. Фріс, інтелектуальна ознака вини характеризується усвідомленням особою суспільної небезпеки власної поведінки, що охоплює розуміння суб'єкта злочину, об'єктивної сторони (зокрема часу, місця, обставин, способу, знарядь), а також засобів вчинення злочину, коли ці ознаки були включені як конструктивні до складу конкретного злочину або кримінального правопорушення. У разі вчинення кваліфікованого або привілейованого злочину обставини, що його характеризують, повинні бути вловлені свідомістю особи. У разі вчинення злочинів із матеріальним складом наслідки злочину або кримінального правопорушення також повинні бути усвідомлені особою. Бажана ознака вини визначається як «бажання»: або «свідоме прийняття», або «легковажне очікування запобігти настанню суспільно небезпечних наслідків власних дій». Як можна помітити, сфера волі поширюється винятково на наслідки дій. Водночас різні типи бажаного ставлення до наслідків зумовлюють різні види вини [99, с. 387].

Вольовий момент необережності характеризується тим, що особа або легковажно сподівалася на відвернення суспільно небезпечних наслідків

(кримінально протиправна самовпевненість), або повинна була й могла передбачити суспільно небезпечні наслідки (кримінально протиправна недбалість) [96, с. 116].

Ще однією ознакою кримінального правопорушення є його протиправність. Відповідно до пункту 22 статті 92 Конституції України кримінальна відповідальність діяння визначається лише законами України. Як формальна ознака кримінального правопорушення протиправність є обов'язковою нормою кримінального права, як результат – неможливість застосування Закону «Про кримінальну відповідальність» за аналогією до діяння, не передбаченого в ньому [91].

Водночас багато прихильників такого розуміння протиправності кримінального правопорушення роблять застереження, що вона (протиправність) може бути виражена у двох видах. В. Борисов та О. Пащенко залежно від вираження протиправності в Законі України «Про кримінальну відповідальність» виділяють її два види: 1) пряму кримінальну протиправність, під якою розуміють безпосередню заборону відповідної дії (бездіяльності) Законом «Про кримінальну відповідальність» незалежно від того, чи заборонена вона також нормами інших галузей права; 2) змішану протиправність, якою називають заборону діяння в Законі «Про кримінальну відповідальність» з огляду на те, що воно визнане протиправним нормами іншої галузі права [100, с. 106].

Вважають, що «пряма» («безпосередня», «чиста») кримінальна протиправність може полягати в установленні «кримінально-правової заборони» вчиняти діяння, начебто «не заборонені» жодним іншим, крім кримінального закону, актом законодавства.

З такою ознакою, як протиправність, пов'язана й така обов'язкова ознака кримінального правопорушення, як караність, тобто загроза застосування за вчинення кримінального правопорушення покарання, передбаченого в санкціях до статей Кримінального кодексу України.

Караність, як і протиправність, прямо не зазначена в законодавчому визначенні поняття кримінального правопорушення, а випливає з інших ознак. Ураховуючи той факт, що всі статті Особливої частини Кримінального кодексу України, які визначають діяння як кримінальні правопорушення, одночасно встановлюють покарання за їх вчинення, це є підставою вважати караність обов'язковою ознакою кримінального правопорушення. Крім того, варто зауважити, що караність пов'язана з такими ознаками кримінального правопорушення, як суспільна небезпека, протиправність, винність, і є похідною від них.

Розглянувши загальні ознаки кримінальних правопорушень, пропонуємо зосередити увагу на специфічних, характерних лише для кримінальних правопорушень у кіберпросторі. Зокрема, серед таких ознак, на нашу думку, варто виділити: 1) інтелектуальний характер; 2) анонімність; 3) транснаціональний характер; 4) латентність; 5) простір, у якому вчиняють кримінальні правопорушення; 6) застосування навичок соціальної інженерії; 7) суб'єктна складова; 8) дистанційність; 9) доступність матеріалів, необхідних для їх скоєння.

Надання специфічних характеристик кримінальних правопорушень у кіберпросторі, на нашу думку, доцільно почати саме з інтелектуальної характеристики. Інтелектуальний характер кримінальних правопорушень у кіберпросторі означає, що їх вчинення потребує певного набору як технологіних, так і комунікативних навичок та знань. Крім того, залежно від виду кримінального правопорушення в кіберпросторі особа, яка його вчиняє, може мати ті чи інші специфічні навички. Наприклад, особа, яка здійснює кібершахрайство, повинна гарно володіти навичками соціальної інженерії, а особа, яка створює та розповсюджує віруси, – навичками програмування для створення небезпечного програмного забезпечення й навичками маркетингу для його збуту.

Наступною ознакою, що потрібно охарактеризувати, є анонімність. Анонімність як ознака кримінального правопорушення в кіберпросторі дає змогу особі, яка вчинила кримінальне правопорушення, видавати себе за іншу особистість, змінювати біографічні дані про себе, свій соціальний статус або загалом залишатися інкогніто. Варто зауважити, що можливість використання чужих даних, неправдивої інформації або взагалі «нікнеймів» створює в кримінального правопорушника певне відчуття безкарності, оскільки ідентифікувати його надзвичайно складно. На нашу думку, саме анонімність як ознака кримінального правопорушення в кіберпросторі підштовхує користувачів інтернет-мережі до початку кримінально протиправної діяльності в кіберпросторі. Крім того, як уже було зазначено, у користувачів створюється атмосфера вседозволеності діяльності в кібернетичному просторі.

Ще однією ознакою кримінального правопорушення в кіберпросторі є їх транснаціональний характер. Він означає, що фактично така кримінально протиправна діяльність може посягати одночасно на велику кількість жертв, які перебувають у різних куточках світу. Варто акцентувати увагу, що 60 % кримінальних правопорушень у кіберпросторі вчиняють організовані групи, учасники яких є громадянами різних держав і які перебувають на території різних країн. Сама така ознака, як транснаціональність, робить кримінальні правопорушення в кіберпросторі фактично недосяжними для правоохоронних органів різних держав світу саме на рівні локальної протидії їм. На нашу думку, варто зазначити, що, незважаючи на транскордонність кіберпростіру, не всі кримінальні правопорушення в ньому транснаціональні. Наприклад, якщо кримінальний правопорушник і жертва живуть в одній країні.

Кримінальні правопорушення в кіберпросторі наразі є одним із найбільш латентних видів кримінальних правопорушень серед усіх інших. Насамперед це зумовлено самим фактом не звернення осіб, які стали

жертвами кримінальних правопорушень у кіберпросторі, до правоохоронних органів, уповноважених розслідувати зазначений вид кримінальних правопорушень. Також як один із визначальних факторів латентності кримінальних правопорушень у кіберпросторі варто виділити те, що жертви навіть не розуміють, що щодо них скоїли кримінальне правопорушення. Наприклад, у разі поширення вірусних програм або шкідливого програмного забезпечення жертва може ніколи не помітити некоректності роботи свого персонального комп'ютера, а в разі викрадення даних із веббраузера (реквізитів банківських карт) – не здогадається про скоєне доти, доки такі реквізити не будуть використані кримінальним правопорушником. Також не можна не наголосити на тому, що велика частка осіб, які стали жертвами кримінальних правопорушень у кіберпросторі, одночасно хотіли придбати в особи, що вчиняє кримінальне правопорушення, заборонені товари, послуги, документи чи інформацію, тим самим скоївши протиправне діяння. Зокрема, часто самі кредитні організації, банки, сервіси електронних переказів і магазини електронної комерції не повідомляють про скоєння кримінальних правопорушень щодо них самих, щоб уберегти свою репутацію. Причиною високої латентності серед кримінальних правопорушень у кіберпросторі можна вважати також те, що збитки від них часто здаються незначними порівняно з витратами, необхідними для їх розслідування. Здебільшого процедура розслідування кримінальних правопорушень у кіберпросторі потребує дуже багато часу, а водночас гарантій притягнути особу до відповідальності за скоєне немає.

Як було зазначено в розділі 1.3, кіберпростір – це певне віртуальне середовище діяльності, сформоване з безлічі каналів зв'язку, електронно-телекомунікаційних пристроїв, інформаційно-телекомунікаційних мереж, що дають безпосередній доступ до кіберпростору. Саме простір, у якому вчиняють кримінальне правопорушення, є однією з його основних ознак. На нашу думку,

обмежувати кримінальні правопорушення в кіберпросторі певними гаджетами, інтернет-мережею або комп'ютером не правильно, оскільки особа, яка вчиняє кримінальне правопорушення, використовує у своїй діяльності різноманітні інформаційно-телекомунікаційні мережі й технології для доступу до кібернетичного простору. Як результат – можемо наголосити, що кіберпростір є обов'язковим фактором скоєння кримінального правопорушення.

Наступною ознакою наведених кримінальних правопорушень є застосування навичок соціальної інженерії для вчинення фактично половини кримінально протиправних діянь у кіберпросторі. Соціальна інженерія – це вид атаки, що спирається на взаємодію людей, часто супроводжується маніпулюванням ними з порушенням нормальної процедури безпеки та є передовою практикою з метою одержання доступу до систем, мереж або фінансової вигоди [101].

Така ознака, як суб'єктивна складова, характеризується зниженим віком осіб, які скоюють кримінальні правопорушення в кіберпросторі. Варто зазначити, що це наслідок того, що, по-перше, кримінальні правопорушення в кіберпросторі – дуже прибуткова форма зайнятості, а, по-друге, інформація щодо їх скоєння є у вільному доступі.

Дистанційність кримінальних правопорушень у кіберпросторі як одна з основних специфічних ознак передбачає певну зміну психологічної взаємодії між самим правопорушником і кримінальним правопорушенням та відносини між правопорушником і жертвою. Якщо в разі вчинення традиційних кримінальних правопорушень спостерігається прямий зв'язок між жертвою й особою, яка вчинила кримінальне правопорушення, то в разі вчинення кримінальних правопорушень у кіберпросторі такий зв'язок стає опосередкованим. Замість системи «особа, яка вчинила кримінальне правопорушення» – «жертва», маємо іншу конструкцію, а саме: «особа, яка вчинила кримінальне правопорушення» – «кіберпростір» – «жертва»; як

результат – повне невелювання матеріального аспекту діяльності кримінального правопорушника та взаємодії з жертвою.

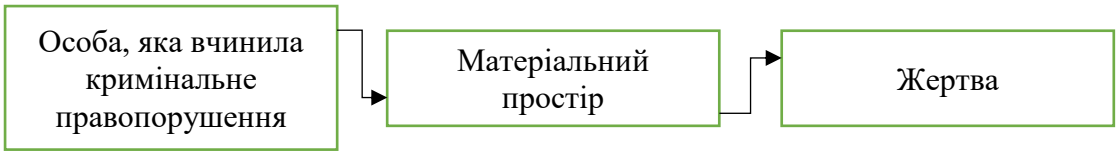

Рисунок 2 – Традиційна модель вчинення кримінального правопорушення

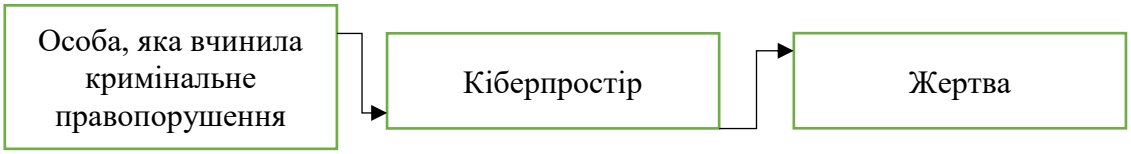

Рисунок 3 – Модель вчинення кримінального правопорушення в кіберпросторі

Д. Валл зазначає, що особа, яка вчинила кримінальне правопорушення в кіберпросторі, не бачить свою жертву під час вчинення правопорушення, тому не може помітити матеріальних наслідків скоєного. На думку вченого, це призводить до зниження відчуття відповідальності за скоєне кримінальне правопорушення, з огляду на яке він не може усвідомити серйозності правопорушення [102].

Крім того, зауважимо, що відповідно до досліджень Массачусетського технологічного інституту кримінальні правопорушники в разі незаконного поширення чи використання інформації або інформаційних продуктів здебільшого психологічно не сприймають свої дії як кримінально протиправні, оскільки мова йде про нематеріальні блага, що, на думку кримінальних правопорушників, не завдає вагомих матеріальних збитків [103].

Зловмисники, які мають спеціальні знання про комп'ютерні мережі, можуть викрасти декілька мільйонів у банківському секторі, розвернути супутник на 180°, вимкнути систему життєзабезпечення пацієнтів у лікарні, перебуваючи в будь-якому куточку світу й залишаючись непоміченими [104].

Доступність матеріалів, необхідних для скоєння кримінального правопорушення в кіберпросторі, – ще одна його ознака. Наразі є кілька форумів, на яких розміщена як платна, так і безкоштовна інформація щодо того, як вчиняти окремі кримінальні правопорушення в кіберпросторі (кардинг, фішинг, скамінг). Крім того, на таких ресурсах можна знайти інформацію щодо створення окремого програмного забезпечення для подальшої кримінально протиправної діяльності.

Сьогодні одним із найдискусійніших як у доктринальних джерелах, так і на законодавчому рівні є питання, що врешті-решт являє собою кримінальне правопорушення в кіберпросторі. Варто зауважити, що в доктринальних вітчизняних джерелах наразі немає єдиної точки зору щодо цього питання. На нашу думку, основна проблема полягає в недосконалості чинного кримінального законодавства, у якому не передбачені регламентація й нормативна база відповідальності за кримінальні правопорушення в кіберпросторі. Водночас у чинному Кримінальному кодексі України закріплена лише певна обмежена група кримінальних правопорушень у кіберпросторі, для яких використовують поняття «кримінальні правопорушення у сфері використання електронно-обчислювальних машин, систем та комп'ютерних мереж і мереж електрозв'язку».

Поняття кримінального правопорушення в кіберпросторі нерідко ототожнюють із комп'ютерним кримінальним правопорушенням, кримінальним правопорушенням у сфері комп'ютерної інформації, цифровими кримінальними правопорушеннями та кримінальними

правопорушеннями з використанням інформаційно-комунікаційних технологій, тому що їх об'єднує використання комп'ютерної техніки.

Легальне визначення кримінального правопорушення в кіберпросторі містить Закон України «Про основні засади забезпечення кібербезпеки України». У зазначеному законі використовують поняття «кіберзлочин (комп'ютерний злочин)», що трактують як суспільно небезпечне винне діяння в кіберпросторі та/або з його використанням, відповідальність за яке передбачена Законом України «Про кримінальну відповідальність» та/або яке визнано злочином міжнародними договорами України [56].

Зауважимо, що в зазначеному законі поряд із поняттям «кіберзлочин» у дужках наведено «комп'ютерний злочин». Цей закон був ухвалений з урахуванням зауважень науково-експертного та юридичного управлінь Апарату Верховної Ради України, які не заперечують можливості введення нової термінології в національне правове поле. Проте її потрібно вводити комплексно й узгоджувати з чинним законодавством. Зокрема, наголошено на необхідності визначення співвідношення понять «комп'ютерні злочини» та «кіберзлочини». Також поняття «кіберзлочин» повинне бути узгодженим із термінологією Кримінального кодексу України, у якому є окремий розділ XVI «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку», та іншими актами законодавства, у яких установлене поняття «комп'ютерного злочину» [105, с. 53].

Як уже зазначено, з 1 січня 2020 року набрав чинності Закон України «Про внесення змін до деяких законодавчих актів України щодо спрощення досудового розслідування окремих категорій злочинів», у якому було запроваджено поняття «кримінального правопорушення», а отже, необхідне узгодження інших нормативно-правових актів із положеннями Кримінального кодексу України, зокрема Закону України «Про основні

засади забезпечення кібербезпеки України». Тому вважаємо доцільним вживання терміна «кримінальне правопорушення в кіберпросторі».

Проблема кримінальних правопорушень у кіберпросторі в останні роки набула істотного як наукового, так і практичного значення, що зумовлено передусім розвитком інформаційно-телекомунікаційних систем та їх широким рівнем упровадження в повсякденне життя суспільства. Насьогодні сфера правопорушень у кіберпросторі не є достатньо дослідженою й урегульованою на законодавчому рівні, як наслідок – багато країн застосовують аналогію закону для правового регулювання кримінальних правопорушень у кіберпросторі та адаптування їх складу до складу інших кримінальних правопорушень. Наприклад, Кримінальний кодекс Індії пов’язує та прирівнює до кримінальних правопорушень у кіберпросторі крадіжку, шахрайство й підробку документів із використанням електронно-обчислювальних машин [106].

Кримінальні правопорушення в кіберпросторі – досить широке коло кримінальних правопорушень, що налічує більше ніж 100 кримінально протиправних діянь, вчинених у кіберпросторі. В Україні, як зазначено, є правове регулювання кримінальних правопорушень у кіберпросторі, але воно не може врегулювати ці питання в повному обсязі. Також на законодавчому рівні залишається законодавчо незакріпленим поняття кримінального проступку в кіберпросторі, що має велике значення для розуміння законодавства в зазначеній сфері й проведення процесу тлумачення.

Не всі кримінальні правопорушення є злочинами, а отже, не всі кримінальні правопорушення в кіберпросторі є кіберзлочинами. Зважаючи на це, на нашу думку, варто розмежовувати такі поняття, як «кіберзлочин» і «кіберпроступок».

Водночас потребує уваги питання дослідження та визначення категорії кримінальних правопорушень у кіберпросторі в законодавстві

інших держав. Пропонуємо розглянути систему кримінальних правопорушень, що передбачають кримінальну відповідальність за кримінально протиправні діяння в кіберпросторі країн англо-американської, романо-германської правових сімей та пострадянських країн, до яких близький за структурою Кримінальний кодекс України.

Зокрема, в Кримінальному кодексі Вірменії главою XXV визначені «злочини проти безпеки комп'ютерної інформації», що охоплюють сім видів суспільно небезпечних діянь у кіберпросторі. Крім того, статтею 181 «Крадіжка, здійснена за допомогою комп'ютерної техніки» визначено кримінальне правопорушення в кіберпросторі, фактично наведене в розділі «Злочини проти власності» [107].

Кримінальний кодекс Грузії визначає систему кримінальних правопорушень у кіберпросторі як «кіберзлочини», глава XXXV охоплює п'ять суспільно небезпечних діянь у кіберпросторі. Варто зауважити, що в примітках до Кримінального кодексу Грузії в разі кваліфікації кримінального правопорушення за статтею 324 «Кібертероризм» обов'язковим є додаткова кваліфікація за статтями 284–286 цього кодексу [108].

Таку саму назву розділу має глава XXX Кримінального кодексу Азербайджану [109].

У главі XIII Кримінального кодексу Туркменістану ця категорія кримінальних правопорушень визначається як «злочини у сфері комп'ютерної інформації». Варто звернути увагу, що до цього розділу входять кримінальні правопорушення, що відповідно до їх безпосереднього об'єкта посягання не належать до кримінальних правопорушень у кіберпросторі, сам кіберпростір є лише місцем вчинення злочину, а сам комп'ютер – засобом вчинення кримінального правопорушення. Зокрема, «надання послуг із розміщення інтернет-ресурсів із незаконними цілями» та «розповсюдження завідомо сфальсифікованої інформації» [110].

Подібно визначена досліджувана система кримінальних правопорушень у Кримінальному кодексі Естонії – «Злочини у сфері комп'ютерної інформації та оброблення даних». Варто зауважити, що таке кримінальне правопорушення, як «комп'ютерне шахрайство», законодавство Естонії класифікує не до кримінальних правопорушень проти власності, а саме до правопорушень у кіберпросторі [111].

У Кримінальному кодексі Литовської Республіки система кримінальних правопорушень у кіберпросторі згідно з главою XXX визначається як «злочини проти інформатики». У Кримінальному Законі Латвії немає окремого розділу, у якому було б розглянуто й визначено систему кримінальних правопорушень у кіберпросторі, самі кримінальні правопорушення в кіберпросторі наведені в розділі XX під назвою «кримінальні правопорушення проти безпеки та громадського порядку» [112]

На відміну від розглянутих вище систем кримінальних правопорушень у кіберпросторі, що не мають насильницького характеру, Кримінальний кодекс Республіки Таджикистан у главі XX-1 «Злочини у сфері інформаційних технологій» у частині 3 статті 301 «Незаконне заволодіння комп'ютерною інформацією» містить кваліфікаційну ознаку «якщо таке діяння вчинено заподіянням насилля» [113].

Якщо розглядати країни романо-германської правової сім'ї, то варто зауважити, що система кримінальних правопорушень у кіберпросторі не виділена в окремі розділи взагалі. Зокрема, в Кримінальному кодексі Німеччини [115] зазначені правопорушення знаходяться в розділі XV «Порушення недоторканності приватного життя та приватних таємниць». У Кримінальному кодексі Австрії є лише дві статті, за які особа несе відповідальність у кіберпросторі: 263 «Комп'ютерне шахрайство» та 303 «Комп'ютерний саботаж» [114]. Така сама ситуація спостерігається в Кримінальному кодексі Португалії, у якому визначений лише один вид

кримінального правопорушення в кіберпросторі – стаття 193 «Зловживання комп'ютером» [116]. Кримінальне законодавство Іспанії не є винятком і також не виділяє кримінальні правопорушення в кіберпросторі в окремий розділ, але на відміну від вищезгаданих країн у багатьох статтях Кримінального кодексу Іспанії вчинення кримінального правопорушення за допомогою комп'ютера використовують як кваліфікаційну ознаку [117].

Країни англо-саксонської правової сім'ї, зокрема Сполучені Штати Америки та Великобританія, закріпили систему кримінальних правопорушень у кіберпросторі у своїх нормативно-правових актах. Зокрема, у Зводі законів Сполучених Штатів Америки № 1030 Титул 18 «Шахрайство та пов'язана з ним діяльність у зв'язку з комп'ютерами» установлено відповідальність, предметом посягання якої є «комп'ютерна інформація». Водночас у законі виокремлено такі види кримінальних правопорушень у кіберпросторі: 1) несанкціонований доступ особи до комп'ютерної мережі іззовні; 2) перевищення рівня доступу до одержання інформації з комп'ютерної мережі, здійснене особою без повноважень; 3) комп'ютерне шпигунство, яке полягає в несанкціонованому доступі до інформації, що стосується національної безпеки держави, питань атомної енергетики й міжнародних відносин; 4) шахрайство з використанням комп'ютера; 5) несанкціоноване втручання в роботу комп'ютерної системи, що перебуває у винятковому користуванні урядового відомства Сполучених Штатів Америки або порушення її функціонування; 6) умисне чи необережне пошкодження захищеної комп'ютерної мережі; 7) шахрайство шляхом торгівлі інформацією, що дає змогу одержати несанкціонований доступ, якщо така торгівля впливає на торговельні відносини між штатами; 8) вимагання, погрози, шантаж, вчинені з використанням електронно-обчислювальної техніки [118].

Основним законом Сполученого Королівства, що визначає та регламентує кримінальну відповідальність за кримінальні правопорушення

в кіберпросторі, є Закон «Про неправомірне використання комп'ютерних технологій», ухвалений у 1990 р. Він спрямований безпосередньо на неналежне використання комп'ютерних технологій.

У зазначеному законі виділено п'ять видів кримінальних правопорушень у кіберпросторі: 1) несанкціонований доступ до комп'ютерних матеріалів; 2) несанкціонований доступ із метою вчинення або сприяння вчиненню подальших правопорушень; 3) несанкціоновані дії з наміром зашкодити або з необережності порушити роботу комп'ютера тощо; 4) несанкціоновані дії, що спричиняють або створюють ризик серйозної шкоди; 5) виготовлення, постачання або отримання предметів для використання в кримінальному правопорушенні, передбаченому розділами 1–3 [119].

Спостерігаємо, що в більшості пострадянських держав система кримінальних правопорушень у кіберпросторі визначається так: злочини проти інформаційних технологій, кіберзлочини, злочини проти комп'ютерної інформації та злочини проти інформаційної безпеки. Здебільшого законодавець виділяє таку систему в окремі розділи закону про кримінальну відповідальність.

На противагу пострадянським країнам держави романо-германської правової сім'ї у своїх кримінальних законодавствах не виділяють кримінальні правопорушення в кіберпросторі в окремий розділ.

Відповідно до результатів аналізу кримінального законодавства Сполучених Штатів Америки та Великобританії про кримінальні правопорушення в кіберпросторі варто зазначити, що англо-саксонська правова система є більш гнучкою й максимально відповідає потребам часу. У своїх нормативних актах вона визначає широкий перелік видів кримінальних правопорушень у кіберпросторі, зазвичай поділених за предметом посягання або засобом вчинення кримінального правопорушення.

На сьогодні в доктринальних джерелах немає єдиного підходу до розуміння поняття кримінального правопорушення в кіберпросторі. Одні науковці вважають поняття «кримінальне правопорушення в кіберпросторі» та «комп'ютерне кримінальне правопорушення» синонімічними, інші визначають зазначені поняття як подібні, але не синонімічні. Водночас одні науковці вважають термін «комп'ютерне кримінальне правопорушення» ширшим за «кримінальне правопорушення в кіберпросторі», а інші, навпаки, що кримінальні правопорушення в кіберпросторі охоплюють комп'ютерні кримінальні правопорушення як один зі своїх видів.

Д. Азаров та А. Музика наголошують, що значна кількість науковців відмовляються від розроблення теоретичного поняття кримінальних правопорушень у кіберпросторі, а фахівці в галузі кримінального права під час розроблення рекомендацій щодо протидії комп'ютерним кримінальним правопорушенням обмежуються лише переліком протиправних посягань, за яких комп'ютерна техніка є знаряддям вчинення кримінального правопорушення [120, с. 176].

Пропонуємо розглянути такі підходи до розуміння специфіки поняття «кримінальне правопорушення в кіберпросторі»: 1) поняття «кримінальне правопорушення в кіберпросторі» вужче за поняття «комп'ютерне кримінальне правопорушення» та поняття «кримінальне правопорушення у сфері комп'ютерної інформації»; 2) поняття «кримінальне правопорушення в кіберпросторі», «комп'ютерне кримінальне правопорушення» та «кримінальне правопорушення у сфері комп'ютерної інформації» є тотожними; 3) поняття «кримінальне правопорушення в кіберпросторі» ширше за «комп'ютерне кримінальне правопорушення» та «кримінальне правопорушення у сфері комп'ютерної інформації»; 4) поняття «кримінальне правопорушення в кіберпросторі» з точки зору криміналістичної позиції.

Згідно з першим підходом М. Карчевський зазначає, що поняття «кримінальне правопорушення в кіберпросторі» та «комп'ютерне кримінальне правопорушення» можуть бути ефективно використані під час проведення кримінологічних, кримінально процесуальних і криміналістичних досліджень. Водночас він пропонує вживати поняття «кримінальне правопорушення у сфері використання інформаційних технологій» і визначає його як один із видів кримінальних правопорушень у сфері комп'ютерного кримінального правопорушення, передбачених Кримінальним кодексом України: суспільно небезпечне, винне, вчинене суб'єктом кримінального правопорушення діяння, що заподіює шкоду забезпеченим засобам обчислювальної техніки, відносинам у сфері реалізації інформаційної потреби. Ми не погоджуємося з думкою М. Карчевського, оскільки згідно з його визначенням поняття «комп'ютерні кримінальні правопорушення» ширше за «кримінальні правопорушення в кіберпросторі», але містять у собі винятково передбачені в Кримінальному кодексі України статті, що входять до розділу XVI Особливої частини Кримінального кодексу України. Основним об'єктом посягання вбачаються відносини у сфері інформаційної безпеки, з одного боку, та визначення інформаційних технологій як предмета кримінального правопорушення – з іншого. Проте, базуючись на такому розумінні, маємо, що крадіжка, вчинена в кіберпросторі, не шкодить суспільним відносинам у сфері реалізації інформаційної потреби й не вчиняється за допомогою засобів електронно-обчислювальної техніки [121, с. 12].

І. Васильківський трактує кримінальне правопорушення в кіберпросторі як правопорушення, пов'язане з використанням кібернетичних комп'ютерних систем і вчинене в кіберпросторі. Крім того, він зазначає, що поняття «комп'ютерне кримінальне правопорушення» ширше за «кримінальне правопорушення в кіберпросторі», оскільки таке кримінальне правопорушення вчиняється в кібернетичному середовищі,

яке, на думку автора, є вужчим за змістом від комп'ютерного середовища, не надаючи поняття «комп'ютерного кримінального правопорушення».

Водночас І. Васильковський виділяє обмежений перелік кримінальних правопорушень у кіберпросторі: несанкціоноване одержання прав контролю над такою системою (наприклад, використання шкідливого програмного забезпечення, фальсифікація інформації про стан об'єкта в зворотному каналі, фальсифікація керування сигналу в прямому каналі зв'язку тощо) та її нерегламентоване використання (наприклад, із метою спричинення аварії на виробництві, дезорганізації діяльності підприємства тощо), а також створення й використання кібернетичної комп'ютерної системи в злочинних цілях проти інших осіб (наприклад, створення мережі комп'ютерів-ботів), щоб здійснювати атаки на вебсайти, створювати неавторизовану робочу станцію в системі електронних переказів коштів тощо). Проте переліку «комп'ютерних кримінальних правопорушень» І. Васильковський не наводить [122, с. 199].

Ми не можемо погодитися з позицією автора, оскільки, на нашу думку, кримінальні правопорушення в кіберпросторі охоплюють одночасно як кіберзалежні кримінальні правопорушення, передбачені розділом XVI Особливої частини Кримінального Кодексу, так і ті традиційні кримінальні правопорушення, що внаслідок використання цифрових пристроїв, інформаційно-телекомунікаційних мереж і систем перейшли в площину кіберпростору.

А. Ставер визначає кримінальне правопорушення в кіберпросторі як суспільно небезпечне діяння, що походить від комп'ютерного кримінального правопорушення, здійснюється з використанням технологій перетворення інформації, репрезентованої у вигляді комп'ютерних даних, і тягне за собою юридичну відповідальність. На думку автора, кримінальне правопорушення в кіберпросторі має всі загальні ознаки кримінального правопорушення, виділені в Законі України «Про кримінальну

відповідальність», а відрізняється від нього лише факультативними ознаками, за якими кіберпростір є засобом або метою вчинення кримінального правопорушення. Ураховуючи, що юридична відповідальність може бути як кримінальною, так і цивільною й адміністративною, у позиції автора залишається незрозумілим, які саме діяння належать до кримінальних правопорушень у кіберпросторі. Відповідно до частини 2 статті 11 Кримінального кодексу України не є кримінальним правопорушенням дія або бездіяльність, що хоча формально містить ознаки будь-якого діяння, передбаченого цим Кодексом, але через малозначущість не становить суспільної небезпеки, тобто не заподіяла й не могла заподіяти істотної шкоди фізичній чи юридичній особі, суспільству або державі. Ураховуючи зазначене, можна дійти висновку, що крадіжку за частиною першою статті 185, вчинену на суму 150 грн, не вважатимуть ані кіберзлочином, ані кіберпроступком, але шахрайство за частиною 3 статті 190, вчинене на 150 грн, буде кваліфіковано як кримінальне правопорушення в кіберпросторі, зокрема кіберзлочин, і особа нестиме покарання у вигляді позбавлення волі від 3 до 8 років [123, с. 145].

Цікаву думку наводить М. Простосердов, який зазначає, що комп'ютерні кримінальні правопорушення можуть бути вчинені як у матеріальному середовищі, так і в кіберпросторі, що робить їх вужчим поняттям за комп'ютерні кримінальні правопорушення. На нашу думку, кримінальні правопорушення в кіберпросторі мають певні специфічні ознаки й відрізняються від інших кримінальних правопорушень підвищеним рівнем суспільної небезпеки, вони можуть бути спрямовані на будь-які суспільні відносини: як у сфері нормального обороту комп'ютерної інформації, так і на відносини у сфері власності або економічної діяльності. Водночас сам комп'ютер як предмет чи засіб вчинення кримінального правопорушення може не бути використаний [124, с. 106].

О. Амелін надає визначення, найбільш наближене до легального, з доповненням щодо раціоналізації проблеми саме у сфері інформаційних відносин: «комп'ютерне кримінальне правопорушення – суспільно небезпечне, протиправне, кримінально каране, винне діяння, яке завдає шкоди інформаційним відносинам, засобом забезпечення нормального функціонування яких є електронно-обчислювальні машини, автоматизовані системи, комп'ютерні мережі або мережі електрозв'язку» [125, с. 8].

Підтримує подібне бачення С. Буз, зокрема під кримінальним правопорушенням у кіберпросторі він розуміє будь-яке суспільно небезпечне діяння, скоєне за допомогою інформаційних технологій або в інформаційному просторі» [126, с. 80].

Ця дефініція не враховує того, що поле дії кримінальних правопорушень у кіберпросторі не зупиняється винятково в інформаційній сфері. Зокрема, у Німеччині кібератака на медичний госпіталь призвела до зупинки необхідного обладнання на тиждень і смерті пацієнта [127].

Подібне бачення в А. Мохамеда: «На нашу думку, це поняття можна визначити як сукупність кримінальних правоворушень, що здійснюються за допомогою ІКТ (інформаційно-комунікаційних технологій)» [128, с. 71].

Акцентуємо увагу на тому, що науковці, розглядаючи питання кримінально-правової охорони кіберпростору, наголошують, що поняття «кримінальне правопорушення в кіберпросторі» є синонімічним до поняття «кримінальне правопорушення у сфері комп'ютерної інформації». Ми не погоджуємося з таким ототожненням, оскільки кримінальні правопорушення у сфері комп'ютерної інформації є підтипом кримінальних правопорушень у сфері обігу цифрової інформації, який так само належить до системи кримінальних правопорушень у кіберпросторі [120].

На думку В. Болгова, вислів «кримінальні правопорушення, що вчиняються з використанням інформаційних технологій» є не дуже зручним

для вживання в побутовій мові, тому науковець визнає доцільним короткий термін «кіберзлочини», тим паче, що об'єктом цієї категорії правопорушень є інформація та тісно пов'язані з нею технології її оброблення – інформаційні технології [129, с. 122].

Аналізуючи інший підхід до розуміння поняття «кримінальне правопорушення в кіберпросторі», підкреслимо, що В. Вехов наводить таке його визначення: передбачене кримінальним законом суспільно небезпечне діяння, вчинене з використанням електронно-обчислювальної техніки (комп'ютерів). Водночас не має значення, на якому етапі вчинення кримінального правопорушення було застосовано цей прийом: під час підготовки, у процесі вчинення чи приховування слідів. На нашу думку, такий підхід є дещо універсальним, і фактична підготовка й приховування слідів вчинення кримінального правопорушення за допомогою електронно-обчислювальної техніки можуть бути застосовані до будь-якого кримінального правопорушення, зазначеного в особливій частині Кримінального кодексу України, що робить усі кримінальні правопорушення кіберзлочинами та кіберпроступками залежно від використання такої техніки [130, с. 13].

О. Довженко визначає кримінальне правопорушення в кіберпросторі у двох підходах. Відповідно до першого підходу ним є будь-яке протиправне діяння, скоєне за допомогою комп'ютерної техніки. Зокрема, до таких кримінальних правопорушень він класифікує зберігання чи поширення інформації шляхом використання комп'ютерних технологій, тобто науковець пов'язує кримінальні правопорушення в кіберпросторі з правопорушеннями, вчинюваними в електронних мережах. Відповідно до другого підходу кримінальними правопорушеннями в кіберпросторі є протиправні, винні діяння, що вчиняють за допомогою комп'ютерного й мобільного зв'язку в інтернет-мережі [131, с. 81].

В. Бєлєнький визначає кримінальне правопорушення в кіберпросторі як винне, суспільно небезпечне, кримінально каране втручання у сферу безпеки обігу комп'ютерної інформації, роботу комп'ютерів, комп'ютерних програм, комп'ютерних мереж, несанкціоновану модифікацію комп'ютерних даних та інші протиправні суспільно небезпечні діяння, вчинені за допомогою комп'ютерів, комп'ютерних мереж і програм, а також за допомогою інших пристроїв з убудованими процесорами й контролерами, що можуть мати доступ до інформаційного простору [132].

Ми підтримуємо такий підхід до трактування поняття кримінального правопорушення в кіберпросторі та погоджуємося, що під ознаки цього поняття підпадають будь-які кримінальні правопорушення, вчинені з використанням електронно-обчислювальних машин або в кібернетичному середовищі, зокрема шпигунство, наклеп, крадіжка, державна зрада, терористичний акт, вимагання, шахрайство та ін. Водночас вважаємо потрібним виокремити підвид кримінальних правопорушень у кіберпросторі – «кримінальні правопорушення у сфері комп'ютерної інформації», зазначивши, що вони охоплюють вужче коло кримінальних правопорушень, зокрема такі: неправомірне використання комп'ютерної інформації; створення, використання й розповсюдження шкідливих комп'ютерних програм; порушення правил експлуатації засобів зберігання, оброблення або передавання комп'ютерної інформації та інформаційно-телекомунікаційних мереж, тобто фактично всі кримінальні правопорушення, передбачені розділом XVI Особливої частини Кримінального кодексу України.

Інше за змістом визначення було надане Р. Сабілліоном: суспільно небезпечне діяння, вчинюване з використанням засобів комп'ютерної техніки щодо інформації, оброблюваної й використовуваної в інтернет-мережі. На нашу думку, таке визначення, навпаки, надто вузьке, оскільки, по-перше, крім Інтернету, є багато глобальних мереж, що

фактично формують кібернетичний простір, а, по-друге, у кіберпросторі вчиняють кримінальні правопорушення, предметом та об'єктом посягання яких є не лише інформація, а й інші суспільні відносини (власність, честь, гідність, національна безпека тощо) [133].

Прихильники третього підходу зазначають, що «кримінальне правопорушення» є ширшим за «комп'ютерне кримінальне правопорушення» та «кримінальне правопорушення у сфері комп'ютерної інформації». Зокрема, О. Користін вважає, що термін «комп'ютерне кримінальне правопорушення» вужчий за своїм значенням і зводить кримінальні правопорушення до вчинюваних лише за допомогою комп'ютера.

Ю. Бельський тлумачить кіберзлочини як злочини, що вчиняються в процесі автоматизованого оброблення інформації за допомогою електронно-обчислювальних машин або через комп'ютерні системи, об'єктом посягання яких є суспільні відносини у сфері обігу електронної інформації, та інші суспільні відносини, у яких комп'ютер є кваліфікаційною ознакою вчинення злочину (наприклад, комп'ютерне шахрайство або кібертероризм) [134, с. 415].

Доволі цікаво визначає «кримінальне правопорушення в кіберпросторі» І. Васильковський, а саме: «Кіберзлочинність (або «злочин із використанням комп'ютерних технологій») – це економічне кримінальне правопорушення, скоєне з використанням обчислювальної техніки та мережі Інтернет» [23, с. 278]. Проте негативні наслідки вчинення кіберзлочину не завжди мають економічний характер [135, с. 280].

Н. Савчук дає таке визначення «кіберзлочинності» (англ. cybercrime): це поняття, що охоплює комп'ютерну злочинність (у якій комп'ютер – предмет кримінального правопорушення, а інформаційна безпека – об'єкт кримінального правопорушення) та інші посягання, у яких комп'ютер є

знаряддям або способом кримінального правопорушення проти власності, авторських прав, громадської безпеки, моралі тощо [136, с. 339].

К. Тарасюк під «кіберзлочинами» розуміє суспільно небезпечні діяння, так чи інакше пов'язані з кіберпростором і комп'ютерною інформацією, модельованою комп'ютерами. Він виділяє такі ознаки кіберзлочинів: висока латентність, складність виявлення й розслідування, складність доказування в суді подібних справ, транснаціональна складова (здебільшого з використанням інформаційної мережі Інтернет), високий збиток навіть від одиничного кримінального правопорушення [137, с. 180].

Т. Тропіна пропонує визначати кримінальне правопорушення в кіберпросторі як винне, суспільно небезпечне, кримінально каране втручання в роботу комп'ютерів, комп'ютерних програм, комп'ютерних мереж, несанкціоновану модифікацію комп'ютерних даних, а також інші протиправні суспільно небезпечні діяння, вчинені за допомогою комп'ютерів, комп'ютерних програм, комп'ютерних мереж та інших засобів доступу [138, с. 130].

Звернімо увагу, що науковець оперує саме термінами «комп'ютер» і «комп'ютерна інформація», але предметом та засобом вчинення кримінальних правопорушень, зокрема кіберзалежних, може бути також інша цифрова інформація, крім комп'ютерної, а засобом вчинення – будь-які цифрові пристрої.

Д. Уолл пропонує таке визначення: «кримінальне правопорушення в кіберпросторі – це дія або шкідлива діяльність, що є інформаційною, глобальною та мережевою, і його варто відрізняти від кримінальних правопорушень, у яких просто використовують комп'ютери». Кримінальні правопорушення в кіберпросторі є продуктом мережевих технологій, що перетворили поділ кримінально протиправної праці на створення абсолютно нових можливостей і нових форм злочинності, які зазвичай передбачають збирання чи маніпулювання інформацією та її цінністю в

глобальних мережах із метою отримання прибутку. Їх можна поділити на такі: 1) кримінальні правопорушення, пов'язані з цілісністю системи; 2) кримінальні правопорушення, у яких мережеві комп'ютери використовуються для сприяння вчиненню кримінальному правопорушенню; 3) кримінальні правопорушення, що стосуються саме комп'ютерів [139].

Словник термінів із кібербезпеки за редакцією О. Копана надає два визначення поняття кримінального правопорушення в кіберпросторі. Водночас автори поділяють кримінальні правопорушення в кіберпросторі на комп'ютерні й кібернетичні.

1. Кримінальне правопорушення в кіберпросторі (комп'ютерне кримінальне правопорушення) – протиправне втручання в роботу кібернетичних систем, основною правлячою ланкою яких є комп'ютер (наприклад, спотворення інформації про стан об'єкта в каналі зворотного шкідливого програмного забезпечення тощо), створення та використання в злочинних цілях певної кібернетичної (комп'ютерної) системи, використання в злочинних цілях кібернетичних (комп'ютерних) систем (наприклад, комп'ютерних чи телекомунікаційних мереж у шахрайстві, вимаганні тощо).

2. Кримінальне правопорушення в кіберпросторі (кібернетичне кримінальне правопорушення) – кримінальне правопорушення, пов'язане з використанням кібернетичних комп'ютерних систем, і кримінальне правопорушення в кіберпросторі [140].

Д. Гальдер та К. Джайшанкар визначають кримінальні правопорушення в кіберпросторі як правопорушення, вчинені проти окремих осіб або груп осіб із кримінально протиправним мотивом навмисно заподіяти шкоду репутації жертви, завдати потерпілому фізичної чи психічної шкоди або втрати прямо чи опосередковано, використовуючи

сучасні телекомунікаційні мережі, такі як Інтернет (різні онлайн-месенджери) та мобільні телефони (SMS / MMS) [141].

Професор Ф. Ахмед дав три визначення поняттю «кримінальне правопорушення в кіберпросторі»: 1) будь-яка протиправна дія, у якій комп'ютер є інструментом чи об'єктом кримінального правопорушення, тобто будь-яке кримінальне правопорушення, засіб чи мета якого полягає у впливі на функціонування комп'ютера; 2) будь-який інцидент, пов'язаний із комп'ютерними технологіями, під час якого постраждала жертва або хтось міг зазнати збитків, а кримінальний правопорушник умисно одержав або міг би одержати вигоду; 3) зловживання комп'ютером розглядається як будь-яка протиправна, неетична чи несанкціонована поведінка, пов'язана з автоматичним обробленням та передаванням даних [142; 143, с. 341].

Так само А. Русецький та Д. Куцолабський пропонують під кримінальним правопорушенням у кіберпросторі розуміти протиправне винне діяння, що передбачає втручання в дані персональних комп'ютерів, комп'ютерних програм і комп'ютерних мереж, або діяння, вчинене за допомогою комп'ютерів, за яке передбачається кримінальна відповідальність і яке може створити особисту небезпеку громадянинові, загрозу національній безпеці держави й світовій безпеці [144, с. 75].

На нашу думку, таке визначення поняття «кримінальне правопорушення в кіберпросторі» хоча й розкриває природу зазначеного виду кримінального правопорушення, але є надто широким і неточним. Зокрема, можна дійти висновку, що до «діянь, вчинених за допомогою комп'ютера» належать такі кримінальні правопорушення, за яких комп'ютер було використано не за своїм фактичним призначенням. Наприклад, ним було нанесено удар по голові, наслідок якого – тілесне ушкодження середньої тяжкості. Водночас варто зауважити, що в кримінальних правопорушеннях у кіберпросторі різні об'єкти посягання, різні способи вчинення, різні предмети посягання й безпосередньо різні

рівні використання електронно-обчислювальних машин, як результат – різні рівні суспільної небезпеки.

На думку В. Болгова, кримінальне правопорушення в кіберпросторі – це сукупність передбачених чинним законодавством кримінально караних суспільно небезпечних діянь (дій чи бездіяльності), що посягають на право захисту від несанкціонованого поширення й використання інформації, негативних наслідків впливу інформації чи функціонування інформаційних технологій, а також інші суспільно небезпечні діяння, пов’язані з порушенням права власності на інформацію та інформаційні технології, права власників або користувачів інформаційних технологій вчасно одержувати або поширювати достовірну й повну інформацію. Ця дефініція є більш наближеною до легальної та доповнює її в сенсі виділення такої специфічної ознаки, як негативний наслідок кримінального правопорушення в кіберпросторі [129, с. 129].

Дещо подібне визначення за своїми ознаками дає О. Сіренко: «кримінальне правопорушення в кіберпросторі – це суспільно небезпечне діяння, що вчиняється за допомогою або через комп’ютерні системи, посягає на право захисту від несанкціонованого поширення й використання інформації, негативних наслідків впливу інформації чи функціонування інформаційних технологій, а також інші суспільно небезпечні діяння, пов’язані з порушенням права власності на інформацію та інформаційні технології, права власників або користувачів інформаційних технологій вчасно одержувати або поширювати достовірну й повну інформацію і за які передбачено кримінальну відповідальність» [145, с. 48].

Як ми зазначали, в науковій доктрині немає єдиної думки щодо поняття кримінального правопорушення в кіберпросторі. На наш погляд, найбільш вдалим є поділ кримінальних правопорушень у кіберпросторі на «кіберзлочини» й «кіберпроступки» залежно від їх суспільної небезпеки та шкоди, що вони завдають суспільству й державі.

А. Завршник наголошує, що кримінальні правопорушення в кіберпросторі є найбільш широким поняттям, яке визначає сутність і зміст зазначених діянь. До таких діянь, на думку дослідника, належать усі кримінальні правопорушення, вчинювані з використанням комп'ютера або інтернет-мережі, через публічні домашні та приватні мережеві зв'язки [146]. Тому можемо констатувати той факт, що поняття «кримінальні правопорушення в кіберпросторі» є ширшим за своїм змістом, ніж «кримінальні правопорушення у сфері комп'ютерної інформації» та «комп'ютерні кримінальні правопорушення». І як акцентує увагу О. Столяр, попри наявні альтернативні дефініції («комп'ютерний злочин», «злочин у сфері високих технологій», «комунікаційний злочин», «злочин у сфері комп'ютерної інформації», «мережевий злочин») саме термін «кримінальне правопорушення в кіберпросторі», що є або «кіберпроступком», або «кіберзлочином», найбільше відображає суть зазначеного явища [147, с. 186].

Зважаючи на це, ми можемо стверджувати, що саме найменування «кримінальне правопорушення в кіберпросторі» є найбільш вдалим і доволі об'ємно розкриває сутність явища подібного виду злочинності. Проаналізувавши доктринальні джерела вітчизняних та зарубіжних учених, можемо стверджувати, що на сьогодні в юридичній науці простежується дихотомія доктринальних і легальних дефініцій. Науковці по-різному трактують поняття «кримінальне правопорушення в кіберпросторі» та відповідно виділяють різні специфічні особливості (ознаки) таких правопорушень. Найбільш вдало, хоча й не повністю, на наш погляд, специфіку кримінальних правопорушень у кіберпросторі розкриває саме законодавче визначення, зазначене в Законі України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року № 2163-VIII. Проте, зауважимо, що це тлумачення не виділяє всіх фундаментальних ознак «кіберзлочинів» і «кіберпроступків».

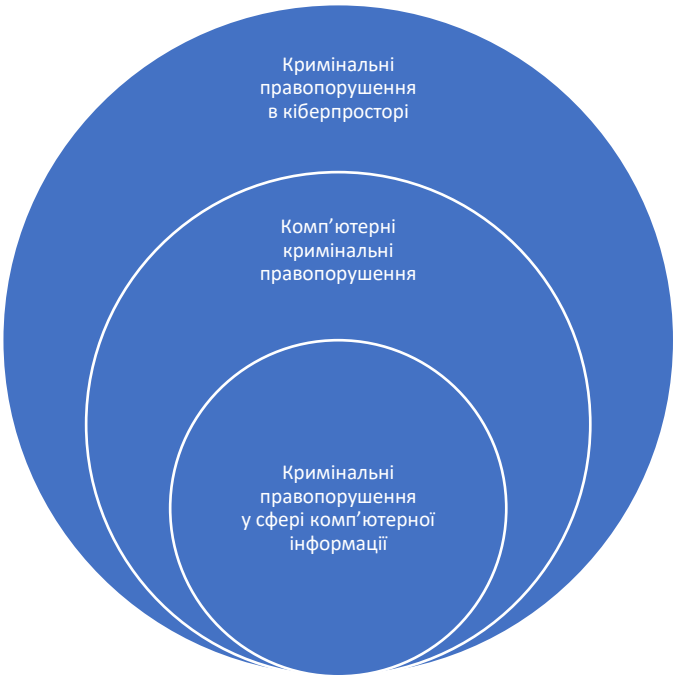

Рисунок 4 – Розмежування понять «кримінальні правопорушення в кіберпросторі», «комп'ютерні кримінальні правопорушення» та «кримінальні правопорушення у сфері комп'ютерної інформації»

На рисунку 4 можна помітити, що виділяють такі кримінальні правопорушення:

– скоєні з використанням кіберпростору, але що не є «комп'ютерними кримінальними правопорушеннями» та «кримінальними правопорушеннями у сфері комп'ютерної інформації», наприклад скоєні з використанням засобів високих технологій (СМС-шахрайство (фішинг) із використанням телефонів);

– скоєні з використанням кіберпростору, що є «кримінальними правопорушеннями у сфері комп'ютерної інформації» та «комп'ютерними кримінальними правопорушеннями» (порушення правил експлуатації засобів зберігання, оброблення чи передавання комп'ютерної інформації);

– скоєні з використанням кіберпростору, що є «кримінальними правопорушеннями у сфері комп'ютерної інформації», але не є

«комп'ютерними кримінальними правопорушеннями» (вимагання в соціальній мережі з використанням смартфона);

– скоєні з використанням кіберпростору, що є «комп'ютерними кримінальними правопорушеннями», але не є «кримінальними правопорушеннями у сфері комп'ютерної інформації» (DDoS-атаки на вебресурси).

На нашу думку, варто проаналізувати визначення дефініції поняття «кримінального правопорушення в кіберпросторі» з криміналістичної позиції. Різноманіття підходів до розуміння цього явища було проаналізовано В. А. Дуленко, Р. Р. Мамлеєвим і В. А. Пестриковим. Вони вважають, що кримінальні правопорушення в кіберпросторі в широкому сенсі – це будь-які протиправні діяння, здійснювані за допомогою або в зв'язку з комп'ютерними пристроями, зокрема такі злочини, як незаконне зберігання, пропонування або поширення інформації за допомогою комп'ютерних технологій [148].

Інші вчені класифікують кримінальні правопорушення в кіберпросторі до протиправних діянь, здійснюваних за допомогою комп'ютерного й мобільного (стільникового) зв'язків у мережах.

На думку І. Чекунова, кримінальними правопорушеннями в кіберпросторі є суспільно небезпечні діяння, вчинені з використанням засобів і способів комп'ютерної та мобільної (стільникової) техніки, їх програмних компонентів щодо інформації, розміщеної, використовуваної, оброблюваної, змінюваної у віртуальному просторі мережі Інтернет [149, с. 15].

Так само В. Курушин і В. Мінаєв вважають, що кримінальні правопорушення в кіберпросторі – це дії в Інтернеті, за яких комп'ютер є або знаряддям, або предметом кримінальних посягань у віртуальному просторі [150, с. 18].

Будучи обізнаними зі значними прогалинами в законодавстві, яке регламентує відносини в кіберпросторі, керівник кафедри ЮНЕСКО з авторського права та інших галузей права інтелектуальної власності М. Яцишин наголошує, що правопорушники в деяких випадках навмисно вибирають цю «територію», щоб загубитися в ній та уникнути відповідальності. Фактично кримінально протиправні діяння, «породжені» новими інформаційними й телекомунікаційними технологіями, – банальна крадіжка, замасковані вандалізм, плагіат, «піратство» щодо інтелектуальної власності, ухилення від виплати авторської винагороди [151, с. 24].

Пізнаючи кіберпростір із позицій криміналістики, виділимо найважливішу методологічну специфіку цієї науки: вона досліджує будь-які предмети матеріального й ідеального макро- та мікросвіту. Іншими словами, склад виконуваних завдань під час дослідження кіберпростору й кіберзлочинів обумовлений нескінченною різноманітністю слідчо-судових та експертних ситуацій, тому методологічний потенціал вивчення віртуальної злочинності з обов'язковою необхідністю повинен втілити в собі все багатство загальнонаукового й спеціального криміналістичних знань.

Узагальнення різних аспектів здійснення релігійної та розслідування віртуальної злочинності, досліджуваних багатьма авторами, дає змогу говорити про те, що кіберпростір необхідно пізнавати через сферу взаємопроникнення й взаємодії в ракурсі системного підходу у вигляді об'єкта як складного явища, утворюваного з елементів, зв'язки між якими становлять його порівняно незмінну структуру та забезпечують його цілісність.

Отже, відповідно до проаналізованих легальних і доктринальних визначень поняття «кримінальне правопорушення в кіберпросторі» та запропонованих його специфічних ознак пропонуємо таке визначення

кримінального правопорушення в кіберпросторі: суспільно небезпечне, протиправне, винне, каране діяння, що посягає та заподіює шкоду різним суспільним відносинам шляхом використання інформаційно-телекомунікаційних технологій, інформаційно-телекомунікаційних мереж і створюваного ними кіберпростору.

Підбиваючи підсумки, варто констатувати: поняття «кримінальне правопорушення в кіберпросторі» надано в Законі України «Про основні засади забезпечення кібербезпеки в Україні» як «кіберзлочин». Одночасно в цьому законі визначено його ототожнення з «комп'ютерним кримінальним правопорушенням», що спричинило колізії в законодавстві та порушення принципу системної узгодженості.

Сьогодні серед науковців немає єдиної точки зору щодо дефініції зазначеного поняття, що зумовлено недосконалістю чинного кримінального законодавства, у якому фактично відсутні регламентація та нормативна база відповідальності за кримінальні правопорушення в кіберпросторі. Окреслено, що поняття «кримінальне правопорушення в кіберпросторі» не тотожне поняттям «комп'ютерне кримінальне правопорушення» та «кримінальне правопорушення у сфері комп'ютерної інформації», а вони є його підтипом.

До основних характеристик кримінальних правопорушень у кіберпросторі належать такі: 1) інтелектуальний характер та анонімність; 2) транснаціональність; 3) латентність; 4) застовування навичок соціальної інженерії; 5) суб'єктна складова; 6) дистанційність; 7) доступність матеріалів, необхідних для їх скоєння.

Загалом під кримінальним правопорушенням у кіберпросторі ми розуміємо суспільно небезпечне, протиправне, винне, каране діяння, що посягає й шкодить різним суспільним відносинам шляхом використання інформаційно-телекомунікаційних технологій, інформаційно-телекомунікаційних систем і мереж та створюваного ними кіберпростору.

РОЗДІЛ 2.
КРИМІНАЛЬНО-ПРАВОВА ХАРАКТЕРИСТИКА КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ У КІБЕРПРОСТОРІ

2.1. Теоретико-прикладні аспекти типологізації кримінальних правопорушень у кіберпросторі

Після дослідження поняття, сутності «кримінальних правопорушень у кіберпросторі» наступним кроком вбачаємо визначення їх типологізаційних підстав і видів.

Будь-яка сфера людської діяльності, будь-яка система знань потребує внутрішньої структурної впорядкованості, без якої неможливо організувати складний процес, розробити методологію наукових досліджень, побудувати навчальний процес. Необхідного порядку можна досягти шляхом типологізації.

Типологізація є одним із найпоширеніших методів правової інженерії, застосовуваних ученими-юристами для встановлення істини під час вивчення правових явищ, правових рішень чи виконання інших наукових завдань. Проблема типологізації є складною та багатошаровою, тому її можна розглядати в різних аспектах (економічному, філософському, правовому). Проблема побудови й використання типологізації особливо загострилася в період сучасної науково-технічної революції, що призвела до інформаційного вибуху. Велика кількість і недосконала організація нових понять та термінів, друкованих і неопублікованих матеріалів ускладнюють пошук та використання необхідних даних, що спричинює дефіцит інформації, який уповільнює суспільний прогрес. Розроблення оптимальної типологізації стає одним із найважливіших завдань сучасної науки кримінального права [152, с. 21].

Правова типологізація кримінальних правопорушень має важливе значення для вирішення низки питань, пов'язаних із розмежуванням кримінальної відповідальності, визначенням обсягу обмежень, застосовуваних до осіб, які вчинили кримінальне правопорушення, правильною кваліфікацією, індивідуалізацією кримінальної відповідальності й застосуванням звільнення від покарання та відбування покарання, а також низкою інших кримінально-правових інститутів. Можна наголосити, що виокремлення типологізаційних норм за відповідними критеріями шляхом аналізу Особливої частини Кримінального кодексу України дає змогу чітко зрозуміти, які саме кримінальні правопорушення є кримінальними проступками, а які – злочинами, а також визначити їх переважну видову належність.

Ефективність розслідування кримінальних правопорушень у кіберпросторі значно залежить від виду та обсягу інформації, що є в розпорядженні слідчого на його початкових етапах розслідування. З огляду на предмет нашого дослідження такою інформаційною базою очевидно є розгляд кримінально-правової типологізації кримінальних правопорушень у кіберпросторі.

На нашу думку, варто почати з визначення поняття й сутності тупологізації в її загальноприйнятому розумінні. Під типологізацією потрібно розуміти певний поділ понять, явищ, предметів на певні групи за певними ознаками, що в подальшому полегшує процес їх систематизації. Водночас необхідно зауважити, що власне систематизації піддається вся сукупність накопичених знань у галузі кримінального права та створення власної системи типологізації кримінально-правових понять.

Погоджуємося з думкою А. Яковенко, яка зазначає, що за допомогою типологізації можна одержати загальне уявлення про групу досліджуваних явищ, охарактеризувати окремий об'єкт із виділеного кола явищ, визначити ступінь взаємозв'язку окремих видів і, як результат, на цій основі виділити

певні закономірності таких взаємозв'язків, а також передбачити можливості розвитку явищ в тому чи іншому напрямку [153, с. 246].

Кримінальна правова типологізація кримінальних правопорушень є своєрідним шляхом до пізнання об'єкта кримінального правопорушення, невід'ємним засобом визначення його сутності, дає змогу розпізнати закономірності, необхідні для його наукового обґрунтування та опису. Варто зауважити, що кримінально-правова типологізація набуває найбільш практичного й безпосереднього застосування в діяльності органів прокуратури та суду, забезпечує правильне розуміння суті досліджуваних справ, грамотну побудову й вибір застосування слідчим методик розслідування окремих видів кримінальних правопорушень у кіберпросторі.

Дуже неоднозначними є підходи до сутності та побудови типологізації кримінальних правопорушень. Зокрема, одні дослідники під кримінально-правовою типологізацією розуміють поділ багатьох предметів, явищ, відношень, властивостей, ознак тощо на окремі групи за тими чи іншими ознаками; другі визначають типологізацію об'єктів на групи за подібністю елементів усередині кожної групи та їх відмінністю від об'єктів інших груп; треті розуміють під типологізацією певну систему підпорядкованих понять (класів, предметів, ознак) [154, с. 244].

Проте ці судження фактично об'єднані двома ідеями: типологізація або систематизація об'єктів на групи, класи й види; визначення результату цієї процедури.

Як зазначає М. Люликова, типологізація найчастіше здійснюється в нашій уяві, а сам поділ на групи, класи та об'єкти не є випадковим групуванням, одночасно потрібно застосовувати принципи діалектичної логіки й правило поділу поняття. Очевидно, що для здійснення процесу кримінально-правової типологізації необхідно визначити її об'єкти. Автор зазначає, що об'єкт кримінально-правової типологізації – думка, що

відображає суттєві ознаки самого об’єкта чи явища, що є предметом зазначеної типологізації [155].

Відповідно до позиції Д. Стітіліса об’єктами кримінально-правової типологізації є певні групи кримінальних правопорушень, що характеризуються відповідними кримінально-криміналістичними поняттями, які в подальшому поділяють на взаємозв’язані підгрупи для цілей слідчої й криміналістичної практик [156, с. 61].

Дещо ширше об’єкт кримінально-правової типологізації визначає В. Антипов. Зокрема, як певну сукупність кримінальних правопорушень, що характеризується відповідною сукупністю кримінально-правових, кримінально-процесуальних і криміналістичних ознак, поділених на взаємозв’язані частини [157, с. 333].

Водночас О. Дудоров вважає, що під час типологізації кримінальних правопорушень у методиці їх розслідування потрібно керуватися не стільки кримінально-правовими ознаками, скільки кримінологічними залежно від способу їх вчинення [158, с. 86].

З таким підходом погоджується Н. Ахтирська, яка стверджує, що «кримінальне правопорушення як предмет типологізаційного дослідження в кримінології не вичерпується лише його кримінально-правовим значенням». Предметом судового дослідження є саме кримінальне правопорушення як конкретна подія з ознаками кримінального правопорушення, що має особливу структуру й характеризується специфічними закономірностями механізму її здійснення [159, с. 88].

Отже, з вищенаведеного можна зробити висновок, що кримінально-правова типологізація базується на симбіозі криміналістичних і кримінально-правових особливостей.

Виконання низки завдань у процесі кваліфікування кримінальних правопорушень у кіберпросторі було б дуже проблематичним без правильної кримінально-правової типологізації. Зростання статистики й

видова різноманітність кримінальних правопорушень у кіберпросторі потребують її систематизації з різних причин.

Варто акцентувати увагу, що в доктринальних джерелах підходи до типологізації кримінальних правопорушень у кіберпросторі є досить загальними, але водночас відображають специфіку цього виду кримінальних правопорушень. Ми зупинимося на тих підходах, що, на нашу думку, точніше відображають структуру кримінальних правопорушень у кіберпросторі. Більшість науковців типологізує до кримінальних правопорушень у кіберпросторі лише кримінальні правопорушення, передбачені розділом XVI Особливої частини Кримінального кодексу України.

Отже, щодо типологізації кримінальних правопорушень у кіберпросторі можна дійти висновку, що більшість дослідників, які вивчають проблему кіберзлочинності, пропонує поділяти їх на види залежно від об'єкта й предмета посягання. Зокрема, В. Хахановський виділяє два типи кримінальних правопорушень у кіберпросторі:

– нові злочини, що стали можливими завдяки новітнім комп'ютерним технологіям (злочини, передбачені розділом XVI Кримінального кодексу України);

– традиційні злочини, вчинювані за допомогою комп'ютерних технологій та Інтернету [160, с. 101].

Так само В. Г. Кундеус зазначає, що залежно від об'єкта посягання кримінальні правопорушення в кіберпросторі можна класифікувати за такими видами:

1) кримінальні правопорушення, вчинені в кіберпросторі та/або з його використанням, відповідальність за які передбачена різними розділами Кримінального кодексу України. Такі кримінальні правопорушення посягають на різні об'єкти кримінально-правової охорони: основи національної безпеки, громадську безпеку, відносини у сфері охорони права

на об’єкти інтелектуальної власності, власність, господарські відносини, права й свободи тощо. Ознакою типологізації цих кримінальних правопорушень до кримінальних правопорушень у кіберпросторі, на думку науковця, є те, що їх вчиняють із використанням сучасних інформаційних технологій і засобів комп’ютерної техніки;

2) злочини у сфері використання електронно-обчислювальних машин (комп’ютерів), систем і комп’ютерних мереж, передбачені розділом XVI Кримінального кодексу України [161, с. 45].

О. Користін пропонує типологізувати кримінальні правопорушення в кіберпросторі на такі: 1) насильницькі чи інші потенційно небезпечні кримінальні правопорушення в кіберпросторі; 2) ненасильницькі кримінальні правопорушення в кіберпросторі. Зокрема, до першої групи належать такі кримінальні правопорушення в кіберпросторі, як кібертероризм, погроза фізичної розправи в мережі Інтернет, кіберпереслідування, кіберсталкінг, дитяча порнографія. До другої групи він типологізує кіберкрадіжки, кібершахрайства, кібершпигунство, розповсюдження спаму й вірусних програм [162, с. 455].

Н. Міщук також переконаний, що кримінальні правопорушення в кіберпросторі потрібно типологізувати відповідно до об’єкта посягання. Він виділяє такі групи кримінальних правопорушень у кіберпросторі: 1) кримінальні правопорушення проти конфіденційності, цілісності та доступності комп’ютерних даних і комп’ютерних мереж; 2) економічні комп’ютерні кримінальні правопорушення; 3) комп’ютерні кримінальні правопорушення проти особистих прав та недоторканності приватної сфери; 4) комп’ютерні кримінальні правопорушення проти суспільних і державних інтересів [163, с. 176].

В. Голіна у своїх кримінологічних наукових працях визначає, що кримінальні правопорушення в кіберпросторі можуть бути агресивними й неагресивними. До агресивних автор класифікує кримінальні

правопорушення, у яких основним об’єктом посягання є життя, честь і гідність особи, нормальний моральний стан та розвиток дитини, а до неагресивних – склади кримінальних правопорушень у сфері власності, господарської діяльності [164, с. 388].

Однією з найбільш цікавих типологізацій кримінальних правопорушень у кіберпросторі є типологізація, запропонована В. Дзюндзюком: 1) кримінальні правопорушення проти конституційних прав і свобод людини й громадянина, такі як порушення недоторканності приватного житла, порушення таємниці листування, телефонних переговорів, поштових, телеграфних та інших повідомлень, порушення авторських і суміжних прав; 2) кримінальні правопорушення проти життя й здоров’я; 3) кримінальні правопорушення проти честі та гідності особи; 4) кримінальні правопорушення проти власності; 5) кримінальні правопорушення у сфері комп’ютерної інформації, такі як неправомірний доступ до інформації, створення, використання й розповсюдження шкідливих програм; 6) кримінальні правопорушення проти суспільної моральності; 7) кримінальні правопорушення проти безпеки держави [165].

А. Русецький вважає, що найпоширенішими видами кримінальних правопорушень у світі є такі: 1) кардинг; 2) вішинг; 3) фішинг; 4) онлайн-шахрайство; 5) кард-шаринг; 6) кіберпіратство; 7) мальваре; 8) соціальна інженерія; 9) рефайлінг [166, с. 75].

С. Баджаг у своїй науковій праці «Цифрове шахрайство» визначив такий поділ кримінальних правопорушень у кіберпросторі: 1) насильницькі або інші потенційно небезпечні суспільно небезпечні дії, що посягають на життя та здоров’я людини; 2) суспільно небезпечні дії, які порушують конфіденційність даних (незаконна модифікація, знищення, передавання, розкриття інформації); 3) суспільно небезпечні дії, що порушують цілісність даних; 4) суспільно небезпечні дії у сфері охорони права власності; 5) суспільно небезпечні дії, які посягають на моральність

громадськості; 6) суспільно небезпечні дії, що посягають на громадську безпеку [167, с. 148].

Shailendra Singh пропонує типологізацію кримінальних правопорушень у кіберпросторі залежно від характеру використання електронно-обчислювальної техніки: 1) електронно-обчислювальну техніку використовують як засіб вчинення кримінального правопорушення; 2) електронно-обчислювальна техніка є предметом кримінального правопорушення [168, с. 5].

S. Altowaijri виділяє два типи кримінальних правопорушеннь у кіберпросторі: 1) кримінальні правопорушення в кіберпросторі, пов'язані з втручанням у роботу електронно-обчислювальної техніки; 2) кримінальні правопорушення, у яких електронно-обчислювальна техніка є засобом для скоєння кримінально протиправного діяння [169].

Не можна оминути типологізацію кримінальних правопорушень у кіберпросторі на основі кодифікатора, розроблену ще в 1990-х роках Інтерполом: 1) QA – несанкціонований доступ і перехоплення (QAH – комп'ютерний саботаж; 2) QAI – перехоплення за допомогою спеціальних технічних засобів; 3) QAT – крадіжка часу (ухилення від плати за користування); 4) QAZ – інші види несанкціонованого доступу та перехоплення; 5) QD – зміна комп'ютерних даних (QDL – логічна бомба; QDT – троянський кінь; QDV – комп'ютерний вірус; QDW – комп'ютерний черв'як; QDZ – інші види зміни даних); 6) QF – комп'ютерне шахрайство (QFC – шахрайство з банкоматами; QFF – комп'ютерна підробка; QFG – шахрайство з ігровими автоматами; QFM – маніпуляції з програмами введення – виведення; QFP – шахрайство з платіжними засобами; QFT – телефонне шахрайство; QFZ – інші комп'ютерні шахрайства); 7) QR – незаконне копіювання (QRG – комп'ютерні ігри; QRS – інше програмне забезпечення; QRT – топологія напівпровідникових пристроїв; QRZ – інше незаконне копіювання); 8) QS – комп'ютерний саботаж (QSH – з апаратним

забезпеченням (порушення роботи ЕОМ); QSS – із програмним забезпеченням (знищення, блокування інформації); QZ – інші комп'ютерні злочини, зокрема QZB – із використанням комп'ютерних дошок оголошень); 9) QZE – розкрадання інформації, що становить комерційну таємницю (QZS – передавання інформації, що підлягає судовому розгляду; QZZ – інші комп'ютерні злочини) [170].

Проаналізувавши доктринальні підходи до типологізації кримінальних правопорушень у кіберпросторі, дослідивши їх сутнісну характеристику, пропонуємо перейти до авторських підстав типологізації. На нашу думку, найважливішою підставою типологізації кримінальних правопорушень у кіберпросторі є їх поділ відповідно до статті 12 Кримінального кодексу України на кримінальні проступки та злочини [14]. У подальшому в праці пропонуємо використовувати поняття кіберпроступку й кіберзлочину. Аналіз особливої частини Кримінального кодексу України та загальна суспільна небезпечність кримінальних правопорушень у кіберпросторі дають змогу зробити висновок, що переважна частина всіх кримінальних правопорушень досліджуваного виду є саме кіберзлочинами. Така ситуація зумовлена насамперед суспільною небезпечністю такого діяння й швидкою динамікою його поширення. Згідно з Кримінальним кодексом України до кіберпроступків належать такі кримінальні правопорушення в кіберпросторі: 1) порушення рівноправності громадян залежно від їх расової, національної, регіональної належності, релігійних переконань, інвалідності та за іншими ознаками (стаття 161 Кримінального кодексу України); 2) порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передається засобами зв'язку або через комп'ютер (стаття 163 Кримінального кодексу України); 3) розголошення таємниці усиновлення (удочеріння) (стаття 168 Кримінального кодексу України); 4) порушення авторського права й суміжних прав (стаття 176 Кримінального кодексу

України); 5) порушення недоторканності приватного життя (стаття 182 Кримінального кодексу України); 6) незаконне використання інсайдерської інформації (стаття 232-1 Кримінального кодексу України); 7) заклики до вчинення дій, що загрожують громадському порядку (стаття 295 Кримінального кодексу України); 8) увезення, виготовлення або розповсюдження творів, що пропагують культ насильства й жорстокості, расову, національну чи релігійну нетерпимість та дискримінацію (стаття 300 Кримінального кодексу України).

Так само до кіберзлочинів варто типологізувати такі кримінальні правопорушення в кіберпросторі, як: 1) державна зрада (стаття 111 Кримінального кодексу України); 2) колабораційна діяльність (стаття 111-1 Кримінального кодексу України); 3) пособництво державі-агресору (стаття 111-2 Кримінального кодексу України); 4) шпигунство (стаття 114 Кримінального кодексу України); 5) несанкціоноване поширення інформації про направлення, переміщення зброї, озброєння та бойових припасів в Україну, рух, переміщення або розміщення Збройних Сил України чи інших утворених відповідно до законів України військових формувань, вчинене в умовах воєнного або надзвичайного стану (стаття 114-2 Кримінального кодексу України); 6) торгівля людьми (стаття 149 Кримінального кодексу України); 7) розбещення неповнолітніх (стаття 156 Кримінального кодексу України); 8) крадіжка (стаття 185 Кримінального кодексу України); 9) вимагання (стаття 189 Кримінального кодексу України); 10) шахрайство (стаття 190 Кримінального кодексу України); 11) заподіяння майнової шкоди шляхом обману або зловживання довірою (стаття 192 Кримінального кодексу України); 12) незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, електронними грошима, обладнанням для їх виготовлення (стаття 200 Кримінального кодексу України); 13) легалізація (відмивання) майна, одержаного злочинним шляхом (стаття 209

Кримінального кодексу України); 14) створення, керівництво злочинною спільнотою або злочинною організацією, а також участь у ній (стаття 255 Кримінального кодексу України); 15) терористичний акт (стаття 258 Кримінального кодексу України); 16) фінансування тероризму (стаття 258-5 Кримінального кодексу України); 17) сутенерство або втягнення особи в заняття проституцією (стаття 303 Кримінального кодексу України); 18) незаконне виробництво, виготовлення, придбання, зберігання, перевезення, пересилання чи збут наркотичних засобів, психотропних речовин або їх аналогів (стаття 307 Кримінального кодексу України); 19) викрадення, привласнення, вимагання прекурсорів або заволодіння ними шляхом шахрайства або зловживання службовим становищем (в частині збуту через Інтернет) (стаття 312 Кримінального кодексу України); 20) незаконне втручання в роботу автоматизованої системи документообігу суду (стаття 376 Кримінального кодексу України); 21) пропаганда війни (стаття 436 Кримінального кодексу України); 21) виготовлення, поширення комуністичної, нацистської символіки й пропаганда комуністичного та націонал-соціалістичного (нацистського) тоталітарних режимів (стаття 436-1 Кримінального кодексу України); 22) виправдовування, визнання правомірною, заперечення збройної агресії Російської Федерації проти України, глорифікація її учасників (стаття 436-2 Кримінального кодексу України); 23) несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж (стаття 361 Кримінального кодексу України); 24) створення з метою протиправного використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут (стаття 361 Кримінального кодексу України); 25) несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп’ютерах), автоматизованих

системах, комп'ютерних мережах або на носіях такої інформації (стаття 361 Кримінального кодексу України); 26) несанкціоновані дії з інформацією, що оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї (стаття 362 Кримінального кодексу України); 27) порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, що в них оброблюється (стаття 363 Кримінального кодексу України); 28) перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку (стаття 363 Кримінального кодексу України) [14].

Варто зазначити, що більшість кримінальних правопорушень у кіберпросторі є кіберпроступками лише за першою частиної відповідної статті Особливої частини Кримінального кодексу України.

Структура розділів Особливої частини Кримінального кодексу України повністю обумовлена об'єктом кримінальних правопорушень. Тому іншою підставою для типологізації кримінальних правопорушень у кіберпросторі ми вбачаємо родовий об'єкт складу кримінального правопорушення. Незважаючи на наукові дискусії, в чинному Кримінальному кодексі України немає розділу, який би повністю регулював питання кримінальної відповідальності за кримінальні правопорушення в кіберпрострі, а самі кримінальні правопорушення зазначеної групи входять до різних складів кримінальних правопорушень.

Відповідно до цієї підстави першим різновидом кримінальних правопорушень у кіберпросторі є кіберзлочини проти основ національної безпеки України (ст. 111, 111-1, 111-2, 114, 114-2 Кримінального кодексу

України). Ще десять років тому про групу злочинів проти національної безпеки України, вчинюваних із використанням кіберпростору, навіть не йшла мова. Проте з розвитком інформаційно-телекомунікаційних технологій, переходом до нових методів і заходів зберігання інформації, що становить державну, військову таємниці й такої, яка може зашкодити суверенітету, територіальній цілісності та недоторканності, обороноздатності, державній, економічній чи інформаційній безпеці України, змінилися й самі підходи до засобів і способів вчинення зазначених кримінальних правопорушень у кіберпросторі. Зокрема, Закон України «Про національну безпеку України» від 15 червня 2022 визначив, що державна політика у сферах національної безпеки та оборони спрямовується на забезпечення воєнної, зовнішньополітичної, державної, економічної, інформаційної, екологічної безпеки, безпеки критичної інфраструктури, кібербезпеки України та на її інші напрями [171].

Крім того, відповідно до зазначеного Закону визначений перелік органів, що прямо виконують функції щодо забезпечення кібербезпеки України, зокрема Служба Безпеки України та Державна служба спеціального зв'язку та захисту інформації України. Також Законом установлений основний документ довгострокового планування у сфері національної безпеки та оборони країни – Стратегія кібербезпеки України. Зокрема, в Стратегії наведені питома вага кіберпростору й тенденції його поширення на обороноздатне життя держави в найближчі десять років, а сам кіберпростір визначений як майбутній театр воєнних дій.

Також наведено кіберзагрози, основними серед яких, на нашу думку, є такі: 1) збройна агресія Російської Федерації проти України в кіберпросторі; 2) здійснення державою-агресором кібератак і кібердеверсій із метою активного маніпулювання та впливу на населення держави щодо дискредитації української державності; 3) використання кіберпростору для вчинення злочинів проти основ національної безпеки України;

4) здійснення урядами іноземних держав кібератак, пов’язаних із викраденням військової інформації й інформації оборонного значення (кібершпигунство), та розвідувальної діяльності [172].

З поміж іншого в документі визначені засади розбудови системи національної кібербезпеки та наведені її основні цілі. Тому, на нашу думку, аналіз групи кримінальних правопорушень у кіберпросторі проти основ національної безпеки є одним із паритетних напрямків розбудови якісної національної системи кібербезпеки.

Необхідно наголосити, що кримінальними правопорушеннями в кіберпросторі зазначеної групи будуть лише кримінальні правопорушення, вчинені з використанням кіберпростору. Як ми вже зазначали, до них належать такі: 1) державна зрада (стаття 111 Кримінального кодексу України); 2) колабораційна діяльність (стаття 111-1 Кримінального кодексу України); 3) пособництво державі-агресору (стаття 111-2 Кримінального кодексу України); 4) шпигунство (стаття 114 Кримінального кодексу України); 5) несанкціоноване поширення інформації про направлення, переміщення зброї, озброєння та бойових припасів в Україну, рух, переміщення або розміщення Збройних Сил України чи інших утворених відповідно до законів України військових формувань, вчинене в умовах воєнного або надзвичайного стану (стаття 114-2 Кримінального кодексу України)[173].

Родовим об’єктом цієї групи кримінальних правопорушень є суспільні відносини з охорони основ національної безпеки України: її конституційного ладу, суверенітету, територіальної недоторканності, обороноздатності, тобто відносини, що забезпечують саме існування України як суверенної, незалежної, демократичної, соціальної й правової держави, а основний безпосередній об’єкт кожного окремого злочину проти основ національної безпеки, вчиненого в кіберпросторі, – національна безпека в тій чи іншій її сфері [174, с. 73].

На нашу думку, варто зосередити увагу на предметі злочинного посягання, характерному для цієї групи кримінальних правопорушень. Зокрема, предметом державної зради (стаття 111 Кримінального кодексу України) може бути інформація, що містить державну таємницю, а також відомості, які не становлять державної таємниці, але передаються чи збираються за завданням іноземної розвідки для використання їх на шкоду інтересам та обороноздатності, економічному й політичному суверенітету [175, с. 86].

Відповідно до Закону України «Про державну таємницю» до державної таємниці в порядку, встановленому зазначеним документом, належить інформація у сферах оборони, економіки, науки й техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, що підлягає охороні з боку держави. Як приклад можна навести нещодавнє затримання контррозвідкою Служби безпеки України законспірованої шпигунки Федеральної служби безпеки Російської Федерації на Луганщині, яка намагалася ввійти в довіру до представників Служби безпеки України й передавати розвідувальні дані представникам держави агресора. Службою безпеки України було встановлено, що особа завербована в 2019 році на бік країни-агресора й виконувала завдання з передавання через різні месенджери відомостей про діяльність Збройних сил України, переміщення техніки та іншу інформацію на шкоду територіальній цілісності й суверенітету України. Ця особа була вчасно викрита співробітниками Служби безпеки України, і шляхом виманювання зрадниці на територію, підконтрольну Україні, вона була затримана. Наразі затриманій повідомлено про підозру за частиною 2 статті 111 Особливої частини Кримінального кодексу України (державна зрада, вчинена в умовах воєнного стану). Їй вибрано запобіжний захід у вигляді тримання під вартою. [176].

Предметом кримінального правопорушення відповідно до статті 114-2 Кримінального кодексу України є інформація про направлення, переміщення зброї, озброєння та бойових припасів в Україну, рух, переміщення або розміщення Збройних Сил України чи інших утворених згідно із законами України військових формувань. Прикладом зазначеного кримінально протиправного діяння є дії громадянки України Особи 1, яка, будучи працівником АК «Укралізниця» на посаді касира, усвідомлюючи обставини й достовірно знаючи про заборону поширення інформації про направлення, переміщення зброї, озброєння територією України, о 17:00 19 червня 2022 року, перебуваючи на залізничній станції міста Жмеринка (платформа № 1) за адресою м. Жмеринка, вул. Олійника, 1, діючи з прямим умислом, використовуючи власний мобільний телефон марки «Samsung A-75» здійснила відеофіксацію військової техніки Збройних Сил України – артилерійського озброєння, що знаходилося на вагонних платформах для подальшого переміщення. Відразу о 17:03 години Особа 1 поширила записаний нею відеоматеріал шляхом його пересилання в мобільному додатку «Telegram» на номер Особи 2. Варто зауважити, що офіційних відомостей щодо переміщення військової техніки 19 червня 2022 року через станцію Жмеринка не було у відкритому доступі й на офіційних сайтах, сторінках і соціальних мережах Генерального штабу Збройних Сил України, Міністерства оборони України, Служби безпеки України та Головного управління розвідки Міністерства оборони України. За результатами дослідження всіх матеріалів справи Особу 1 було визнано винною у вчиненні кримінального правопорушення, передбаченого частиною 1 статті 114^2 Кримінального кодексу України. Їй призначили покарання три роки позбавлення волі, але на підставі статті 75 Кримінального кодексу України було визначено звільнити Особу 1 від відбування призначеного покарання з випробувальним терміном 1 рік [177].

Ще як один із прикладів варто навести діяльність громадянина України, який збирав розвіддані про місця дислокації й переміщення підрозділів ЗСУ та Територіальної оборони, функціонування резервних аеродромів і військових полігонів на півдні Одеської області. Зокрема, агент спецслужб Російської Федерації через різноманітні месенджери на зразок «Telegram», «Signal», «WhatsApp» і «Viber» передавав інформацію по закритих каналах зв'язку про точні координати об'єктів оборони й інформував про кількість особового складу та військової техніки на об'єктах і їх переміщення. Наразі слідчими підрозділами Служби безпеки України повідомлено про підозру агентові спецслужб Російської Федерації за частиною 2 статті 111 Кримінального кодексу України (державна зрада, вчинена в умовах воєнного стану) та вибрано запобіжний захід у вигляді тримання під вартою [178; 179].

Як можна помітити з наведених судових рішень у формі вироків, фактично ідентичні за своєю сутністю протиправні діяння кваліфікують за різними статтями Особливої частини Кримінального кодексу України. Варто зауважити, що протиправні діяння особи, яка вчинила кримінальне правопорушення з передавання інформації про переміщення й направлення зброї, бойових припасів та озброєння будуть кваліфіковані за статтею 111 «Державна зрада» лише тоді, коли така інформація була передана іноземним кураторам або спецагентам іноземних держав і суб'єктом такого правопорушення є винятково громадянин України. З об'єктивної сторони таке діяння буде шпигунством. У диспозиції статті 114-2 Особливої частини Кримінального кодексу України передбачено передавання й оприлюднення зазначеної інформації у відкритих джерелах, наприклад телеграм-каналі [180].

Водночас суб'єктом вчинення такого кримінального правопорушення може бути як громадянин України, так і іноземець або особа без громадянства. Крім того, ще однією особливістю кваліфікації діяння за

частинами 1–2 статті 114-2 Особливої частини Кримінального кодексу України є час вчинення кримінального правопорушення, а саме: воєнний стан. Також у частині 3 статті 114-2 Особливої частини Кримінального кодексу України законодавець прямо зазначає, що діяння кваліфікують за цією частиною статті лише за відсутності ознак державної зради та шпигунства.

З об'єктивної сторони кримінальні правопорушення проти основ національної безпеки України, вчинені в кіберпросторі, характеризуються таким переліком протиправних дій: 1) державна зрада (стаття 111 Кримінального кодексу України) – шпигунством (кібершпигунством), тобто передаванням або збиранням із метою передавання іноземній державі, іноземній організації або їх представникам відомостей, що становлять державну таємницю, якщо таке діяння вчинене громадянином України шляхом використання кіберпростору; 2) шпигунство (кібершпигунство) (стаття 114 Кримінального кодексу України) – передаванням або збиранням із метою передавання іноземній державі, іноземній організації або їх представникам відомостей, що становлять державну таємницю, якщо таке діяння вчинене іноземцем або особою без громадянства шляхом використання кіберпростору; 3) колабораційна діяльність (стаття 111-1 Кримінального кодексу України) – публічним запереченням громадянином України здійснення збройної агресії проти України, публічними закликами громадянина України до підтримки рішень або дій держави-агресора, збройних формувань, здійсненням інформаційної діяльності в співпраці з державою-агресором або його окупаційною адміністрацією, спрямованих на підтримку держави-агресора, якщо такі діяння вчиняються в кіберпросторі. Склади зазначеної категорії кримінальних правопорушень також відрізняються. Зокрема, у статті 111 «Державна зрада у формі шпигунства» та власне статті 114 «Шпигунства» склад кримінального правопорушення є

усіченим, тобто кримінальне правопорушення вважають завершеним із моменту початку збирання відомостей, що становлять державну таємницю. У статтях 111-1 і 114-2 склад кримінального правопорушення є формальним, тобто з моменту вчинення передбачених у диспозиції статей дій.

Обов'язковою ознакою об'єктивної сторони кримінального правопорушення, передбаченого статтею 114-2 Кримінального кодексу України, є воєнний або надзвичайний стан.

Для визначення кримінальних правопорушень зазначеної категорії як таких, що вчиняють у кіберпросторі, обов'язковим елементом ознаки об'єктивної сторони повинні бути засоби вчинення кримінального правопорушення. Для кримінальних правопорушень, визначених статтями 111-1 і 114-2 Кримінального кодексу України, засобом вчинення кримінального правопорушення можуть бути електронно-обчислювальні машини, телекомунікаційні мережі, різні гаджети (телефон, планшет), а для кримінального правопорушення, визначеного статтею 111-1, крім зазначеного, – різноманітні форуми, сайти, канали в месенджерах, тобто будь-які канали зв'язку із зовнішнім світом у рамках кіберпростору, через які здійснюють публічні заклики, виправдування громадянином України збройної агресії проти неї.

На нашу думку, саме засіб вчинення зазначеного виду кримінальних правопорушень у кіберпросторі є своєрідним каталізатором збільшення їх динаміки, особливо в умовах воєнного чи надзвичайного стану. Сьогодні фактично кожний громадянин України має смартфон і доступ до Інтернету. Розгалужена система месенджерів як відкритого, так і закритого типу дає змогу правопорушникам залишатися непокараними. Варто зауважити, що кримінальні правопорушення зазначеної групи, вчинювані в кіберпросторі, є дуже латентними, тому зіставити реальну картину відкритих

кримінальних проваджень та кількість скоєних кримінальних правопорушень фактично неможливо.

Велику проблематику також утворює суб'єкт зазначеної групи кримінальних правопорушень у кіберпросторі. За загальним правилом суб'єктами цієї групи є фізичні осудні особи, які досягли віку кримінальної відповідальності на момент вчинення кримінального правопорушення, а саме: 16 років. Проте практика, що склалася з моменту початку повномасштабного вторгнення країни-агресора, показує, що насправді суб'єктами таких кримінальних правопорушень є особи, які не досягли 16-річного віку. Зокрема, на Харківщині було викрито 12-річного підлітка, який за допомогою мережі Інтернет і телеграм-каналів надсилав інформацію щодо розташування техніки, блокпостів та військових Збройних сил України з наміром отримати за це грошову винагороду. Аналогічний факт зафіксовано в Луганській області [181].

Варто наголосити, що випадки вербування неповнолітніх до вчинення дії протиправного характеру, зокрема у сфері національної безпеки, об'єктивна сторона яких зазвичай окреслюється передаванням відомостей про позиції Збройних сил України та ін., стають дедалі масовішими. Водночас латентність і складна процедура розслідування таких кримінальних правопорушень у кіберпросторі не дають змоги своєчасно викривати й запобігати передаванню інформації. Наголосимо, що зазначені дії є грубим порушенням статті 4 Факультативного протоколу до Конвенції ООН «Про права дитини, щодо участі дітей у збройних конфліктах», якою встановлена заборона на вербування й використання у військових діях осіб, які не досягли 18-річного віку [182].

У час, коли від однієї фотографії, одного допису, розміщеного в соціальній мережі, месенджері чи пересланому конкретній особі, залежить життя людини, енергетична, економічна, інформаційна незалежність, а також обороноздатність держави, на нашу думку, ураховуючи суспільну

небезпечність кримінальних правопорушень проти основ національної безпеки України, вчинених у кіберпросторі, та зважаючи на практичні кейси, які з'являються щодня в кожному регіоні України, доцільним є зниження віку, з якого настає кримінальна відповідальність, до 14 років. Зокрема, це стосується статей 111, 111-1, 114, 114-2 Кримінального кодексу України. Суб'єктивна сторона аналізованої групи кримінальних правопорушень, вчинюваних у кіберпросторі, характеризується прямим умислом, у статті 114-2 особа може ставитися до наслідків необережно.

Другий вид – кримінальні правопорушення в кіберпросторі проти власності. Основною особливістю зазначеної групи кримінальних правопорушень є їх вчинення безпосередньо в кіберпросторі або з його використанням, тобто з використанням інформаційно-телекомунікаційних мереж та електронно-обчислювальної техніки. Варто зазначити, що незважаючи на те, що кримінальні правопорушення проти власності вчиняють у кіберпросторі з використанням електронно-обчислювальної техніки та інформаційно-телекомунікаційних технологій, об'єкт їх посягання не змінюється. У цьому разі відбувається приєднання додаткового об'єкта посягання, тим самим збільшуючи суспільну небезпеку цього протиправного діяння. Усе це зумовлює вдосконалення системи норм, що відображає кримінальні правопорушення проти власності, вчинювані в кіберпросторі, оскільки вона повністю не відображає всього рівня загроз, наразі актуальних у ньому.

Звернімо увагу, що серед кримінальних правопорушень проти власності в доктринальних джерелах точаться дискусії щодо того, які види кримінальних правопорушень зазначеного розділу можна типологізувати власне до кіберзлочинів і кіберпроступків. Безумовно, за допомогою електронно-обчислювальних машин як знаряддя вчинення кримінального правопорушення, шкідливих вірусних програм може вчинятися більшість кримінальних правопорушень проти власності, передбачених розділом VI

Особливої частини Кримінального кодексу України. Виняток становлять лише кримінальні правопорушення, пов'язані з безпосереднім контактом правопорушника й потерпілого, а також та частина кримінальних правопорушень, предметом яких може бути лише матеріалізоване майно.

Зокрема, до кримінальних правопорушень проти власності, вчинених у кіберпросторі, належать: 1) телефонний скамінг (фішинг); 2) фішинг; 3) кібервимагання. У цьому підрозділі ми не будемо детально зупинятися на кримінально-правовій кваліфікації зазначених діянь, а лише коротко розглянемо особливості наведених кримінальних правопорушень проти власності, вчинених у кіберпросторі.

Фішинг можна визначити як одержання шляхом обману або методів соціальної інженерії, тобто хакерства з використанням людського фактору, персональних даних для подальшого використання в злочинних цілях. Реалізація фішингу має два механізми: по-перше, посередницьке одержання персональних даних; по-друге, одержання особистих даних у самого власника інформації [183, с. 146].

Загалом принцип роботи фішингу полягає в перенаправленні користувачів кіберпростору, зокрема мережі Інтернет, на підроблені мережеві ресурси, створені зловмисниками, що зовні нічим не відрізняються від офіційних вебсайтів. Отже, переходячи за посиланням, користувач потрапляє на підроблений зловмисником вебсайт, що виглядає ідинтично справжньому офіційному вебсайту банку, магазину чи соціальної мережі. Наступним етапом є заповнення користувачем форми з логіном і паролем для входження у свій акаунт, як результат – уведені дані швидко передаються на сервери зловмисників. Злочинець, маючи пароль від особистого електронного гаманця чи сервісу потерпілого, надалі може здійснювати протиправні дії щодо вмісту одержаного на свій розсуд.

Наприклад відомий сервіс криптовалютних платежів «myetherwallet», на якому можна завести віртуальний криптовалютний гаманець і купити й

зберігати криптовалюту. Зловмисники у своїх повідомленнях або надсилаючи посилання нібито цього сайта змінюють декілька або взагалі одну букву на інші знаки так, щоб це було не помітно. Наприклад, справжнє посилання цієї системи www.myetherwallet.com, а посилання зловмисника буде виглядати приблизно так: www.myetherwalIet.com.

Необхідно наголосити, що фішинг не передбачає впливу програмних засобів на комп'ютер жертви. Потерпілий сам переходить за надісланим лінком та вводить логін і пароль. Надалі розкрадання грошових коштів проводиться за допомогою одержаних логіна й пароля, але не в результаті впливу на пристрій потерпілого.

Інше кримінальне правопорушення цієї групи – вішинг. За своєю сутністю він є підвидом фішингу й становить вид телефонного або смс-шахрайства, що полягає у випитуванні конфіденційної інформації в особи з метою її використання у своїх протиправних намірах. Сьогодні через телефонні дзвінки шахраї дізнаються дані від банківських карт і рахунків, примушуючи методами соціальної інженерії до переказування грошових коштів зловмисникам [184, с. 114].

Найвразливішою категорією людей, які найчастіше стають жертвами вішингу, є особи пенсійного віку. Це зумовлено насамперед низьким рівнем як правової, так і інформаційної культури. Однією з основних особливостей вішингу є його транснаціональний характер, що фактично не дає змоги встановити особу зловмисника через його територіальне перебування, зазвичай в іншій країні. Наприклад, зловмисники з України переважно здійснюють свою діяльність щодо жителів інших країн СНГ, зокрема Росії, Казахстану, Литви, Латвії та Естонії, і, навпаки, зловмисники з наведених країн застосовують вішинг щодо громадян України. Варто зауважити, що в період пандемії та власне збройної агресії Російської Федерації шахраї безжально користуються скрутним становищем українців під час війни й продовжують пропонувати фейкові виплати.

Як ми зазначали, внаслідок збройної агресії Російської Федерації кількість різноманітних виплат анонсується дуже часто, а тому зловмисники все частіше й ретельніше використовують довіру та скрутне становище українців для заподіяння їм матеріальної шкоди.

Варто визначити основні сучасні прояви вішингу. Першим є представлення зловмисника працівником правоохоронного органу й подальше вимагання грошових коштів за звільнення нібито затриманого члена сім'ї. Такий прояв вішингу становив значну частку серед вчинених кримінальних правопорушень у період із 2010 по 2017 рік. Загроза кримінальної відповідальності для близького родича, на якій наголошує шахрай, не дає змоги жертві тверезо мислити, тому здебільшого вона пересилає йому грошові кошти. Сьогодні зазначений вид телефонного шахрайства поступово втрачає актуальність через його широке висвітлення в засобах масової інформації й підвищення рівня культури кібербезпеки в громадян зокрема.

Іншим проявом вішингу є випадки, за яких шахрай, телефонуючи жертві та представляючись працівником технічної підтримки або служби безпеки банку, намагається дізнатися особисті банківські дані особи, зокрема пінкод, номер банківської карти, CVV-код і секретне запитання. У цьому разі швидко перевірити, чи дійсно шахрай працює в банку, неможливо, адже на сайтах банків немає інформації щодо співробітників та їх особистих даних [185, с. 250].

Ще одним проявом вішингу, на нашу думку, варто визначити саме інтерент-вішинг. Як приклад можна навести схему щодо соціальної допомоги від Національного Банку України. Зокрема, в соціальних мережах з'являються повідомлення, у яких шахраї стверджують, що Національний банк України нібито проводить благодійну акцію разом із фондом «Твоя опора»: усім українцям виплачують «соціально-індивідуальну виплату». Для заповнення заявки на виплату такої допомоги зловмисники

пропонують перейти в шахрайський чат-бот. У ньому необхідно ввести номер картки, на яку будуть нараховані грошові кошти у вигляді допомоги від Національного банку України, і для погашення комісії пропонують унести перший платіж. Зазвичай після здійснення платежу грошові кошти у вигляді допомоги не приходять, а зловмисники отримують переведені від жертви комісійні кошти, а також інформацію про дані банківської картки, яку потім можуть використовувати в інших видах кримінальних правопорушень у кіберпросторі [186].

Предметом зазначеного виду кримінальних правопорушень у сфері власності, вчинених у кіберпросторі, є конфіденційна інформація. Загалом можна виділити декілька видів інформації, використовуваної шахраєм у своїй протиправній діяльності для досягнення злочинного результату, відповідно до рівня її небезпеки для жертви. Зокрема, такі: 1) публічну інформацію, маючи доступ до якої шахрай може одержати доступ до так званої допоміжної інформації, така інформація не становить ніякої таємниці й здебільшого жертва завжди повідомляє її (прізвище, ім'я, по батькові; чи є вона утримувачем картки того чи іншого банку, працівником тієї чи іншої юридичної особи тощо); 2) допоміжну інформацію, що дає доступ до інформації з високим рівнем складкості одержання (номери карток, кодові слова та ін.); 3) конфіденційну інформацію, що дає прямий доступ до того, що цікавить скаммера. Це можуть бути пінкоди, паролі й подібні дані.

Останнім кримінальним правопорушенням проти власності в кіберпросторі є вимагання (кібервимагання).

Що стосується об'єктивної сторони кримінальних правопорушень проти власності, вчинених у кіберпросторі, їх особливість проявляється не в обов'язкових ознаках, а у факультативних, таких як спосіб, місце та засіб вчинення. Зокрема, засобами вчинення кримінальних правопорушень зазначеної групи є інформаційно-телекомунікаційні мережі, Інтернет,

електронно-обчислювальні машини, різні месенджери, вебресурси й гаджети, програмне забезпечення.

Спосіб вчинення зазначеного типу кримінальних правопорушень проти власності в кіберпросторі буде визначатися як сукупність прийомів і методів, застосовуваних під час їх вчинення. Наголосимо, що майже всі кримінальні правопорушення в кіберпросторі мають дистанційний спосіб вчинення, що не зменшує, а, навпаки, збільшує їх суспільну небезпеку. Дистанційність як спосіб вчинення кримінальних правопорушень зазначеної групи дає змогу зловмисникам не залишати фізичних слідів, властивих класичним злочинам цієї групи, як наслідок – ускладнюється процес виявлення правопорушника та власне процес доказування. Дистанційність є обов'язковою ознакою об'єктивної сторони кожного кримінального правопорушення в кіберпросторі зазначеного виду.

Безумовно, залежно від виду кримінального правопорушення проти власності, вчиненого у кіберпросторі, спосіб вчинення буде відрізнятися. Зокрема, у разі вчинення особою кримінального правопорушення, передбаченого статтею 189 Кримінального кодексу України, спосіб вчинення кримінального правопорушення буде полягати в незаконному впливі на потерпілу особу або його близького родича з метою змусити зазначених осіб вчинити дії в інтересах зловмисника [187, с. 110].

У рамках кіберпростору виділяють такі способи незаконного впливу на потерпілу особу: 1) погроза обмеження прав, свобод і законних інтересів особи; 2) погроза розголошення відомостей, які потерпілий чи його близькі родичі бажають зберегти в таємниці; 3) погроза пошкодження або знищення майна.

Кримінальне правопорушення, передбачене статтею 190 Кримінального кодексу України, визначається як вчинене шляхом обману чи зловживання довірою. Крім того, фішинг як різновид шахрайства в кіберпросторі може вчинятися таємним способом, тобто коли потерпіла

особа не усвідомлює самого факту вчинення шахрайських дій щодо неї [188].

Власне сам кіберпростір можна розглядати як місце вчинення кримінального правопорушення. Це дає змогу зрозуміти простоту й легкість вчинення кримінальних правопорушень проти власності в кіберпросторі.

Як елемент складу злочину суб'єкт кримінальних правопорушень проти власності характеризується певними ознаками, однією з яких є вік особи. У частині 1 статті 22 Кримінального кодексу України закріплено: «кримінальній відповідальності підлягають особи, яким до вчинення кримінального правопорушення виповнилося шістнадцять років». Проте в частині 2 статті 22 Особливої частини Кримінального кодексу України закріплено таке: «щодо віку осіб, які вчинили вимагання, вік притягнення до відповідальності знижено – у разі вчинення цих кримінальних правопорушень проти власності в кіберпросторі він становить 14 років» [189, с. 254].

Однією з причин сучасного стану кіберзлочинності серед неповнолітніх варто вважати стрімкий розвиток інформаційно-телекомунікаційних технологій, що фактично формує інформаційно-комунікативне середовище, якому властиві такі характеристики: «віртуальність – існування речей, подій, процесів тощо; глобальність – існування єдиних, універсальних для всієї системи відносин, усіх локальних співтовариств (формальних і неформальних) та інститутів взаємодії; фрагментарність, що характеризується уривчастістю й неповнотою» [190, с. 23].

Суб'єктивна сторона цього виду кримінальних правопорушень проти власності, вчинених у кіберпросторі, передбачає прямий умисл і корисливий мотив.

Третій вид кримінальних правопорушень у кіберпросторі, що необхідно виділити відповідно до різновиду родового об'єкта, – кримінальні правопорушення у сфері господарської діяльності, вчинені в кіберпросторі. Вони репрезентовані двома кримінальними правопорушеннями: 1) незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, електронними грошима, обладнанням для їх виготовлення (стаття 200 Кримінального кодексу України); 2) легалізація майна, одержаного злочинним шляхом (стаття 209 Кримінального кодексу України); 3) незаконна діяльність з організації або проведення азартних ігор, лотерей (стаття 203-2 Кримінального кодексу України).

Родовим об'єктом зазначеної групи кримінальних правопорушень у кіберпросторі є суспільні відносини у сфері здійснення господарської діяльності. Безпосередній об'єкт кримінальних правопорушень у кіберпросторі цього типу – конкретні суспільні відносини, що склалися в певній сфері господарської діяльності, зокрема: 1) безпосереднім об'єктом кримінального правопорушення, передбаченого статтею 200 Кримінального кодексу України, буде встановлений порядок використання та обігу документів на переказ, платіжних карток, засобів доступу до банківських рахунків електронних грошей, що забезпечує нормальне функціонування банківської й фінансової систем України; 2) безпосереднім об'єктом кримінального правопорушення, передбаченого статтею 209 Кримінального кодексу України, буде встановлений із метою протидії залучення в економіку злочинних коштів порядок здійснення підприємницької та іншої господарської діяльності [191]; 3) безпосереднім об'єктом кримінального правопорушення, передбаченого статтею 203-2, є встановлений порядок провадження діяльності з організації або проведення азартних ігор, лотерей (у кіберпросторі).

Предмет аналізованого типу кримінальних правопорушень у кіберпросторі також відрізняється. Наприклад, у складі кримінального правопорушення, передбаченого статтею 200 Особливої частини Кримінального кодексу України, ними можуть бути віртуальні картки, електронні рахунки, віртуальна валюта, а також документи на їх переказ. Предметом легалізації майна, одержаного злочинним шляхом, будуть злочинні грошові кошти, отримані в результаті протиправних діянь, що передували легалізації.

Об'єктивна сторона цього виду кримінальних правопорушень у кіберпросторі також має свої особливі форми вираження відповідно до конкретного кримінального правопорушення. Об'єктивна сторона кримінального правопорушення, передбаченого статтею 200 Кримінального кодексу України, полягає у вчиненні таких дій: 1) підробка документів на переказ чи пластикових банківських карток; 2) придбання пластикових чи віртуальних карток; 3) використання банківських карток та електронних грошей.

До об'єктивної сторони кримінального правопорушення, передбаченого статтею 209 Кримінального кодексу України, належать: 1) фінансові операції з коштами, зокрема віртуальними активами та іншим майном, отриманими внаслідок предикатного кримінально-протиправного діяння; 2) набуття, володіння або використання злочинних грошових коштів чи віртуальних активів; 3) дії, спрямовані на приховування чи маскування незаконного походження, володіння, джерела походження, переміщення, знаходження злочинного майна, грошових коштів і віртуальних активів.

Засобами вчинення кримінальних правопорушень у сфері господарської діяльності, вчинюваних у кіберпросторі, є інформаційно-телекомунікаційні мережі, інтернет-мережа, електронно-обчислювальні машини, різні месенджери, вебресурси та гаджети, програмне забезпечення.

Суб’єктом зазначеної групи кримінальних правопорушень у кіберпросторі є фізичні особи, які досягли 16 років. Суб’єктивна сторона кримінальних правопорушень зазначеної групи характеризується прямим умислом та спеціальною метою. Зокрема, для кримінального правопорушення, передбаченого статтею 209 Кримінального кодексу України, такою метою є надання злочинним грошовим коштам легального походження. Для кримінального правопорушення, передбаченого статтею 200, також визначається корисливий мотив.

Четвертий різновид – кримінальні правопорушення у сфері обігу наркотичних засобів, психотропних речовин, їх аналогів або прекурсорів (статті 307, 311, 221 Кримінального кодексу України). Родовим об’єктом цих кримінальних правопорушень у кіберпросторі є встановлений порядок обігу наркотичних засобів, психотропних речовин, їх аналогів і прекурсорів, сильнодійних, отруйних речовин та одурманюючих засобів, радіоактивно забрудненої продукції, мікробіологічних та інших біологічних агентів і токсинів як складової частини здоров’я населення [192, с. 144].

Предмет кримінального правопорушення в кіберпросторі цього типу репрезентований широким колом речей матеріального світу, адже прямо випливає з міжнародних конвенцій і протоколів. Водночас через динамічний розвиток світової фармацевтичної галузі промисловості списки наркотичних речовин, прекурсорів та їх аналогів потребують постійного перегляду. Часто маємо факти появи нового наркотичного засобу, хімічна складова якого є новою й відрізняється від інших наркотичних речовин, а отже, не наведена в списках наркотичних засобів. Зокрема, перелік наркотичних засобів, сильнодійних і психотропних речовин, їх аналогів та прекурсорів – це згруповані в списки наркотичні засоби, психотропні речовини й прекурсори, внесені до таблиць I–IV згідно із законодавством України та міжнародними договорами, згода на обов’язковість яких надана

ВР України. Перелік затверджує КМУ за поданням спеціально вповноваженого органу виконавчої влади в галузі охорони здоров'я. Його публікують в офіційних друкованих виданнях [193, с. 55].

Об'єктивна сторона кримінальних правопорушень у сфері обігу наркотичних засобів, психотропних речовин, їх аналогів або прекурсорів, вчинених у кіберпросторі, характеризується діяннями у формі збуту зазначених наркотичних речовин у рамках кіберпростору, зокрема через Інтернет. Для аналізованого типу суспільно небезпечних діянь одними з визначальних факторів об'єктивної сторони є засіб, спосіб і місце вчинення кримінального правопорушення. Зокрема, засобом вчинення цієї групи кримінальних правопорушень у кіберпросторі є інформаційно-телекомунікаційні мережі й електронно-обчислювальна техніка. Спосіб вчинення кримінальних правопорушень у кіберпросторі зазначеної групи є дистанційним щодо збуту заборонених законом речовин.

Варто зауважити, що інтернет-мережа розвивається набагато швидше, ніж розробляються ефективні механізми збирання електронних доказів і документування такої протиправної діяльності. Інтернет розмив усі межі співпраці, тому члени однієї злочинної групи можуть перебувати в різних куточках світу й ніколи не бачитися в житті. Наприклад, є інтернет-ресурс, на якому українські користувачі купують наркотики. Адміністратор такого ресурсу може перебувати в будь-якій точці світу та інформувати українського покупця, де взяти наркотичні засоби, сам ніколи безпосередньо не стикаючись із цими засобами [194].

Суб'єкт кримінальних правопорушень у сфері обігу наркотичних засобів, психотропних речовин, їх аналогів або прекурсорів, вчинених у кіберпросторі, є загальним. Суб'єктивна сторона зазначених кримінальних правопорушень у кіберпросторі характеризується прямим умислом і корисливою метою.

П’ятий тип кримінальних правопорушень у кіберпросторі відповідно до родового об’єкта – кримінальні правопорушення проти громадської безпеки, вчинені в кіберпросторі (статті 255, 258, Кримінального кодексу України). До кримінальних правопорушень у кіберпросторі цього виду належать три кримінальні правопорушення. По-перше, створення, керівництво злочинною спільнотою або злочинною організацією, а також участь у ній (стаття 255 Кримінального кодексу України). Відповідно до абзацу 1 п. 10 ППВСУ «Про практику розгляду судами кримінальних справ про злочини, вчинені стійкими злочинними об’єднаннями» від 23 грудня 2005 року № 13 і частини 4 статті 28 Кримінального кодексу України злочинна організація – це внутрішньо й зовнішньо стійке ієрархічне об’єднання п’яти та більше осіб або двох і більше організованих груп (структурних частин), метою діяльності якого є або вчинення тяжких та особливо тяжких злочинів чи лише одного, що вимагає ретельної довготривалої підготовки, або керівництво чи координація злочинної діяльності інших осіб, або забезпечення функціонування як самої злочинної організації, так і інших злочинних груп [195].

Родовим об’єктом складу цього кримінального правопорушення в кіберпросторі є громадська безпека.

З об’єктивної сторони аналізоване кримінальне правопорушення може виражатися в таких формах: 1) створенні злочинної організації; 2) керівництві злочинною організацією; 3) участі в злочинній організації; 4) участі в злочинах, вчинюваних такою організацією; 5) організації, керівництві чи сприянні зустрічі («сходці») представників злочинних організацій або організованих груп для розроблення планів та умов спільного вчинення злочинів, матеріального забезпечення злочинної діяльності чи координації дій об’єднань злочинних організацій або організованих груп – стисло такі діяння можна назвати консолідацією організованої злочинної діяльності.

Важливим аспектом об’єктивної сторони аналізованого кримінального правопорушення в кіберпросторі є спосіб створення злочинної організації, а саме: дистанційність. Дистанційність у цьому разі виражається в тому, що безпосередньо в інтернет-мережі особа може створити злочинну організацію, підбір учасників якої може відбуватися на злочинних форумах або в месенджерах. Зазвичай учасники такої злочинної організації не знайомі один з одним у реальності, а їх комунікація відбувається за допомогою «нікнеймів» безпосередньо в кіберпросторі. Злочинні організації такого типу переважно створюють для вчинення конкретного одного кримінального правопорушення й мають чіткий розподіл ролей. Наприклад, було повідомлено про підозру двом особам як учасникам злочинної організації в привласненні 10 мільйонів гривень із банківських карток громадян. За даними слідства, учасники злочинної організації поширювали фішингові посилання під виглядом соціальних виплат за програмою «е-підтримка». Для отримання соціальних виплат за нібито цією програмою громадяни вводили свої персональні дані та дані банківських карток на фішинговому сайті. Учасники злочинної організації після одержання доступу до рахунків потерпілих осіб здійснювали з них перекази грошових коштів на свої рахунки. Затриманим учасникам злочинної організації повідомили про підозру за частинами 1 і 2 статті 255, частинами 3 та 4 статті 190 Кримінального кодексу України [196].

Суб’єкт цього складу кримінального правопорушення в кіберпросторі є загальним. Суб’єктивна сторона злочину характеризується прямим умислом, тобто винна особа усвідомлювала суспільно небезпечний характер свого діяння щодо створення злочинної організації, керування нею або участі в ній, а також передбачає, що її дії створюють загрозу громадській безпеці, і хоче настання таких наслідків.

У цьому розділі ми детально не аналізуватимемо склад кримінального правопорушення, передбаченого статтею 258 «Терористичний акт», а

зупинимося лише на визначенні поняття «тероризм у кіберпросторі» та в якій формі він проявляється. Тероризм у кіберпросторі, або кібертероризм, – це певні небезпечні для життя людей дії, що проявляються в дезорганізації інформаційних систем, призводять до майнової шкоди чи інших тяжких суспільно небезпечних наслідків і спрямовані на залякування населення й провокування воєнного конфлікту з метою порушення громадської безпеки. Основною формою кібертероризму є інформаційна атака на комп'ютерну інформацію, електронно-обчислювальні системи, електронні носії передавання даних та інші складові інформаційної структури держави.

Останній тип кримінальних правопорушень у кіберпросторі, що необхідно виділити на підставі родового об'єкта, – кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.

Родовим об'єктом аналізованого типу кримінальних правопорушень є суспільні відносини у сфері забезпечення захисту інформаційно-телекомунікаційних процесів і нормальної роботи електронно-обчислювальних машин та електронних комунікаційних мереж. Основним безпосереднім об'єктом цих кримінальних правопорушень є окремі інформаційні процеси, зокрема такі: 1) цілісність, доступність, конфіденційність інформації, її оброблення й передавання (стаття 361 Кримінального кодексу України); 2) порядок створення, використання та розповсюдження програмних і технічних засобів (стаття 361^1 Кримінального кодексу України); 3) порядок доступу та обігу конфіденційної інформації, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації (стаття 361^2 Кримінального кодексу України); 4) порядок санкціонованого використання інформації, яка зберігається в електронно-обчислювальних машинах (комп'ютерах),

автоматизованих системах, комп'ютерних мережах або на носіях такої інформації (стаття 362 Кримінального кодексу України); 5) безпека використання електронно-обчислювальних машин, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку та інформації, що в них зберігається (стаття 363 Кримінального кодексу України); 6) порядок нормальної роботи електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку (стаття 363^1 Кримінального кодексу України).

Предметом зазначеної групи кримінальних правопорушень у кіберпросторі може бути інформація, шкідливі програми й технічні засоби, повідомлення електрозв'язку.

З об'єктивної сторони більшість кримінальних правопорушень аналізованої групи вчиняють шляхом активних дій у кіберпросторі. Виняток становить лише склад кримінального правопорушення, передбаченого статтею 362 Кримінального кодексу України. Його можуть вчиняти як у формі дії, так і шляхом бездіяльності.

Суб'єкт кримінальних правопорушень цього типу щодо складу кримінального правопорушення, передбаченого статтями 361, 361-1, 362-2, 363-1 Кримінального кодексу України, загальний, тобто фізична осудна особа, яка досягла 16 років. Склад кримінальних правопорушень у кіберпросторі, передбачених статтями 362 та 363 Кримінального кодексу України, є спеціальним.

З точки зору суб'єктивної сторони кримінальні правопорушення в кіберпросторі аналізованого типу вчиняють із прямим умислом, за винятком складу кримінального правопорушення, передбаченого статтею 363 Кримінального кодексу України, у якому можливе як умисне, так і необережне ставлення особи до протиправного діяння.

Третьою підставою типологізації кримінальних правопорушень у кіберпросторі є типологізація відповідно до Конвенції Ради Європи «Про кіберзлочинність». На нашу думку, на сьогодні вона є еталоном нормативно-правового акту, оскільки має не лише певні регіональні регулювання, а й міжнародні. Крім того, доктринальна практика орієнтована саме на визначені Конвенцією кримінальні правопорушення в кіберпросторі.

Перший тип кримінальних правопорушень у кіберпросторі відповідно до Конвенції охоплює протиправні діяння, що посягають на конфіденційність, цілісність та доступність комп'ютерних даних і систем, зокрема: 1) незаконний доступ; 2) нелегальне перехоплення; 3) втручання в дані; 4) втручання в систему; 5) зловживання пристроями.

Другий тип містить у собі кримінальні правопорушення в кіберпросторі, пов'язані з комп'ютером. Зокрема, до нього належать такі: 1) підробка, пов'язана з комп'ютером; 2) шахрайство, пов'язане з комп'ютером.

Третій тип кримінальних правопорушень стосується змісту інформації в кіберпросторі. Найпоширеніший вид цієї групи кримінальних правопорушень у кіберпросторі пов'язаний із дитячою порнографією.

Четвертий тип становлять такі кримінальні правопорушення в кіберпросторі, як порушення авторських і суміжних прав. Водночас установлення кримінальної відповідальності за такі кримінальні правопорушення є компетенцію законодавств держав [18].

П'ятий тип кримінальних правопорушень у кіберпросторі зафіксований у додатковому протоколі до Конвенції «Про кіберзлочинність», зокрема це акти расизму, ксенофобії, вчинені через комп'ютерні системи [197].

Четвертою підставою типологізації є спрямованість кримінальних правопорушень у кіберпросторі, що охоплює такі види кримінально

протиправних діянь: 1) несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж: а) неправомірне одержання й використання чужих облікових даних для доступу до електронних та інформаційних комунікаційних мереж, зокрема мережі Інтернет; б) неправомірне підключення до мережі електронних комунікаційних мереж із метою несплати за одержані послуги; в) підміна особистих облікових даних в інформаційно-телекомунікаційних системах та електронних комунікаційних мережах для неправомірного доступу до зазначених мереж і систем; 2) створення з метою протиправного використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут; 3) вимагання в кіберпросторі; 4) шахрайство в кіберпросторі: а) продаж неіснуючих товарів, надання фіктивних послуг, здійснене з використанням кіберпростору; б) шахрайство у сфері онлайн-казино й букмекерських контор; в) шахрайство у сфері електронних платіжних систем; г) шахрайство у сфері краудфандингу й фандрейзингу; ґ) фішинг; д) телефонний скамінг; 5) порушення авторських і суміжних прав та незаконне використання чужого товарного знаку, якщо такі дії вчинено в кіберпросторі; 6) кібертероризм і фінансування тероризму, здійснене за допомогою віртуальних активів; 7) кардинг (розкрадання безготівкових грошових коштів, електронних грошових коштів і віртуальної валюти); 8) незаконне виготовлення, зберігання, розповсюдження, рекламування або публічна демонстрація інформації, забороненої до вільного доступу: а) незаконне виготовлення, зберігання, розповсюдження, рекламування або публічна демонстрація порнографічних матеріалів у кіберпросторі; б) порушення таємниці листування, переписки, телефонних розмов, поштових та інших повідомлень у кіберпросторі; в) приниження честі й гідності особи в кіберпросторі; г) незаконне розголошення відомостей, що

становлять комерційну, банківську або податкову таємницю в кіберпросторі; ґ) незаконне розповсюдження інформації про приватне життя, зокрема персональних даних, які особа бажає зберегти в таємниці.

П’ятою підставою є типологізація кримінальних правопорушень у кіберпросторі залежно від цілі використання електронно-обчислювальних машин інформаційно-телекомунікаційних мереж: 1) кримінальні правопорушення, у яких комп’ютерна інформація, електронно-обчислювальні машини, інформаційно-комунікаційні мережі – основна ціль посягання, зокрема це такі кримінальні правопорушення, як знищення, блокування, зміна інформації, що міститься в електронно-обчислювальних машинах, а також порушення порядку роботи електронно-обчислювальних машинах, інформаційних та електронних комунікаційних мереж; 2) кримінальні правопорушення, у яких комп’ютерна інформація, електронно-обчислювальні машини, інформаційно-комунікаційні мережі – проміжна ціль, а саме: в рамках використання електронно-обчислювальних машин, інформаційно-комунікаційних мереж, мереж електрозв’язку досягають іншої цілі, зокрема здійснення шахрайства в кіберпросторі, незаконне одержання конфіденційної інформації; 3) кримінальні правопорушення, у яких електронно-обчислювальні машини, інформаційно-комунікаційні мережі є засобом забезпечення злочинної діяльності: незаконний збір і систематизація інформації; ведення «чорної» бухгалтерії; ведення баз даних щодо поширення предметів, що перебувають в обмеженому обігу (наркотиків, зброї), листування електронною поштою.

Шостою підставою типологізації кримінальних правопорушень у кіберпросторі є кількість суб’єктів вчинення кримінального правопорушення. За нею можна виділити кримінальні правопорушення, вчинені одним суб’єктом та групою осіб (злочинною організацією, організованою групою).

Сьома підстава типологізації кримінальних правопорушень у кіберпросторі – поділ залежно від кількості об'єктів посягання, зокрема однооб'єктні й багатооб'єктні. Однооб'єктні кримінальні правопорушення в кіберпросторі завдають шкоди лише одному об'єкту, наприклад відносинам у сфері власності. Двооб'єктні поряд з основним об'єктом, який характеризується відносинами, наприклад, у сфері власності, шкодять відносинам у сфері комп'ютерної інформації [198].

Наприклад, шахрайство, вчинене з використанням соціальних мереж і месенджерів із застосуванням засобів соціальної інженерії, буде однооб'єктним кримінальним правопорушенням проти власності, вчиненим за допомогою кіберпростору. Соснівський районний суд міста Черкаси виніс обвинувальний вирок особі за частиною 1 статті 190 «Шахрайство». З матеріалів справи суд установив, що Особа 1 шляхом обману заволоділа персональними даними Особи 2 щодо доступу до букмекерської контори «1хбет». Особа 1 перевела грошові кошти з акаунту «1хбет» Особи 2 на власний рахунок, а під виглядом ставок переконала Особу 2, що гроші були програні на букмекерській платформі [199].

Щодо двооб'єктного кримінального правопорушення проти власності, вчиненого в кіберпросторі, то його яскравим прикладом є дії Особи 1, яка працювала провідним фахівцем у контактному центрі ПАТ «Кредобанк» і шляхом несанкціонованого втручання в систему банківської програми одержала номер і CVV-код розрахункової картки клієнта зазначеного банку. Маючи єдиний умисел, вона таємно викрала грошові кошти на наведеному рахунку, що належали потерпілій Особі 2, на загальну суму 10 116 гривень. Сихівський районний суд міста Львова ухвалив визнати Особу 1 винною у пред'явленому обвинуваченні за частиною 1 статті 185 та частиною 1 статті 361 Кримінального кодексу України. Спостерігаємо, що було завдано шкоди, з одного боку, відносинам у сфері власності, а з іншого – відносинам у сфері комп'ютерної інформації.

Восьмою підставою типологізації кримінальних правопорушень у кіберпросторі ми виділили кваліфікацію суб'єктів вчинення кримінального правопорушення.

1. Кримінальні правопорушення, вчинені «звичайними» користувачами. Ці кримінальні правопорушення в кіберпросторі вчиняють із застосуванням звичайних «примітивних» методів роботи з інформаційно-телекомунікаційними системами та електронно-обчислювальною технікою. Вони не потребують певних спеціальних навичок і професійних компетенцій у сфері інформаційних технологій. Зокрема, до таких кримінальних правопорушень належать кібервимагання, шахрайство в кіберпросторі, торгівля наркотичними речовинами в кіберпросторі, продаж неіснуючих товарів, надання фіктивних послуг, здійснене з використанням кіберпростору, та інші «прості» кримінальні правопорушення в кіберпросторі.

2. Кримінальні правопорушення, вчинені досвідченими користувачами, які мають достатній рівень використання електронно-обчислювальної техніки та інформаційно-телекомунікаційних систем. Зокрема, такі суб'єкти можуть вчиняти: а) несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж; б) порушення авторських і суміжних прав та незаконне використання чужого товарного знака в кіберпросторі; в) незаконне виготовлення, зберігання, розповсюдження, рекламування або публічна демонстрація порнографічних матеріалів у кіберпросторі; г) порушення таємниці листування, переписки, телефонних розмов, поштових та інших повідомлень у кіберпросторі.

3. Кримінальні правопорушення, вчинені користувачем-спеціалістом, за яких такий користувач може застосовувати складні методи роботи з інформаційно-телекомунікаційними технологіями та електронно-

обчислювальними машинами. До таких кримінальних правопорушень належать: а) створення шкідливих програм і програмного забезпечення; б) незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, електронними грошима; в) неправомірне підключення до мережі електронних комунікаційних мереж із метою несплати одержаних послуг; г) підміна особистих облікових даних в інформаційно-телекомунікаційних системах та електронних комунікаційних мережах із метою неправомірного доступу до зазначених мереж і систем; ґ) створення з метою протиправного використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут.

Дев'ятою підставою є типологізація відповідно до об'єкта 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, оброблюваної в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах чи комп'ютерних мережах.

Десятою підставою типологізації кримінальних правопорушень у кіберпросторі є мета їх вчинення. На нашу думку, варто виділити кримінальні правопорушення в кіберпросторі, вчинювані з метою: 1) отримати прибуток; 2) завдати шкоди національним інтересам та

обороноздатності держави; 3) порушити громадську безпеку; 4) надати злочинним грошовим коштам легального статусу; 5) змусити особу до вчинення протиправних дій.

Одинадцятою підставою типологізації кримінальних правопорушень у кіберпросторі є повнота ознак. Згідно з цією підставою кримінальні правопорушення в кіберпросторі можуть бути безумовно кіберорієнтованими або умовно кіберорієнтованими. Зокрема, безумовно кіберорієнтовані кримінальні правопорушення містять у собі обов'язкову кібернетичну складову, без якої неможливе вчинення суспільно небезпечного діяння, передбаченого Особливою частиною Кримінального кодексу України. До таких кримінальних правопорушень законодавець класифікує кримінальні правопорушення, передбачені розділом XVI Особливої частини Кримінального кодексу України, а також кримінальне правопорушення, передбачене частиною 4 статті 190 Кримінального кодексу України. На нашу думку, перелік ознак, за допомогою яких можна типологізувати кримінальні правопорушення до безумовно кіберорієнтованих, такий: 1) основним об'єктом посягання є відносини у сфері використання електронно-обчислювальних машин, комп'ютерних мереж і мереж електрозв'язку; 2) предметом посягання є комп'ютерна інформація; 3) засоби вчинення кримінального правопорушення – обов'язкова ознака його об'єктивної сторони.

Щодо умовно кіберорієнтованих кримінальних правопорушень, то вони мають не всі ознаки кібернетичної складової. Об'єктом посягання цих кримінальних правопорушень можуть бути різні суспільні відносини, що охороняються кримінальним законодавством.

Дванадцята підстава типологізації – правовий режим інформації, що є предметом цих кримінальних правопорушень: конфіденційна інформація, інформація з обмеженим доступом, секретна інформація.

Тринадцятою підставою типологізації ми виділяємо сутність кримінальних правопорушень у кіберпросторі. У рамках зазначеного типу кримінальних правопорушень у кіберпросторі варто зробити поділ на кіберзалежні кримінальні правопорушення й кіберутворювальні.

Кіберзалежні кримінальні правопорушення – це ті кримінальні правопорушення, що 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. До таких кримінальних правопорушень належать зламування серверів для одержання інформації, що становить інтерес для правопорушника, викрадення акаунтів у соціальних мережах, віртуальних активів, персоналізованих вебсайтів. Особливістю кіберзалежних кримінальних правопорушень є пошкодження самої електронно-обчислювальної техніки, мережі й блокчейну. 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. На відміну від кіберзалежних кримінальних правопорушень кіберутворювальні можуть вчиняти без застосування кібернетичного елементу, наприклад класична крадіжка [200, с. 29].

Можемо помітити, що кримінальні правопорушення в кіберпросторі є надзвичайно соціально небезпечним, протиправним явищем, яке становить загрозу не лише національним, а й міжнародним інтересам. Сьогодні боротьба з феноменом кримінальних правопорушень у кіберпросторі є одним із головних завдань правоохоронних органів як національного, так і міжнародного рівня. На нашу думку, для комплексної боротьби на національному рівні насамперед необхідно узгодити та

законодавчо закріпити основні кримінальні правопорушення в кіберпросторі в рамках чинних нормативно-правових актів. Удосконалення чинного законодавства щодо визначення основних видів кримінальних правопорушень у кіберпросторі, завершення процесу імплементації норм міжнародно-правових актів в законознавство України дадуть змогу точніше визначати в рамках кримінально-правової типологізації, що саме може належати до кримінальних правопорушень у кіберпросторі.

Підбиваючи підсумки вищевикладеного, доцільно підкреслити, що ми пропонуємо виділяти кілька підстав типологізації кримінальних правопорушень у кіберпросторі. Залежно від виду кримінальних правопорушень їх поділяють на злочини (кіберзлочини) та проступки (кіберпроступки).

За видом родового об'єкта складу кримінального правопорушення ми виділяємо 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.

Відповідно до кваліфікації суб'єктів вчинення кримінальних правопорушень у кіберпросторі, на нашу думку, можна виділити: 1) звичайних користувачів; 2) досвідчених користувачів; 3) спеціалістів.

Також була здійснена типологізація за такими критеріями: 1) залежно від кількості об'єктів посягання; 2) залежно від спрямованості кримінальних правопорушень у кіберпросторі; 3) залежно від кількості суб'єктів вчинення кримінального правопорушення; 4) залежно від цілі використання електронно-обчислювальних машин інформаційно-телекомунікаційних мереж; 5) залежно від мети вчинення кримінальних

правопорушень у кіберпросторі; 6) залежно від повноти ознак; 7) залежно від правового режиму інформації, що є предметом кримінальних правопорушень у кіберпросторі.

2.2. Кримінально-правова характеристика кіберзалежних кримінальних правопорушень у кіберпросторі

Аналізуючи кримінальні правопорушення, вчинені в кіберпросторі в сучасному кримінальному законодавстві України, хочемо наголосити, що кримінальні правопорушення у сфері обігу цифрової інформації та функціонування інформаційно-телекомунікаційних технологій не є ідентичними за своєю сутністю з кримінальними правопорушеннями у сфері використання інформаційно-телекомунікаційних технологій. У першому разі кримінальні правопорушення прийнято вважати кіберзалежними, тобто основним предметом цього типу кримінальних правопорушень у кіберпросторі є цифрова інформація у сфері цифрових технологій, інформаційно-телекомунікаційних систем та мереж. Кіберутворювальні кримінальні правопорушення є класичними кримінальними правопорушеннями, що внаслідок використання інформаційно-телекомунікаційних технологій перейшли в кіберпростір.

Кіберзалежні кримінальні правопорушення наведені в главі XVI Особливої частини Кримінального кодексу України. Вони мають назву «кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку». Варто зауважити, що норми глави XVI Особливої частини Кримінального кодексу України імплементовані з Конвенції «Про кіберзлочинність», зокрема її розділ II «Правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних та систем» [18; 14].

Не можна не наголосити, що в доктринальних джерелах зазначений тип кримінальних правопорушень визначається як «комп'ютерне кримінальне правопорушення», або «кримінальне правопорушення у сфері комп'ютерної інформації». На нашу думку, це зумовлено насамперед предметом кримінального правопорушення, яким є комп'ютерна інформація. Водночас серед науковців точаться дискусії щодо сутності поняття «комп'ютерне кримінальне правопорушення». Зокрема, П. Біленчук зазначає, що до цієї категорії кримінальних правопорушень належать усі кримінально протиправні дії, за яких комп'ютер є знаряддям, засобом чи метою їх вчинення [201, с. 155].

На нашу думку, це дуже узагальнене розуміння категорії кримінальних правопорушень у кіберпросторі, що повністю не розкриває його сутнісних особливостей, адже за допомогою цифрових технологій можна вчиняти більшість кластичних кримінальних правопорушень, безпосереднім об'єктом яких будуть різні суспільні відносини, не пов'язані з кіберпростором.

На думку А. Селюк, комп'ютерні кримінальні правопорушення об'єднують усі протизаконні дії, що завдають збитків майну й пов'язані з електронним опрацюванням даних [202, с. 84]. Д. Дердюк наголошує, що під комп'ютерним кримінальним правопорушенням потрібно розуміти суспільно небезпечну діяльність чи бездіяльність, здійснювану з використанням сучасних інформаційних технологій і засобів комп'ютерної техніки з метою спричинити збитки суспільним, майновим або інтересам держави, підприємствам, відомствам, організаціям, кооперативам та громадянам, а також правам окремої особи [203, с. 226].

Кримінальні правопорушення у сфері комп'ютерної інформації – це всі суспільно небезпечні діяння, родовим об'єктом яких є комп'ютерна інформація. Отже, можна зробити висновок, що в доктринальних джерелах поняття комп'ютерного кримінального правопорушення ширше за

кримінальне правопорушення у сфері комп'ютерної інформації, що є його складовою частиною як певний підтип.

На нашу думку, істотним недоліком чинного кримінального законодавства є невідповідність термінології сучасному стану науки й техніки. Сам термін «електронно-обчислювальна мишина» був уведений ще наказом Міністерства праці та соціальної політики України від 10 лютого 1999 року. У ньому він визначений як персональний комп'ютер із необов'язковими додатковими приладами, системними елементами (дисководами, пристроями для друку, сканерами, модемами, блоками безперервного живлення та іншими спеціальними периферійними пристроями) [204]. Але відповідно до наказу Міністерства соціальної політики України від 14 лютого 2018 року його замінено на поняття екранний пристрій – електронний засіб для відтворення будь-якої графічної або алфавітно-цифрової інформації (на основі електронно-променевої трубки, рідкокристалічні, плазмові, проєкційні, органічні світлодіодні монітори та інші новітні розробки у сфері інформаційних технологій) [205].

На нашу думку, таке визначення більш якісно окреслює специфіку та сутність кримінальних правопорушень, передбачених розділом XVI Особливої частини Кримінального кодексу України. Аналізуючи поняття електронно-обчислювальної машини хочемо зазначити, що відповідно до змісту статей розділу XVI Особливої частини Кримінального кодексу України законодавець під цим поняттям розуміє елемент зберігання інформації, що є частиною електронно-обчислювальної машини. Проте сучасними носіями цифрової інформації можуть бути, крім електронно-обчислювальних машин, флеш-носії, жорсткі та компакт-диски, що, на наш погляд, не підпадають під категорію електронно-обчислювальних машин. Тому ми переконані, що варто виключити термін «електронно-обчислювальні машини (комп'ютери)» з назви розділу XVI Особливої частини Кримінального кодексу України та замінити його на термін

«цифрові пристрої». Цифрові пристрої пропонуємо визначити як інформаційно-телекомунікаційні засоби, призначені для оброблення, передавання, розподілу інформації в цифровій формі.

Також у назві цього розділу пропонуємо замінити словосполучення «автоматизовані системи та комп'ютерні мережі і мережі електрозв'язку» на «інформаційно-комунікаційні системи», що охоплює як системи й мережі електрозв'язку, так і комп'ютерні мережі. У Законі України «Про захист інформації в інформаційно-комунікаційних системах» від 16 грудня 2020 року надано поняття інформаційної та інформаційно-комунікаційної систем. Інформаційна (автоматизована) система – це організаційно-технічна система, в якій реалізується технологія оброблення інформації з використанням технічних і програмних засобів. Інформаційно-комунікаційна система – це сукупність інформаційних та електронних комунікаційних систем, що в процесі оброблення інформації діють як єдине ціле. Саму електронну комунікаційну систему Закон України «Про захист інформації в інформаційно-комунікаційних системах» визначає як сукупність технічних і програмних засобів, призначених для обміну інформацією шляхом передавання, випромінювання та/або приймання її у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб [206].

З огляду на це пропонуємо назву розділу XVI Особливої частини Кримінального кодексу України в такій редакції: «Кримінальні правопорушення у сфері функціонування цифрових пристроїв оброблення інформації, інформаційно-комунікаційних систем та телекомунікаційних мереж», і надалі для кваліфікації кримінальних правопорушень у кіберпросторі використовувати зазначену термінологію. Водночас інформаційні (автоматизовані), електронні комунікаційні, інформаційно-комунікаційні системи, електронні комунікаційні мережі визначати в сукупності як інформаційно-телекомунікаційні технології, системи та

мережі. Такі зміни зумовлені насамперед узгодженням законодавчих термінів і загалом сутності зазначеного типу кримінальних правопорушень у кіберпросторі.

Правове регулювання кримінальних правопорушень у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку здійснюється завдяки закріпленню шести складів кримінального правопорушення: 1) несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж (стаття 361 Кримінального кодексу України); 2) створення з метою протиправного використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут (стаття 361-1 Кримінального кодексу України); 3) несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації (стаття 361-2 Кримінального кодексу України); 4) несанкціоновані дії з інформацією, що оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї (стаття 362 Кримінального кодексу України); 5) порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється (стаття 363 Кримінального кодексу України); 6) перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового

розповсюдження повідомлень електрозв'язку (стаття 363-1 Кримінального кодексу України) [14].

Сутність кримінальних правопорушень у кіберпросторі, передбачених розділом XVI Особливої частини Кримінального кодексу України, полягає в недопущенні суспільно небезпечних, протиправних діянь, що посягають на безпеку цифрової інформації й нормальне функціонування інформаційно-телекомунікаційних систем. Водночас самі цифрові пристрої завжди являють собою засіб вчинення кримінального правопорушення.

Суспільна небезпека цього типу кримінальних правопорушень у кіберпросторі полягає в тому, що несанкціоноване втручання чи модифікація цифрової інформації може порушувати діяльність різноманітних державних систем, зокрема оборонного, енергетичного, транспортного, банківського характеру, та спричинити не лише матеріальну шкоду, а й людські жертви.

Варто зауважити, що майже в усіх кримінальних правопорушеннях цього типу цифрова інформація в тому чи іншому вигляді є предметом протиправного посягання. Закон України «Про авторське право та суміжні права» від 23 грудня 1993 року надає таке визначення цифрової інформації: аудіовізуальні твори, музичні твори (з текстом або без тексту), комп'ютерні програми, фонограми, відеограми, програми (передавання) організацій мовлення, що знаходяться в електронній (цифровій) формі, придатній для зчитування й відтворення комп'ютером, які можуть існувати і (або) зберігатися у вигляді одного або декількох файлів (частин файлів), записів у базі даних на зберігаючих пристроях комп'ютерів, серверів тощо в мережі Інтернет, а також програми (передавання) організацій мовлення, що ретранслюються з використанням мережі Інтернет [207].

На нашу думку, наведене визначення поняття «цифрова інформація» характерне саме для сфери захисту інтелектуальної власності. Під

цифровою інформаціє ми пропонуємо розуміти сукупність даних і програмних компонентів, що обробляються, передаються, зберігаються в інформаційно-телекомунікаційних технологіях, системах або мережах. Варто відмітити, що в доктринальних джерелах під час визначення предмета кримінальних правопорушень у кіберпросторі, передбачених розділом XVI Особливої частини Кримінального кодексу України, часто зустрічається поняття «комп'ютерна інформація». Комп'ютерна інформація – це текстова, цифрова, графічна чи інша інформація (дані, відомості) про осіб, предмети, події, явища, що існує в електронному вигляді й знаходиться в електронно-обчислювальній машині, автономній системі чи комп'ютерній мережі, а також зберігається на відповідних електронних носіях, до яких належать гнучкі магнітні диски (дискети), жорсткі магнітні диски (вінчестери), касетні магнітні стрічки (стримери), магнітні барабани, магнітні та електронні карти, зокрема засоби флеш-пам'яті, інші електронно-магнітні носії електронної інформації, зафіксованої з використанням сучасних електронно-інноваційних технологій, та ін. [208].

Незважаючи на відсутність законодавчого визначення поняття «комп'ютерна інформація», вважаємо, що за своєю сутнісною характеристикою та з технічної точки зору воно є ширшим за поняття «комп'ютерна інформація». В інформаційно-телекомунікаційних системах і мережах обробляється, розповсюджується й зберігається саме цифрова інформація, а комп'ютерна інформація є її підвидом.

Визначивши основні категорії інформаційно-телекомунікаційної складової, пропонуємо перейти безпосередньо до кримінально-правової характеристики зазначеного типу кримінальних правопорушень у кіберпросторі. Першим кримінальним правопорушенням, передбаченим розділом XVI Особливої частини Кримінального кодексу України, є несанкціоноване втручання в роботу інформаційних (автоматизованих),

електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж (стаття 361 Особливої частини Кримінального кодексу України).

Безпосереднім об’єктом несанкціонованого втручання в роботу інформаційно-телекомунікаційних технологій, систем та мереж є суспільні відносини в інформаційному середовищі щодо забезпечення конфіденційності, цілісності й доступності цифрової інформації та нормальних процесів їх обігу, оброблення й передавання.

Основним предметом зазначеного кримінального правопорушення є цифрова інформація, оброблювана в електронних комунікаційних мережах, інформаційно-комунікаційних системах, електронних комунікаціях і цифрових пристроях.

Об’єктивна сторона кримінального правопорушення, передбаченого статтею 361 Особливої частини Кримінального кодексу України, полягає в: 1) активних діях у вигляді несанкціонованого втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж; 2) суспільно небезпечних наслідках у формі одержання неправомірного доступу до цифрового пристрою жертви, перехоплення цифрової інформації, витоку, втрати, підробки, блокування, спотворення процесу оброблення інформації та порушення установленого порядку маршрутизації інформації; 3) причиново-наслідковому зв’язку.

Кримінальне правопорушення несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж за частинами 1 та 2 є кримінальним правопорушенням із формальним складом, а за частиною 3 – кримінальним правопорушенням із матеріальним складом.

У доктринальних джерелах, зокрема науково-практичних коментарях до Особливої частини Кримінального кодексу України, наведено, що склад зазначеного суспільно небезпечного діяння є матеріальним, тобто з настанням альтернативних наслідків, передбачених у частині 3 [209].

Відповідно до частини 1 статті 361 Особливої частини Кримінального кодексу України «Несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж» можна дійти виковку, що кримінальна відповідальність за скоєне суспільно небезпечне діяння настає саме внаслідок несанкціонованого втручання, тобто доступу до інформаційно-телекомунікаційних систем за дозволом власника інформаційно-телекомунікаційної системи, мережі чи цифрового пристрою. На нашу думку, такі дії повинні бути пов’язані зі зміною нормального режиму роботи інформаційно-телекомунікаційних технологій, але без передбачених наслідків, зазначених у частині 3 цієї статті. Несанкціоноване втручання фактично свідчить про порушення установленого власником режиму доступу до системи, його розмежування або відсутність. Фактично відповідно до частин 1 та 2 статті 361 склад кримінального правопорушення буде формальним, тобто незалежно від настання суспільно небезпечних наслідків. Власне сам факт проникнення в інформаційно-телекомунікаційну систему або мережу обумовлює кримінальну відповідальність за вчинене діяння. На практиці маємо зовні протилежне розуміння значення словосполучення «несанкціоноване втручання». Зокрема, виникає проблема в разі кваліфікації за частиною 1 статті 361. Наприклад, Деснянським районним судом міста Чернігів було винесено вирок Особі 1, яка, використовуючи свій персональний комп’ютер, маючи підключення до Інтернету, переслідуючи прямий умисел та усвідомлюючи суспільну небезпеку свого діяння у формі витоку й блокування інформації, шляхом подолання систем логічного захисту

автоматизованої системи «Steam» несанкціоновано втрутилася в роботу та здійснила вхід до системи акаунту Особи 2 (потерпілої). Одержавши інформацію, розміщену в акаунті, Особа 1 змінила ідентифікаційні дані акаунту, чим спричинила його блокування [210].

У зазначеному прикладі ми бачимо суспільно небезпечні наслідки у формі витоку й блокування інформації, передбачені як кваліфікаційні ознаки за частиною 3 статті 361, але суд ухвалив визнати Особу 1 винною в пред'явленому їй обвинуваченні за частиною 1 статті 361 Особливої частини Кримінального кодексу України. На нашу думку, потрібно було кваліфікувати зазначене діяння за частиною 1 статті 361 відповідно за сам факт несанкціонованого втручання й за частиною 3 статті 361 за наслідки у формі витоку та блокування інформації. Проаналізувавши судові рішення у формі судових вироків у кримінальних справах за кримінальні правопорушення, передбачені статтею 361 Особливої частини Кримінального кодексу України, хочемо зауважити, що в разі кваліфікації зазначеного кримінального правопорушення за частиною 1 статті 361 завжди простежується хоча б один з альтернативних наслідків, передбачених частиною 3 статті 361.

На нашу думку, потрібно на законодавчому рівні закріпити поняття «несанкціоноване втручання», під яким пропонуємо розуміти одержання можливості для ознайомлення та (або) використання цифрової інформації, що міститься в інформаційно-телекомунікаційній технології, системі або мережі, шляхом 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.

Ураховуючи зміст запропонованого поняття «несанкціоноване втручання», ми переконані, що основними наслідками є такі : 1) витік цифрової інформації; 2) блокування цифрової інформації; 3) знищення

цифрової інформації; 4) модифікація цифрової інформації; 5) перехоплення цифрової інформації; 6) копіювання цифрової інформації; 7) спотворення процесу оброблення цифрової інформації.

Варто окремо розглянути кожний із зазначених суспільно небезпечних наслідків. Зокрема, в Законі України «Про захист інформації в інформаційно-комунікаційних системах» витік інформації визначено як результат дій, унаслідок яких інформація в системі стає відомою чи доступною фізичним та/або юридичним особам, які не мають права доступу до неї [211].

Як приклад можна навести дії особи, яка за допомогою шкідливого програмного забезпечення втрутилася в цифровий пристрій жертви, яким був комп'ютер, та одержала доступ до цифрової інформації, збереженої в браузері жертви. Варто зауважити, що здебільшого в разі несанкціонованого втручання наслідки у формі витоку цифрової інформації є завжди незалежно від того, чи була така інформація в подальшому використана в злочинних намірах особою, яка вчинила кримінальне правопорушення. Необхідно звернути увагу на кримінальне провадження № 522/14602/13-к – вирок Приморського райсуду м. Одеса від 27 червня 2013 року, яким установлено, що Особа 1 із метою незаконного одержання та подальшого використанням інформації з фізичних банківських карток інших громадян несанкціоновано втрутилася в роботу цифрового пристрою (банкомату), встановивши на ньому спеціальний технічний засіб (скімер) для подальшого зчитування цифрової інформації з банківських платіжних карток. У цьому разі витік цифрової інформації ототожнено зі зчитуванням інформації. Проте, на нашу думку, зчитування цифрової інформації є саме способом вчинення кримінального правопорушення, адже це активні дії, а витік цифрової інформації – наслідок [212].

Блокування цифрової інформації – це дії, унаслідок яких унеможливлюється доступ до інформації в системі [211]. Наразі наслідок

несанкціонованого втручання у формі блокування цифрової інформації є одним із найбільш суспільно небезпечних серед усіх інших. Шкідливе програмне забезпечення, метою якого є блокування цифрової інформації, оброблюваної в інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних системах, електронних комунікаційних мережах, зараз є як у відкритому доступі, так і продається на різноманітних даркнет-форумах. Можливості масового розповсюдження такого програмного забезпечення лише додають суспільної небезпеки цьому діянню. Сьогодні фактично кожний користувач кіберпростору є потенційною жертвою такого протиправного діяння. Варто зауважити, що здебільшого в разі кваліфікації за статтею 361 Особливої частини Кримінального кодексу України й наслідків у формі блокування цифрової інформації додатковою за сукупністю кримінальних правопорушень буде кваліфікація за статтею 361-1 Особливої частини Кримінального кодексу України. Як приклад хочемо навести масовану атаку, що спричинила блокування комп'ютерів по всьому світу вірусом «Petya». Масштабна кібератака на корпоративні та державні інформаційні (автоматизовані) системи, внаслідок якої було заблоковано більшу частину комп'ютерів державного й приватного сектору, сталася 27 червня 2017 року. Вірус «Petya» шифрує інформацію на комп'ютері, після чого виводить на екран повідомлення-вимогу перевести 300 доларів у біткоїнах за розблокування. Найімовірніше, що дія вірусу поширюється лише на комп'ютери із системою «Windows». Зараження комп'ютерів відбувається через фішингові листи (фішинг – вид інтернет-шахрайства, за якого під виглядом листів від імені популярних брендів злочинці одержують доступ до конфіденційних даних користувачів). Фахівці стверджують, що вірус використовував сфальшований електронний підпис Microsoft [213].

Знищення цифрової інформації є дією, унаслідок якої інформація в системі зникає. Тобто це її пряме видалення, за якого вона може видалятися

автоматизовано, тобто, наприклад, самим шкідливим програмним забезпеченням, або цілеспрямовано особою, у якої внаслідок несанкціонованого втручання в систему є віддалений доступ до неї. Здебільшого внаслідок автоматизованого знищення видаляється або вся інформація з інформаційно-телекомунікаційної системи або інформація за чітко вибраними критеріями, наприклад doc-файли. У разі віддаленого доступу особа, яка вчинила кримінальне правопорушення, може видаляти інформацію на власний розсуд, не піддаючись будь-якій типологізаційній складовій цифрової інформації. Одним із прикладів можна навести дії Особи 1, яка, працюючи інженером програмного забезпечення банківської установи, мала намір знищити інформацію, оброблювану на сервері банківської установи. Вона розмістила шкідливе програмне забезпечення в бібліотеці операційної системи банківської установи, але реалізувати свій умисел до кінця не змогла через звільнення й відмову в подальшому допуску до системи серверних даних. Як результат – наслідків у формі знищення цифрової інформації не настало, а дії Особи 1 суд кваліфікував за частиною першою статті 361-1 Особливої частини Кримінального кодексу України. Ми вважаємо, що таке діяння є завершеним замахом на кримінальне правопорушення, передбачене частиною 3 статті 361 Особливої частини Кримінального кодексу України та вчинене в сукупності з кримінальним правопорушенням, передбаченим частиною 1 статті 361-1 Особливої частини Кримінального кодексу України [214].

На наш погляд, наслідки у формі знищення цифрової інформації за рівнем суспільної небезпеки є значно вищими за її блокування або витік. Загалом знищення цифрової інформації може відбуватися шляхом видалення цифрової версії документа прямо з цифрового пристрою або безпосереднього пошкодження носія цифрової інформації, унаслідок якого внеможливлюється зчитування з нього інформації. Варто акцентувати увагу, що в разі умислу особи лише завдати шкоди у формі знищення або

пошкодження носія цифрової інформації відповідальність за статтею 361-1 не настає.

Модифікація цифрової інформації передбачає внесення в неї змін і характеризується наслідками у формі зміни змісту такої інформації без згоди власника.

Перехоплення цифрової інформації можна розуміти як створення додаткової лінії її маршруту, унаслідок якого цифрова інформація потрапляє до осіб, які не мають права доступу до неї, якщо під час цього не було спотворено процес її оброблення.

Зауважимо, що в чинному кримінальному законодавстві не приділено уваги кримінально правовій відповідальності за перехоплення цифрової інформації. Вважаємо, що в статті 361 Особливої частини Кримінального кодексу України необхідно виокремити додаткові ознаки, що передбачатимуть диференціацію способів несанкціонованого втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж.

Варто зауважити, що на відміну несанкціонованого копіювання несанкціоноване перехоплення цифрової інформації за способом вчинення неможливе без спеціальних технічних засобів, використовуваних для негласного одержання інформації, що перебуває в обмеженому цивільному обігу [215].

Копіювання цифрової інформації передбачає певні дії, спрямовані на створення дублікату вже існуючої інформації. У доктринальних джерелах під копіюванням цифрової інформації розуміють відтворення даних зі збереженням вихідної інформації. Відповідно несанкціоноване копіювання цифрової інформації розглядають як відтворення з перевищенням наданих власником прав доступу комп’ютерної інформації з обмеженим доступом зі збереженням вихідної інформації [216].

Варто зауважити, що серед науковців точиться дискусія стосовно класифікації поняття «перехоплення цифрової інформації» аналогічно до «копіювання цифрової інформації».

На нашу думку, це різні за змістом і наслідками суспільно небезпечні діяння. Якщо в разі несанкціонованого копіювання цифрової інформації спостерігаються обов'язкові наслідки у вигляді дублікату інформації як форми завершеного кримінального правопорушення, то в разі її перехоплення наслідки у формі дублікату можуть і не настати, а саме кримінальне правопорушення буде завершеним із моменту початку активних дій зі створення додаткової лінії зв'язку в інформаційно-телекомунікаційних системах.

Потрібно наголосити, що легального визначення дефініції поняття «спотворення процесу оброблення інформації» в законодавстві немає, проте в доктринальних джерелах його прийнято визначати як зміну послідовності оброблення цифрової інформації, порядок якої встановлює власник інформаційно-телекомунікаційної систем. Унаслідок спотворення процесу оброблення цифрової інформації одержують інший інформаційний результат [217].

М. Карчевський під цим суспільно небезпечним наслідком розуміє одержання в результаті операцій із комп'ютерною інформацією, здійснюваних за допомогою технічних чи програмних засобів, результатів, що не відповідають характеристикам технічних засобів або алгоритму комп'ютерної програми [218].

Як приклад хочемо навести узагальнення судової практики кримінальних справ і кримінальних проваджень про злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку за період із 2012 по 2014 роки. Зокрема, Особа 1 за матеріальну вигоду встановила Особі 2 супутникову антену, призначену для приймання супутникових радіосигналів, до якої

були підключені технічні засоби Особи 1, зокрема модифікований роутер і конвектор, завдяки якому Особа 2 змогла здійснити несанкціоноване декодування з подальшим переглядом телепрограм із платним доступом безкоштовно [219].

Ми погоджуємося з М. Дмитрук, яка акцентує увагу, що порушення встановленого порядку маршрутизації цифрової інформації є одним із наслідків спотворення процесу її оброблення. Відповідно до Закону України від 1 грудня 2022 року «Про платіжні послуги» маршрутизація – це обмін даними між учасниками платіжної системи під час виконання платіжних операцій [220].

Власне під порушенням установленого порядку маршрутизації цифрової інформації ми розуміємо протиправну зміну адресата цифрової інформації, оброблюваної в інформаційно-телекомунікаційних системах, шляхом несанкціонованого втручання в їх роботу.

Хочемо наголосити, що внаслідок стрімкого розвитку інформаційно-телекомунікаційних технологій, систем і мереж з’являються все нові способи вчинення несанкціонованого втручання. Також пропонуємо шляхом узагальнення понять інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж, у яких циркулює цифрова інформація, визначити їх за сукупністю ознак як інформаційно-телекомунікаційні технології, системи та мережі.

Суб’єктом кримінального правопорушення в кіберпросторі є фізична осудна особа, яка досягла віку кримінальної відповідальності, а саме: 16 років.

Суб’єктивна сторона проявляється у вигляді прямого або непрямого умислу.

Кваліфікаційними ознаками аналізованого кримінального правопорушення є такі: 1) вчинення дій повторно або групою осіб; 2) якщо

дії у формі несанкціонованого втручання призвели до наслідків у вигляді витоку, втрати, підробки, блокування інформації, спотворення процесу її оброблення або порушення установленого порядку її маршрутизації; 3) якщо такі дії заподіяли значну шкоду чи створили небезпеку тяжких технологічних аварій або екологічних катастроф, загибелі або масового захворювання населення чи інших тяжких наслідків; 4) якщо дії, визначені частиною 3 або 4 аналізованої статті, вчинені під час воєнного або надзвичайного стану.

У примітці до статті 361 Особливої частини Кримінального кодексу України визначено, що значною шкодою в статтях 361 і 363-1 вважається шкода, що в триста й більше разів перевищує неоподатковуваний мінімум доходів громадян. Станом на 2023 рік значна в грошовому еквіваленті шкода становить близько 372 150 гривень.

Варто наголосити, що кримінальне правопорушення, передбачене статтею 361 Особливої частини Кримінального кодексу України, має спеціальні умови звільнення від кримінальної відповідальності. Зокрема, відповідно до частини 6 статті 361 Особливої частини Кримінального кодексу України дії, передбачені частинами 1–4 цієї статті, не вважаються несанкціонованим втручанням у роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж, якщо вони були вчинені відповідно до порядку пошуку й виявлення потенційних вразливостей таких систем чи мереж.

Вважаємо недоречною й соціально не обумовленою диспозицію частини 5 статті 361 Особливої частини Кримінального кодексу України, що містить у собі кваліфікаційну ознаку у формі вчинення дій, передбачених частиною 3 або 4 цієї статті, – в умовах воєнного або надзвичайного стану, оскільки фактично будь-яке несанкціоноване втручання в інформаційно-телекомунікаційні технології, системи та

мережі, що має один з альтернативних наслідків у формі витоку, втрати, підробки, блокування інформації, спотворення процесу її оброблення або порушення встановленого порядку її маршрутизації, в умовах воєнного або надзвичайного стану буде кваліфікуватися за частиною 5 статті 361 Особливої частини Кримінального кодексу України незалежно від заподіяної шкоди.

Пропонуємо викласти статтю 361 Особливої частини Кримінального кодексу України у такій редакції.

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

1. Несанкціоноване втручання в роботу інформаційно-телекомунікаційних технологій, систем та мереж, тобто одержання можливості для ознайомлення та (або) використання цифрової інформації, що міститься в інформаційно-телекомунікаційній технології, системі або мережі, шляхом 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 та (або) знищення цифрової інформації.

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

3. Дії, передбачені частинами 1 або 2 цієї статті, якщо вони призвели до витоку, перехоплення, копіювання, спотворення процесу оброблення та (або) модифікації цифрової інформації.

4. Дії, передбачені частинами 1 або 2 цієї статті, якщо вони призвели до блокування та (або) знищення цифрової інформації.

5. Дії, передбачені частинами 1–4 цієї статті, якщо вони вчинені організованою групою чи злочинною організацією або заподіяли значну

шкоду чи створили небезпеку тяжких технологічних аварій чи екологічних катастроф, загибелі або масового захворювання населення чи інших тяжких наслідків.

6. Дії, передбачені частинами 3–4 цієї статті, якщо вони вчинені під час дії воєнного стану.

7. Дії, передбачені частинами 1–4 цієї статті, не вважаються несанкціонованим втручанням в інформаційно-телекомунікаційні технології, системи та мережі, якщо вони були вчинені відповідно до порядку пошуку й виявлення потенційних вразливостей таких систем чи мереж.

Запропоновані зміни до статті 361 Особливої частини Кримінального кодексу України базуються саме на нагальності градації кримінальної відповідальності за настання суспільно небезпечних наслідків. Водночас, маючи визначення поняття «несанкціоноване втручання в інформаційно-телекомунікаційні технології, системи та мережі» можемо відмежувати дії особи, яка вчиняє кримінальне правопорушення у формі незаконного доступу до цифрового пристрою потерпілої особи, якщо воно не спричинило наслідків у формі витоку, копіювання, перехоплення, модифікації, спотворення процесу оброблення, блокування й знищення цифрової інформації.

Як приклад кваліфікації суспільно небезпечного діяння за частиною 1 аналізованої статті хочемо навести таку ситуацію. Особа 1, працюючи у фірмі з наданням ІТ-послуг і маючи пароль від персонального комп'ютера Особи 2, шляхом уведення паролю авторизувалася під обліковим записом Особи 2. Не маючи на меті копіювання інформації, Особа 1 здійснила огляд цифрових документів, що містили звіти про роботу Особи 2, з подальшим використанням зазначеної інформації у своїй роботі.

Наведений приклад чітко відображає, як кваліфікувати дії особи, яка вчинила кримінальне правопорушення, передбачене запропонованою нами частиною 1 статті 361 Особливої частини Кримінального кодексу України.

Проте, на нашу думку, вчиняючи діяння, передбачене як запропонованою нами частиною 1 статті 361 Особливої частини Кримінального кодексу України, так і чинним Кримінальним кодексом України, особа має на меті досягти альтернативні наслідки у формі витоку, копіювання, перехоплення, модифікації, спотворення процесу оброблення, блокування та знищення цифрової інформації. Тому, ми переконані, що фактично в усіх випадках суд повинен додатково кваліфікувати дії особи як замах на кримінальне правопорушення, передбачене частинами 3–4 аналізованої статті (зі змінами).

На нашу думку, використання такої конструкції більш прийнятне для чинного кримінального законодавства України, оскільки в ній ураховано суспільну небезпеку того чи іншого наслідку, завданого несанкціонованим втручанням у роботу інформаційно-телекомунікаційних технологій, систем і мереж. Водночас суспільно небезпечне діяння, передбачене в статті 361 Особливої частини Кримінального кодексу України, не завжди буде кваліфікуватися за частиною 1 цієї статті як додатковою, а лише в разі ознайомлення особи, яка вчинила кримінальне правопорушення, з цифровою інформацією жертви.

Наприклад, у разі настання наслідків несанкціонованого втручання в роботу інформаційно-телекомунікаційних технологій, систем і мереж у формі блокування, копіювання, перехоплення, модифікації цифрової інформації завжди буде додатковий наслідок у вигляді ознайомлення (витоку) інформації, а отже, дію кваліфікуватимуть за частиною 1 статті 361 в обов'язковому порядку. Наприклад, у разі знищення цифрової інформації, особа, яка вчинила кримінальне правопорушення, може не спричинити наслідків у формі ознайомлення (витоку) цифрової інформації, а отже, її дії кваліфікуватимуть за частиною 3 статті 361, запропонованою до змін.

Варто зауважити, що згідно зі статистичною інформацією про стан злочинності на теренах України кримінальне правопорушення, передбачене

статтею 361 Особливої частини Кримінального кодексу України, становить 40 % від усіх інших кримінальних правопорушень у кіберпросторі розділу XVI [221].

Інше кримінальне правопорушення, що ми проаналізуємо, стало популярним за останні декілька років. Стаття 361-1 Особливої частини Кримінального кодексу України одержала назву «Створення з метою протиправного використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут».

Окремим масивом у рамках кримінальних правопорушень у кіберпросторі є суспільно небезпечні діяння, пов'язані зі створенням, збутом і розповсюдженням шкідливого програмного забезпечення й технічних засобів, що перешкоджають нормальному функціонуванню інформаційно-телекомунікаційних технологій, систем та мереж.

Зазначений тип кримінальних правопорушень у кіберпросторі сьогодні став організованим і транснаціональним, а ризику шкідливого впливу піддаються не лише комп'ютери, а й інші цифрові пристрої та інформаційно-телекомунікаційні системи й мережі. Протиправність і суспільна небезпека використання шкідливого програмного забезпечення та технічних засобів полягають здебільшого в тому, що користувачі навіть не здогадуються, що їх цифрові пристрої було заражено такими програмами.

Німецької компанією, що опікується й спеціалізується на питаннях забезпечення інформаційної безпеки, «G Data Software AG» було опубліковано статистичні дані щодо наявності на приватних цифрових пристроях шкідливого програмного забезпечення. Опитування проходило серед 15 тисяч користувачів інтернет-мережі, віком від 15 до 65 років в усьому світі. Зокрема, більше ніж 90 % опитаних переконані в тому, що шкідливе програмне забезпечення завдає помітної шкоди їх цифровим пристроям, насамперед комп'ютеру. Приблизно 45 % вважають, що

внаслідок зараження комп’ютера шкідливим програмним забезпеченням його функціональність і роботоздатність відразу погіршуються. На думку майже 55 %, у такому разі хоча б одна з функцій, що забезпечують нормальну роботу комп’ютера, пошкоджена або взагалі перестає функціонувати.

Безпосереднім об’єктом аналізованого кримінального правопорушення є порядок створення та обігу програмного забезпечення й технічних засобів, яким повинні забезпечуватися вимоги до конфіденційності, доступності та цілісності цифрової інформації.

Предметом цього кримінального правопорушення в кіберпросторі є шкідливі програмні й технічні засоби.

На нашу думку, варто детальніше зупинитися на шкідливому програмному забезпеченні та шкідливих технічних засобах, визначити їх основні види й відмінності.

Основна відмінність шкідливого програмного забезпечення від шкідливих технічних засобів полягає в їх матеріальній складовій. Шкідливе програмне забезпечення циркулює лише в кіберпросторі й не має матеріального вираження, оскільки є програмним кодом. Так само шкідливі технічні засоби – це предмети матеріального світу, що з огляду на свою специфіку можуть бути використані для вчинення кримінальних правопорушень у кіберпросторі, зокрема несанкціонованого втручання в роботу інформаційно-телекомунікаційних систем і мереж. Фактично можемо говорити, що традиційні цифрові технології переходять до групи шкідливих технічних засобів шляхом їх модифікації.

Ми вважаємо, що шкідливі технічні засоби можна класифікувати за процесом створення, зокрема: 1) шкідливі технічні засоби, створені спеціально для вчинення певної категорії кримінальних правопорушень, які не можуть бути використані для іншої роботи; 2) традиційні технічні засоби, які після модифікації застосовують для вчинення

кримінальних правопорушень; 3) традиційні технічні засоби, що можуть використовуватися для вчинення кримінальних правопорушень.

До першої групи шкідливих технічних засобів належать автомобільні кодграбери, банкоматні скімери.

Автомобільний кодграбер – це пристрій для зчитування, аналізу й генерування кодових послідовностей радіочастотних сигналів та імпульсів, основне призначення якого – несанкціоноване вимкнення й управління радіоелектронними пристроями [222].

Банкоматний скімер являє собою мініатюрний модуль, що зазвичай кріплять на банкомат. Зловмисники розміщують його всередині карткоприймача, що дає змогу зробити модуль максимально непомітним і спрощує процедури зчитування й копіювання необхідних даних [223].

До другої групи можна класифікувати такий технічних засіб, як банківський термінал із NFC-модулем, за допомогою якого можна безконтактно, дистанційно та несанкціоновано одержати дані банківської картки з телефона, у якому є NFC-модуль. Безконтактні картки – це RFID-технологія (Radio Frequency IDentification, радіочастотна ідентифікація), тобто спосіб автоматичної ідентифікації об’єктів, за якого зчитуються радіосигнали або записуються дані, що зберігаються в так званих транспондерах (RFID-мітках). Зазначені мітки інтегрують у собі чип та антену для приймання – передавання сигналу. Коли антена потрапляє в поле зчитувача, генерується електричний струм, що живить чип. Дальність дії зчитувача залежить від його типу й може становити від декількох сантиметрів до 30 метрів (зчитувачі дальньої ідентифікації). Для передавання даних застосовують технологію NFC (Near field communication, зв’язок ближнього поля), що функціонує на дистанції до 10 сантиметрів на частоті 13,56 МГц.

Дальність передавання даних через NFC – перший бар’єр захисту. Якщо картку підносять впритул до терміналу, зчитати інформацію

неможливо. Але якщо транзакція проходить на відстані, то шахраї вже придумали нестандартний зчитувач, що працює на дистанції. Також іспанські хакери Рікардо Родрігес і Хосе Вілла розробили концепт троянця. Він перетворює смартфон користувача на щось на зразок ретранслятора NFC-сигналу. Це відбувається тоді, коли телефон і картка лежать разом. Через NFC можна вкрасти не саму «транзакцію» (вона досить надійно захищена шифруванням одноразовим кодом), а інформацію про банківську картку [224].

До останнього виду належать традиційні технічні засоби, що не мають ознак шкідливого технічного засобу, але водночас є засобом вчинення кримінального правопорушення. Зокрема, через Інтернет можна замовити технічний пристрій, що кодуватиме стрічку банківської картки за заданими параметрами, тобто параметрами вже існуючої банківської картки, створюючи дублікат.

Як ми вже акцентували увагу, на відміну від шкідливих технічних засобів шкідливе програмне забезпечення не має матеріального характеру, а виражається саме в кіберзалежній складовій і пов’язане із заподіянням шкоди суспільним відносинам у сфері обігу цифрової інформації, що зберігається в цифрових пристроях.

Основними особливостями шкідливого програмного забезпечення є швидке саморозповсюдження 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) примусове перезавантаження операційної системи цифрового пристрою; 3) знищення цифрової інформації, що знаходилася на цифровому пристрої; 4) унесення змін до файлової системи цифрового пристрою; 5) уповільнення режиму роботи цифрового пристрою або її повне зупинення.

На основі специфічних особливостей шкідливого програмного забезпечення пропонуємо зробити класифікацію цієї категорії та охарактеризувати його основні типи. За функцією розмноження (саморозповсюдження) виділяємо таке шкідливе програмне забезпечення: 1) здатне до саморозмноження (саморозповсюдження); 2) не здатне до саморозмноження (саморозповсюдження).

До першої групи належать такі шкідливі програми: 1) комп'ютерний вірус; 2) комп'ютерні хробаки; 3) троянські комп'ютерні віруси.

Комп'ютерні віруси – це програмні засоби, здатні самовідтворюватися, тобто відтворюватися й використовуватися як інший програмний код, що вони змінюють таким чином, щоб убудувати в нього свою копію. У результаті замість коду програми, запущеного користувачем, виконується код вірусу. Детальніше комп'ютерні віруси буде розглянуто далі в цьому розділі. Віруси – це зловмисне програмне забезпечення з механізмом самовідтворення. Вони існують як виконуваний файл і розповсюджуються шляхом копіювання в інші хост-системи. Оскільки це пасивний тип програмного забезпечення, зараження відбувається через файли, носії інформації або мережеві файли. Залежно від того, наскільки складним є програмний код, він може навіть модифікувати свої дублікати [225].

Варто зауважити, що комп'ютерні віруси можна використовувати не лише для пошкодження комп'ютерних мереж та вузлів, а і як елементи знаряддя під час вчинення крадіжки цифрової інформації, відображання небажаної реклами, створення ботнетів та DDOS-атак.

Комп'ютерні хробаки – це мережеві віруси, здатні до розповсюдження по комп'ютерній мережі шляхом своєї реплікації [226, с. 445].

Комп’ютерні хробаки є активними шкідливими програмами, що поширюються по комп’ютерній мережі за допомогою різних вразливих особливостей операційної системи цифрового пристрою. Водночас вони здатні робити це самостійно, без будь-якого втручання користувача. Комп’ютерні хробаки виконують дві основні функції: 1) передають свій програмний код на інший цифровий пристрій; 2) віддалено активують свій програмний код на іншому, уже ураженому цифровому пристрої [227].

Незважаючи на шкідливість програми цього типу, її здебільшого використовують для введення корисних навантажень, що можуть бути іншими шкідливими програмами, зокрема такими, як троянські віруси або бекдори [228].

Троянський комп’ютерний вірус – це різновид шкідливого програмного забезпечення, що виконує небажані функції, маскуючи себе під корисну програму. Троянські програми зазвичай не розповсюджуються шляхом убудовування в код інших програм, а поширюються з використанням соціальної інженерії. Зловмисники можуть одержати контроль над інфікованим комп’ютером і заволодіти персональними даними [229].

Основною особливістю програм цього типу є саме функція розмноження, здійснювана автоматизовано незалежно від дії особи, яка створила шкідливу програму, чи користувача (власника) цифрового пристрою.

До другої класифікаційної групи належить таке шкідливе програмне забезпечення: 1) бекдор (backdoor); 2) викрадач інформації (stealer); 3) руткіт (rootkit); 4) залякувальне програмне забезпечення (scareware); 5) кілогер (keylogger); 6) вірус-вимагач (ransomware); 7) кліпери (clippers); 8) майнери (miners).

Бекдор (backdoor) – це шкідливий програмний код, що встановлюється в систему, щоб надати зловмисникові віддалений доступ.

Бекдори зазвичай дають змогу підключитися до комп’ютера з мінімальною аутентифікацією або зовсім без неї й виконувати команди в локальній системі [230].

У контексті вчинення кримінальних правопорушень у кіберпросторі бекдор проявляється саме через надання віддаленого доступу до комп’ютера жертви з подальшим використанням потужностей цифрового пристрою для здійснення DDOS-атак, за яких системно цифровий пристрій жертви є одним із тисячі знарядь вчинення одного кримінального правопорушення, під час якого всі дії на цифровому пристрої жертви здійснюються в автоматизованому режимі.

Ще одним шкідливим програмним забезпеченням є руткіт (rootkit), що являє собою програму або набір програм для приховування слідів присутності зловмисника або шкідливої програми в системі [231]. Це дуже небезпечний інструмент у розпорядженні зловмисника. Специфіка цього типу шкідливого програмного забезпечення полягає в тому, що він не завдає шкоди цифровому пристрою, а його головною метою є саме приховування іншої шкідливої програми як від самого користувача, так і від антивірусного програмного продукту [232].

Залякувальне програмне забезпечення (scareware) являє собою шкідливий програмний код, здебільшого графічний, що спонукає користувача до купівлі чогось. Таке програмне забезпечення в разі потрапляння на комп’ютер жертви спливанням різних вікон може повідомляти користувача про те, що його цифровий пристрій, наприклад, заражений вірусною програмою, з подальшим його схилянням до купівлі певного програмного забезпечення, яке пропонує шкідлива програма.

Напевно, найпопулярнішою шкідливою програмою серед осіб, які вчиняють кримінальні правопорушення в кіберпросторі, є саме викрадач інформації (stealer), що являє собою шкідливий програмний код, який збирає інформацію на цифровому пристрої жертви й направляє її особі, яка

вчиняє кримінальне правопорушення. Такі шкідливі програми збирають хеші паролів і кілогери. Викрадач інформації (stealer) використовують для одержання паролів, доступу до облікових записів, інтернет-банкінгу та всієї іншої цифрової інформації, збереженої в браузері жертви. Варто наголосити, що він одночасно є найпримітивнішим шкідливим забезпеченням та одним із найбільш суспільно небезпечних. Це зумовлено низкою причин. Зокрема, серед основних причин суспільної небезпеки цього типу шкідливого програмного забезпечення є:

1) доступність. Варто звернути увагу, що більшість шкідливих програм того чи іншого типу можна з легкістю знайти в інтернет-просторі, викрадач інформації не є винятком. Водночас потрібно підкреслити, що якість таких безкоштовних шкідливих програм перебуває на низькому технічному рівні, тому їх переважно виявляє антивірусне програмне забезпеченням;

2) велика кількість способів поширення цього типу шкідливого програмного забезпечення. Зазвичай його поширюють через різні doc-, pdf-, png- та jpeg-файли шляхом крипування власне шкідливого програмного коду в зазначеному файлі. Крипування – це процес приєднання шкідливої програми до файлу з певним умістом, наприклад поширення pdf-файлу з цим шкідливим кодом через соціальні мережі або за допомогою рекламних платформ. Водночас на такому файлі міститься корисна або така, що зацікавить користувача, інформація, яку потенційна жертва завантажує на свій цифровий пристрій;

3) вразливість користувачів до цього типу шкідливого програмного забезпечення. Унаслідок фактичної абсорбації кіберпростором звичних сфер життєдіяльності людини та переведення фізичних процесів у кібернетичні все більше й більше сфер діяльності переходять в інтернет-простір. Водночас його користувачі не завжди встигають набути навичок інтернет-безпеки, унаслідок чого стають легкою здобиччю зловмисників. У

доктринальних джерелах цей тип шкідливого програмного забезпечення входить до підтипу шпигунського програмного забезпечення.

Ще одним підтипом шпигунського програмного забезпечення є кілогер (keylogger). Це шкідливе програмне забезпечення реєструє кожну дію користувача, зокрема рух комп'ютерної миші, натискання кнопок на клавіатурі, відтворення аудіо- й відеоряду, даючи змогу заволодіти даними користувача, уведеними ним після зараження цифрового пристрою. Потім ці дані передаються зловмисникові через мережу Інтернет. Ці програми використовують для перехоплення паролів, наприклад паролів для інтернет-банкінгу. Зловмисники також можуть застосовувати це шпигунське програмне забезпечення для потреб викрадення іншої особистої інформації, наприклад документів, збережених на вебсайті комп'ютера [233, с. 7076].

Вірус-вимагач (ransomware) – це тип шкідливого програмного забезпечення, що блокує доступ до системи або внеможливлює роботу з файлами (часто за допомогою методів шифрування), після чого вимагає від жертви викуп для відновлення вихідного стану. Щороку, за статистикою агенції цифрового захисту «Splunk», напади шкідливих програм у формі вимагачів різко зросли. Такі програми або шифрують абсолютно всі користувацькі файли на цифровому пристрої жертви, або обмежують доступ до них. Обмежуючи або шифруючи файли, особа, яка вчиняє кримінальне правопорушення в кіберпросторі, змушує жертву платити грошові кошти за відновлення доступу до них.

Кліпери – це шкідливе програмне забезпечення, що полягає в зараженні цифрового пристрою жертви з подальшою заміною банківських реквізитів, реквізитів електронних гаманців і віртуальних активів жертви на реквізити зловмисника. Тобто під час переказування грошових коштів особа, вводячи реквізити потенційного отримувача, зіштовхується з наслідками кліперу – заміною введених реквізитів на переказ на реквізити

особи, яка вчиняє кримінальне правопорушення, як результат – грошові кошти перераховуються зловмисникові. Кліпер є новим типом шкідливого програмного забезпечення. Його використовують переважно у сфері віртуальних активів, у якій неможливе здійснення чарджбеку.

Ще одним типом шкідливого програмного забезпечення, пов'язаним із віртуальними активами, є майнер. Необхідно зауважити, що за своїми характеристиками він не є шкідливим програмним забезпеченням, а переходить у цей тип лише в разі несанкціонованої інсталяції на цифровий пристрій жертви без її відома. Основне завдання майнеру полягає в добуванні віртуальних активів, що залежно від його налаштувань матиме негативні наслідки. Зокрема, якщо в налаштуваннях майнеру задані найвищі характеристики, він може призвести до значного спотворення роботи цифрового пристрою (сповільнення, гальмування), а за певних умов – його виходу його з ладу внаслідок перевантаження.

Хочемо наголосити, що перелік шкідливого програмного забезпечення не обмежується проаналізованим нами. Ми зупинилися лише на його найбільш інноваційних і поширених типах.

Розглянувши характеристику предмета кримінального правопорушення в кіберпросторі цього типу, переходимо до аналізу об'єктивної сторони.

Ми переконані, що суспільна небезпечність діяння, передбаченого статтею 361-1 Особливої частини Кримінального кодексу України, обумовлює формальний склад кримінального правопорушення, за якого сам факт створення шкідливого програмного забезпечення чи технічного засобу є достатнім для притягнення особи до кримінальної відповідальності за вчинене.

Аналізована норма передбачає такі форми реалізації об'єктивної сторони: 1) створення з метою протиправного використання, розповсюдження або збуту шкідливих програмних чи технічних засобів;

2) розповсюдження шкідливих програм і технічних засобів;
3) збут шкідливих програм та технічних засобів;

Під створенням шкідливих програмних чи технічних засобів розуміють розроблення абсолютно нового шкідливого програмного чи технічного засобу, а також модифікацію вже існуючого засобу чи програми, результатом якої є зміна його властивостей [234].

А. Боровик та І. Коптун під створенням шкідливого програмного забезпечення й технічних засобів розуміють творчу діяльність, у результаті якої одержують якісно нову програму або технічний засіб, явно наділений функціями, виконання яких може заподіювати шкоду конфіденційності, цілісності та доступності інформації, оброблюваній в інформаційно-телекомунікаційних системах [235, с. 244].

М. Карчевський пропонує розуміти під створенням шкідливих програмних або технічних засобів результат діяльності з розроблення таких засобів у вигляді нового шкідливого програмного або технічного засобу [236].

Шкідливе програмне забезпечення – це зловмисна програма або код, що шкодять кінцевим пристроям. Якщо пристрій уражено шкідливим програмним забезпеченням, може відбуватися несанкціонований доступ, ураження даних або блокування пристрою, поки ви не сплатите викуп [237].

Хочемо акцентувати увагу, що під створенням шкідливих програмних або технічних засобів варто розуміти діяльність зі створення та (або) модифікації програмного забезпечення й технічних засобів, унаслідок якої вони починають виконувати негативні функції: знищення, блокування, модифікації, копіювання цифрової інформації, оброблюваної в інформаційно-телекомунікаційних системах і мережах.

Під розповсюдженням шкідливого програмного забезпечення, на нашу думку, варто розуміти дії щодо введення шкідливої програми в господарський товарообіг або надання доступу до неї в будь-якій формі.

Крім того, під уведенням шкідливої програми в господарський товарообіг варто розуміти можливість особи, яка вчинила кримінальне правопорушення, продати чи подарувати шкідливе програмне забезпечення. Надання в будь-якій формі доступу до шкідливого програмного забезпечення полягає в його розміщення на серверах із подальшим віддаленим наданням прав на користування цією програмою.

На думку А. Боровика, розповсюдження шкідливого програмного забезпечення полягає в оплатному або безоплатному наданні копій шкідливих програм або доступу до них невизначеному колу осіб, поширення таких копій через телекомунікаційні мережі [235, с. 248].

Збут шкідливого програмного забезпечення чи технічних засобів визначають як оплатне чи безоплатне (наприклад, подарунок) передавання зазначених засобів певній особі [238]. На перший погляд може здаватися, що зміст протиправних дій у формі розповсюдження й збуту шкідливого програмного забезпечення та технічних засобів є аналогічною. Проте в доктринальних джерелах точаться дискусії з цього приводу. Зокрема, А. Боровик вважає, що між збутом і розповсюдженням шкідливого програмного забезпечення та технічних засобів є різниця в тому, що в разі розповсюдження шкідливого програмного забезпечення особа докладає певних зусиль щодо якомога більшого розширення кола осіб, які одержать копію цієї програми. Збут науковець характеризує певною обмеженістю екземплярів шкідливого програмного забезпечення, що можуть одержати особи. Ми повністю погоджуємся з позицією науковця. На нашу думку, основна відмінність розповсюдження шкідливого програмного забезпечення й технічних засобів від збуту полягає в тому, що в першому випадку особа бажає своїми діями надати доступ до шкідливого програмного забезпеченням якомога більшій кількості користувачів кіберпростору, водночас мета отримання прибутку від таких дій є необов’язковою ознакою. Навпаки, у разі збуту шкідливого програмного

забезпечення та технічних засобів першочергова мета особи полягає в отриманні прибутку від кримінально-протиправної діяльності. Крім того, на нашу думку, ще однією відмінністю буде саме якість шкідливого програмного забезпечення чи технічного засобу. У разі розповсюдження шкідливого програмного забезпечення й технічних засобів унаслідок масового характеру такої діяльності їх якість здебільшого є низькою, а сама особа, яка вчиняє кримінальне правопорушення, має на меті якомога більше ураження цифрових пристроїв своїх жертв.

Суб'єктом цього кримінального правопорушення є фізична осудна особа, яка досягла 16 років.

Суб'єктивна сторона характеризується виною у формі прямого умислу. Водночас особа, яка вчинила кримінальне правопорушення, усвідомлює, що створювані, розповсюджені або збуті технічні засоби чи програмне забезпечення призначені для несанкціонованого втручання в роботу інформаційно-телекомунікаційних пристроїв, систем і мереж.

До кваліфікаційних ознак аналізованого кримінального правопорушення належать дії, передбачені частиною 1 цієї статті, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду.

Наступним кримінальним правопорушенням у кіберпросторі цього типу, що ми розглянемо, є несанкціонований збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації, передбаченої статтею 361-2 Особливої частини Кримінального кодексу України. Відразу хочемо акцентувати увагу на пропозиції щодо узгодження термінології із сучасними досягненнями науки й техніки та викласти назву цієї статті в такій редакції:

Несанкціонований збут або розповсюдження цифрової інформації з обмеженим доступом, що зберігається в інформаційно-телекомунікаційних технологіях (пристроях), системах і мережах.

Основним безпосереднім об'єктом аналізованого кримінального правопорушення є нормальний режим функціонування цифрової інформації з обмеженим доступом.

Предмет кримінального правопорушення – цифрова інформація з обмеженим доступом, що зберігається в інформаційно-телекомунікаційних технологіях (пристроях), системах і мережах.

А. Боровик зазначає, що така інформація може бути комп'ютерною або належати до мереж електрозв'язку. Водночас науковець наголошує, що вона має свої додаткові ознаки, зокрема такі: 1) є цифровою інформацією з обмеженим доступом; 2) зберігається в інформаційно-телекомунікаційній системі; 3) створена відповідно до чинного законодавства; 4) захищена відповідно до чинного законодавства [235, с. 250].

Правова регламентація інформації з обмеженим доступом міститься в Законі України «Про доступ до публічної інформації» від 19 лютого 2022 року та Законі України «Про інформацію» від 20 листопада 2022 року [239; 240].

Статтею 21 Закону України «Про інформацію» установлено, що інформацію з обмеженим доступом поділяють на конфіденційну, таємну й службову. Варто зауважити, що в Законі України «Про інформацію» дається визначення поняття лише конфіденційної інформації, зокрема як інформації про фізичну особу, інформації, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень, а також інформацію, визнану такою на підставі закону. На основі легального визначення поняття «конфіденційна інформація» можемо виокремити її основні особливості: 1) може поширюватися за бажанням відповідної особи (власника інформації); 2) поширюється у визначеному порядку її

власником; 3) поширення здійснюється відповідно до умов її власника й згідно із законом.

Стаття 8 Закону України «Про доступ до публічної інформації» надає визначення таємної інформації. Таємна інформація – це інформація, доступ до якої обмежується відповідно до частини 2 статті 6 цього Закону та розголошення якої може завдати шкоди особі, суспільству й державі. Таємною вважають інформацію, що містить державну, професійну, банківську, розвідувальну таємницю, таємницю досудового розслідування та іншу передбачену законом таємницю [240].

Частина 2 статті 6 зазначеного Закону визначає вимоги, за яких обмежують доступ до інформації: 1) винятково в інтересах національної безпеки, територіальної цілісності або громадського порядку для запобігання заворушенням чи кримінальним правопорушенням, охорони здоров'я населення, захисту репутації або прав інших людей, запобігання розголошенню інформації, одержаної конфіденційно, або підтримання авторитету й неупередженості правосуддя; 2) розголошення інформації може завдати істотної шкоди цим інтересам; шкода від оприлюднення такої інформації переважає суспільний інтерес у її одержанні [240].

Звернімо увагу, що Закон України «Про доступ до публічної інформації» під час визначення підтипів таємної інформації відсилає до інших нормативно-правових актів. Зокрема, в статті 1 Закону України «Про державну таємницю» надається таке визначення державної таємниці: це відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України та які визнані в порядку, установленому Законом України «Про державну таємницю», державною таємницею і підлягають охороні державою. Визначення адвокатської таємниці містить стаття 22 Закону України «Про адвокатуру», нею є будь-яка інформація, що стала відома адвокатові, помічнику адвоката,

стажистові адвоката, особі, яка перебуває в трудових відносинах з адвокатом, про клієнта, а також питання, з яких клієнт (особа, якій відмовлено в укладенні договору про надання правової допомоги з передбачених цим Законом підстав) звертався до адвоката, адвокатського бюро, адвокатського об'єднання, зміст порад, консультацій, роз'яснень адвоката, складені ним документи, інформація, що зберігається на електронних носіях, та інші документи й відомості, одержані адвокатом під час здійснення адвокатської діяльності [241].

Нотаріальна таємниця – це сукупність відомостей, отриманих під час вчинення нотаріальної дії або звернення до нотаріуса заінтересованої особи, зокрема про особу, її майно, особисті майнові та немайнові права і обов'язки тощо [242].

Банківська таємниця – це інформація щодо діяльності й фінансового стану клієнта, що стала відомою банку в процесі обслуговування клієнта та взаємовідносин із ним чи третім особам під час надання послуг банку, розголошення якої може завдати матеріальної чи моральної шкоди клієнтові, зокрема: 1) відомості про банківські рахунки клієнтів, зокрема кореспондентські рахунки банків у Національному банку України; 2) інформація про операції, проведені на користь чи за дорученням клієнта, вчинені ним правочини; 3) фінансово-економічний стан клієнтів; 4) інформація про організацію й здійснення охорони банку та осіб, які перебувають у його приміщеннях; 5) інформація про організаційно-правову структуру юридичної особи – клієнта, її керівників, напрями діяльності; 6) відомості стосовно комерційної діяльності клієнтів чи комерційної таємниці, будь-якого проєкту, винаходів, зразків продукції та інша комерційна інформація; 7) інформація щодо звітності за окремим банком, за винятком тієї, що підлягає опублікуванню; 8) коди, використовувані банками для захисту інформації; 9) інформація про фізичну особу, яка має намір укласти договір про споживчий кредит, одержана під час оцінювання

її кредитоспроможності; 10) інформація про організацію та проведення інкасації коштів та/або перевезення валютних цінностей; 11) інформація про банки чи клієнтів банків, що збирається від банків під час здійснення банківського нагляду, валютного нагляду, нагляду (оверсайту) платіжних систем і систем розрахунків, а також нагляду у сфері запобігання й протидії легалізації (відмиванню) доходів, отриманих злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення; 12) інформація про банки чи клієнтів банків, одержана Національним банком України відповідно до міжнародного договору або за принципом взаємності від органу банківського нагляду іншої держави; 13) рішення Національного банку України про застосування заходів впливу, крім рішень про накладення штрафів, віднесення банку до категорії неплатоспроможних, відкликання банківської ліцензії та ліквідацію банку [243].

За конструкцією об’єктивної сторони кримінальне правопорушення, передбачене статтею 361-2 Особливої частини Кримінального кодексу України, формальне, тобто є завершеним із моменту вчинення несанкціонованого збуту або розповсюдження цифрової інформації з обмеженим доступом. Тобто об’єктивна сторона цього кримінального правопорушення виражається у двох формах: 1) несанкціонований збут цифрової інформації; 2) несанкціоноване розповсюдження цифрової інформації.

Несанкціонований збут або розповсюдження цифрової інформації з обмеженим доступом, що зберігається в інформаційно-телекомунікаційних пристроях, визначають як дії з поширення цифрової інформації без дозволу власника на платній чи безоплатній основі.

Розповсюдження цифрової інформації з обмеженим доступом являє собою платне або безоплатне надання копій такої інформації або доступу до неї невизначеному колу осіб.

Під збутом цифрової інформації з обмеженим доступом необхідно розуміти платне або безоплатне відчуження [244, с. 257].

Суб'єкт кримінального правопорушення загальний – особа, яка досягла віку кримінальної відповідальності.

Суб'єктивна сторона цього кримінального правопорушення в кіберпросторі характеризується виною у формі прямого умислу. Особа, яка вчиняє кримінальне правопорушення, повинна усвідомлювати, що цифрова інформація, яку вона розповсюджує або збуває, є інформацією з обмеженим доступом і те, що вона не має дозволу від власника такої інформації.

До кваліфікаційних ознак аналізованого кримінального правопорушення належать дії, передбачені частиною 1 цієї статті, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду.

Іншим кримінальним правопорушенням цього типу є несанкціоновані дії з інформацією, що обробляється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї, передбачені статтею 362 Особливої частини Кримінального кодексу України.

Хочемо наголосити, що вважаємо необхідним замінити термін «електронно-обчислювальна машина» на «цифровий пристрій», а «автоматизовані системи та комп'ютерні мережі» визначати в сукупності як «інформаційно-телекомунікаційні мережі», ураховуючи, що така інформація може зберігатися не лише в комп'ютерній мережі.

Основним безпосереднім об'єктом цього кримінального правопорушення в кіберпросторі є встановлений порядок зберігання й використання цифрової інформації.

Відповідно до диспозиції цієї статті предметом кримінального правопорушення є цифрова інформація, що обробляється в

телекомунікаційних пристроях та інформаційно-телекомунікаційних мережах. Закон України від 16 грудня 2020 року «Про захист інформації в інформаційно-комунікаційних системах» визначає обробку інформації в системі як виконання однієї або кількох операцій, зокрема збирання, введення, записування, перетворення, зчитування, зберігання, знищення, реєстрації, приймання, отримання, передавання, здійснювані в системі за допомогою технічних і програмних засобів. Варто зауважити, що згідно з диспозицією частин 1 та 2 статті 362 Особливої частини Кримінального кодексу України кримінально протиправними діяннями вважають лише несанкціоновану зміну, знищення, блокування, копіювання й перехоплення цифрової інформації особою, яка має право доступу до неї. Проаналізувавши об'єктивну сторону цього кримінального правопорушення, вважаємо, що варто окремо розглядати кваліфікацію діяння за частиною 1 та відповідно за частиною 2 статті 362 Особливої частини Кримінального кодексу України.

Зокрема, об'єктивна сторона кримінального правопорушення, передбаченого частиною 1 статті 362 Особливої частини Кримінального кодексу України має формальний склад і характеризується наявністю хоча б однієї форми суспільно небезпечного діяння: 1) несанкціонованої зміни цифрової інформації; 2) несанкціонованого знищення цифрової інформації; 3) несанкціонованого блокування цифрової інформації.

Несанкціонована зміна цифрової інформації являє собою діяльність, пов'язану з порушенням порядку доступу до цифрової інформації в інформаційно-телекомунікаційних технологіях, системах і мережах, модифікацією її змісту, спотворенням процесу оброблення.

Під несанкціонованим знищенням цифрової інформації варто розуміти дії, що проводяться з порушенням порядку доступу до неї, унаслідок яких вона зникає (видаляється) з інформаційно-

телекомунікаційних технологій, мереж чи систем або піддається такому спотворенню, що повністю втрачає свій зміст.

Кримінальне правопорушення, передбачене частиною 2 статті 362 Особливої частини Кримінального кодексу України, має матеріальний склад. Ним є: 1) дія у формі несанкціонованого перехоплення цифрової інформації та її несанкціонованого копіювання; 2) наслідки у формі витоку інформації; 3) причиново-наслідковий зв'язок.

Ми не будемо детально зупинятися на об'єктивній стороні цього кримінального правопорушення, оскільки всі його форми й наслідки, що можуть бути ним спричинені, наведено в статті 361 Особливої частини Кримінального кодексу України, а зосередимо увагу лише на діянні у формі перехоплення цифрової інформації. Незважаючи на те, що наслідки у формі перехоплення цифрової інформації були розглянуті під час аналізу статті 361 Особливої частини Кримінального кодексу України, хочемо зупинитися на його певних аспектах.

Насамперед нагадаємо, що перехопленням цифрової інформації варто вважати процес неправомірного одержання інформації в кіберпросторі. Водночас копіювання й витік, на нашу думку, будуть лише наслідками такого діяння. Хочемо зауважити, що дії у формі перехоплення цифрової інформації не підпадають під кваліфікацію за цією статтею, оскільки в її диспозиції чітко зазначено, що така особа має право доступу до інформації. У разі перехоплення 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 вважаємо формою її витоку. Тому пропонуємо виключити з частини 2 статті 362 Особливої частини Кримінального кодексу України дії у формі перехоплення цифрової інформації й викласти її в такій редакції:

«Несанкціоноване копіювання цифрової інформації, оброблюваної в інформаційно-телекомунікаційних технологіях, системах і мережах, якщо воно призвело до її витоку, вчинене особою, яка має право доступу до такої інформації».

Суб'єкт кримінального правопорушення, передбаченого статтею 362 Особливої частини Кримінального кодексу України, спеціальний, тобто особа, яка має право доступу до цифрової інформації. У Законі України «Про захист інформації в інформаційно-комунікаційних системах» статтею 4 визначено, що порядок доступу до інформації, перелік користувачів та їх повноваження щодо цієї інформації встановлюються її володільцем. Порядок доступу до державних інформаційних ресурсів або інформації з обмеженим доступом, вимога стосовно захисту якої встановлена законом, а також перелік користувачів та їх повноваження щодо цього типу інформації встановлюються законодавством [245].

Законом України «Про захист інформації в інформаційно-комунікаційних системах» також установлено, що власник системи забезпечує захист інформації в ній у порядку й на умовах, визначених у договорі, укладеному ним із володільцем інформації. Крім того, власник системи забезпечує користувача доступом до інформації в ній відповідно до порядку такого доступу.

Отже, можна виділити такі особливості спеціального статусу суб'єкта цього типу кримінального правопорушення в кіберпросторі: 1) установлення доступу до цифрової інформації в інформаційно-телекомунікаційній системі; 2) такий доступ установлюють відповідно до законодавства; 3) особа одержує право доступу до цифрової інформації на основі наказу, розпорядження, договору тощо.

Суб'єктивна сторона аналізованого кримінального правопорушення в кіберпросторі характеризується виною у формі прямого або непрямого умислу. Особа, яка вчинила кримінальне правопорушення, повинна

усвідомлювати, що здійснила несанкціоновані дії щодо цифрової інформації в інформаційно-телекомунікаційний системі з порушенням порядку доступу до такої інформації, установленого відповідно до законодавства.

Кваліфікаційними ознаками статті 362 Особливої частини Кримінального кодексу України є такі: 1) несанкціоноване перехоплення або копіювання інформації, що оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, якщо воно призвело до її витоку, вчинене особою, яка має право доступу до такої інформації; 2) дії, передбачені частиною 1 або 2 цієї статті, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду.

Протиправне діяння у формі несанкціонованого перехоплення або копіювання інформації, що оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, якщо воно призвело до її витоку, вчинене особою, яка має право доступу до такої інформації, ми розглянули в аналізі об'єктивної сторони цього кримінального правопорушення, тому зупинимося лише на нагальності заміни й уніфікації термінів «електронно-обчислювальна машина», «автоматизована система», «комп'ютерна мережа».

Кримінальну відповідальність за порушення правил експлуатації інформаційно-телекомунікаційних технологій, систем і мереж або порядку правил захисту цифрової інформації, що в них оброблюється, установлено статтею 363 Особливої частини Кримінального кодексу України «Порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж

електрозв’язку або порядку чи правил захисту інформації, яка в них оброблюється».

Основним безпосереднім об’єктом аналізованого кримінального правопорушення в кіберпросторі є суспільні відносини, пов’язані з внутрішньою безпекою засобів зберігання, оброблення й передавання цифрової інформації, що міститься в інформаційно-телекомунікаційних технологіях, системах і мережах. Можна сказати, що це суспільні відносини у сфері нормальної експлуатації інформаційно-телекомунікаційних технологій, систем та мереж.

Особливістю об’єктивної сторони цього кримінального правопорушення в кіберпросторі є бланкетний характер диспозиції, тобто воно містить терміни, визначення й пояснення, що варто шукати в інших нормативно-правових актах, зокрема: 1) правила експлуатації; 2) порядок захисту цифрової інформації; 3) правила захисту цифрової інформації.

Зазначені альтернативні дії полягають у невиконанні правил щодо режиму роботи технологій, передбачених інструкціями, правил внутрішнього розпорядку, а також правил обігу цифрової інформації. Варто зазначити, що правила експлуатації інформаційно-телекомунікаційних технологій, систем і мереж, а також правила й порядок захисту інформації можуть установлювати на підставі положень як закону, так і договору між власником цифрової інформації та, наприклад, її розпорядником за договором

Водночас стаття 363 Особливої частини Кримінального кодексу України є відсильною, оскільки не містить у собі конкретних технічних вимог. Для визначення, чи є зазначені дії порушенням правил експлуатації інформаційно-телекомунікаційних технологій чи правил захисту інформації, стаття відсилає до певних інструкцій або правил, що обумовлюють порядок роботи з інформаційно-телекомунікаційними

технологіями, системами та мережами, які встановлюються правоможною особою та доводяться до користувачів.

Аналізоване кримінальне правопорушення має матеріальний склад і характеризується такими ознаками: 1) суспільно небезпечне діяння у формі порушення правил експлуатації інформаційно-телекомунікаційних технологій, систем і мереж, порядку чи правил захисту цифрової інформації; 2) суспільно небезпечні наслідки у формі значної шкоди; 3) необхідний причиновий зв'язок між суспільно небезпечним діянням і суспільно небезпечними наслідками.

Під порушенням правил експлуатації інформаційно-телекомунікаційних технологій, систем і мереж необхідно розуміти недотримання вимог до власника інформаційно-телекомунікаційної технології, системи чи мережі щодо її використання та обслуговування. Варто зауважити, що таке порушення може виражатися у формі самовільної інсталяції нового програмного або апаратного забезпечення. Наприклад, особа, відповідальна за вебсайт підприємства, інсталює в КСМ-систему нові неперевірені плагіни із сумнівного ресурсу, що містять у собі шкідливий програмний код, як наслідок – зараження вебресурсу, яке призвело до витоку даних, або встановлення на сервер, на якому розміщений вебсайт, шкідливого коду, що копіює інформацію. Також порушення правил експлуатації інформаційно-телекомунікаційних технологій, систем і мереж може полягати в підключенні комп'ютерної техніки чи інших цифрових пристроїв до інформаційно-телекомунікаційної мережі без фільтрів, що призвело до нівелювання додаткового процесу фільтрації шкідливого програмного забезпечення в системі [246].

Порушення порядку захисту цифрової інформації – це визначені нормативно-правовими актами вимоги до створення й організації роботи системи захисту цифрової інформації, що полягають у забезпеченні запобігання несанкціонованим діям щодо інформації, яка обробляється в

інформаційно-телекомунікаційній системі. Прикладом такого діяння може бути робота з інформацією, що має таємний доступ, за відсутності належно сертифікованої системи захисту. Вироком Шевченківського районного суду міста Києва обвинувачений визнаний винним у вчиненні кримінального правопорушення, передбаченого частиною 1 статті 363 Особливої частини Кримінального кодексу України. Особа 1 порушила правила експлуатації інформаційно-телекомунікаційної системи, адміністратором якої вона була, що призвело до подальшого несанкціонованого втручання в зазначену систему, зокрема службових серверів і поштових серверів клієнтів Державної міграційної служби, з подальшим завантаженням шкідливого програмного коду та наслідків у формі витоку конфіденційної інформації.

Варто зауважити, 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 порушенням правил захисту цифрової інформації потрібно розуміти недотримання вимог до реалізації системи захисту цифрової інформації певного інформаційного ресурсу. Прикладом порушення правил може бути неналежне зберігання паролів доступу до цифрової інформації.

Наприклад, Особа 1, яка є адміністратором і має в обслуговуванні декілька вебресурсів певного підприємства, зрозуміла, що внаслідок одержання паролів від вебресурсів третьою особою інформація підприємства, розміщена на вебсерверах, може бути модифікована, скопійована, знищена або заблокована. Таку інформацію з паролями від вебресурсів і вебсерверів вона зберігала на багатьох носіях, зокрема своїй поштовій скриньці. Унаслідок того, що Особа 1, працюючи за іншим комп’ютером, забула вийти зі своєї поштової скриньки, цим скористалася Особа 2, знайшовши у вибраних повідомленнях файл із паролями від

вебресурсів та вебсерверів підприємства. Використавши зазначені паролі доступу, Особа 2 скопіювала всю інформацію про клієнтів підприємства.

Необхідно акцентувати увагу, що наразі відповідальність за забезпечення захисту інформації покладається на власника системи. Крім того, сьогодні немає уніфікованих норм і правил, що регулюють експлуатацію інформаційно-телекомунікаційних технологій, а також порядку й правил захисту інформації.

Наслідки у формі значної шкоди є обов'язковою умовою настання кримінальної відповідальності за вчинене діяння. Вважаємо, що в примітці до цієї статті варто визначити, що саме розуміється під значною шкодою. Пропонуємо в примітці до статті 363 Особливої частини Кримінального кодексу України «шкода, передбачена цією статтею, визнається значною, якщо вона в п'ятдесят і більше разів перевищує неоподатковуваний мінімум доходів громадян».

Суб'єктом кримінального правопорушення в кіберпросторі, передбаченого статтею 363 Особливої частини Кримінального кодексу України, є особа, яка відповідає за експлуатацію інформаційно-телекомунікаційних технологій, мереж чи систем, або та, на яку покладено забезпечення захисту цифрової інформації. Такий статус особи встановлюється відповідним наказом, розпорядженням або договором. Крім того, вказівка на відповідальність особи може бути визначена в правилах внутрішнього розпорядку підприємства, установи, організації. У будь-якому разі особа, яка несе відповідальність за експлуатацію інформаційно-телекомунікаційних технологій, мереж чи систем, або та, на яку покладено забезпечення захисту цифрової інформації, здійснює таку діяльність відповідно після ознайомлення з правилами чи інструкціями, що регламентують роботу наведених технологій, систем чи мереж, під особистий підпис. Отже, суб'єкт цього кримінального правопорушення в кіберпросторі спеціальний.

З точки зору суб'єктивної сторони кримінальне правопорушення може бути вчинене у формі умислу або необережності, водночас ставлення до наслідків завжди повинне бути необережним. Якщо настання наслідків охоплюється прямим умислом особи, яка вчинила кримінальне правопорушення, складу кримінального правопорушення, передбаченого статтею 363 Особливої частини Кримінального кодексу України, немає.

А. Боровик зазначає, що, якщо умисні дії особи внаслідок порушення експлуатації інформаційно-телекомунікаційних технологій спричинили їх пошкодження, то діяння варто кваліфікувати за статтею 194 Особливої частини Кримінального кодексу України «Умисне знищення або пошкодження майна». Водночас, якщо порушенням правил захисту цифрової інформації було спричинено наслідки у вигляді блокування, копіювання, знищення, модифікації або розповсюдження та збуту такої інформації, дії особи, яка вчинила кримінальне правопорушення, необхідно кваліфікувати як пособництво за частинами 2 та 4 статті 361 Особливої частини кримінального кодексу України «Несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж» або за статтею 362 Особливої частини кримінального кодексу України «Несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї» [235, с. 260].

На нашу думку, особа, яка умисно порушила правила й порядок захисту цифрової інформації, унаслідок чого відбувся її витік або інші суспільно небезпечні наслідки, передбачені частиною 3 статті 361 Особливої частини Кримінального кодексу України, повинна нести кримінальну відповідальність за сукупністю кримінальних правопорушень, лише тоді, коли вона не виконувала об'єктивну сторону кримінального

правопорушення, передбаченого статтею 362 Особливої частини Кримінального кодексу України.

Пропонуємо викласти диспозицію статті 363 Особливої частини Кримінального кодексу України в такій редакції:

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

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

Останнім кримінальним правопорушенням у кіберпросторі цього типу, що ми розглянемо, є перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку, передбачене статтею 363-1 Особливої частини Кримінального кодексу України.

Безпосереднім об'єктом аналізованого кримінального правопорушення в кіберпросторі є процеси оброблення цифрової інформації в інформаційно-телекомунікаційних технологіях, системах і мережах. До них належить передавання, отримання, перетворення, реєстрація, зберігання цифрової інформації, здійснювані за допомогою засобів програмної й технічної підтримки.

Предметом цього кримінального правопорушення є повідомлення електрозв'язку, що умисно та масово надсилаються на адресу споживача певної інформаційно-телекомунікаційної системи без попередньої з ним згоди, крім повідомлень самого власника інформаційно-телекомунікаційної системи.

Під повідомленням електрозв'язку варто розуміти відомості, подані у вигляді, що дає змогу передавати їх за допомогою комп'ютерних мереж або мереж електрозв'язку [218].

Оскільки склад кримінального правопорушення є матеріальним, об'єктивна сторона виражена у формі: 1) діяння, що полягає в масовому поширенні повідомлень електрозв'язку, здійсненому без попередньої згоди отримувача; 2) суспільно небезпечні наслідки у формі порушення або припинення режиму роботи інформаційно-телекомунікаційних технологій, систем і мереж; 3) необхідний причиновий зв'язок між діяннями й наслідками.

Суспільно небезпечна дія як одна з ознак об'єктивної сторони аналізованого кримінального правопорушення полягає в розповсюдженні повідомлень електрозв'язку, тобто направленні певним адресатам копій цих повідомлень, що характеризуються масовістю й відсутністю попередньої згоди адресатів [246]. А. Боровик вважає, що розповсюдження варто вважати масовим тоді, коли одне або декілька повідомлень одержують більше ніж один адресат [235, с. 230].

А. Бойко переконаний, що розповсюдження повідомлень електрозв'язку є масовим, якщо такі повідомлення не готують окремо для кожного адресата, а створюють із використанням можливостей комп'ютера шляхом багаторазового автоматичного копіювання й розсилають автоматично на адреси, що тим чи іншим способом опинилися в розпорядженні відправника та внесені ним до певного списку, згідно з яким провадиться розсилання [247].

Масове розповсюдження повідомлень електрозв'язку визначається як «спам». Відповідно до Закону України від 16 грудня 2020 року «Про електронні комунікації» спамом є електронні, текстові та/або мультимедійні повідомлення, що без попередньої згоди (замовлення) користувачів неодноразово (більше ніж п'ять повідомлень одному

абонентові) надсилаються на їхні адреси електронної пошти або кінцеве (термінальне) обладнання, крім повідомлень постачальника електронних комунікаційних послуг щодо надання ним електронних комунікаційних послуг або повідомлень від органів державної влади чи органів місцевого самоврядування з питань, що належать до їх повноважень.

Необхідно зазначити, що в цьому разі така ознака, як масовість, є оцінковою, тобто щодо розповсюдження повідомлень електрозв'язку вона буде обов'язковою характеристикою, а стосовно адресатів має необов'язковий характер.

Така характеристика, як відсутність попередньої згоди адресата, полягає у відсутності в будь-якій формі згоди на надсилання йому повідомлень електрозв'язку, що є предметом кримінального правопорушення.

Суспільно небезпечні наслідки у формі порушення роботи інформаційно-телекомунікаційних технологій, систем чи мереж полягають у зміні встановлених власником чи уповноваженими ним особами параметрів процесу оброблення цифрової інформації в зазначених технологіях, системах і мережах. Зокрема, до таких процесів належать: 1) уповільнення чи прискорення процесу оброблення цифрової інформації; 2) припинення процесу оброблення частини цифрової інформації; 3) модифікація результатів оброблення цифрової інформації [248].

Припинення роботи інформаційно-телекомунікаційних технологій, систем чи мереж полягає в остаточному або тимчасовому припиненні їх функціонування.

Найпопулярнішим типом цього кримінального правопорушення є DDoS-атаки. DDoS-атака – це атака на комп'ютерні системи органу, організації, установи або окремого власника вебресурсу з метою порушення доступності атакованих вебресурсів. Простими словами, під час атаки одночасно створюється така величезна кількість зовнішніх запитів (рахунок

може йти на мільйони), що атакована система функціонально не здатна їх обробити. Як наслідок – виникають збої в її роботі або вона взагалі перестає повноцінно функціонувати [249].

Варто зазначити, що наслідками DDoS-атак можуть бути як порушення, так і припинення роботи інформаційно-телекомунікаційних технологій, систем чи мереж.

Суб'єктом аналізованого кримінального правопорушення є фізична осудна особа, яка досягла 16-річного віку.

Суб'єктивна сторона характеризується виною у формі прямого умислу стосовно вчиненого суспільно небезпечного діяння та умисним або необережним ставленням до наслідків.

Кваліфікаційними ознаками кримінального правопорушення, передбаченого статтею 363-1 Особливої частини Кримінального кодексу України, є вчинення дій повторно або за попередньою змовою групою осіб, якщо вони заподіяли значну шкоду.

Потрібно наголосити, що значна шкода визначається для кожного правопорушення окремо й здебільшого міститься в примітці до статті. Наприклад, у примітці до статті 185 Особливої частини Кримінального кодексу України зазначено, що в статтях 185, 186, 189 та 190 Особливої частини Кримінального кодексу України шкода визнається значною з урахуванням матеріального становища потерпілого та якщо йому спричинені збитки на суму від 100 до 250 неоподатковуваних мінімумів доходів громадян. У примітці до статті 176 Особливої частини Кримінального кодексу України визначено, що значною шкодою вважається завдана шкода, якщо її розмір у 20 і більше разів перевищує неоподатковуваний мінімум доходів громадян. У примітці до статті 188-1 шкода визнається значною, якщо вона в 100 та більше разів перевищує неоподатковуваний мінімум доходів громадян. У примітці до статті 192 Особливої частини Кримінального кодексу України визначено, що майнова

шкода визнається значною, якщо вона в 50 і більше разів перевищує неоподатковуваний мінімум доходів громадян.

Незважаючи на те, що в примітці до статті 361 Особливої частини Кримінального кодексу України визначений розмір значної шкоди для всіх кримінальних правопорушень розділу XVI, вважаємо, що для суспільно небезпечного діяння, передбаченого аналізованою статтею, визначення розміру значної шкоди на рівні триста й більше неоподаткованих мінімумів доходів громадян є значно завищеним відповідно до градації суспільно небезпечного діяння у формі масового розповсюдження повідомлень електрозв'язку.

Пропонуємо визначити в примітці до статті 363-1 Особливої частини Кримінального кодексу України, що буде вважатися значною шкодою, а саме: «шкода, передбачена цією статтею, визнається значною, якщо вона в сто й більше разів перевищує неоподатковуваний мінімум доходів громадян».

Водночас, ураховуючи специфіку аналізованого кримінального правопорушення в кіберпросторі, ввести як додаткову кваліфікаційну ознаку до часини 2 цієї статті вчинення таких дій із корисливих мотивів.

Наразі корисливий мотив цього типу кримінальних правопорушень у кіберпросторі набув неабиякого значення. Наприклад, усе частіше в інтернет-мережі можна натрапити на заголовки «DDoS-атаки на вашого конкурента», тобто DDoS-атаки набули статусу послуг, за які фахівці отримують плату. Загалом DDoS-атаки можна поділити на такі види: 1) DDoS-атаки на замовлення; 2) DDoS-атаки з подальшим вимаганням грошових коштів. У першому разі замовник звертається до фахівця з DDoS-атак із завданням порушити роботу, наприклад, вебсервісу з електронної комерції конкурента, унаслідок чого сервіс конкурента може не функціонувати визначений із фахівцем час. Залежно від термінів непрацездатності сервісу електронної комерції будуть коштувати послуги

фахівця з DDoS-атак. У мережні DarkNet такі послуги варіюються від 100 доларів за один день непрацездатності вебресурсу, а найнижча ціна залежить від складності захисту вебресурсу й прогнозованого часу його непрацездатності. У другому випадку фахівець із DDoS-атак знаходить вебресурси, зазвичай електронної комерції, визначає за допомогою фільтрів приблизний денний прибуток такого вебресурсу та починає здійснювати DDoS-атаки на цей вебресурс. Наступник кроком є звернення до володільця атакованого вебресурсу щодо виплати певної грошової суми, переважно у віртуальних активах, з обіцянкою припинення протиправних діянь. Варто зауважити, що DDoS-атаки здійснюють за допомогою або ботнетів, або стресерів. Ботнетом є комп'ютерна мережа, інфікована шкідливим програмним забезпеченням, яку особи, які вчиняють кримінальні правопорушення в кіберпросторі, використовують для різних кримінально-протиправних дій без відома користувачів [250]. На хакерських форумах ботнет із 400 000 користувачами оцінюється від 10 000 доларів. На відміну від ботнета стресер є сервісом із перевірки мережі або сервера на стійкість. Ще одна відмінна риса стресера від ботнета – його доступність, тобто будь-яка особа може купити підписку на той чи інший стресер, замовити бажані характеристики й у подальшому здійснювати кримінально-протиправні дії. Найпопулярнішими сервісами-стресерами є «Str3ssed Booter», «Free ip stress», «free stresser».

Необхідно звернути увагу, що час від часу такі вебсервіси блокують правоохоронні органи, як, наприклад, сталося з https://www.ipstresser.com/, який заблокувало Федеральне Бюро Розслідувань.

Сьогодні DDoS-атаки через стресери одержали назву «booter-сервіси» – незаконне використання IP-адрес із метою виведення з ладу вебресурсів або інформаційно-телекомунікаційних систем чи мереж. Варто зауважити, що дуже часто IP-стресери приховують особу, яка вчиняє кримінальне правопорушення за допомогою проксі-серверів, що значно

ускладнює встановлення особи, яка вчинила кримінальне правопорушення в кіберпросторі [250].

Хочемо наголосити, що DDoS-атаки та «спам» дуже часто вчиняються як предикатне кримінальне правопорушення. Зокрема, DDoS-атаки можуть вчинятися для пошуку вразливостей в інформаційно-телекомунікаційній системі чи мережі. Спам передбачений для розповсюдження або збуту шкідливого програмного забезпечення чи його використання для подальшого несанкціонованого втручання в інформаційно-телекомунікаційні технології, системи та мережі.

Події 2022 року показали, що основним пріоритетом DDoS-атак стали інформаційно-телекомунікаційні системи й мережі державного значення. Зокрема, основної шкоди зазнали оборонний і фінансовий сектори. Уже є перший прецедент відкриття провадження за статтею 363-1 Особливої частини Кримінального кодексу України: 15 лютого почалися перебої в роботі Приват24, Ощадбанку, сайтів Міністерства оборони та Збройних Сил України. Як повідомили в Центрі стратегічних комунікацій та інформаційної безпеки, проблеми сталися через DDoS-атаку. Також атакували сайт Українського радіо, як повідомив відповідальний за платформу радіо член правління НСТУ Дмитро Хоркін. Доцільно ввести як додаткову кваліфікаційну ознаку цього кримінального правопорушення в кіберпросторі «вчинення дій проти інформаційної інфраструктури держави» [251].

Загалом пропонуємо викласти диспозицію статті 363-1 Особливої частини Кримінального кодексу України в такій редакції:

«Перешкоджання роботі інформаційно-телекомунікаційних технологій, систем і мереж шляхом масового розповсюдження повідомлень електрозв'язку.

1. Умисне масове розповсюдження повідомлень електрозв'язку, здійснене без попередньої згоди адресатів, що призвело до порушення або

припинення роботи інформаційно-телекомунікаційних технологій, систем і мереж.

2. Ті самі дії, вчинені повторно або за попередньою змовою групою осіб, або якщо вони завдали значної шкоди.

3. Дії, передбачені частиною 1 або 2 цієї статті, якщо вони вчинені з корисливих мотивів.

4. Дії, передбачені частиною 1 або 2 цієї статті, якщо вони спричинили тяжкі наслідки або вчинені проти інформаційної інфраструктури держави».

Підбиваючи підсумки, хотіли б зауважити, що норми розділу XVI Особливої частини Кримінального кодексу України імплементовані з Конвенції про кіберзлочинність, зокрема її розділ II «Правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних та систем». Родовим об'єктом цього типу кримінальних правопорушень є цифрова інформація, оброблювана в цифрових пристроях, інформаційно-телекомунікаційних технологіях, системах і мережах. Основна проблема чинного кримінального законодавства у сфері забезпечення кібербезпеки полягає в невідповідності термінології сучасному стану науки й техніки. Пропонуємо замінити термін «електронно-обчислювальна техніка (комп'ютер)» на термін «цифровий пристрій», оскільки засобом або предметом кримінального правопорушення може бути не лише комп'ютер. Інформаційні (автоматизовані), електронні комунікаційні, інформаційно-комунікаційні системи, електронні комунікаційні мережі пропонуємо визначати в сукупності як інформаційно-телекомунікаційні технології, системи та мережі.

Детально проаналізовані елементи складів кримінальних правопорушень, передбачених розділом XVI Особливої частини Кримінального кодексу України. Визначено, що більшість кримінальних правопорушень цього типу є предикатними. На основі аналізу судової

практики визначені проблеми, що виникають під час кваліфікації окремих кримінальних правопорушень цієї групи. Розглянуті найпоширеніші типи шкідливого програмного забезпечення, зокрема такі: 1) віруси; 2) комп'ютерні хробаки; 3) бекдор (backdoor); 4) викрадач інформації (stealer); 5) руткіт (rootkit); 6) залякувальне програмне забезпечення (scareware); 7) кілогер (keylogger); 8) вірус-вимагач (ransomware); 9) кліпери (clippers); 10) майнери (miners).

2.3 Кримінально-правова характеристика кіберутворювальних кримінальних правопорушень у кіберпросторі

Розглянувши кіберзалежні кримінальні правопорушення й визначивши, що чинний Кримінальний кодекс України класифікує до них шість складів (статті 361, 361-1, 361-2, 362, 363, 363-1 Особливої частини Кримінального кодексу України), хочемо констатувати, що кримінальних правопорушень, вчинюваних у кіберпросторі, істотно більше. Кримінальні правопорушення, основний засіб яких – інформаційно-телекомунікаційні технології, системи та мережі, якщо водночас їх родовим об'єктом не є суспільні відносини, регламентовані розділом XVI Особливої частини Кримінального кодексу України, прийнято називати кіберутворювальними кримінальними правопорушеннями.

Хочемо виділити основні особливості, що характеризують кіберутворювальні кримінальні правопорушення: 1) об'єктом таких кримінальних правопорушень є різні суспільні відносини, передбачені різними розділами Особливої частини Кримінального кодексу України; 2) засобом вчинення кримінального правопорушення завжди будуть елементи інформаційно-телекомунікаційних технологій, систем і мереж; 3) в окремих кримінальних правопорушеннях цього типу кіберпростір є місцем вчинення суспільно небезпечного діяння; 4) закріплені в Законі

України шляхом уведення в окремі статті Особливої частини Кримінального кодексу України або визначені в рамках кваліфікаційних ознак, що передбачають кримінальну відповідальність за конкретні суспільно небезпечні діяння.

Пропонуємо зосередити увагу на кожній із наведених особливостей. Кіберутворювальні кримінальні правопорушення на відміну від кіберзалежних репрезентовані в різних розділах Особливої частини Кримінального кодексу України. Як уже зазначалося, їх родовим об'єктом є різні відносини. Варто зауважити, що законодавець передбачив використання в процесі вчинення того чи іншого кримінального правопорушення інформаційно-телекомунікаційних технологій, систем і мереж як засобу вчинення, установивши кваліфікаційні ознаки. Ці кваліфікаційні ознаки передбачені такими статтями Особливої частини Кримінального кодексу України: 1) шахрайство (стаття 190 Особливої частини Кримінального кодексу України); 2) незаконне заволодіння транспортним засобом (стаття 289 Особливої частини Кримінального кодексу України); 3) увезення, виготовлення, збут і розповсюдження порнографічних предметів (стаття 301 Особливої частини Кримінального кодексу України); 4) фальсифікація лікарських засобів або обіг фальсифікованих лікарських засобів (стаття 301 Особливої частини Кримінального кодексу України) [14].

Крім того, хочемо зауважити, що чинний Кримінальний кодекс України в певних статтях Особливої частини прямо містить вказівку на використання тих чи інших інформаційно-телекомунікаційних елементів під час вчинення кримінального правопорушення, зокрема: 1) домагання дитини для сексуальних цілей (стаття 156-1 Особливої частини Кримінального кодексу України); 2) порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв'язку або через комп'ютер (стаття 163 Особливої частини

Кримінального кодексу України); 3) незаконна діяльність з організації або проведення азартних ігор, лотерей (стаття 203-2 Особливої частини Кримінального кодексу України); 4) одержання доступу до дитячої порнографії, її придбання, зберігання, ввезення, перевезення чи інше переміщення, виготовлення, збут і розповсюдження (стаття 301-1 Особливої частини Кримінального кодексу України); 5) незаконне втручання в роботу автоматизованих систем в органах та установах системи правосуддя (стаття 376-1 Особливої частини Кримінального кодексу України) [14].

Водночас спостерігаємо кримінальні правопорушення, у яких кіберпростір є елементом підвищеної суспільної небезпеки, але не має свого закріплення ані в статті, ані в рамках визначення кваліфікаційних ознак певної статті Особливої частини Кримінального кодексу України. Насамперед мова йде про статті 185, 189 та 200 Особливої частини Кримінального кодексу України.

Зауважимо, що ми будемо здійснювати нашу кримінально-правову характеристику кіберутворювальних кримінальних правопорушень, ураховуючи використання елементів інформаційно-телекомунікаційних технологій під час вчинення суспільно небезпечного діяння й підвищеного рівня суспільної небезпеки в разі використання елементів кіберпростору як засобу вивчення кримінального правопорушення. Ми зупинимося лише на тих особливостях характеристики кіберутворювальних кримінальних правопорушень, у яких застосовані елементи кіберпростору.

Відповідно до статистики Департаменту кіберполіції Національної поліції України в 2020 році 80 % повідомлень громадян стосувалися шахрайських дій у кіберпросторі [252]. Загалом за 2021 рік співробітниками Департаменту кіберполіції супроводжувалося розслідування 10 659 кримінальних правопорушень у кіберпросторі, зокрема: 1) 731 кримінальне правопорушення у сфері протидії обігу

протиправного контенту; 2) 3 716 кримінальних правопорушень у банківській сфері; 3) 3 263 кримінальні правопорушення у сфері протидії різним видам онлайн-шахрайства; 4) 2 949 кримінальні правопорушення у сфері комп'ютерних систем [253].

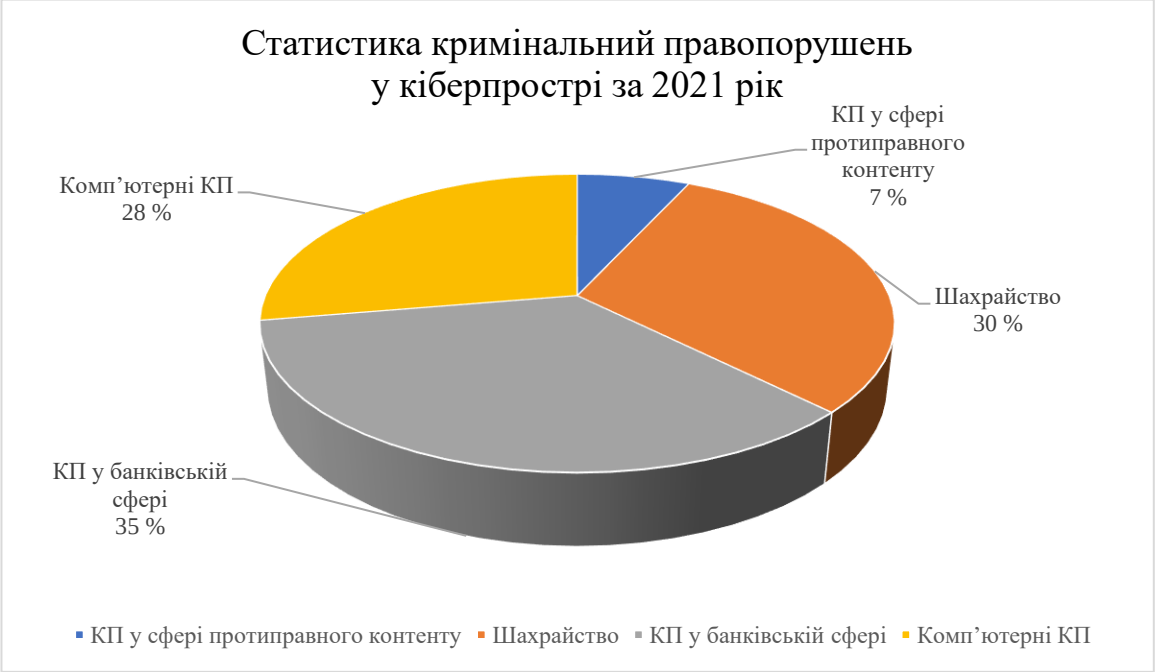

Рисунок 5 – Статистика кримінальний правопорушень
у кіберпросторі за 2021 рік

Водночас хочемо зауважити, що кількість завершених розслідувань становить приблизно 20 %, тобто на загальну кількість 10 659 кримінальних правопорушень у кіберпросторі за 2021 рік припадає лише 2 320 розкритих. Не можемо не акцентувати увагу на тому, що до кримінальних правопорушень у сфері банківської діяльності Департамент кіберполіції відносить суспільно небезпечні діяння, що з об'єктивної сторони вчиняють шляхом обману або зловживання довірою. Як можемо помітити зі статистичних даних, третину всіх кримінальних правопорушень у кіберпросторі в Україні становлять суспільно небезпечні діяння,

передбачені статтею 190 Особливої частини Кримінального кодексу України. Наголосимо, що кримінальні правопорушення в кіберпросторі є найбільш латентними з-поміж усіх видів кримінальних правопорушень, тому реальна статистика буде значно більшою.

Першу групу кіберзалежних кримінальних правопорушень, що ми проаналізуємо, становлять суспільно небезпечні діяння проти власності. На нашу думку, до цієї групи кіберзалежних кримінальних правопорушень належать такі склади: 1) шахрайство (стаття 190 Особливої частини Кримінального кодексу України); 2) вимагання (стаття 189 Особливої частини Кримінального кодексу України); 3) крадіжка (стаття 185 Особливої частини Кримінального кодексу України).

Шахрайство в кіберпросторі справедливо можна вважати найбільш обговорюваним кримінальним правопорушенням як у вітчизняній, так і в зарубіжній науковій спільноті. Згідно зі статистикою Департаменту кіберполіції Національної поліції України понад 80 % звернень громадян пов’язані з шахрайськими діями в кіберпросторі [253].

Відповідно до даних Агентства Європейського Союзу з питань мережевої та інформаційної безпеки частка шахрайства в кіберпросторі серед усіх вчинених у ньому кримінальних правопорушень становить 24 %. Зауважимо, що це майже чверть від усіх правопорушень у кіберпросторі, проаналізованих Агентством Європейського Союзу з питань мережевої та інформаційної безпеки. На рисунку 5 детально висвітлені статистика кримінальних правопорушень у кіберпросторі за 2021 рік і частка кожного з них у системі правопорушень у кіберпросторі [254].

Рисунок 6 – Статистика кримінальних правопорушень у кіберпросторі у 2021 році згідно з даними Агентства Європейського Союзу з питань мережевої та інформаційної безпеки

Зауважимо, що відповідно до Конвенції «Про кіберзлочинність» такий склад кримінального правопорушення, як «шахрайство, пов'язане з комп'ютером» повинен був бути імплементований у кримінальне законодавство України. Проте на практиці, незважаючи на наявність у Конвенції норми про шахрайство, пов'язане з комп'ютером, у національному законодавстві відсутня ця норма, що регулювала б подібні за змістом суспільно небезпечні діяння. Натомість, у Кримінальному кодексі України від 5 квітня 2001 року частиною 3 статті 190 Особливої частини Кримінального кодексу України законодавець передбачив кваліфікаційну ознаку, а саме: знаряддя вчинення у вигляді електронно-обчислювальної техніки. Хочемо наголосити, що з моменту ухвалення Кримінального кодексу України й до сьогодні ця норма не зазнала ніяких змістових змін. Пропонуємо розглянути шахрайство в кіберпросторі в двох аспектах: по-перше, як норму чинного кримінального

законодавства України; по-друге, як норму, передбачену в Конвенції «Про кіберзлочинність». Визначити, які суспільно небезпечні діяння підпадають під зміст зазначених норм, а також доцільність уведення в кримінальне законодавство спеціального складу шахрайства, пов'язаного з інформаційно-телекомунікаційними технологіями.

Відповідно до частини 1 статті 190 Особливої частини Кримінального кодексу України шахрайство – це заволодіння чужим майном або придбання права на майно шляхом обману чи зловживання довірою.

Зауважимо, що, незважаючи на еволюційні процеси в інформаційному сегменті, шахрайство в кіберпросторі залишається кримінальним правопорушенням проти власності, вчинюваним із використанням обману чи зловживання довірою. Основною відмінністю від класичного шахрайства є лише той факт, що обман відбувається не під час безпосереднього фізичного контакту з жертвою, а в дистанційній формі, тобто саме з використанням інформаційно-телекомунікаційних технологій (пристроїв, систем або мереж) [255, с. 162].

Сам факт обману чи зловживання довірою в кіберпросторі можливий шляхом спілкування з жертвою через різні чати, форуми, відео- й аудіодзвінки, публікації оголошень про продаж чи купівлю неіснуючого товару або надання послуги. Загалом шахрайських схем у кіберпросторі дуже велика кількість, водночас варто зазначити, що розвиток технічного прогресу прямо впливає на інноваційну складову шахрайських схем.

Велику різноманітність шахрайських схем у кіберпросторі пояснив М. Мацякявич: по-перше, обман або зловживання довірою є порівняно простим у реалізації способом вчинення кримінальних правопорушень і здебільшого не потребує набуття спеціальних навичок чи знань; по-друге, сам кіберпростір уже проник майже в усі сфери життя суспільства, тим самим створивши передумови для існування різних способів обману користувачів інформаційного простору [256].

На думку М. Маккінона, різноманітність видів шахрайства в кіберпросторі зумовлена насамперед анонімністю як самого кіберпростору, так і його користувачів. Кіберпростір дає змогу особі, яка вчиняє кримінальне правопорушення, з легкістю видавати себе за іншу людину, змінюючи реальний вік, соціальний статус та інші особливості ідентифікації, одержуючи завдяки цьому переваги під час вчинення шахрайства [257].

Зазначимо, що сьогодні найпоширенішими сферами діяльності суспільства в кіберпросторі є такі: 1) фінансова сфера (інтернет-банкінг, інтернет-аукціони, цифрові гаманці, віртуальні активи); 2) сфера електронної комерції (інтернет-магазини, різні оголошення купівлі – продажу); 3) сфера розваг (інтернет-ігри, інтернет-казино). Відповідно до даних аналізу компанії у сфері інформаційної безпеки «CrowdStrike» найчастіше шахрайство в кіберпросторі спрямоване саме на сферу електронної комерції, на другому місці фінансовий сектор. На рисунку 7 зображена статистика різних сфер шахрайства в кіберпросторі.

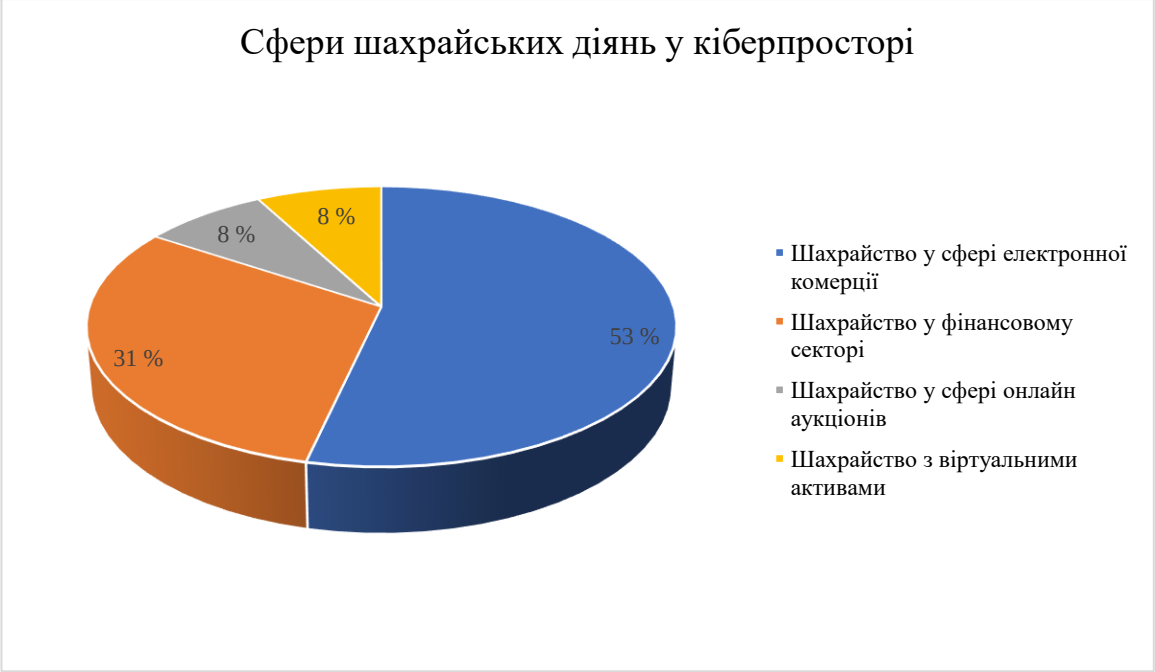

Рисунок 7 – Сфери шахрайських діянь у кіберпросторі

Пропонуємо коротко охарактеризувати основні схеми, використовувані шахраями у своїй протиправній діяльності, які ми поділили на сектори, зокрема: 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. На рисунку 8 ми розподілили найпопулярніші шахрайські схеми, що належать до того чи іншого напрямку діяльності шахраїв. Хочемо зазначити, що шахрайські схеми в кіберпросторі не є вичерпними, а динамічно змінюються й пристосовуються до потреб суспільства. Вибір суспільно небезпечних діянь, вчинених у формі обману або зловживання довірою, ми робили на основі їх суспільної небезпеки, статистики вчинення й поширеності. Пропонуємо проаналізувати саме види шахрайських дій у кожному секторі [258].

Рисунок 8 – Сектори вчинення шахрайства

Шахрайство у сфері електронної комерції (або, як його часто називають, шахрайство, пов’язане, з торгівлею – купівлею товарів в інтернет-мережі), напевно, є одним із лідерів рейтингу з-поміж інших шахрайських схем. Це пояснюється насамперед легкістю в реалізації зазначеної шахрайської схеми, яка не потребує спеціальних навичок, та протиправним доходом особи, яка вчинила кримінальне правопорушення [259]. Під час реалізації зазначеної шахрайської схеми особа може діяти як продавець товару чи послуги, так і як його покупець. Перший варіант передбачає створення фейкових оголошень із продажу товарів чи послуг на різних онлайн-маркетплейсах на зразок «Olx», «Prom», «Rozetka», «Shafa», «Skidka» та ін. Фейковість оголошення в цьому разі означає виконання

шахраєм об’єктивної сторони цього кримінального правопорушення у формі обману. Шахрай заздалегідь має на меті не надати послугу або не відправити товар покупцеві, водночас його основне завдання полягає саме в отриманні передплати за товар чи послугу, рідше – повної суми. Здебільшого шахраї оперують саме товарами або послугами, що в конкретний період часу мають суспільну необхідність. Наприклад, під час пандемії вони надавали послуги з отримання довідки про вакцинацію, яку або не надсилали за необхідною адресою, або видавали без дійсного сертифікаційного номера [260].

У період початку збройної агресії Російської Федерації шахраї пропонують послуги з перетину державного кордону або довідку про відстрочку від мобілізаційного призиву. Сьогодні в період ракетних ударів по енергетичній інфраструктурі держави все більше й більше людей переходять на живлення осель та інших приміщень від генераторів та акумуляторів. Звісно, шахраї не могли не помітити цей новий тренд, фактично щотижня на офіційному сайті Департаменту кіберполіції Національної поліції України з’являється інформація щодо нових інцидентів, пов’язаних із цією шахрайською схемою [261].

Варто зауважити, що суб’єкти електронної комерції використовують свої внутрішні важелі кібербезпеки для повного нівелювання або зменшення шахрайських інцидентів на своїх торгових платформах. Прикладом такого сервісу є «OLX-доставка», що фактично заміняє накладний платіж і виключає комісію: покупець оплачує товар лише після огляду й отримання у відділенні «Нова пошта», «Укрпошта» «Meest», а вартість доставки вже резервується на умовному рахунку в рамках самої послуги «OLX-доставка» (тому немає потреби відправляти передоплату за доставку особисто продавцеві); продавець не втрачає на доставці товару, якщо покупець від нього відмовиться або не прийде у відділення пошти

зовсім. Як результат – продавець не несе втрат за доставку товару, а кошти покупця захищені до отримання, огляду й прийняття товару [262].

Варто наголосити, що незважаючи на те, що такий сервіс функціонує вже декілька років, лише 10 % від користувачів платформи користуються ними, а шахраї так само активно це використовують. Зокрема, дуже часто продавці товарів створюють фейкові, фішингові вебсайти, що зовні повністю копіюють оригінальні (дизайн, домен, функції, платіжні системи для безготівкової купівлі) з подальшим надсиланням фейкової форми покупцеві товару. Покупець товару вносить на фейковий «гарантійний» рахунок свої грошові кошти з упевненістю, що вони будуть перераховані продавцеві товару лише після огляду та схвалення покупцем такої угоди. Але фактично жертва перераховує грошові кошти напряму на мерчант-систему шахрая [263].

Хочемо звернути увагу, що саме шахрайство із сервісами доставки вчиняється в співучасті, організованими групами. Є цілі центри, що займаються такою протиправною діяльністю. Водночас сам шахрай може не створювати фейковий вебресурс і мерчант-систему, а одержати доступ до такого сервісу за певний відсоток від кожної шахрайської угоди, в подальшому отримавши завдяки цьому «чисті» грошові кошти від власника сервісу.

Поширення інтернет-торгівлі через соціальні мережі одночасно зумовило збільшення шахрайства цієї категорії. Водночас, якщо в першому розглянутому варіанті реалізації були певні моменти локальної протидії цьому суспільно небезпечному явищу з боку власників маркетплейсів, то під час купівлі товарів через умовний «інстаграм» жертва обов’язково стикується з проблемою передплати за товар у певному обсязі нібито для покриття витрат у разі відмови від нього після отримання. За цією схемою діють шахраї й досягають свого злочинного результату завдяки масовості

пропозицій на ринку та відповідної заниженої ціни за аналогічний товар на маркетплейсі [264].

Відповідно до другого варіанта шахрай діє як покупець певного товару. Як приклад хочемо навести такий різновид шахрайства, як рефаундинг. Рефаундинг – це кредитова фінансова операція, здійснювана після списання грошових коштів із карткового рахунку власника картки, ініціатором якої є підприємство в разі відмови власника картки від отримання товару або його повернення.

Такий вид шахрайства на відміну від першого розглянутого варіанта спрямований на великі мережеві підприємства, що спеціалізуються на продажі товарів, наприклад «asos», «amazon», «apple» та ін. Сама сутність цього виду шахрайства полягає в отриманні від суб'єкта електронної комерції товару, заздалегідь оплаченого карткою або електронним гаманцем (paypal), із подальшим поверненням сплачених коштів шахраєві, водночас оплачений товар також залишається в шахрая. Зауважимо, що кожна запропонована компанія має свій алгоритм повернення грошових коштів за сплачений товар із певних причин, зокрема отримання товару неналежної якості, неотримання товару або отримання іншого товару. Варто наголосити, що реалізація кожного варіанта рефаундингу напряму залежить від навичок соціальної інженерії й ціни на замовлений товар.

Реалізація способу «отримання товару неналежної якості» полягає в навмисному, незначному псуванні товару та одночасній відеофіксації процесу поломки з подальшим використанням відеозапису як доказової бази для повертання грошових коштів. Зазначимо, що товар також залишається в шахрая й після незначного ремонту підлягає продажу.

К. Голдман у своїй праці «Протидія фінансовим кіберзлочинам» серед найпопулярніших способів рефаундингу, пов'язаного з отриманням товару неналежної якості, виділив: 1) вміст коробки з посилкою був наповненим паразитами чи комахами, які її зіпсували; 2) вміст коробки з посилкою був

наповненим порошком, візуально подібним до наркотичної речовини, як наслідок – коробка із вмістом була викинута [265].

Такий спосіб рефаундингу, як «неотримання товару», також популярний серед шахраїв через складність доведення факту отримання чи неотримання шахраєм посилки. Здебільшого для успішної реалізації цього способу шахраї використовують безкоштовні сервіси з доставки або сервіси, що не передбачають або рідно оновлюють трекери на посилці. У результаті шахрай отримує замовлений товар, а потім через деякий час звертається до служби підтримки й вимагає заміну товару, який «не отримав», або повернення грошових коштів на свою картку [266].

Іншим видом шахрайства з використанням інформаційно-телекомунікаційних технологій є шахрайство на інтернет-аукціонах. Шахраї пропонують взяти участь в аукціоні, на якому лотом є певний рідкісний товар або товар специфічної категорії, скажімо нумізматика. Початкова ціна на такі товари завжди занижена, а самого лота реально не існує, тобто шахраї пропонують купити неіснуючий товар за привабливою ціною. Після того як жертва перемагає в аукціоні, сервіс автоматично списує із зазначеного карткового рахунку грошові кошти на гарантійний рахунок сервісу, що після схвалення жертвою надсилаються шахраєві [267, с. 207].

Різновидом шахрайства на інтернет-аукціонах є так званий «скандинавський аукціон», який полягає в тому, що товар виставляється за ціною 1–2 долари, а учасники роблять мінімальні ставки, водночас із кожної ставки з учасників знімається певна сума, після чого жертви втрачають гроші й не отримують товарний лот [255, с. 162].

Наступним сектором шахрайський дій, що ми хочемо проаналізувати, є шахрайство у сфері використання інформаційно-телекомунікаційних технологій. Особливість цього сектору діяльності полягає в тому, що такі суспільно небезпечні діяння можна вважати традиційними в разі вчинення

шахрайських дій, але внаслідок їх перенесення в рамки кіберпростору вони набувають більшої суспільної небезпеки. Шахрайство, за якого телефон або інший подібний телекомунікаційний ґаджет є основним знаряддям вчинення кримінального правопорушення, набуло свого активного розвитку на початку XXI століття. Поява соціальних мереж, месенджерів та інших віртуальних засобів комунікації лише посилила діяльність шахраїв у цьому секторі. На відміну від традиційного шахрайства, за якого особа, яка вчиняє кримінальне правопорушення, ретельно все планує для вчинення одного або декількох суспільно небезпечних діянь, телефонне шахрайство в кіберпросторі здебільшого спрямоване на масовість, тобто реалізацію діяння заміняють кількістю можливих жертв. Така ознака, як дистанційність і відсутність фізичного контакту шахрая з жертвою, лише підвищує рівень суспільної небезпеки. Варто наголосити, що ми розглядаємо сектор телефонного шахрайства винятково в контексті тих кримінальних правопорушень, що передбачають пряму комунікацію жертви й шахрая, а сама реалізація шахрайських схем напряму залежить від навичок соціальної інженерії особи, яка вчиняє кримінальне правопорушення.

Напевно, найпопулярнішою схемою серед телефонних шахраїв є телефонний скамінг. Телефонний скамінг – це діяльність із переконання жертви щодо переказу грошових коштів або отримання особистих, робочих, банківських чи корпоративних даних жертви, що становлять інтерес для шахрая, із метою як використання, так і продажу третім особам, що відбувається через розмову телефоном чи за допомогою мережі, ґрунтується на навичках соціальної інженерії.

На початку 2010 року телефонний скамінг супроводжувався примітивними схемами обману, спрямованими на незахищені категорії населення, а саме: на людей пенсійного віку. Найпопулярнішою схемою, якою шахраї успішно користуються до сьогодні, є «ваш родич у біді».

Шахраї під виглядом лікаря чи працівника поліції телефонують громадянам, щоб вони за гроші допомогли родичеві вирішити проблему або уникнути відповідальності. Це один із найпоширеніших методів шахраїв, яким найчастіше ошукують людей похилого віку. Зокрема, на початку серпня у Вінниці 82-річна пенсіонерка віддала 300 тисяч гривень незнайомцеві. Їй подзвонив «лікар» і повідомив, що донька потрапила в аварію й потрібні гроші для лікування. Зловмисника затримали, ним виявився раніше судимий за аналогічний злочин 34-річний житель Донецької області [268].

Ще одним різновидом телефонного скамінгу, який шахраї активно застосовують у своїй діяльності, є дзвінки від співробітників банку, що одержав назву «банківський працівник». Сутність цієї схеми полягає в тому, що шахрай, представляючись співробітником банку або його служби безпеки, намагається дізнатися дані банківської картки, пароль від інтернет-банкінгу та CVV-код із подальшим привласненням коштів жертви. Зокрема, такі шахрайські дії роблять у декілька етапів із певним проміжком часу між кожним і здійснюють в організованій групі. Наприклад, на першому етапі шахрай, маючи певний «бекґраунд» про володільця картки, може ставити певні уточнювальні запитання, інформація про які вже є в шахрая, але це створює певні передумови та довірливі відносини з боку жертви. На цьому етапі головне завдання шахраїв – дізнатися, скільки коштів у жертви на картковому рахунку. На наступному етапі шахрай телефонує жертві, представляючись представником служби безпеки банку, й під приводом можливої небезпеки щодо її рахунку переконує її зняти гроші з основного рахунку та перевести їх на резервний рахунок банку. Як результат – жертва втрачає свої грошові кошти [269].

Зловживання співчуттям є традиційним видом шахрайства, але з появою соціальних мереж воно набуло нового типу реалізації. Зазначений вид шахрайства, як і «телефонний скамінг», прямо залежить від навичок

соціальної інженерії. Зауважимо, що в умовах збройної агресії Російської Федерації цей вид шахрайства динамічно зростає. Хочемо зазначити, що його реалізація відбувається у двох форматах: 1) масовому; 2) цільовому [270].

Відповідно до масового способу шахраї через спам-розсилки (соціальні мережі, імейл) надсилають користувачам повідомлення жалісливого змісту, у яких описують неіснуючі життєві проблеми, сподіваючись на емпатію жертви. Здебільшого в цьому разі кількість жертв порівняно з кількістю розісланих спам-листів незначна, але саме завдяки масовості шахрай може отримати чималу грошову допомогу.

Цільовий спосіб на відміну від масового спрямований на конкретну категорію людей і передбачає тривалу комунікацію із жертвою. Як приклад можна навести популярну на сьогодні схему «постраждалі під час війни», за якої шахраї переконують жертву, що вони втратили свій дім і потребують грошових коштів на життя, прикріпляючи фейкові фото й відео. Дуже часто маємо ситуації, коли шахраї, прикидаючись військовослужбовцями, просять гроші на пальне, військовий одяг або дрони [271].

Фраудштошинг – це підвид шахрайства, цільовою аудиторією якого є неповнолітні, але нерідко на гачок шахраїв потрапляють і повнолітні люди, які, проте, не мають правової свідомості. Сутність схеми полягає в тому, що жертва одержує повідомлення про вчинення нею злочинних дій шляхом відвідування заборонених вебресурсів злочинного або сумнівного змісту чи ведення аморального способу життя. Шахраї залякують жертву, що про такі нібито суспільно небезпечні дії буде повідомлено до правоохоронних органів, засобів масової інформації, знайомим або родичам, якщо особа не переведе визначену шахраями грошову суму. Жертва, неправильно оцінюючи ситуацію переважно внаслідок свого малолітства та загрози настання негативних наслідків у вигляді повідомлення про таку її діяльність батькам або правоохоронним органам, переводить грошові кошти шахраям.

Останнім підвидом шахрайства цього сектору є скамеринг – обдзвонювання жертви псевдопредставниками компаній «Microsoft», «Dell», «McAfee», які повідомляють про серйозне зараження персонального комп'ютера жертви шкідливим програмним кодом, що може вплинути на функціонування комп'ютера й призвести до його повної нероботоздатності, пропонуючи купити софт, що його «вилікує» [255, с. 162].

Останнім сектором вивчення шахрайських дій, що ми хочемо проаналізувати, є фінансовий, або шахрайство у сфері надання фінансових послуг. Один із способів вчинення шахрайства в кіберпросторі – шахрайство у сфері кредитування. В інтернет-мережі велика кількість фінансових установ і банків, що надають послуги у сфері мінікредитування лише за наявності паспортних даних. Грошові кошти в такому разі зараховуються на карткові рахунки клієнта. Наразі такі послуги є дуже популярними, ними користуються тоді, коли для оплати певного товару не вистачає власних грошових коштів, а купувати товар у кредит особа не хоче. Шахрай може взяти кредити на чуже ім'я, надаючи фінансовій кредитній установі чужі паспортні дані [272].

Зауважимо, що такий спосіб шахрайства вчиняється без спеціального програмного забезпечення або технічних засобів чи шляхом втручання у функціонування засобів зберігання, оброблення або передавання цифрової інформації. Може вчинятися як у кіберпросторі, так і традиційними офлайн-способами, різницю буде становити лише спосіб отримання кредитних коштів (готівка або безготівковий картковий переказ) та власне уникнення фізичного контакту з працівниками фінансової установи, що в результаті значно підвищує латентність і суспільну небезпеку аналізованого способу вчинення шахрайства в кіберпросторі.

Особливість зазначеного способу вчинення шахрайства в кіберпросторі полягає в тому, на яку банківську картку шахрай отримує кредитні кошти. Здебільшого шахраї створюють мережу «дропових

банківських карток». Дроп, або «грошовий мул», – це та людина, яка погоджується, щоб її банківська картка стала «транзитною» для вкрадених шахраями грошей. Дроп переводить незаконно отримані грошові кошти між різними рахунками. Такий ланцюжок переказів потрібний, щоб заплутати сліди кіберзлочинців та ускладнити роботу слідства [273].

Дуже часто «дропи» навіть не здогадуються, що вони стали співучасниками кримінального правопорушення.

Інноваційним видом шахрайства в кіберпросторі сьогодні можна вважати суспільно небезпечну діяльність у сфері обміну безготівкової валюти. На нашу думку, ці шахрайські дії можна умовно поділити на такі підвиди: 1) шахрайство у сфері обміну безготівкової валюти; 2) шахрайство у сфері обміну віртуальної валюти.

Відповідно до постанови Правління Національного банку України від 24 лютого 2022 року № 18 «Про роботу банківської системи в період запровадження воєнного стану» безготівкова купівля валюти в банках була заборонена. Водночас курс валют, визначений Національним банком України, істотно відрізнявся від курсу на «чорному ринку». Саме це зумовило попит на купівлю безготівкової валюти через різні інтернет-обмінники, як результат – активізація діяльності шахраїв у цьому напрямку. Здебільшого шахраї створюють спеціальні боти для обміну безготівкової валюти з гривні на будь-яку іншу за привабливими цінами, встановленими на рівні Національного банку України. Вони активно рекламують свої послуги в соціальних мережах, на дошках оголошень тощо. Жертва, знаходячи привабливий для себе валютний курс, перераховує згідно з інструкцією сервісу свої безготівкові кошти в національній валюті, але обіцяного сервісом обміну так і не отримує, стаючи ошуканою. Як і в першому аналізованому способі вчинення шахрайства в кіберпросторі у сфері кредитування, шахраї використовують

чужі банківські картки для прийому безготівкової національної валюти [274].

Шахрайство у сфері обміну віртуальної валюти на відміну від шахрайства у сфері обміну безготівкової почалося з моменту впровадження віртуальних активів у світову економіку. Так само, як і шахрайство з обміном безготівкової валюти, аналізований спосіб вчинення характеризується широким залученням комунікаційних систем і мереж як засобу вчинення кримінального правопорушення. Як приклад можна навести викриту Департаментом кіберполіції Національної поліції України групи онлайн-шахраїв, які створили мережу фейкових вебобмінників із конвертації віртуальних активів, за допомогою яких ошукували громадян, охочих провести операції з обміну віртуальних активів. Шахраї створили власну CMS-систему з обміну віртуальних активів, на яку за допомогою реклами в соціальних мережах перенаправляли жертв, як результат – втрата безготівкової національної валюти жертвами цього суспільно небезпечного діяння [275].

Не менш актуальна й суспільно небезпечна шахрайська схема, переважно реалізовувана в співучасті, – шахрайство у сфері надання інвестиційних послуг. Зазначений вид шахрайства є найбільш високоприбутковими серед інших і потребує ретельної підготовки для якісної реалізації. Загалом реалізацію цього виду шахрайства можна поділити на декілька етапів: 1) початковий; 2) підготовчий; 3) реалізація; 4) втрата грошових коштів.

На першому етапі створюється злочинна організація з чітким розподілом ролей. Зокрема, організатор організовує роботу, пособники підшукують персонал співучасників для подальшої шахрайської діяльності, виконавці можуть здійснювати як об’єктивну сторону кримінального правопорушення, так і діяльність щодо навчання нових співучасників

навичкам соціальної інженерії, що полягають в обмані майбутніх клієнтів фейкової інвестиційної контори.

На другому етапі здійснюється створення власної інвестиційної платформи у вигляді цільового вебресурсу й підключення до неї мерчант-системи для поповнення вкладниками своїх рахунків. На платформі імітується зростання активів вкладника. Також на другому етапі створюються call-центри, здебільшого в декількох містах або навіть країнах, та набирається персонал.

Третій етап полягає в реалізації злочинного умислу шляхом обдзвонювання потенційних жертв із метою пропонування інвестицій у цінні папери, акції й віртуальні активи, що начебто незабаром зростуть, і вкладник отримає непоганий відсоток до вже вкладених коштів. Після того як вкладник на фейковій платформі бачить зростання активу, в який йому пропонували вкластися, працівники call-центру закликають подвоїти свій внесок для більшого прибутку.

На четвертому етапі, коли вкладник уже не планує інвестувати в актив або хоче зняти свої зароблені гроші, фейкова інвестиційна платформа проводить маніпуляцію на своїй фейковій платформі з імітацією падіння активу, який закуповувала жертва, як результат – втрата грошових коштів [276].

Незважаючи на віднесення проаналізованих способів вчинення шахрайства до кримінальних правопорушень у кіберпросторі, не всі вони за своїм сутнісним змістом можуть кваліфікуватися за частиною 3 статті 190 Особливої частини Кримінального кодексу України. Передусім це зумовлено неузгодженістю понятійного апарату, визначеного чинним кримінальним законодавством. Зокрема, в частині 3 цієї статті чітко зазначено, що таке шахрайство вчинене шляхом незаконних операцій із використанням електронно-обчислювальної техніки. Водночас законодавець не надає визначення, що саме розуміється під незаконними операціями.

Крім того, визначення електронно-обчислювальної техніки як засобу кримінального правопорушення істотно обмежує суспільно небезпечні діяння, що підпадають під об'єктивну сторону цього кримінального правопорушення, зокрема телефони, планшети. Наприклад, Ковельський міськрайонний суд розглядав справу Особи 1 у вчиненні кримінального правопорушення, передбаченого частиною 3 статті 190 Особливої частини Кримінального кодексу України, у якій за обставинами справи Особа 1 вчинила суспільно небезпечне діяння у формі обману: незаконно заволоділа грошовими коштами Особи 2, прийнявши оплату за неіснуючий товар, розміщений на платформі «OLX». Суд визначив, що телефон як засіб вчинення кримінального правопорушення не є електронно-обчислювальною технікою. Водночас у вироку суду визначено, що обставиною, з огляду на яку можна кваліфікувати шахрайство, є лише операції, здійснення яких без використання електронно-обчислювальної техніки неможливе [277].

Органи досудового розслідування кваліфікували дії обвинуваченого щодо наведених епізодів за частиною 3 статті 190 Особливої частини Кримінального кодексу України як шахрайство, вчинене шляхом незаконних операцій із використанням електронно-обчислювальної техніки, що, на думку суду, є неправильним.

Хочемо звернути увагу на те, що Департамент кіберполіції Національної поліції України аналогічні суспільно небезпечні діяння з ознаками шахрайства в разі оголошення підозри розглядає саме як вчинені з використанням електронно-обчислювальної техніки, незважаючи на те, вчинене зазначене діяння шляхом використання телефона або комп'ютера [278; 279; 280; 281].

Така неузгодженість породжує правові прогалини правильної кваліфікації фактично аналогічних за змістом кримінальних правопорушень. На нашу думку, саме використання інформаційно-

телекомунікаційних технологій, систем і мереж, а також дистанційність, тобто відсутність будь-якого фізичного контакту особи, яка вчинила кримінальне правопорушення, та жертви, робить його більш суспільно небезпечним, ніж традиційне вчинення шахрайських дій, що передбачають прямий контакт між шахраєм і жертвою. Також пропонуємо звернути увагу й визначити, що розуміється під незаконними операціями. На нашу думку, операцію з використанням електронно-обчислювальної техніки можна вважати незаконною лише в разі несанкціонованого проникнення в інформаційно-телекомунікаційні технології, системи та мережі. Водночас розміщення оголошень на маркетплейсах або в соціальних мережах із продажу неіснуючих товарів чи надання неіснуючих послуг не можна вважати незаконними, адже фактичного втручання в систему за цих умов немає. На нашу думку, в разі дотримання нинішнього підходу законодавця до аналізованого кримінального правопорушення обов'язковою є необхідність додаткової кваліфікації за статтею 361 Особливої частини Кримінального кодексу України.

На нашу думку, норма частини 3 цієї статті не є соціально обумовленою через невідповідність її змісту й категорії діянь, вчинюваних у кіберпросторі шляхом обману чи зловживання довірою. Крім того, вважаємо необхідним акцентувати увагу на специфічних засобах вчинення аналізованого кримінального правопорушення, що робить його більш суспільно небезпечним за традиційне шахрайство. Пропонуємо доповнити частину 2 статті 190 Особливої частини Кримінального кодексу України й запропонувати таку редакцію:

«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 і мереж».

Водночас у Постанові пленуму Верховного суду України необхідно акцентувати увагу, що кваліфікаційна ознака «шляхом операцій із використанням інформаційно-телекомунікаційних технологій, систем і мереж» доцільна лише тоді, коли кримінальне правопорушення було вчинене від початку до кінця в рамках кіберпростору, тобто повної відсутності фізичного контакту з потерпілою особою. Тобто не вважати шахрайством шляхом операцій із використанням інформаційно-телекомунікаційних технологій, систем і мереж дії особи, за яких кіберпростір використовується лише для пошуку потенційних жертв із подальшим фізичним контактом упродовж реалізації шахрайських дій.

Проаналізувавши склад кримінального правопорушення, передбаченого частиною 3 статті 190 Особливої частини Кримінального кодексу України, та визначивши його специфічні риси, постає питання нагальності виключення цієї кваліфікаційної ознаки з чинного кримінального законодавства й можливості запровадження спеціальної норми, що визначала б кримінальну відповідальність за шахрайство у сфері цифрової інформації.

Насамперед хочемо звернути увагу, які саме діяння можуть підпадати під кваліфікаційну ознаку аналізованої статті. Відповідно до статті 8 Конвенції про кіберзлочинність, що має назву «Шахрайство, пов’язане з комп’ютером», до таких суспільно небезпечних діянь належать: 1) заволодіння чужим майном або правом на майно шляхом уведення, зміни, знищення чи приховування комп’ютерних даних; 2) заволодіння чужим майном або правом на майно шляхом будь-якого втручання у функціонування комп’ютерної системи [18].

З огляду на практику вирішення судами справ за частиною 3 статті 190 Особливої частини Кримінального кодексу України маємо ситуацію, за якої фактично тотожні за своїм змістом діяння кваліфікують по-різному.

Проблемою законодавства в цьому питанні є відсутність тлумачення таких понять, як уведення інформації або будь-яке втручання у функціонування комп'ютерної системи [282].

Водночас хочемо наголосити, що сам зміст аналізованої кваліфікаційної ознаки виходить за рамки шахрайських дій, тобто не можна вважати зміну, модифікацію, видалення інформації здійсненими шляхом обману або зловживання довірою, адже фактично в цьому разі обманюють не фізичну особу, а сам комп'ютер [283].

Не можемо не звернути увагу на те, що більшість науковців розуміє під незаконними операціями з використанням електронно-обчислювальної техніки такі суспільно небезпечні дії, як фішинг [284]. Крім того, Департамент кіберполіції Національної поліції України також розуміє під фішингом суспільно небезпечні діяння, за якими відкриті кримінальні провадження за частиною 3 статті 190 Особливої частини Кримінального кодексу України. На нашу думку, фішинг не можна кваліфікувати за статтею 190 Особливої частини Кримінального кодексу України [285].

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. У цьому разі обман є лише способом одержання персональних даних у вигляді цифрової інформації, тобто предмет фішингу – цифрова інформація, що вже не може кваліфікуватися як шахрайство, основним предметом якого є чуже майно або право на майно. Ми вважаємо, що діяння у формі фішингу варто кваліфікувати за частиною 3 статті 361 Особливої частини Кримінального кодексу України – «несанкціоноване втручання в роботу інформаційно-телекомунікаційних технологій, мереж і систем, яке призвело до витоку інформації у формі копіювання». Постає закономірне запитання: що буде, якщо особа в результаті фішингу одержала персональні дані онлайн-

банкінгу або дані картки з подальшим заволодінням грошовими коштами, тобто чи підглядає вона кримінальній відповідальності за частиною 3 статті 190 Особливої частини Кримінального кодексу України? На нашу думку, зазначене суспільно небезпечне діяння не можна кваліфікувати за частиною 3 статті 190 Особливої частини Кримінального кодексу України з огляду на відсутність обману або зловживання довірою [286]. Водночас предикатне діяння у формі несанкціонованого втручання в роботу інформаційно-телекомунікаційних технологій, систем або мереж, що призвело до витоку цифрової інформації, не буде впливати на кваліфікацію. Ураховуючи специфіку реалізації аналізованого діяння, вважаємо, що заволодіння майном або правом на майно може буде здійснене винятково таємним способом. Проте на практиці маємо, що предметом крадіжки не може бути майно або право на майно нематеріального характеру, у цьому разі – безготівкові або електронні гроші [287].

Залишається не вирішеним питання кваліфікації низки суспільно небезпечних діянь, вчинених таємним способом і спрямованих на викрадення чужого майна або права на таке майно. Ми вважаємо, що не доцільно вводити до статті 185 Особливої частини Кримінального кодексу України кваліфікаційну ознаку, спрямовану на викрадення чужого нематеріального майна, оскільки це призведе до деформації змісту цієї статті й проблем кваліфікації такого кримінального правопорушення.

Водночас, на нашу думку, ураховуючи підвищену суспільну небезпечність таких діянь, вчинених у кіберпросторі, та статистичні дані Департаменту кіберполіції Національної поліції України, є нагальна потреба введення в кримінальне законодавство нової спеціальної норми, що визначала б кримінальну відповідальність за крадіжку в кіберпросторі, тим самим дематеріалізувавши предмет крадіжки. Ураховуючи той факт, що поза увагою традиційного складу кримінального правопорушення залишаються безготівкові й електронні гроші, вважаємо, що новий,

спеціальний склад кримінального правопорушення потрібно назвати «крадіжка у сфері обігу безготівкових або електронних грошей і віртуальних активів».

Незважаючи на те, що фактично зазначене кримінальне правопорушення вчиняється в кіберпросторі шляхом впливу на інформаційно-телекомунікаційні технології, основним безпосереднім об'єктом залишаються суспільні відносини у сфері власності. Предметом аналізованого кримінального правопорушення є безготівкова валюта, електронна валюта та віртуальні активи.

Крадіжці безготівкових, електронних грошей або віртуальних активів властивий таємний спосіб вчинення. Сутність таємного способу вчинення крадіжки полягає в тому, що особа, яка вчиняє кримінальне правопорушення, уникає безпосереднього контакту з потерпілою особою – володільцем безготівкових, електронних грошей або віртуальних активів [287].

Залежно від фінансового інструмента ми виділили такі способи таємного викрадення безготівкових, електронних грошей або віртуальних активів: 1) шляхом оплати покупок із використанням персональних даних володільця картки або електронного гаманця в інформаційно-телекомунікаційних мережах; 2) шляхом одержання доступу до системи дистанційного банківського обслуговування; 3) шляхом зняття грошових коштів у банкоматі.

Крадіжка безготівкових грошових коштів або електронних грошей шляхом оплати покупок із використанням персональних даних володільця картки або електронного гаманця в інформаційно-телекомунікаційних мережах може виражатися у двох різних формах: 1) шляхом уведення персональних даних володільця картки або електронного гаманця у вигляді цифрової інформації; 2) шляхом іншого втручання в роботу інформаційно-телекомунікаційних технологій.

У першому разі ми вбачаємо ситуацію, за якої особа, одержавши будь-яким способом персональні дані володільця картки, шляхом уведення даних цієї картки на будь-якому маркетплейсі купує товари чи послуги за його кошти. Варто зауважити, що нерідко особи, які вчиняють кримінальне правопорушення, купують товари або послуги в самих себе, тобто відразу виконують об'єктивну сторону статті 190 Кримінального кодексу України. Для досягнення злочинного результату особа, яка вчиняє кримінальне правопорушення, повинна виконати низку заходів під час реалізації цього способу вчинення. Зокрема, фактично кожна платформа електронної комерції має свою антифрод-систему. Антифрод-система – це система, призначена для оцінювання фінансових транзакцій в Інтернеті на предмет підозрілості з точки зору шахрайста, пропонуючи рекомендації щодо їх подальшого оброблення. Здебільшого сервіс антифроду складається зі стандартних та унікальних правил, фільтрів і списків, за якими перевіряється кожна транзакція. Залежно від популярності й дохідної частини платформи антифрод-сервіс буде складнішим для подолання [288].

До таких фільтрів належить регіон, із якого вчиняється купівля, девайс, IP-адреса, відбиток браузера та багато іншого. Наприклад, змоделюємо таку ситуацію: Особа 1 територіально перебуває в Латвії, купивши персональні дані банківської платіжної картки Особи 2, яка є громадянином України. Особа 1 захотіла здійснити покупку подарункового сертифікату з певним грошовим номіналом через популярний маркетплейс «Amazon», використавши дані банківської картки Особи 2, з IP-адреси Литви. Антифрод-система, розуміючи, що дані банківської картки належать до Української банківської системи, а транзакція здійснюється з Литовської IP-адреси, блокує незаконну транзакцію. Прикладом успішної реалізації схеми є використання Особою 1 індивідуального проксі-серверу із zip-кодом та адресою походження України. Така реалізація схеми крадіжки безготівкових грошей матиме значно більше шансів на успіх, але ключову

роль у цьому разі буде відігравати саме надійність антифрод-системи платформи електронної комерції. Варто зауважити, що те, що особа може здійснювати операції з незаконної купівлі даними чужої банківської картки в безлічі маркетплейсів, незважаючи на факти блокування транзакції антифрод-системою, лише підвищує суспільну небезпеку.

Фактично за допомогою введення цифрової інформації особа, яка вчиняє кримінальне правопорушення, може обійти систему захисту тієї чи іншої платіжної мережі.

Відповідно до другого випадку, тобто шляхом іншого втручання в роботу інформаційно-телекомунікаційних технологій, особа, яка вчиняє кримінальне правопорушення, використовує не персональні дані володільця банківської картки або електронного гаманця, а лог-файли для своєї протиправної діяльності. Лог-файли – це файли, що містять системну інформацію про роботу сервера або комп'ютера, до яких заносяться певні дії користувача або програми [289].

У розглянутому нами прикладі ми будемо оперувати лог-файлами браузера. Вони містять інформацію про всі дії користувача цього браузера й зберігають абсолютно всю інформацію, яку він дозволяє. Тобто, простими словами, лог-файли браузера можуть містити всі фінансові дані користувача, що водночас будуть у режимі автозбереження, тобто не потребуватимуть логіну й паролю до акаунту. Варто зауважити: маючи лог-дані браузера, особа, яка вчиняє кримінальне правопорушення, може використати не лише доступ до інтернет-банкінгу або електронного гаманця платіжної системи. Переважно вона використовує збережені дані від різних маркетплейсів та перевіряє їх на збережені платіжні інструменти. Такий спосіб таємного викрадення має більшу суспільну небезпеку, оскільки навіть антифрод-система не завжди може розпізнати неправомірного користувача й відмінити незаконну транзакцію. Фактично система сприймає зловмисника за правомірного користувача.

Ще одним способом таємного викрадення можна вважати одержання доступу до системи дистанційного банківського обслуговування. Зазначимо, що найпоширенішими видами системи дистанційного банківського обслуговування є інтерент-банкінг та електронні платіжні системи. Одержання доступу до інтернет-банкінгу або електронної платіжної системи може відбуватися шляхом як купівлі доступу до неї, так і неправомірного втручання в роботу інформаційно-телекомунікаційної технології. На відміну від попереднього зазначений спосіб не передбачає купівлі товарів або послуг в Інтернеті. Цьому способу характерні прямі перекази з одного банківського рахунку чи електронної платіжної системи на іншу. Варто наголосити, що такий спосіб супроводжується підвищеним довірливим ставленням антифрод-системи банку або електронного платіжного сервісу до проведення фінансових транзакцій.

Також хочемо звернути увагу на такий спосіб вчинення крадіжки безготівкових або електронних грошей та віртуальних активів, як модифікація цифрової інформації, оброблюваної в інформаційно-телекомунікаційній технології, системі або мережі. Відповідно до такого способу особа, яка вчиняє кримінальне правопорушення шляхом протиправного використання шкідливого програмного забезпечення у вигляді «кліперу», модифікує введену жертвою цифрову інформацію у формі платіжних даних у цифрову інформацію, закладену особою, яка вчиняє кримінальне правопорушення. Зокрема, Особа 1 «заражає» цифровий пристрій Особи 2 вірусним програмним кодом, що змінює реквізити платіжної картки або електронного гаманця чи гаманця віртуального активу на реквізити Особи 1. Здійснюючи переказ, платіжні реквізити, що вводить Особа 2, будуть автоматично змінені на реквізити Особи 1, як результат – Особа 1 отримає грошові кошти замість правомірного одержувача. На нашу думку, зазначена суспільно небезпечна

дія не буде потребувати додаткової кваліфікації за статтею 361-1 Особливої частини Кримінального кодексу України.

Пропонуємо викласти нову статтю, що містить спеціалізований склад крадіжки «крадіжка у сфері обігу безготівкових або електронних грошей і віртуальних активів» у такому вигляді:

«Крадіжка у сфері обігу безготівкових або електронних грошей і віртуальних активів.

Крадіжка у сфері обігу безготівкових або електронних грошей та віртуальних активів, вчинена шляхом уведення цифрової інформації в інформаційно-телекомунікаційні технології, системи й мережі.

Крадіжка у сфері обігу безготівкових або електронних грошей і віртуальних активів унаслідок іншого втручання в роботу інформаційно-телекомунікаційної технології, системи й мережі.

Діяння, передбачене частинами 1–2 цієї статті, вчинене повторно або за попередньою змовою групою осіб, або таке, що завдало значної шкоди потерпілому.

Діяння, передбачене частинами 1–3 цієї статті, якщо воно вчинене шляхом модифікації цифрової інформації.

Діяння, передбачене частинами 1–2, вчинене у великих розмірах або організованою групою.

Діяння, передбачене частинами 1–4 цієї статті, вчинене в умовах воєнного або надзвичайного стану.

Водночас у примітках до цієї статті визначити, що є введенням цифрової інформації та іншим втручанням у роботу інформаційно-телекомунікаційної технології, системи й мережі.

Під уведенням цифрової інформації під час вчинення крадіжки безготівкових або електронних грошей і віртуальних активів варто розуміти втручання у функціонування засобів оброблення, зберігання або передавання цифрової інформації, унаслідок якого відбувається додавання

нової цифрової інформації в інформаційно-телекомунікаційну технологію, систему або мережу.

Під іншими втручаннями в роботу інформаційно-телекомунікаційної технології, системи та мережі під час вчинення крадіжки безготівкових або електронних грошей і віртуальних активів варто розуміти втручання у функціонування засобів оброблення, зберігання або передавання цифрової інформації, внаслідок якого можливе використання вже наявної цифрової інформації, що міститься в інформаційно-телекомунікаційній технології, системі або мережі, не пов'язане з її блокуванням, модифікацією або видаленням.

У разі крадіжки у сфері обігу безготівкових або електронних грошей та віртуальних активів шляхом блокування, модифікації або видалення цифрової інформації суспільно небезпечне діяння варто додатково кваліфікувати за частиною 3 статті 361 Особливої частини Кримінального кодексу України.

Ми переконані, що введення спеціального складу такого кримінального правопорушення, як крадіжка, обумовлене ризиками розвитку злочинності в кіберпросторі. Крім того, на нашу думку, новий склад кримінального правопорушення започаткує тенденцію до дематеріалізації предмета крадіжки й у майбутньому буде визначено, що фізичний характер предмета під час крадіжки є необов'язковим.

Наступним кримінальним правопорушенням у кіберпросторі проти власності, що ми хочемо проаналізувати, є вимагання, передбачене статтею 189 Особливої частини Кримінального кодексу України. Під час кваліфікації вимагання, вчиненого в кіберпросторі, доцільно поставити запитання стосовно характеру погроз. Традиційними способами вимагання прийнято вважати: 1) погрозу насильства над потерпілою особою або його близькими родичами; 2) погрозу знищення майна потерпілої особи; 3) погрозу розголошення відомостей, які потерпілий або його близькі

родичі хотіли зберегти в таємниці; 4) погрозу вбивства чи заподіяння тяжких тілесних ушкоджень [290, с. 261].

Зазначимо, що вимагання в кіберпросторі принципово відрізняється від традиційного вимагання відсутністю фізичного контакту між особою, яка вчинила кримінальне правопорушення, та потерпілим. На нашу думку, така характерна ознака вимагання в кіберпросторі не зменшує суспільну небезпеку діяння, а, навпаки, підвищує її. Крім того, вимагання в кіберпросторі є гіперлатентним кримінальним правопорушенням.

Характер погроз вимагання в кіберпросторі може бути виражений через месенджери, соціальні мережі, відеочати, електронну адресу або особисті повідомлення [291].

Найбільш поширеним способом вимагання в кіберпросторі на сьогодні є погроза розголошення відомостей, що потерпілий або його близькі родичі хотіли зберегти в таємниці. Розглянемо два різних способи скоєння цього кримінального правопорушення. Зокрема, за першим варіантом не потрібна додаткова кваліфікація за відповідною статтею розділу XVI Особливої частини Кримінального кодексу України, а за другим – так. Відповідно до першого варіанта хочемо навести приклад. Потерпіла Особа 1 – працівник великої фірми – забула закрити свою особисту електронну адресу, де на гугл-диску були розміщені особисті фотографії інтимного характеру. Особа 2, скориставшись доступом до електронної пошти Особи 1, скопіювала інтимні фотографії Особи 1. Маючи електронну адресу потерпілої особи, Особа 2 написала електронного листа Особі 1 із вимаганням грошових коштів, зазначивши наслідки у вигляді розповсюдження цих фотографій третім особам у разі неотримання грошових коштів на свою банківську картку. Це класична схема вимагання в кіберпросторі, за якої може використовуватися будь-яка соціальна мережа або месенджер. Водночас вимагач може залишатися анонімним, а можливість отримувати грошові кошти – супроводжуватися

різними електронними платіжними системами, що значно ускладнює ідентифікацію особи, яка вчинила кримінальне правопорушення [292].

Відповідно до другого способу вимагач може одержати інформацію про жертву шляхом несанкціонованого втручання в її цифровий пристрій із використанням шкідливого програмного забезпечення. У цьому разі таке діяння буде потребувати додаткової кваліфікації за статтею 361 або 361-1 Особливої частини Кримінального кодексу України. Варто наголосити, що здебільшого жертвами такого способу вимагання стають цільові особи, які є публічними. Як приклад хочемо навести нещодавні несанкціоновані втручання в сервіс зберігання інформації «Icloud», що призвели до витоку інформації, унаслідок якого особи, які вчинили кримінальне правопорушення, вимагали грошові кошти за нерозповсюдження інформації інтимного характеру потерпілих [293].

Іншим способом вимагання, що полягає в погрозі обмеження прав, свобод або законних інтересів, є DDoS-атака. Ми детально розглядали вчинення DDoS-атак шляхом масового розповсюдження повідомлень електрозв'язку в підрозділі 2.3, тому не будемо аналізувати зазначений спосіб вчинення кримінального правопорушення. Проте хочемо зауважити, що кваліфікація кримінального правопорушення як вимагання в разі вчинення DDoS-атаки можлива лише з огляду на факт самого вимагання й припинення такої атаки в обмін на грошову винагороду. Водночас суспільно небезпечне діяння буде потребувати додаткової кваліфікації за статтею 363-1 Особливої частини Кримінального кодексу України.

Ще одним способом незаконного впливу на потерпілу особу може бути погроза незаконного знищення чи пошкодження цифрової інформації шляхом її блокування, модифікації або видалення. Наразі така законодавча ініціатива не набула свого розвитку, але вже є країни, у яких широко запроваджується відповідальність за зазначені суспільно небезпечні дії в разі вимагання.

На нашу думку, погроза видалення, блокування, модифікації або інше неправомірне втручання в роботу інформаційно-телекомунікаційних технологій, систем або мереж варто розглядати як новий інноваційний характер загроз під час вчинення вимагання. Зауважимо, що відповідно до чинного законодавства такі суспільно небезпечні дії виходять за рамки статті 190 Особливої частини Кримінального кодексу України з огляду на те, що їх не можна розцінювати як пошкодження або знищення майна. Ми переконані, що варто виділити такий спосіб як окрему кваліфікаційну ознаку, зокрема: «*погроза блокування, видалення, знищення, модифікації або іншого несанкціонованого втручання в роботу інформаційно-телекомунікаційних технологій, систем і мереж, що може завдати шкоди правам та інтересам потерпілої особи»*.

На нашу думку, подібне нововведення в кримінальне законодавство дасть змогу повністю оцінити суспільну небезпеку зазначеного способу вчинення вимагання. Водночас додаткова кваліфікація за відповідною статтею розділу XVI Особливої частини Кримінального кодексу України не потребується, якщо особа, яка вчинила кримінальне правопорушення, дійсно не виконала об'єктивну сторону відповідної статті розділу XVI Особливої частини Кримінального кодексу України.

Ще одним кримінальним правопорушенням зазначеної групи є умисне знищення чи пошкодження майна, передбачене статтею 194 Особливої частини Кримінального кодексу України. У цьому разі основним предметом кримінального правопорушення може бути персональний комп'ютер, ноутбук, планшет, телефон або інший цифровий пристрій. Проте зауважимо, що для кваліфікації за статтею 194 Особливої частини Кримінального кодексу України повинна бути спричинена шкода у великому розмірі, а саме: понад 250 неоподатковуваних мінімумів доходів громадян. Ураховуючи ціни на наведені елементи цифрових технологій, таке діяння не буде містити складу кримінального правопорушення.

Аналогічну ситуацію спостерігаємо в частині 4 статті 361 Особливої частини Кримінального кодексу України: спричинена шкода повинна бути значною, тобто перевищувати 300 неоподатковуваних мінімумів доходів громадян. На практиці маємо, що, якщо Особа 1 шляхом несанкціонованого втручання в роботу цифрового пристрою завантажила на нього шкідливе програмне забезпечення, яке призвело до пошкодження або знищення цифрового пристрою, вартість якого оцінено в 35 000 тисяч гривень, вона буде нести лише цивільну відповідальність. Проте, на нашу думку, сам характер дій у кіберпросторі цьому у разі явно виходить за межі цивільно правової відповідальності. Це зумовлено насамперед: 1) масовістю таких дій, тобто особа, яка вчинила кримінальне правопорушення, не має потреби в цільовому виробі своїх жертв, а в кіберпросторі такою жертвою може стати кожний; 2) дистанційністю, яка полягає в тому, що на відміну від традиційного виконання об'єктивної сторони аналізованого кримінального правопорушення особа, яка його вчинила, одночасно може завдати шкоди декільком жертвам, територіально перебуваючи в будь-якому місці; 3) надвисокою латентністю такого діяння (більшість потерпілих може навіть не здогадуватися, що цифровий пристрій вийшов із ладу саме через втручання в його роботу або вірусне програмне забезпечення).

На нашу думку, варто викласти диспозицію частини 1 статті 194 Особливої частини Кримінального кодексу України в такій редакції:

«Умисне знищення або пошкодження чужого майна, що заподіяло шкоду у великих розмірах або вчинене шляхом несанкціонованого втручання в роботу інформаційно-телекомунікаційних технологій, систем і мереж».

Наступну групу кіберзалежних кримінальних правопорушень становлять кримінальні правопорушення проти виборчих, трудових та інших особистих прав і свобод людини й громадянина, передбачені розділом V Особливої частини Кримінального кодексу України. До кримінальних правопорушень, що можуть вчинятися в кіберпросторі, у цій

групі належать: 1) порушення рівноправності громадян залежно від їх расової, національної, регіональної належності, релігійних переконань, інвалідності та за іншими ознаками (стаття 161 Особливої частини Кримінального кодексу України); 2) порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв'язку або через комп'ютер (стаття 163 Особливої частини Кримінального кодексу України); 3) порушення авторського права та суміжних прав (стаття 176 Особливої частини Кримінального кодексу України).

Відповідно до додаткового протоколу Конвенції «Про кіберзлочинність», що стосується криміналізації дій расистського й ксенофобного характеру, вчинених через комп'ютерні системи, такі дії підлягають криміналізації в національному законодавстві. Закріплення такого суспільно небезпечного діяння міститься в статті 161 Особливої частини Кримінального кодексу України. Проте варто зауважити доцільність винесення як окремої кваліфікаційної ознаки до цієї статті вчинення таких дій у рамках кіберпростору. На нашу думку, немає нагальності внесення зміни до зазначеної статті у вигляді кваліфікаційної ознаки, оскільки фактично наразі саме кіберпростір є певним майданчиком для вчинення таких суспільно небезпечних дій [294, с. 104].

Сьогодні спостерігаємо діяльність багатотисячних груп у соціальних мережах, окремі форуми, вебсайти, що спеціалізуються на діях ксенофобного та расистського характеру [295, с. 119]. Вчинення зазначених дій із використанням кіберпростору, а саме: соціальних мереж та Інтернету, значно підвищує суспільну небезпеку такого діяння, ускладнюючи роботу правоохоронних органів щодо виявлення таких кримінальних правопорушень.

Наступне аналізоване суспільно небезпечне діяння, яке також фактично повністю перейшло в рамки кіберпростору, – порушення

таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв'язку або через комп'ютер, передбачене статтею 163 Особливої частини Кримінального кодексу України [296, с. 47].

У зазначеній статті безпосередньо в диспозиції наведено засіб вчинення кримінального правопорушення. Крім того, відповідно до частини 2 аналізованої статті вбачається кваліфікаційна ознака «вчинення таких дій з використанням спеціальних засобів, призначених для негласного зняття інформації». Проаналізувавши судову практику за останні 10 років, нами було встановлено, що в період із 1 січня 2013 р. по сьогодні не було ні одного судового рішення у формі вироку за статтею 363 [297].

Незважаючи на задовільну статистику, суспільну небезпеку цього кримінального правопорушення складно переоцінити. Основним способом реалізації цього суспільно небезпечного діяння в кіберпросторі є несанкціоноване втручання в інформаційно-телекомунікаційні технології, мережі й системи, що призводить до витоку інформації про листування, телефонні розмови або іншу кореспонденцію потерпілої особи. Проте, враховуючи санкцію частини 3 статті 361 Особливої частини Кримінального кодексу України, що повністю поглинає санкцію статті 163 Особливої частини Кримінального кодексу України, вважаємо необхідним закріпити таку кваліфікаційну ознаку: *«вчинення дій, передбачених частиною 1 цієї статті, якщо це спричинено несанкціонованим втручанням в інформаційно-телекомунікаційну технологію, систему або мережу»*.

Також потрібно змінити назву статті, розширивши перелік способів і видів передавання цифрової інформації, та викласти в такій редакції:

«Порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються інформаційно-телекомунікаційними технологіями, системами й мережами».

Розширення переліку видів передавання цифрової інформації дасть змогу внесення до переліку охоронюваних законом способів передавання інформації web3- та VR-комунікації.

Останнім кіберутворювальним кримінальним правопорушенням зазначеної групи є порушення авторського права та суміжних прав, передбачене статтею 176 Особливої частини Кримінального кодексу України. Хочемо наголосити, що відповідно до примітки до аналізованої статті кримінальна відповідальність настає лише за умов заподіяння значної шкоди, а саме: якщо її розмір у 20 і більше разів перевищує неоподатковуваний мінімум доходів громадян. З цього випливає, що більшість суспільно небезпечних діянь не будуть мати складу кримінального правопорушення, а відповідальність буде цивільно-правовою. Наразі найгірша ситуація у сфері порушення авторського права та суміжних прав спостерігається у сфері авторського відео- й вебконтенту. Особи часто використовують чужі медіаматеріали, видаючи їх за власні. Зазвичай особи таки діями переслідують мету отримання прибутку від розміщення рекламних банерів або партнерських програм, використовуючи популярні медіаматеріали первинного автора відеоконтенту. Часто спостерігаємо ситуації, коли аудиторія автора контенту значно менша від аудиторії особи, яка незаконно використовує його контент. Говорячи про завдану матеріальну шкоду, варто зазначити, що на практиці дійсно складно визначити реальну матеріальну шкоду, якої зазнав автор контенту. Водночас, на нашу думку, шкоду не завжди можна оцінити у фінансовому еквіваленті. Зокрема, незаконне використання контенту може призвести до псування ділової репутації автора. Ураховуючи той факт, що в епоху інформаційних технологій 80 % авторського права й суміжних прав

реалізуються через кіберпростір у тому чи іншому його прояві, не вважаємо доцільним унесення кваліфікаційної ознаки до статті 176 Особливої частини Кримінального кодексу України.

Наступні кіберутворювальні кримінальні правопорушення, що ми хочемо проаналізувати, вчиняються у сфері господарської діяльності.

Стаття 200 Особливої частини Кримінального кодексу України визначає відповідальність за незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, електронними грошима, обладнанням для їх виготовлення.

Предметом аналізованого кримінального правопорушення є: 1) у разі підробки – платіжні картки, документи на переказ; 2) у разі придбання, зберігання, перевезення, пересилання, використання та збуту – підроблені платіжні картки або підроблені документи на переказ; 3) у разі випуску – електронні гроші.

Ми не будемо робити повну кваліфікацію кримінального правопорушення, передбаченого статтею 200 Особливої частини Кримінального кодексу України, а зупинимося лише на тих характеристиках, що здійснюються в рамках кіберпростору й мають підвищений рівень суспільної небезпеки.

Першочергово пропонуємо розглянути понятійний апарат, що фігурує в аналізованій статті. Поняття документів на переказ було визначено Законом України «Про платіжні системи та переказ коштів в Україні», а саме: електронний або паперовий документ, що використовується суб'єктами переказу, їх клієнтами, кліринговими, еквайринговими або іншими установами – учасниками платіжної системи для передавання доручень на переказ коштів [298]. Зауважимо, що наразі цей закон втратив чинність і дефініція поняття «документи на переказ» у чинному законодавстві не визначена. Відповідно до Закону України від 30 червня 2021 р. «Про платіжні послуги» платіжною карткою визнається

електронний платіжний засіб у вигляді пластикової чи іншого виду картки. Цей самий закон визначає поняття електронних грошей – одиниця вартості, що зберігається в електронному вигляді, випущена емітентом електронних грошей для виконання платіжних операцій (зокрема, з використанням наперед оплачених платіжних карток багатоцільового використання), приймається як засіб платежу іншими особами, ніж їх емітент, та є грошовим зобов'язанням такого емітента електронних грошей.

З точки зору об'єктивної сторони склад кримінального правопорушення, передбаченого статтею 200 Особливої частини Кримінального кодексу України, є матеріальним. З огляду на наше дисертаційне дослідження вважаємо необхідним розглянути суспільно небезпечні дії, що характеризують аналізоване кримінальне правопорушення, а саме: 1) підробку платіжних карток, документів на переказ і засобів доступу до банківських рахунків; 2) придбання, використання й збут платіжних карток.

Насамперед пропонуємо визначити, яким стандартам повинна відповідати платіжна картка. Відповідно до Американського національного інституту стандартів, що встановлює всі фізичні характеристики платіжної картки, магнітна стрічка банківської платіжної картки на своїй передній стороні повинна мати такі обов'язкові елементи:

1) ідентифікаційний номер. Такий номер зазвичай складається з 16 цифр, але не може буди більшим за 19. У нього закладено назву платіжної системи, використовуваної карткою, тип картки та належність до певного банку. Наприклад, якщо номер банківської платіжної картки: а) 4 – Visa; б) 5 – MasterCard, в) 3 – American Express;

2) ім'я та прізвище володільця картки (здебільшого для пострадянських країн такий обов'язковий пункт не застосовується);

3) термін дії картки;

4) логотип платіжної системи й назву банку, що видав платіжну картку;

5) мікросхему для здійснення NFC-платежів.

Так само на зворотній стороні картки повинні бути: 1) магнітна стрічка; 2) голограма; 3) захисний CVV-код; 4) місце для підпису володільця картки; 5) місце для фотографії володільця картки (для пострадянських країн не обов'язкове).

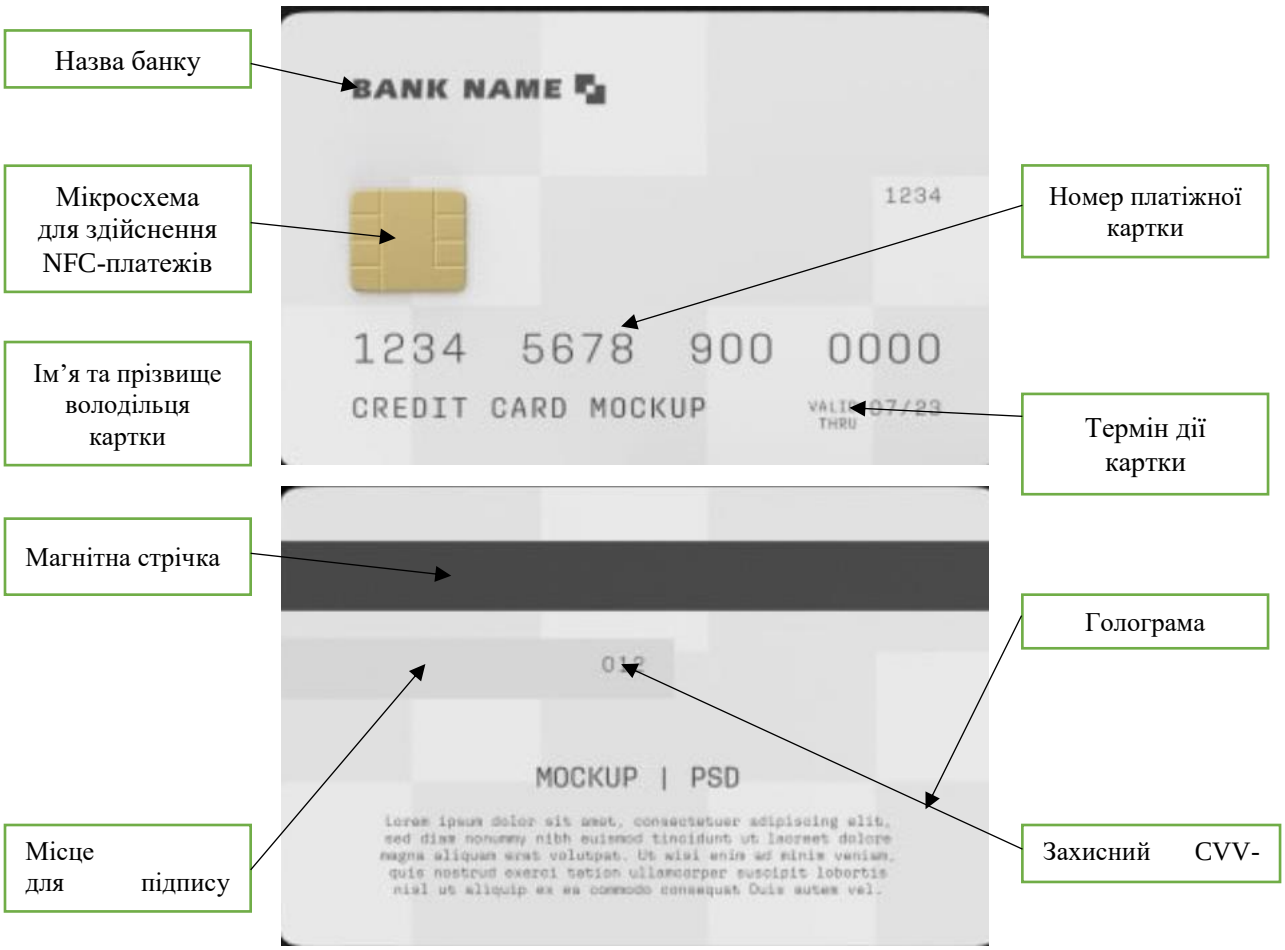

Рисунок 9 – Огляд платіжної картки

Розглянувши технологію побудови платіжної картки, пропонуємо проаналізувати схему щодо її підробки. Власне для підробки платіжної пластикової картки й одержання пін-коду необхідні такі технічні засоби: 1) ембоссер; 2) тайпер; 3) скімер; 4) енкодер. Варто зауважити, що сьогодні

дуже часто функції всіх зазначених технічних засобів суміщаються в одному пристрої. Проте, якщо всі наведені технічні пристрої самі собою не є речами, обмеженими чи виведеними з цивільного обігу, сукупність функцій цих пристроїв, що зосереджуються в одному пристрої, буде визначатися як шкідливий технічний засіб [299, с. 38]. Отже особа, яка незаконно виготовила підробну платіжну картку, нестиме додаткову відповідальність за статтею 361-1 Особливої частини Кримінального кодексу України.

Загалом процес підробки банківської платіжної картки охоплює три основні етапи. На першому етапі особа одержує повну інформацію про банківську платіжну картку. Здебільшого це відбувається за допомогою розміщення POS-систем та POS-терміналів. POS-системи переважно встановлюють на банкоматах у вигляді скімерів, а POS-термінали – це дублікати звичайних терміналів, використовуваних суб'єктами підприємницької діяльності, що мають функцію збереження повної інформації про пластикову картку, зокрема електроімпульс із магнітної стрічки.

Наступним етапом є створення фізичної пластикової картки. На цьому етапі особа, яка вчиняє кримінальне правопорушення, за допомогою ембоссера наносить на пластикову картку елементи, необхідні для того чи іншого типу пластикової картки, зокрема: 1) номер картки; 2) термін її дії; 3) CVV-код; 4) назви банку та платіжної системи. Потім за допомогою тайпера на пластикову карту впаюється чиста магнітна стрічка, тим самим завершаючи етап її повного створення.

Останнім етапом є запис інформації, одержаної на першому етапі, на платіжну картку. Використовуючи енкодер, особа, яка вчинила кримінальне правопорушення та одержала за допомогою скімера інформацію про банківську платіжну карту (пін-код, електромагнітний імпульс магнітної стрічки), наносить такі дані на банківську пластикову

картку, надаючи їй ознак платіжної картки. Фактично після завершення третього етапу особа, яка вчиняє кримінальне правопорушення, має готову до використання банківську пластикову платіжну карту. Власне така діяльність і підпадає під об'єктивну сторону аналізованого кримінального правопорушення, що виражається в підробці платіжних карток.

Ще однією характеристикою об'єктивної сторони цього кримінального правопорушення, що ми хочемо проаналізувати, є суспільно небезпечні діяння у формі придбання, зберігання, перевезення, пересилання з метою збуту підроблених платіжних карток.

Придбання – це отримання підробленої платіжної картки будь-яким способом, зокрема шляхом купівлі, обміну на інший товар або прийняття як повернення боргу чи прийняття за виконану роботу.

Використання підроблених платіжних карток – це їх застосування за їх функціонально-цільовим призначенням, тобто для зняття готівки через банкомат або оплати товарів чи послуг через термінали оплати. Варто звернути увагу, що використання особою справжньої оплаченої банківської платіжної картки, викраденої або в будь-який інший спосіб отриманої особою, з подальшим зняттям коштів не створює складу кримінального правопорушення, передбаченого статтею 200 Особливої частини Кримінального кодексу України, а може кваліфікуватися як таємне викрадення чужого майна. Також варто наголосити, що під використанням, на нашу думку, варто розуміти саме фізичне застосування підробленої платіжної картки. Використання платіжних реквізитів, що особа, яка вчинила кримінальне правопорушення, одержала за допомогою скімера, з подальшою оплатою товарів через Інтернет, тобто без фізичного застосування магнітної стрічки платіжної картки, також не створює складу кримінального правопорушення аналізованої статті [300].

Під збутом підроблених платіжних карток варто розуміти їх умисне оплатне чи безоплатне відчуження, що полягає в їх продажі, обміні,

даруванні або передаванні для погашення боргу. Варто наголосити, що сьогодні інтернет-мережа є найбільшим майданчиком для збуту підроблених платіжних карток.

Окремо хочемо розглянути суспільно небезпечні діяння, що полягають у підробці, використанні й збуті інших засобів доступу до банківських рахунків. У доктринальних джерелах до інших засобів доступу до банківського рахунку належать інші носії інформації (крім документів на переказ і платіжних карток), що зберігають ідентифікаційну інформацію й за допомогою яких особа може одержати доступ до певного банківського рахунку, зокрема: 1) мобільний платіжний інструмент, тобто електронний платіжний засіб, реалізований в апаратно-програмному середовищі мобільного телефона або іншого бездротового пристрою користувача; 2) дорожні та іменні чеки в іноземній валюті, емітовані за кордоном, що пред'являються для сплати на території України [301; 302].

Проте залишається поза увагою питання дистанційного банківського обслуговування інтернет-банкінгу як одного з його найпоширеніших видів і можливості незаконних операцій із ними. Фактично можемо стверджувати, що з об'єктивної сторони такі суспільно небезпечні дії не створюють складу кримінального правопорушення, передбаченого статтею 200 Особливої частини Кримінального кодексу України, адже неможливо підробити інтернет-банкінг. Водночас суспільно небезпечне діяння у формі придбання, зберігання, перевезення, пересилання з метою збуту, доступу до системи дистанційного обслуговування в диспозиції аналізованої статті не визначено. На нашу думку, варто доповнити диспозицію статті: «а так само придбання, зберігання, перевезення, пересилання з метою збуту підроблених документів на переказ, платіжних карток, інших засобів доступу до банківського рахунку та електронних грошей або їх використання чи збут». У цьому разі вважаємо, що діяння у формі створення фіктивної системи дистанційного банківського

обслуговування у формі інтернет-банкінгу або електронної платіжної системи для подальшого неправомірного використання варто кваліфікувати за статтею 190 Особливої частини Кримінального кодексу України як шахрайство.

Останнім кіберутворювальним кримінальним правопорушенням цієї групи є легалізація (відмивання) майна, одержаного злочинним шляхом, передбачене статтею 209 Особливої частини Кримінального кодексу України.

Предметом цього кримінального правопорушення визначено майно, щодо якого фактичні обставини справи дають підставу вважати злочинним шлях його отримання. Водночас зауважимо, що заміна слова «дохід» у Кримінальному кодексі України редакції 2019 року на «майно» виправдана насамперед ширшим тлумаченням останнього, що також охоплює поняття «дохід» [303].

Цивільне законодавство під майном як особливим об'єктом розуміє річ, сукупність речей, а також майнові права та обов'язки. Речами визнаються різноманітні предмети матеріального світу, що задовольняють потреби людей і щодо яких можуть виникати цивільні права та обов'язки (наприклад, нерухомість, транспортні засоби, твори мистецтва) [304].

Відповідно до статті 193 ЦК України одним із видів майна є валютні цінності. Згідно зі статтею 1 Закону України «Про валюту і валютні операції» валютні цінності – це національна валюта (гривня), іноземна валюта й банківські метали [305].

З огляду на це можемо розглядати операції з легалізації майна, одержаного злочинним шляхом у кіберпросторі, як предмет кримінального правопорушення, передбаченого статтею 209 Особливої частини Кримінального кодексу України.

Завдяки транснаціональному характеру й анонімності кіберпростір дає фактично необмежені можливості щодо надання легальної форми

майну, одержаному злочинним шляхом. Пропонуємо розглянути найпоширеніші способи легалізації майна, одержаного злочинним шляхом.

Усі способи легалізації майна в кіберпросторі можна поділити на такі групи: 1) легалізація майна, одержаного злочинним шляхом, за допомогою вже існуючої інтернет-інфраструктури (маркетплейсів, сайтів оголошень, соціальних мереж, інтернет-аукціонів, краудфандингу); 2) легалізація майна, одержаного злочинним шляхом, у результаті створення нової вебінфраструктури (інтернет-магазину); 3) легалізація майна, одержаного злочинним шляхом, завдяки використанню обмінників і цифрових (електронних) валют; 4) легалізація майна, одержаного злочинним шляхом, за допомогою віртуальних активів.

Напевно, одним із найпростіших і водночас найпопулярніших способів легалізації майна, одержаного злочинним шляхом, є продаж неіснуючих товарів на маркетплейсах («prom», «olx»). Реалізація такої схеми виглядає так. Особа, яка вчиняє кримінальне правопорушення, створює декілька акаунтів на маркетплейсах, реєструючись на різні IP-адреси. Одну частину акаунтів вона використовує як продавців, а іншу – як покупців. З акаунтів продавців особа, яка скоює кримінальне правопорушення, розміщує оголошення на продаж різних предметів, що не потребують спеціальної реєстрації або документів (техніки, іграшок). Наголосимо, що зазначених предметів у особи немає, тобто оголошення є фіктивними. З іншого акаунту вона купує виставлені на маркетплейсі «свої фіктивні» товари. Дохід особа отримує на дійсний банківський рахунок, а як докази легального походження отриманих коштів вона може надати виписки з історії покупок або інші документи, які їй надає маркетплейс, що будуть доводити легальність отриманих коштів.

Аналогічна ситуація спостерігається в разі реалізації схеми із залученням інтернет-аукціонів. З одного акаунту особа створює фіктивний

попит, а з іншого – пропозицію. Зазвичай, щоб створити пропозицію, вона використовує декілька акаунтів для помірного збільшення ціни лоту.

Злочинці також знаходять способи відмивання грошей у таких сферах, як краудфандинг. Зокрема, краудфандингові платформи для акціонерного капіталу можна використовувати принаймні двома способами для сприяння відмиванню грошей [306].

По-перше, продавець незаконних товарів, таких як наркотики або незареєстрована вогнепальна зброя, може створити фальшиву компанію й продавати свої цінні папери на будь-якій фінансовій платформі. У результаті покупці можуть «легально» придбати через платформу акції неіснуючої компанії. Отже, дистриб'ютори отримують кошти в електронному вигляді, а не готівкою, і можуть об'єднати декілька платежів в один грошовий потік [307].

Варто зауважити, що особливістю реалізації проаналізованих схем легалізації майна, одержаного злочинним шляхом, є те, що їх може реалізовувати лише одна особа, враховуючи класифікаційний момент щодо вже існуючої вебінфраструктури.

Легалізація майна, одержаного злочинним шляхом, способом створення нової вебінфраструктури дещо складніша порівняно з використанням уже існуючої, але реалізація фактично ідентична. Головна відмінність полягає в тому, що особа, яка вчиняє кримінальне правопорушення, не реєструється на вже існуючому вебресурсі, а створює власний, куди підключає мерчант-системи або електронні гаманці на зразок «Skrill», «PayPal», «Netler», водночас реєструючись як суб'єкт підприємницької діяльності. Зауважимо, що в таких вебмагазинах здебільшого немає реальних покупців і товарів, а фінансові операції через підключені до вебмагазину мерчант-системи протікають винятково з «брудними» грошовими коштами за різноманітними схемами.

Ми не будемо зупинятися на схемах легалізації майна, одержаного злочинним шляхом, за допомогою електронної валюти й віртуальних активів, адже їх характеристика наведена в наступному розділі нашого дослідження.

Підбиваючи підсумки вищевикладеного, хочемо наголосити, що аналізовані нами кіберутворювальні кримінальні правопорушення не є вичерпними. Сьогодні – в епоху інформаційно-телекомунікаційних технологій – фактично кожне кримінальне правопорушення може вчинятися з використанням того чи іншого елемента кіберпростору. У нашому дослідженні ми зосередили увагу на тих кримінальних правопорушеннях, у яких елементи кіберпростору, зокрема інформаційно-телекомунікаційні технології, системи та мережі, значно підвищують суспільну небезпеку діяння, фактично трансформуючи його в новий тип кримінального правопорушення зі своїми специфічними особливостями об'єктивної сторони.

Сьогодні можна стверджувати, що всі кримінальні правопорушення в кіберпросторі, визначені Конвенцією «Про кіберзлочинність», імплементовані в кримінальне законодавство України, але водночас у більшості з них немає наголосу на засобі вчинення, тобто на використанні інформаційно-телекомунікаційних технологій, систем та мереж. Статистичні дані свідчать про щорічне збільшення кіберутворювальних кримінальних правопорушень. Усе частіше спостерігаємо перехід від традиційного вчинення кримінального правопорушення до його перенесення в призму кіберпростору. Було наголошено на необхідності запровадження до певних кримінальних правопорушень кваліфікаційних ознак, що підкреслювали б підвищену суспільну небезпеку діянь, вчинюваних у кіберпросторі. З огляду на проблеми кваліфікації суспільно небезпечного діяння, передбаченого частиною 3 статті 190 Особливої частини Кримінального кодексу України, та невідповідність змісту

об’єктивної сторони такого кримінального правопорушення сучасним реаліям, запропоновано виключити з частини 3 статті 190 Особливої частини Кримінального кодексу України «дії, вчинені шляхом незаконних операцій з використанням електронно-обчислювальної техніки».

Запропоновано дематеріалізувати предмет кримінального правопорушення, передбаченого статтею 185 Особливої частини Кримінального кодексу України, та одночасне запровадження спеціального складу крадіжки, а саме: крадіжки у сфері обігу безготівкових або електронних грошей та віртуальних активів. У статті 189 Особливої частини Кримінального кодексу України запропоновано ввести кваліфікаційну ознаку «погроза блокування, видалення, знищення, модифікації або іншого несанкціонованого втручання в роботу інформаційно-телекомунікаційних технологій, систем і мереж, що може завдати шкоди правам та інтересам потерпілої особи».

РОЗДІЛ 3.
ОСОБЛИВОСТІ КВАЛІФІКАЦІЇ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ У КІБЕРПРОСТОРІ

3.1. Особливості кримінально-правової кваліфікації кримінальних правопорушень у кіберпросторі, предметом і засобом вчинення яких є віртуальні активи

Ураховуючи специфіку кіберпростору й особливості вчинення кримінальних правопорушень у ньому, предмет і засоби вчинення кримінальних правопорушень у кіберпросторі можуть відрізнятися від предмета й засобів вчинення суспільно небезпечного діяння аналогічних кримінальних правопорушень, що вчиняються в матеріальному світі.

Оскільки кіберпростір є частиною інформаційного простору, такі суспільно небезпечні діяння, як, наприклад, шахрайство або крадіжка, що вчиняються в кіберпросторі, не можуть бути спрямовані на конкретні матеріальні предмети (цифрові пристрої, автомобілі, гаманці), оскільки вони просто не можуть існувати в розрізі кіберпростору в тому фізичному вигляді, до якого ми звикли. Незважаючи на це, такі кримінальні правопорушення можуть бути спрямовані на інші предмети, що мають таку саму економічну цінність, але існують винятково в цифровому середовищі, зокрема віртуальні активи [308, с. 143].

Постійний розвиток фінансового сектору загалом і ринку валют зокрема приводить до появи нових фінансових інструментів, грошових сурогатів, товарів та продуктів, одним із яких є віртуальні активи. Водночас виникнення нового фінансового інструменту зумовлює необхідність визначення законодавчого регулювання цього явища й вироблення його правого статусу.

Хочемо наголосити, що Україна здебільшого є лідером антирейтингів, наприклад у розрізі захисту прав інтелектуальної власності або рівня корупції, і, незважаючи на збройну агресію Російської Федерації та реформи, передбачені європейською спільнотою, все ще залишається одним із лідерів за цими показниками. Проте ситуація з віртуальними активами цілком протилежна. Парадоксальним можна вважати той факт, що українське суспільство без будь-якої підтримки з боку держави посіло досить помітні позиції у сфері віртуальних активів серед світової спільноти. Пропонуємо коротко проаналізувати обставини, що стали основоположним підґрунтям розвитку як нормативно-правового регулювання віртуальних активів, так і вироблення методики боротьби із суспільно небезпечними діяннями, в яких віртуальні активи є предметом або знаряддям вчинення кримінального правопорушення [309].

На початку 2016 року на території України вже була сконцентрована значна кількість майнінгових потужностей біткоїну. Уже в грудні 2016 року в Україні пройшла одна з перших на європейському континенті конференція, присвячена віртуальним активам, зокрема останнім винаходам у галузі фінансових технологій «BlockchainUA». На нашу думку, саме з 2016 року на території нашої країни почала формуватися спільнота блокчейн-розробників і криптотрейдерів, які наразі становлять проактивне й впливове ком'юніті [310; 311].

Зауважимо, що часто розвиток суспільних відносин є стрімким, тому державні інституції просто не встигають забезпечити врегулювання, а отже, охорону тих чи інших суспільних явищ чи інституцій. На нашу думку, це зумовлено насамперед тим, що держава повільна й майже завжди фіскально налаштована. Проте хочемо констатувати факт, що великі капітали ринку, що розвивається, переважно просто не залишаються в країні без державних правил регулювання. І хоча віртуальні активи – це ніби про свободу, капітал

іде туди, де є спеціальні ліцензії, а залишається там, де працюють прозорі правила гри й порівняно прийнятні ставки за податками.

Поява віртуальних активів, крім позитивного ефекту, стала каталізатором появи нових злочинних схем, зокрема шахрайства, вимагання та легалізації майна, одержаного злочинним шляхом, адже саме віртуальні активи, враховуючи їх специфічні ознаки, є дієвим засобом реалізації цих суспільно-небезпечних діянь. Ознаками віртуальних активів є наведені далі.

1. Анонімність. Застосування методів криптографії та децентралізованих реєстрів дуже ускладнює розпізнавання користувача. Затребуваність віртуальних активів у кримінальному співтоваристві створює необхідність підвищення рівня їх анонімності. Створено віртуальні активи, що використовують різні способи «замітання слідів» криптовалютних транзакцій. До таких віртуальних активів Європарламент класифікує «Monero», «DASH» і «Zcash» [312].

2. Цифровізація. Віртуальні активи є цифровим кодом, як результат – функціонування відповідної інформаційно-телекомунікаційної програми.

3. Майновий характер. Віртуальні активи є різновидом цифрового майна, що виконує в суспільстві функції засобу платежу й має фіскальну цінність.

4. Конфіденційність операцій із віртуальними активами, що можна охарактеризувати як безконтрольні транзакції віртуальних валют між різними віртуальними рахунками. З огляду на те, що будь-яка операція доступна кожному і її можна відстежити в ланцюжку блоків, немає посилання на конкретного користувача. Ним може бути як фізична, так і юридична особа [313].

5. Транснаціональність. Ця особливість полягає у відсутності можливості встановити кордони під час здійснення операцій. Оскільки обіг і використання віртуальних валют є транскордонними й відбуваються у

віртуальному (онлайн-) середовищі, відмінності між нормами та правила країн – учасниць транзакцій можуть бути вагомими, що значно ускладнює роботу правоохоронних органів [314].

6. Децентралізованість. Дає користувачам змогу обмінюватися фінансовими цінностями безпосередньо, тобто без посередників. Фахівці, які працюють із віртуальними активами, пояснюють, що основна їх відмінність від звичної національної валюти полягає в децентралізованості й непідконтрольності з боку урядів. Факт виникнення цієї незалежної, з відсутнім центром управління, цифрової платіжної системи демонструє, зокрема, наскільки рівень довіри громадян до держави, фінансової системи в усьому світі падає з кожним роком. Проте це не означає, що держава не повинна регулювати цей обіг, адже безконтрольність віртуальних активів відкриває великі можливості для шахраїв, ведення тіньового бізнесу, фінансування військових конфліктів тощо [315, с. 200].

Саме тому з метою врегулювання відносин стосовно віртуальних активів загалом і забезпечення побудови основи для системи заходів протидії відмиванню доходів за допомогою віртуальних активів в Україні було розроблено кілька законопроєктів щодо їх узаконення. Вважаємо доцільним проаналізувати кожний із них.

Відповідно до проєкту закону № 7183 «Про обіг криптовалюти в Україні» від 6 жовтня 2017 року криптовалюта – це програмний код (набір символів, цифр та букв), що є об’єктом права власності, який може бути засобом міни, відомості про який носять і зберігають у системі блокчейн як облікову одиницю цієї поточної системи блокчейн у вигляді даних (програмного коду). Цим проєктом передбачено, що використання криптовалюти потрібно здійснювати шляхом виконання операції з міни (обміну) криптовалюти будь-яких видів на іншу криптовалюту, обміну її на електронні гроші, валютні цінності, цінні папери, послуги, товари тощо. Крім того, згідно з цим законопроєктом криптовалюта – це окремий

специфічний і новий об’єкт цивільних правовідносин, а її узаконення повинно відбуватися за два етапи. Упродовж першого етапу необхідне затвердження правового статусу криптовалюти та суб’єктів господарювання, що надають послуги з обміну. Також заплановані вивчення тенденцій та аналіз проблем ринку криптовалюти. На другому етапі передбачене окреслення зберігачів віртуальних валют. Зберігачами будуть особи, які для захисту приватної інформації від імені своїх клієнтів надаватимуть послуги [316].

Натомість проєкт закону № 3637 від 11 червня 2020 р. «Про віртуальні активи» стосувався комплексу правовідносин, що виникають у зв’язку з обігом віртуальних активів в Україні, і детально визначав права та обов’язки учасників ринку віртуальних активів, засади державної політики у сфері обігу віртуальних активів. Віртуальним активом його автори пропонують називати особливий вид майна, що є цінністю в електронній формі, існує в системі обігу віртуальних активів та може перебувати в цивільному обігу [317].

Віртуальні активи можуть бути забезпеченими й незабезпеченими. Нормативно-правова база, спрямована на врегулювання предмета законопроєкту, в Україні відсутня. Положення чинного Закону України «Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення», що стосуються віртуальних активів, не надають належного правового регулювання піднятим у законопроєкті питанням через вужчу спрямованість зазначеного закону. Цей законопроєкт було прийнято в першому читанні 2 грудня 2020 р., а ухвалено 8 вересня 2021 року Верховною Радою України. Водночас Президент України вважає, що цей Закон не може бути підписаний з огляду на те, що: 1) положення Закону України «Про віртуальні активи» не створюють завершених правових механізмів, необхідних для його

реалізації; 2) положення проєкту закону не відповідають конституційним вимогам щодо правової визначеності як складової принципу верховенства права (стаття 8 Конституції України); 3) положення проєкту не забезпечують зрозумілих і прозорих умов для учасників ринку віртуальних активів та інвесторів, що не сприятиме належному забезпеченню їх прав [318].

Важливо акцентувати увагу, що викладений у законопроєкті підхід також не враховує правової позиції Конституційного Суду України, висловленої в Рішенні від 30 травня 2001 року за № 7-рп/2001, згідно з яким неповнота законодавчого регулювання суспільних відносин не відповідає конституційному визначенню України як правової держави. У Рішенні від 1 червня 2016 року № 2-рп/2016 Конституційний Суд України зазначив, що держава повинна вживати належних заходів для забезпечення можливості повної реалізації прав і свобод людини; з цією метою, зокрема, законодавець повинен забезпечувати ефективне правове регулювання, яке відповідає конституційним нормам і принципам, та створювати механізми, необхідні для задоволення потреб та інтересів людини [319; 320].

Ми переконані, що мета суб'єктів законодавчої ініціативи, безумовно, була дуже виваженою й нагальною. Проте спосіб її викладення свідчить про ігнорування системності права як явища. Для існування злагодженої правової системи та недопущення виникнення правових колізій дуже важливо, щоб, конструюючи ту чи іншу норму, розробник законопроєкту перевіряв її узгодженість з іншими чинними правовими нормами. Крім того, українське законодавство перенасичене термінами, що не мають нормативного обґрунтування й нормативно вираженого та закріпленого роз'яснення. Подібні ситуації призводять до неоднакового правозастосування, адже суб'єкти правозастосування тлумачать ті чи інші поняття по-різному. Безумовно, це є відвертим нівелюванням конституційних норм про правове визначення понять. Такий стан речей

абсолютно недопустимий у праві, що повинно мати загальний характер, а особливо в кримінальному праві, адже залишається поле для зловживань і виникає можливість побудови обвинувачення на основі припущень. На нашу думку, це порушує конституційні приписи та є абсолютно недопустимим для правової держави, якою себе позиціонує Україна.

Отже, бажання законодавця надати правове визначення віртуальних активів і врегулювати їх сутність у правовому полі є дуже позитивним та своєчасним кроком, що, безумовно, забезпечить зменшення відсотка тіньової економічної діяльності. Проте механізм реалізації цього бажання не є досконалим і зараз доопрацьовується. Автори висловлюють сподівання, що поняття «віртуальні активи» знайде своє законодавче закріплення.

Визначивши легальні моменти в питанні врегулювання правового статусу віртуальних активів, не можемо не проаналізувати доктринальні підходи до визначення цього поняття.

У найбільш загальному вигляді можна сформулювати три основні підходи: 1) віртуальні активи принципово можливо розглядати як платіжний засіб; 2) розгляд віртуальних активів як валюти валютних цінностей; 3) розгляд віртуальних активів як особливого майна, здатного до участі в цивільному обороті й такого, що становить певну цінність [321].

Зокрема, Д. Ангел під віртуальними активами розуміє одну з форм вираження цифрової валюти, емісія та облік якої базуються на асиметричному шифруванні й застосуванні різних методів криптографічного захисту [322, с. 603]. А. Гервіс розглядає віртуальний актив із позиції нової, сучасної та інноваційної платіжної мережі, що використовує, зокрема, P2P-технології й діє без центрального контролюючого органу чи банку, транзакції оброблюються спільно зусиллями мереж [323, с. 260]. Так само А. Берестен не розглядає віртуальні активи як новий вид платіжного інструменту. На його думку, вони є одним

із видів електронних грошей, що базуються на децентралізованому механізмі випуску та обігу. Крім того, науковець характеризує віртуальний актив як складну інформаційно-технологічну систему, побудовану на криптографічних методах захисту, що регулюють ідентифікацію власників і фіксують факти їх змін [324].

Подібної точки зору додержується І. Верес. Зокрема, зазначає, що віртуальний актив – це вид цифрових грошей, в якому використовуються розподілені мережі й публічно доступні журнали реєстрації угод, а ключові ідеї криптографії поєднані в них із грошовою системою заради можливості створити безпечну, анонімну та потенційно стабільну віртуальну валюту [325, с. 13].

З-поміж усіх доктринальних визначень поняття «віртуальні активи», напевно, найбільш розгорнуте надав А. Карстенс. На відміну від інших науковців він акцентував увагу на двох ключових моментах обігу віртуальних активів – довірі й конвенції. Поширення віртуальних активів лише підкреслює важливість центральних банків, що відіграють роль керуючих суспільною довірою, нагадує, що гроші є результатом конвенції, але, якщо довіра до грошей не перемагає, юридичний мандат, який надає цінність грошам, стає безглуздим [326].

Більш сучасне визначення поняття «віртуальний актив» надає Ю. Полякова: новий фінансовий інструмент конвертованої цифрової валюти, що базується на математичних принципах, які автоматично генеруються й контролюються програмним забезпеченням [327, с. 713].

На основі розглянутих специфічних особливостей і трактувань поняття «віртуальний актив» хочемо запропонувати його авторське визначення. Зокрема, під віртуальним активом варто розуміти цифрову валюту (віртуальну, без фізичної форми), створення й контроль за якою базується на криптографічних методах, щодо якої встановлена повна

децентралізація, що гарантує коректність операцій у системі, зокрема неможливість впливати на транзакції учасників криптосистеми.

Визначивши основні особливості віртуальних активів, пропонуємо перейти до характеристики кримінальних правопорушень, за яких віртуальні активи можуть бути предметом або засобом вчинення суспільно небезпечного діяння, та розглянемо проблеми кваліфікації таких діянь.

Як ми вже зазначили, за своєю природою будь-який віртуальний актив – унікальне цифрове число, репрезентоване у формі цифрової інформації. Це число використовують як грошовий еквівалент у кіберпросторі: на нього можна щось купити або обміняти на справжні гроші, оскільки кожний віртуальний актив має власну цінність незалежно від свого виду [328, с. 116].

Проте, на нашу думку, враховуючи специфічну природу віртуальних активів і проблеми правового регулювання в Україні, виникає серйозна проблема щодо того, чи можуть бути віртуальні активи предметом кримінальних правопорушень. Наш аналіз ми будемо здійснювати в розрізі розуміння віртуальних активів як іншого нематеріального об’єкта цивільного законодавства, цифрової інформації, що зберігається в інформаційно-телекомунікаційних технологіях, системах і мережах.

Найпопулярнішими кримінальними правопорушеннями, в яких віртуальні активи можуть бути предметом кримінального правопорушення, є шахрайство, крадіжка й легалізація майна, одержаного злочинним шляхом.

Пропонуємо почати з таких кримінальних правопорушень, як шахрайство та крадіжка. У науці кримінального права прийнято вважати, що предмет шахрайства й крадіжки повинен мати три основні ознаки: 1) економічну вартість; 2) матеріальність – предмет крадіжки й шахрайства повинен бути предметом матеріального світу, тобто речовим майном або правом на таке майно; 3) юридичну складову, тобто предметом крадіжки та

шахрайства може бути лише чуже майно, що не належить винній особі. Отже, лише за наявності цих трьох ознак можна стверджувати, що цей предмет буде предметом зазначених кримінальних правопорушень [329, с. 122].

Безперечно, віртуальні активи мають економічну цінність. Цей факт насамперед свідчить про наявність самого ринку віртуальних активів, до якого належать криптовалюти, NFT-токени, токени, токенізовані акції. Водночас у багатьох країнах віртуальні активи не лише одержали правовий статус, а отже, правове регулювання, а й були прирівняні до цінних паперів. Наприклад, Резервний банк Австралії ще в 2013 році визначив криптовалюту як альтернативу валют різних країн світу, але водночас не надав їй статусу цінних паперів [330].

Незважаючи на це, вже у 2014 році Податкова служба Австралії зазначила можливість уведення оподаткування криптовалютних операцій. На сьогодні операції з криптовалютою, криптовалютні транзакції в Австралії обкладаються стандартним прибутковим податком і податком на прибуток. Водночас у разі використання криптовалюти як інвестицій не виникає необхідності сплати податку на приріст капіталу [331]. Крім того, в Австралії є легальна можливість виплачувати заробітну плату в криптовалюті, але лише за наявності договору між працівником і роботодавцем [332].

Аргентина – одна з провідних країн по використанню віртуальних активів. Департамент UIF у липні 2014 року дозволив усім фінансовим інститутам проводити операції з біткоїном та іншими віртуальними валютами й зобов’язав їх інформувати про проведені операції з віртуальними активами [333].

Крім того, відповідно до податкового законодавства Аргентини податки з видів діяльності, пов’язаних із віртуальними активами, сплачують у трьох формах: 1) як інвестиційну діяльність; 2) податок на

доходи у віртуальних активах або від їх продажу; 3) податок на прибуток підприємств, зокрема стосується діяльності майнінгових компаній.

Японія на сьогодні є однією з найліберальніших країн у сфері правового регулювання криптовалюти. Там із 1 квітня 2017 року в результаті внесення парламентом Японії деяких поправок біткоїн та інші криптовалюти були визнані легальним платіжним засобом.

Канада посідає друге місце у світі після США за кількістю біткоїн-банкоматів, що свідчить про високу популярність криптовалюти в цій країні. Для кращого розуміння технології блокчейн держава розробляє цифрову версію канадського долара на його основі [334].

Незважаючи на той факт, що українське суспільство доволі швидко прийняло правила гри з віртуальним активами, з юридичної точки зору згідно із законодавством України поки що віртуальні активи не можна віднести до легальних валют, офіційною грошовою одиницею в Україні є гривня, а випуск та обіг на території України інших грошових одиниць і використання грошових сурогатів як засобу платежу заборонені [335].

У 2014 році НБУ Листом №29-208/72889 (Лист НБУ) визначив, що біткоїн як один із видів віртуальних активів є грошовим сурогатом, що не має забезпечення реальної вартості [336].

Отже, Національний банк України відніс віртуальні активи загалом до грошових сурогатів, і саме на цю позицію посилалася судова практика. Крім того, було визначено, що банки не мають правових підстав для зарахування іноземної валюти, отриманої від продажу віртуальних активів за кордоном. 22 березня 2018 року НБУ видав Лист 40-0006/16290, яким відніс Лист НБУ про визнання біткоїну грошовим сурогатом до таких, що втратили актуальність. Отже, можна сподіватися, що відповідний Лист НБУ та Роз'яснення НБУ перестануть застосовуватися і у власників криптовалют зникнуть ризики визнання криптовалют грошовими сурогатами [337].

Підтвердженням економічної цінності віртуальних активів є той факт, що банкам заборонено здійснювати транзакції клієнтів щодо купівлі віртуальних активів. Тобто фактично держава визнає, що віртуальні активи можуть буди предметом купівлі – продажу, незважаючи на те, що Закон України «Про віртуальні активи» ще не набрав чинності [338].

На нашу думку, неможливо заперечувати факт економічної цінності віртуальних активів, оскільки, по-перше, сьогодні її можна обміняти на справжні як готівкові, так і безготівкові гроші, а, по-друге, за неї можна купити товар або навіть послуги. І наразі мова йде не про зарубіжні країни. Хочемо констатувати факт, що сьогодні в Україні можна купити каву, пальне й навіть ліки, оплачуючи віртуальними активами, а саме: криптовалютою [339].

Друге запитання, на яке необхідно відповісти під час аналізу віртуальних активів як предмета кримінальних правопорушень, що вчиняються в кіберпросторі: чи є віртуальні активи майном? Для відповіді на нього варто звернутися до цивільного законодавства.

Відповідно до статті 177 Цивільного кодексу України об’єктами цивільних прав є речі, зокрема гроші та цінні папери, інше майно, майнові права, результати робіт, послуги, результати інтелектуальної, творчої діяльності, інформація, а також інші матеріальні й нематеріальні блага.

З огляду на специфіку віртуальних активів можемо розглядати їх у трьох «формах»: як інформацію, як валюту та як інші нематеріальні блага. Відповідно до першого варіанта віртуальний актив є певним інформаційним цифровим продуктом, репрезентованим лише у вигляді програмного коду, що існує винятково в інформаційному середовищі. Відповідно до другого варіанта віртуальний актив являє собою грошову одиницю, що, хоча наразі де-юре нею не є, але де-факто вже сьогодні її можна обміняти на національну валюту або оплатити товар чи послуги. Зокрема, у 2013 році суд Східного округу Штату Техас ухвалив рішення,

що «оскільки віртуальні активи можна використовувати як гроші для оплати товарів та послуг, віртуальний актив є валютою – формою грошей».

Швейцарія в цьому напрямку пішла ще далі: у 2014 році швейцарським парламентом було ухвалено рішення, згідно з яким біткоїн варто розглядати як іноземну валюту [340].

Проаналізувавши ситуацію, можна зробити висновок: віртуальні активи однозначно є засобом платежу. Проте лише це не робить їх справжніми грошима. Основна причина, з огляду на яку не можна визнати віртуальні активи грошима, – це те, що вони емітуються децентралізовано, тобто не існує суб'єкта, що забезпечує їх платоспроможність [341].

Відповідно до третього варіанта віртуальний актив є іншим нематеріальним благом. На нашу думку, таке розуміння віртуального активу є найбільш прийнятним. Крім того, воно відображає положення Закону України «Про віртуальні активи». Саме тому Законом України «Про віртуальні активи» вони визначаються як нематеріальне благо, що має вартість [342].

Кожна одиниця віртуальних активів індивідуально визначена. Це унікальне цифрове число, що міститься в захищеному інформаційно-телекомунікаційному цифровому файлі даних. Одночасно двох таких одиниць не може бути. Отже, купуючи віртуальний актив за реальні гроші, покупець набуває унікальної індивідуальної певної речі, що має комерційну цінність, тобто отримує товар.

Аналізуючи кримінальну відповідальності за кримінальні правопорушення проти власності, предметом яких є віртуальний актив, постає закономірне запитання: за якою статтею Особливої частини Кримінального кодексу України кваліфікувати таке діяння? З одного боку, таке діяння може бути вчинене у формі обману або зловживання довірою, а з іншого – у формі таємного викрадення [343].

Зауважимо, що навіть якщо віртуальний актив репрезентований у формі цифрової інформації, неможливо заперечувати той факт, що він був придбаний власником за гроші. З цього можемо визначити, що заподіяння шкоди може бути виражено в грошових коштах, за які були придбані віртуальні активи. Тобто в разі неправомірного списання з рахунку володільця певної кількості віртуального активу без його відома маємо не просто неправомірний доступ до цифрової інформації, що зберігається в інформаційно-телекомунікаційній технології або системі, а крадіжку в кіберпросторі. Власник гаманця віртуальних активів більше не зможе їх використовувати, оскільки просто не матиме до них доступу, а особа, яка вчинила крадіжку, навпаки, зможе вільно здійснювати операції з викраденими віртуальними активами.

Зауважимо, що в наведеному прикладі суспільно небезпечне діяння завдає шкоди не стільки відносинам у сфері цифрової інформації, скільки відносинам у сфері власності, оскільки дії особи, яка вчиняє кримінальне правопорушення, спрямовані саме на заволодіння чужим нематеріальним майном – віртуальним активом, який має свій грошовий еквівалент, а не просто цифровим файлом. Незважаючи на це, залежно від способу одержання доступу до гаманця, на якому зберігалися віртуальні активи, особа, яка вчинила кримінальне правопорушення, буде нести додаткову кримінальну відповідальність за відповідними статтями Особливої частини Кримінального кодексу України, що передбачають кримінальну відповідальність за порушення у сфері використання інформаційно-телекомунікаційних технологій, систем та мереж.

Зауважимо, що сьогодні точиться теоретичний та доктринальний дискурси щодо питання встановлення кримінальної відповідальності за вчинення суспільно небезпечного діяння у формі крадіжки віртуальних активів. Ураховуючи їх неврегульований правовий статус, кримінальна відповідальність буде наставати за статтею 361 Особливої частини

Кримінального кодексу України у формі витоку та втрати цифрової інформації, що зберігається в інформаційно-телекомунікаційних технологіях, системах і мережах.

Водночас визначення шкоди в цьому разі буде лише суб'єктивним переконанням суду незалежно від оцінкової вартості віртуальних активів. Змоделюємо ситуацію. Особа 1 шляхом вивчення крадіжки обернула на свою користь 0,2 Bitcoin. На 10 березня 2023 року ціна такого віртуального активу становила 20 000 доларів, тобто вартість викраденого віртуального активу – 4 000 доларів. Зауважимо, що Особа 1 викрала зазначений віртуальний актив шляхом протиправного використання шкідливого програмного забезпечення з подальшим одержанням несанкціонованого доступу до комп'ютера Особи 2 і виведенням віртуального активу з гаманця Особи 2 на свій гаманець.

Відповідно до статусу віртуального активу Особа 1 буде нести кримінальну відповідальність за сукупністю кримінальних правопорушень, зокрема за частиною 3 статті 361 та частиною 1 статті 361-1 Особливої частини Кримінального кодексу України. Водночас, якщо суд буде кваліфікувати зазначене суспільно небезпечне діяння як крадіжку за частиною 3 статті 185 Особливої частини Кримінального кодексу України, на нашу думку, обов'язковою буде додаткова кваліфікація за частиною 3 статті 361 Особливої частини Кримінального кодексу України. Максимальний термін покарання за частиною 3 статті 185 Особливої частини Кримінального кодексу України сягає 6 років позбавлення волі й не має альтернативи. Водночас максимальний термін покарання за частиною 3 статті 361 Особливої частини Кримінального кодексу України становить 8 років позбавлення волі, але має альтернативу у вигляді штрафу. Припустімо ситуацію, коли суд відповідно до частини 3 статті 185 Особливої частини Кримінального кодексу України встановлює покарання у вигляді 3 років позбавлення волі, а за частиною 3 статті 361 Особливої

частини Кримінального кодексу України – 5 років позбавлення волі. Маємо ситуацію поглинання суворішим покаранням більш м'якого, незважаючи на те, що основним об'єктом під час вчинення крадіжки віртуальних активів є відносини власності, що фактично стають додатковим об'єктом. Так само основним об'єктом будуть відносини у сфері безпечного функціонування інформаційно-телекомунікаційних технологій, систем та мереж. Саме тому необхідно врегулювати правовий статус віртуального активу й визначити його як особливе нематеріальне благо.

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

Цифрова інформація сьогодні поки що не визнана предметом ані шахрайства, ані крадіжки. Це насамперед пов'язано з консерватизмом теорії кримінального права й низкою об'єктивних причин. Не вся цифрова інформація може мати вартість сама по собі, як, наприклад, метадані (тобто відомості про комп'ютерні дані), текстовий файл або просто електронне листування – це лише проста інформація, репрезентована в цифровій формі.

Також виникають суперечки з авторськими й суміжними правами. Наприклад, якщо винний без відома власника завантажить програмне забезпечення й скористається ним, таке діяння не можна кваліфікувати як крадіжку – це неправомірний доступ до комп'ютерної інформації та незаконне використання об'єктів авторського права й суміжних прав. Нічого не вилучають і нікуди не завертаються: особа, яка вчинила кримінальне правопорушення, просто використовує програмне забезпечення та не платить за це.

Звісно, цифрова інформація як така не може бути предметом крадіжки, доки вона не перетворена на конкретний цифровий інформаційний продукт, що буде мати всі ознаки товару. Донедавна такого продукту в повноцінному вигляді просто не існувало. Були програми – об'єкти авторського права. Проте з розвитком інформаційних технологій з'явилися віртуальні активи – фінансовий феномен, що за своєю природою став тим інформаційним продуктом, якого бракує, – нематеріальним об'єктом речового права.

З огляду на це пропонуємо 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 по праву власності іншій особі. У разі крадіжки продукту порушуються не скільки відносини у сфері нормального обороту цифрової інформації або авторські права, стільки відносини власності, тому що правомірний власник більше не може здійснювати права користування, володіння й розпорядження викраденим продуктом. Прикладом такого продукту може бути саме віртуальний актив.

Хочемо зауважити, що сьогодні дуже мало випадків, пов'язаних із крадіжкою віртуальних активів, про які повідомляють у правоохоронні органи. Це пов'язано передусім із тим, що більшість володільців віртуальних активів не знає про його реальний правовий статус, думаючи, що вони володіють чимось забороненим на зразок об'єктів, обмежених у цивільному обігу [344].

Ще одне кримінальне правопорушення, предметом якого часто є віртуальні активи, – шахрайство, передбачене статтею 190 Особливої частини Кримінального кодексу України. Оскільки питання проблем і співвідношення кваліфікації кримінальних правопорушень проти власності та у сфері використання інформаційно-телекомунікаційних технологій,

систем і мереж ми вже розглянули, пропонуємо зупинитися саме на способах та схемах вчинення цього суспільно небезпечного діяння.

За загальним правилом способами вчинення шахрайства є обман та зловживання довірою. Серед найпопулярніших схем, використовуваних шахраями у своїй діяльності, хочемо виділити такі: 1) цільовий фішинг, пов'язаний із перенаправленням цільових користувачів на фіктивні вебсайти віртуальних активів; 2) шахрайство з купівлею та обміном віртуальних активів; 3) інвестування у фіктивні віртуальні активи.

Оскільки цільовий фішинг, пов'язаний із перенаправленням цільових користувачів на фіктивні вебсайти віртуальних активів, і шахрайство з купівлею та обміном віртуальних активів ми аналізували в попередньому розділі нашого дослідження, пропонуємо зосередити увагу на найпопулярнішому виді шахрайства з використанням віртуальних активів, яким є фіктивна купівля нових віртуальних активів, що мають назву токени, з подальшим обманом інвесторів. Загалом, токен – це одиниця обліку активів у певних IT-проєктах, аналог акцій на фондовій біржі. Їх випускають для залучення фінансування в IT-стартапи в рамках процедури ICO (випуску токенів), кредитування й монетизації додаткових сервісів для учасників IT-проєкту [345].

Сама схема шахрайства виглядає наведеним далі чином та охоплює декілька етапів. На першому етапі шахрай створює канал у телеграмі або іншому месенджері чи соціальній мережі й починає збирати аудиторію. Водночас варто зауважити, що останнім часом шахраї намагаються купити вже існуючий телеграм-канал, ціна якого починається від 5 000 доларів за 3 000 підписників. Купівля вже існуючого телеграм-каналу створює для шахрая більш довірливе ставлення, і здебільшого підписники навіть не здогадуються про шахрайську схему, а, навпаки, вважають це певним шансом на заробіток.

Другий етап характеризується створенням шахраєм свого віртуального активу. Зазвичай він використовує назву віртуального активу, що ще не вийшов у публічний доступ і має великі перспективи, та проводить стадію пошуку й залучення коштів від інвесторів. Найкращими платформами для створення свого віртуального активу є «Binance Smart Chain» та «Uiswap» [346; 347].

Третій етап полягає в усебічному рекламуванні в телеграм-каналі свого віртуального активу й створенні більш довірливого ставлення до нього. Так шахрай може за допомогою різних програм робити вирізки з вебсайтів новин, нібито про колаборацію між нібито компанією – засновником фіктивного віртуального активу з інвестиційними фондами, що займаються інвестуванням у віртуальні активи. Як підтвердження шахрай робить переказ значної суми на купівлю фіктивного віртуального активу й дає посилання на платформи, де його можна купити. Зазвичай такими платформами є «pancakeswap» та «biswap», на яких жертви обмінюють свої фіатні віртуальні активи на фіктивні. Звернемо увагу на певну особливість зазначеного виду кібершахрайства: жертва під час переказу своїх фіатних віртуальних активів вибирає саме гаманець шахрая, тим самим відразу переказуючи йому свої віртуальні фіатні активи. На останньому етапі шахрай просто видаляє всі пости щодо шахрайської операції, тим самим замітаючи сліди свого кримінального правопорушення, і починає коло із самого початку в рамках уже існуючого телеграм-каналу [348; 349].

Зауважимо, що відповідно до розглянутої схеми вчинення шахрайства в кіберпросторі особа буде нести кримінальну відповідальність за його основним складом.

Ще одна схема вчинення шахрайства, предметом якого є віртуальні активи, – шахрайство під виглядом інвестування у віртуальні активи, зокрема криптовалюту й NFT-токени. У цьому разі віртуальні активи

будуть предметом кримінального правопорушення, лише якщо інвестори залучали до шахрайського капіталу саме віртуальні активи, а не фіатні гроші [350].

Досліджуючи шахрайство в кіберпросторі, предметом якого є віртуальні активи, хочемо зробити висновок, що наразі цей тип кримінального правопорушення найбільш латентний з-поміж усіх інших. Водночас віртуальні активи з огляду на свої специфічні особливості лише ускладнюють процес розслідування цього типу суспільно небезпечних діянь. Питання міжнародного співробітництва у сфері протидії кіберзлочинності загалом наразі постає дуже гостро, адже щодня виникають усе нові й нові виклики, пов'язані з охороною кіберпростору як на національному, так і на міжнародному рівнях.

Як уже зазначалося, найчастіше віртуальні активи використовують у мережі Darknet під час купівлі послуг і товарів, виведених із цивільного обігу. Сьогодні багато різноманітних способів придбання віртуальних активів, а завдяки розвиненій системі blockchain-технології й транзакцій є можливість конвертації віртуальних активів у реальні готівкові та безготівкові й грошові кошти. Крім того, експерти Financial Action Task Force on Money Laundering зазначили, що жодна біржа віртуальних активів не має універсального захисту від так званих «брудних транзакцій», унаслідок чого стають можливими як шахрайські дії, так і різноманітні способи використання віртуальних активів у злочинних цілях [351].

Ураховуючи особливий контроль, що вживається державою для протидії легалізації майна, одержаного злочинним шляхом, правопорушникам доводиться знаходити нові способи вчинення цього кримінального правопорушення. З огляду на стрімкий розвиток інформаційних технологій та, як ми наголошували, відсутність законодавчого врегулювання віртуальні активи стають тим новим

успішним засобом вчинення легалізації майна, одержаного злочинним шляхом. З розширенням споживчого ринку віртуальних активів зростає кількість факторів легалізації, скоєних із їх використанням. Якщо чотири роки тому цей сегмент злочинності становив 5–7 % від загального обсягу злочинності, то в 2021 році він збільшився в 15 разів [352].

До способів легалізації злочинних доходів за допомогою віртуальних активів належать такі: 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. Пропонуємо проаналізувати кожний із цих способів.

Важливо звернути увагу на стрімкий та масштабний розвиток різноманітних сервісів для конвертації віртуальних активів і подальше переведення в готівковий або безготівковий фіатний засіб. До найпопулярніших сервісів належить сайт bestchange.com, репрезентований найбільшою кількість обмінників віртуальних валют. На таких сервісах можливий обмін будь-якого віртуального активу на безготівковий аналог, виражений у національній або будь-якій іншій валюті. Варто визначити основні особливості легалізації злочинних доходів через сервіси для конвертації віртуальних активів:

1) велика кількість обмінників віртуальних активів. Близько 460 обмінників віртуальних активів на платформі. Ураховуючи характер транзакцій, що викликають інтерес фінансового моніторингу, велика кількість обмінників віртуальних активів дає змогу проведення багатьох різних операцій з обміну віртуальних активів, за яких відправниками безготівкових коштів у національній чи зарубіжній валюті буде не один сервіс, а декілька. Водночас особа, яка здійснює легалізацію злочинних віртуальних активів, переводить невеликі суми: така особливість нівелює

інтерес із боку органів фінансового контролю та фінансового моніторингу зокрема [353];

2) швидкість проведення транзакцій. Обмін віртуальних активів на національну або зарубіжну валюту здійснюється менше ніж за годину;

3) велика кількість платіжних систем як у національній, так і в зарубіжній валюті.

P2P-обмін можна умовно поділити на здійснюваний в інтернет- та офлайн-середовищі. Транзакції P2P (від людини до людини) стали популярними в 2020 році завдяки швидкості проведення, анонімності й невисоким комісіям за транзакцію. Додало популяризації такому способу обміну віртуальних активів і функціонування криптоматів. За інформацією сервісу «Coin ATM Radar», на сьогодні у світі установлено понад тисяча таких пристроїв, а якщо взяти до уваги латентність даних, можна говорити про цифри, більші в 30 разів. За комісію розміром 6 % сервіс забезпечує безперебійність перекладу й анонімність клієнта [354].

Новим і популярним способом легалізації злочинних доходів є їх відмивання через сайти азартних ігор. Саме через ці сервіси відмиваються близько третини всіх «брудних» віртуальних активів. Злочинці все частіше стали використовувати ігрову валюту як спосіб збереження вартості віртуальних активів. Для цього купують валюту найбільш популярних віртуальних ігор. Її продають за криптовалюту, а потім на спеціальних сервісах конвертації обмінюють на фіатную валюту.

Інший спосіб легалізації – використання «програм-міксерів». Вони пропонують клієнтам заплутати історію транзакцій або відмити доходи, придбавши для іншої особи товари в Інтернеті за «брудні» гроші, під час чого покупець компенсує витрати клієнта, за винятком суми комісії. У результаті клієнт сервісу отримує «чисті» гроші, а покупець – дисконт на товар.

Використання фіктивних інтернет-сайтів із продажу цифрових товарів є одночасно найскладнішим у реалізації, проте органам фінансового контролю буде фактично неможливо встановити злочинне походження грошових коштів. Цей спосіб характеризується такими етапами: 1) створення фіктивного інтернет-ресурсу, здебільшого таким інтернет-ресурсом є вебсайт; 2) наповнення такого вебресурсу товарами, що мають цифрову визначеність (giftcard, продаж своїх оригінальних курсів, продаж NFT-токенів); 3) реєстрація фізичної особи – підприємця на 2-й або 3-й групі єдиного податку; підключення мерчант-систем, проведення онлайн-транзакцій у віртуальній валюті, підключення сервісів одночасної конвертації віртуальних валют «AdvCash».

Отже особа, яка безпосередньо здійснює відмивання злочинних коштів, купує певний товар чи послугу через фіктивний сайт за допомогою віртуального активу через сервіс подвійної конвертації та отримує «чистий» дохід у національній валюті на картковий рахунок, зазначений у центрі обслуговування платників податків.

Підсумовуючи вищевикладене, хочемо зазначити, що, незважаючи на фактичну відсутність правового регулювання віртуальних активів в Україні, поширеність їх використання серед українського суспільства лише зростає. Водночас збільшується кількість суспільно небезпечних діянь, спрямованих на використання віртуальних активів як предмета або засобу вчинення кримінального правопорушення.

Зважаючи на специфічні особливості віртуального активу, виникає багато запитань щодо кримінальної кваліфікації суспільно небезпечних діянь, спрямованих на їх протиправне заволодіння, зокрема шахрайства й крадіжка. Визначення віртуального активу як цифрової інформації у формі комп’ютерних даних обумовлює його виключення з кола предмета таких протиправних діянь, як крадіжка або шахрайство. Проте самою сферою

суспільних відносин, яким завдається шкода, незважаючи на традиційність матеріальності предмета, є відносини власності. Класифікація цифрових інформаційних продуктів до предмета крадіжки й шахрайства – адекватна та вчасна реакція на інформаційно-телекомунікаційний розвиток суспільства. Водночас пропонуємо визначити цифровий інформаційний продукт як сукупність унікальних інформаційно-телекомунікаційних даних, об'єднаних у матеріальний чи віртуальний носій, що мають усі ознаки товару, власну вартість і належать по праву власності іншій особі.

Легалізацію злочинних доходів варто охарактеризувати як багатоетапний процес, основна мета якого – за допомогою низки фінансових операцій надати правомірності володіння незаконно отриманим доходам. Для досягнення цієї мети використовують різні засоби й способи, покликані спотворювати справжню інформацію про джерело отримання грошових коштів.

Одним із порівняно нових способів легалізації злочинних доходів, що стає все популярнішим, є вчинення цього діяння за допомогою віртуальних активів. До способів легалізації злочинних доходів за допомогою віртуальних активів належать такі: 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.

3.2 Особливості призначення покарання за вчинення кримінальних правопорушень у кіберпросторі

Проблематика призначення судом покарання сьогодні посідає одне з основних місць як у науці кримінального права, так і в правозастосовній практиці. Сьогодні питання призначення покарання за кримінальні

правопорушення є одними з найскладніших та найбільш неоднозначних із-поміж проблем, що характеризують сучасний стан розвитку кримінальної юстиції в Україні. Щоб визначити, що варто розуміти під загальними засадами призначення покарання, потрібно дійти висновку, що таке призначення покарання загалом [355, с. 116].

Призначення покарання – це діяльність суду з вибору виду й розміру покарання за вчинене особою кримінальне правопорушення. Саме від призначення покарання залежатиме досягнення його мети, а також функціонування всієї системи кримінальної юстиції.

Т. Сахарук вважає, що призначення покарання є діяльність суду щодо ухвалення рішень про вид покарання та його розмір з урахуванням під час цього певних обставин. Проте таке визначення не достатньо розкриває сутність та особливості призначення покарання [356, с. 10].

А. Музика додержується думки, згідно з якою призначення покарання є процесом вибору судом у його обвинувальному вироку конкретного виду й розміру покарання щодо особи, яка вчинила кримінальне правопорушення [357, с. 178].

Так само О. Омельчук вважає, що терміни «призначення покарання» та «застосування покарання» є синонімічними. Водночас він зазначає, що застосування покарання є завершальним етапом процесу вибору судом під час винесення обвинувального вироку конкретного виду та міри кримінально-правового впливу на особу, яку визнано винною у вчиненні кримінального правопорушення, передбаченого відповідною статтею Особливої частини Кримінального кодексу України [358, с. 363].

Зауважимо, що призначення покарання є винятковою прерогативою суду, діяльність якого багатоаспектна й поєднує в собі як суб’єктивне оцінювання обставин вчиненого суспільно небезпечного діяння, так і врахування імперативних вимог Кримінального кодексу України.

Згідно зі статтею 50 Загальної частини Кримінального кодексу України покарання є заходом примусу, що застосовується від імені держави за вироком суду до особи, визнаної винною у вчиненні кримінального правопорушення, і полягає в передбаченому законом обмеженні прав і свобод засудженого. Крім того, у статті 65 Загальної частини Кримінального кодексу України закріплено, що суд наділений правом призначати покарання: 1) у межах, установлених у санкції статті (санкції частини статті) Особливої частини Кримінального кодексу України; 2) відповідно до положень Кримінального кодексу України; 3) ураховуючи ступінь тяжкості вчиненого кримінального правопорушення, особу винного та обставини, що пом'якшують та обтяжують покарання.

Загалом можна стверджувати, що будь-яке призначення покарання є певним етапом застосування норм кримінального права, що полягає у виборі судом конкретної міри покарання за вчинене кримінальне правопорушення із закріпленням в обвинувальному вироку суду.

Об'єктивним є той факт, що будь-яке покарання призначається відповідно до встановлених законодавством засад призначення покарання. Такі правила являють собою не що інше, як установлену Кримінальним кодексом України систему основних вихідних правил, які визначають порядок вибору міри покарання та є обов'язковими для суду.

Як зазначають А. А. Васильєв та О. С. Пироженко, чим тяжчим є вчинений злочин і чим більшу суспільну небезпеку становить винний, тим суворіша настає кримінальна відповідальність і суворішим повинне бути призначене покарання. На думку Т. А. Денисової, ефективність покарання залежить передусім від того, наскільки правильно й справедливо призначено покарання та наскільки воно відповідає тяжкості вчиненого злочину [359, с. 80; 360, с. 260].

Відповідно до статті 51 Загальної частини Кримінального кодексу України до осіб, визнаних винними у вчиненні кримінального правопорушення, судом можуть бути застосовані такі види покарань: 1) штраф; 2) позбавлення військового, спеціального звання, рангу, чину або кваліфікаційного класу; 3) позбавлення права обіймати певні посади або займатися певною діяльністю; 4) громадські роботи; 5) виправні роботи; 6) службові обмеження для військовослужбовців; 7) конфіскація майна; 8) арешт; 9) обмеження волі; 10) тримання в дисциплінарному батальйоні військовослужбовців; 11) позбавлення волі на певний строк; 12) довічне позбавлення волі [14].

Аналізуючи будь-яку норму Особливої частини Кримінального кодексу України та власне її співвідношення з нормами Загальної частини, значну увагу, на нашу думку, варто приділити саме санкції відповідної статті. Призначення покарання в межах санкції статті або санкції частини статті Особливої частини Кримінального кодексу України як одна із засад призначення покарання одночасно є найбільш чітко визначеною й найбільш складною для розуміння та застосування. З одного боку, ця засада передбачає обов'язок суду лише не виходити за межі санкції й забезпечувати вибір такого виду та розміру покарання, що передбачає відповідна санкція. Водночас складною вона є з огляду на те, що більшість статей і частин статей Особливої частини Кримінального кодексу України передбачають відповідальність за вчинення альтернативних діянь, визначаючи альтернативні види покарань, не встановлюючи чітких критеріїв, згідно з якими суддя повинен вибирати той чи інший вид та/або розмір покарання за одним чи іншим альтернативним діянням [361, с. 338].

У теорії кримінального права декілька видів санкцій, зокрема відносно визначені, абсолютно визначені, альтернативні, відсилочні й

неконкретизовані. Зауважимо, що в Кримінальному кодексі України використано лише відносно визначені й альтернативні санкції [362, с. 235].

Відносно визначена санкція статті або частини статті Особливої частини Кримінального кодексу України передбачає можливість застосування лише одного виду основного покарання та визначає межі його розміру. Альтернативні санкції містять вказівку на два або більше основних покарань, із яких суд вибирає лише одне [363].

Пропонуємо розглянути види санкцій за вчинення кіберзалежних кримінальних правопорушень (табл. 3).

Таблиця 3 – Види покарання та санкцій за кіберзалежні кримінальні правопорушення

Санкція частини статті	**Вид покарання**
1	**2**
Несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж	
Частина 1 статті 361 Особливої частини Кримінального кодексу України	Штраф від однієї тисячі до трьох тисяч неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк до трьох років
Частина 2 статті 361 Особливої частини Кримінального кодексу України	Штраф від трьох до семи тисяч неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк від двох до п’яти років, або позбавленням волі на той самий строк

Продовження таблиці 3

1	2
Частина 3 статті 361 Особливої частини Кримінального кодексу України	Штраф від семи до десяти тисяч неоподатковуваних мінімумів доходів громадян або позбавленням волі на строк від трьох до восьми років із позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років або без такого
Частина 4 статті 361 Особливої частини Кримінального кодексу України	Позбавлення волі на строк від восьми до дванадцяти років із позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років або без такого
Частина 5 статті 361 Особливої частини Кримінального кодексу України	Позбавлення волі на строк від десяти до п’ятнадцяти років із позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років
Створення з метою протиправного використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут	

Продовження таблиці 3

1	2
Частина 1 статті 361-1 Особливої частини Кримінального кодексу України	Штраф від двох до чотирьох тисяч неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років, або позбавленням волі на строк до трьох років
Частина 2 статті 361-1 Особливої частини Кримінального кодексу України	Позбавлення волі на строк до п’яти років
Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп’ютерах), автоматизованих системах, комп’ютерних мережах або на носіях такої інформації	
Частина 1 статті 361-2 Особливої частини Кримінального кодексу України	Штраф від двох до чотирьох тисяч неоподатковуваних мінімумів доходів громадян або позбавленням волі на строк до двох років
Частина 2 статті 361-2 Особливої частини Кримінального кодексу України	Позбавлення на строк від двох до п’яти років

Продовження таблиці 3

1	2
Несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї	
Частина 1 статті 362 Особливої частини Кримінального кодексу України	Штраф від двох тисяч до чотирьох тисяч неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років
Частина 2 статті 362 Особливої частини Кримінального кодексу України	Позбавлення волі на строк до трьох років із позбавленням права обіймати певні посади або займатися певною діяльністю на той самий строк
Частина 3 статті 362 Особливої частини Кримінального кодексу України	Позбавлення волі на строк від трьох до шести років із позбавленням права обіймати певні посади або займатися певною діяльністю на строк до трьох років
Порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється	

Продовження таблиці 3

1	2
Стаття 363 Особливої частини Кримінального кодексу України	Штраф від двох до чотирьох тисяч неоподатковуваних мінімумів доходів громадян або обмеження волі на строк до трьох років із позбавленням права обіймати певні посади чи займатися певною діяльністю на той самий строк
Перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку	
Частина 1 статті 363-1 Особливої частини Кримінального кодексу України	Штраф від двох до чотирьох тисяч неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк до трьох років
Частина 2 статті 363-1 Особливої частини Кримінального кодексу України	Обмеження волі на строк до п'яти років або позбавленням волі на той самий строк із позбавленням права обіймати певні посади або займатися певною діяльністю на строк до трьох років

Проаналізувавши систему покарань за вчинення кримінальних правопорушень, передбачених розділом XVI Особливої частини Кримінального кодексу України, можемо констатувати факт, що основними видами покарання є штраф, обмеження й позбавлення волі. У деяких кримінальних правопорушеннях зі спеціальним суб'єктом додатковим

покаранням є позбавлення права обіймати певні посади або займатися певною діяльністю.

Загалом у період із 1 січня 2015 року по 1 січня 2023 року було винесено лише 420 судових рішень у формі вироків за вчинення кримінальних правопорушень, передбачених розділом XVI Особливої частини Кримінального кодексу України. На рисунку 10 зображено найбільш часті кримінальні правопорушення, а на рисунку 11 – види покарання, застосовані до осіб, які вчинили кримінальне правопорушення.

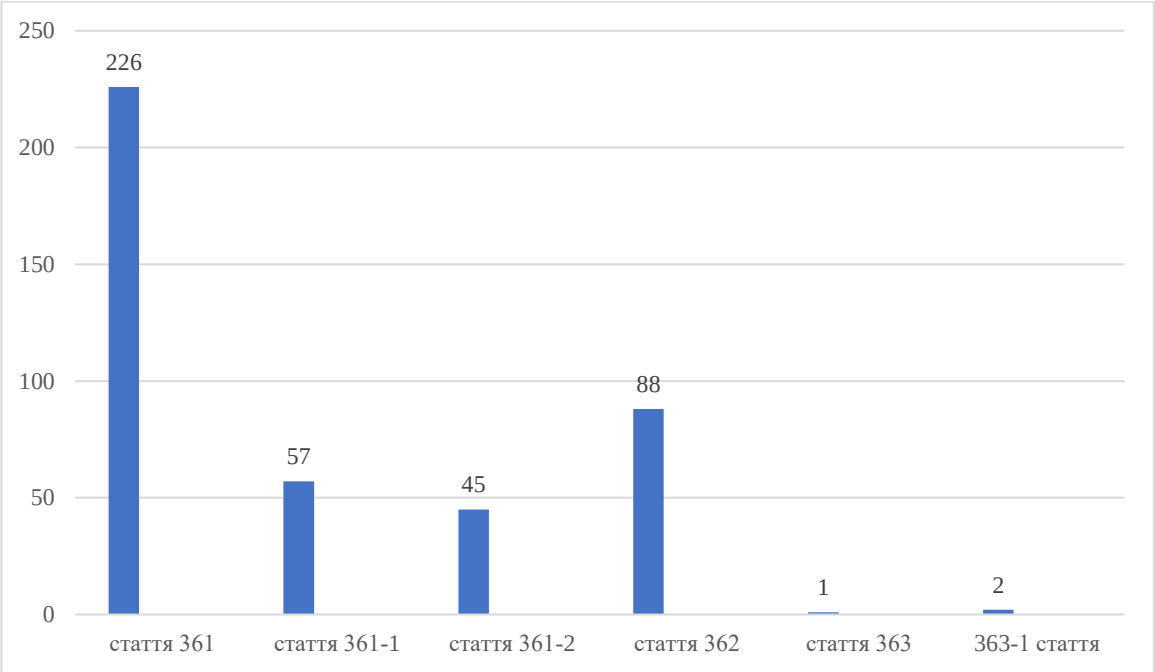

Рисунок 10 – Динаміка вчинення кримінальних правопорушень, передбачених розділом XVI Особливої частини Кримінального кодексу України за період із 1 січня 2015 р. по 1 січня 2023 р.

Крім того, на основі аналізу судової практики, зокрема за період із 1 січня 2015 року по 1 січня 2023 року, було визначено, що фактично в 39 % усіх розглянутих справ було призначено покарання у вигляді штрафу й у 61 % – у вигляді позбавлення волі. Водночас 98 % осіб, які вчинили кримінальне правопорушення за відповідними статтями Особливої частини Кримінального кодексу України та яким призначено 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. На рисунку 11 наведено, які покарання було призначено судом у розрізі статей розділу XVI Особливої частини Кримінального кодексу України.

Рисунок 11 – Вид призначеного покарання за кримінальні правопорушення, передбачені розділом XVI Особливої частини Кримінального кодексу України

Перше покарання, що ми пропонуємо охарактеризувати в розрізі кіберпростору, є штраф, передбачений пунктом 1 статті 51 Загальної частини Кримінального кодексу України. Статистика застосування покарання свідчить про його меншу поширеність серед інших кримінальних правопорушень, передбачених розділом XVI Особливої частини Кримінального кодексу України. На нашу думку, це зумовлено насамперед унікальністю цього виду покарання та його застосуванням як основного й додаткового виду покарання.

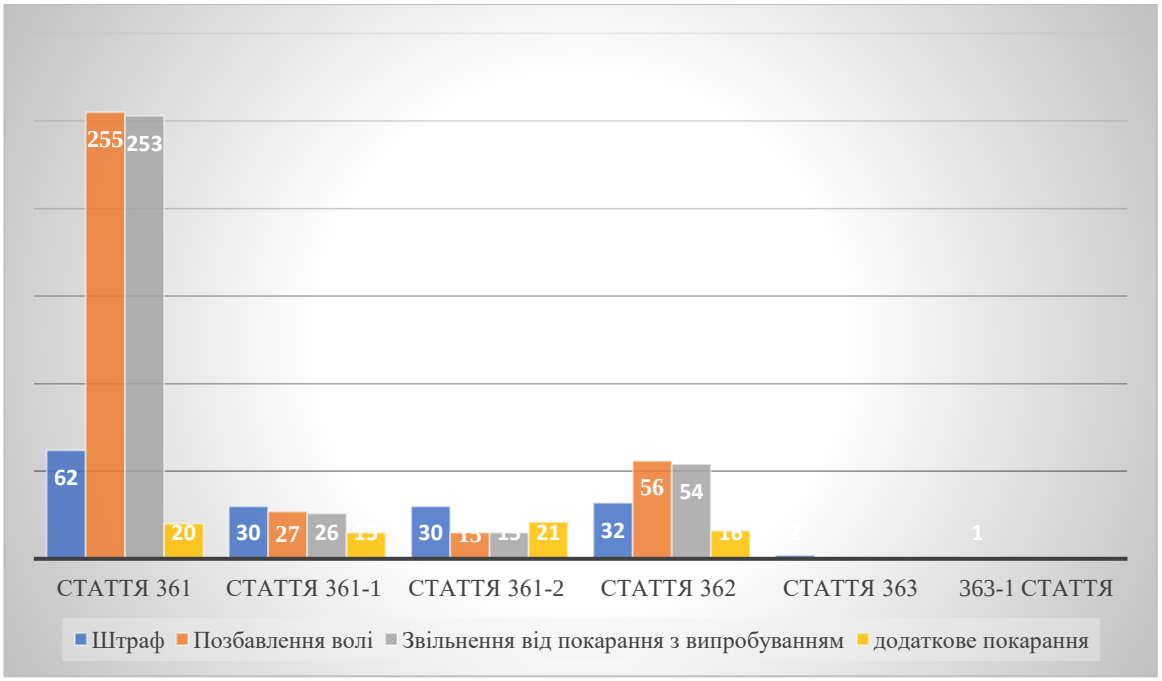

Рисунок 12 – Вид призначеного покарання за кримінальні правопорушення, передбачені розділом XVI Особливої частини Кримінального кодексу України

Штраф як вид основного покарання найбільше застосовується за вчинення кримінальних правопорушень, передбачених статями 361, 361-1 та 362 Особливої частини Кримінального кодексу України.

Відповідно до статті 53 Загальної частини Кримінального кодексу України штрафом визнається грошове стягнення, що накладається судом у випадках і розміром, установленими в Особливій частині Кримінального кодексу України, з урахуванням положень частини 2 статті 53 Загальної частини Кримінального кодексу України.

Щодо доктринального визначення поняття штрафу, то, на нашу думку, варто звернути увагу на такі погляди науковців, які досліджують це питання. Зокрема, К. Щур зазначає, що за своєю правовою природою штраф є майновим обмеженням для особи, якій призначено покарання, тобто фактично науковець розуміє під штрафом певне майнове покарання, згідно

з яким за рішенням суду із засудженого стягується відповідна, визначена грошова сума в дохід держави [364, с. 411].

В. Попрас, намагаючись пов'язати законодавче визначення штрафу із загальним поняттям покарання, дає розширене визначення цього виду покарання, а саме: захід примусу, що застосовується від імені держави за вироком суду до особи, визнаної винною у вчиненні кримінального правопорушення, і полягає в передбаченому законом обмеженні її права власності на певну суму грошових коштів [365, с. 144].

Влучне, на нашу думку, визначення дефініції поняття штрафу дає А. Смирнов, під яким пропонує розуміти вид покарання без ізоляції засудженого від суспільства, водночас сама кара не розглядається як основна мета покарання, хоча її елементи є тією чи іншою мірою в будь-якому покаранні, у штрафі на перше місце висуваються запобіжні та виховні складові, що характеризують штраф як кримінальне покарання [366, с. 170].

А. Попович виділяє такі ознаки штрафу: 1) це захід державного примусу; 2) застосовується винятково державними органами – судом; 2) полягає в обов'язковому грошовому стягненні з особи засудженого; 4) застосовується лише до особи, яка була визнана у вчиненні кримінального правопорушення; 5) полягає в обов'язковому обмеженні права власності особи на певну суму грошових коштів [367, с. 142].

Зауважимо, що розмір штрафу визначається судом, залежить від тяжкості вчиненого кримінального правопорушення та майнового стану винного й може становити від тридцяти до п'ятдесяти тисяч неоподатковуваних мінімумів доходів громадян. Також варто зазначити, що, якщо санкція Особливої частини Кримінального кодексу України встановлює вищий розмір штрафу, то судом може бути призначений штраф у максимальних межах відповідної статті Особливої частини Кримінального кодексу України. Водночас розмір призначеного штрафу не

може бути меншим за розмір майнової шкоди, завданої вчиненим кримінальним правопорушенням.

Варто наголосити, що з огляду на необхідність закріплення в Кримінальному кодексі України покарання, яке повинно відповідати ступеню суспільної небезпеки вчиненого діяння та його суспільно небезпечним наслідкам, у частині 2 статті 53 Загальної частини Кримінального кодексу України наведено, що особі, яку визнано винною у вчиненні кримінального правопорушення, за яке передбачене основне покарання у вигляді штрафу понад три тисячі неоподатковуваних мінімумів доходів громадян, розмір штрафу, що призначається судом, не може бути меншим за розмір майнової шкоди, завданої кримінальним правопорушенням, або отриманого в результаті вчинення кримінального правопорушення доходу. Водночас немає різниці, який граничний розмір штрафу, передбаченого відповідною санкцією Особливої частини Кримінального кодексу України.

Не можемо не звернути увагу на те, що згідно із Законом України від 3 квітня 2022 року № 2149-IX «Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану» мінімальну й граничну межі покарання у вигляді штрафу за вчинення кримінального правопорушення, передбаченого частиною 1 статті 361 Особливої частини Кримінального кодексу України, було визначено в межах від однієї до трьох тисяч неоподатковуваних мінімумів доходів та альтернативне покарання у вигляді обмеження волі строком на три роки [368].

Статистика мінімального й максимального розмірів штрафу як основного покарання показує, що судді на основі свого внутрішнього переконання переважно застосовують саме нижню мінімальну межу штрафу. На рисунку 13 зображена статистика застосування розміру штрафу за аналізовані кримінальні правопорушення в кіберпросторі. Відповідно

можемо спостерігати, що у 80 % випадків судами застосовується саме мінімальна межа штрафу за аналізовані кримінальні правопорушення в кіберпросторі.

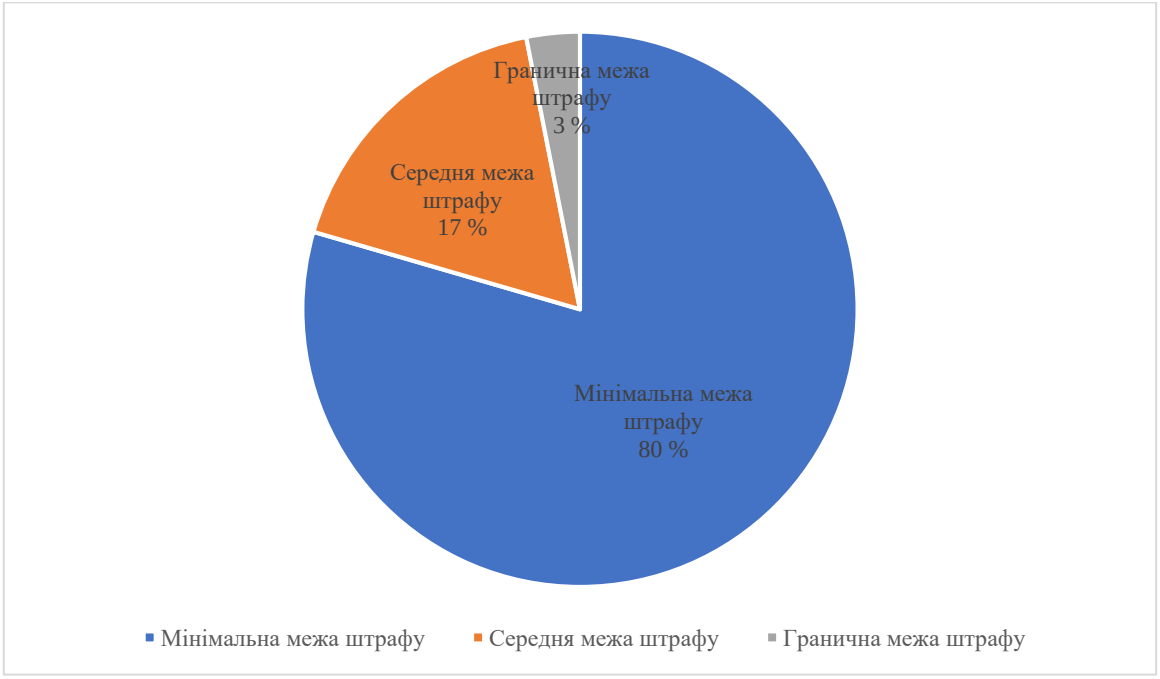

Рисунок 13 – Статистика мінімальної та граничної меж застосування штрафу як основного покарання за кримінальні правопорушення, передбачені розділом XVI Особливої частини Кримінального кодексу України

Друге місце серед застосовуваних покарань за кримінальні правопорушення, передбачені розділом XVI Особливої частини Кримінального кодексу України, посідає покарання у вигляді позбавлення волі.

Позбавлення волі як вид кримінального покарання є правовим наслідком учинення кримінального правопорушення й відповідно до кримінального законодавства (статті 63 Загальної частини Кримінального кодексу України) полягає в ізоляції засудженого й поміщення його на певний строк до кримінально-виконавчої установи закритого типу. Позбавлення волі встановлюється на строк від одного до п’ятнадцяти років,

за винятком випадків, передбачених Загальною частиною Кримінального кодексу України [369, с. 111].

Проблема призначення покарання у вигляді позбавлення волі за кримінальні правопорушення, передбачені розділом XVI Особливої частини Кримінального кодексу України, полягає в їх специфічних особливостях і складності визначення шкоди, завданої такими суспільно небезпечними діяннями. Згідно зі статистикою з 1 січня 2015 року по 1 січня 2023 року покарання у вигляді позбавлення волі було призначене у 255 випадках, тобто фактично 61 % від загальної кількості судових рішень у формі вироків за зазначену групу кримінальних правопорушень.

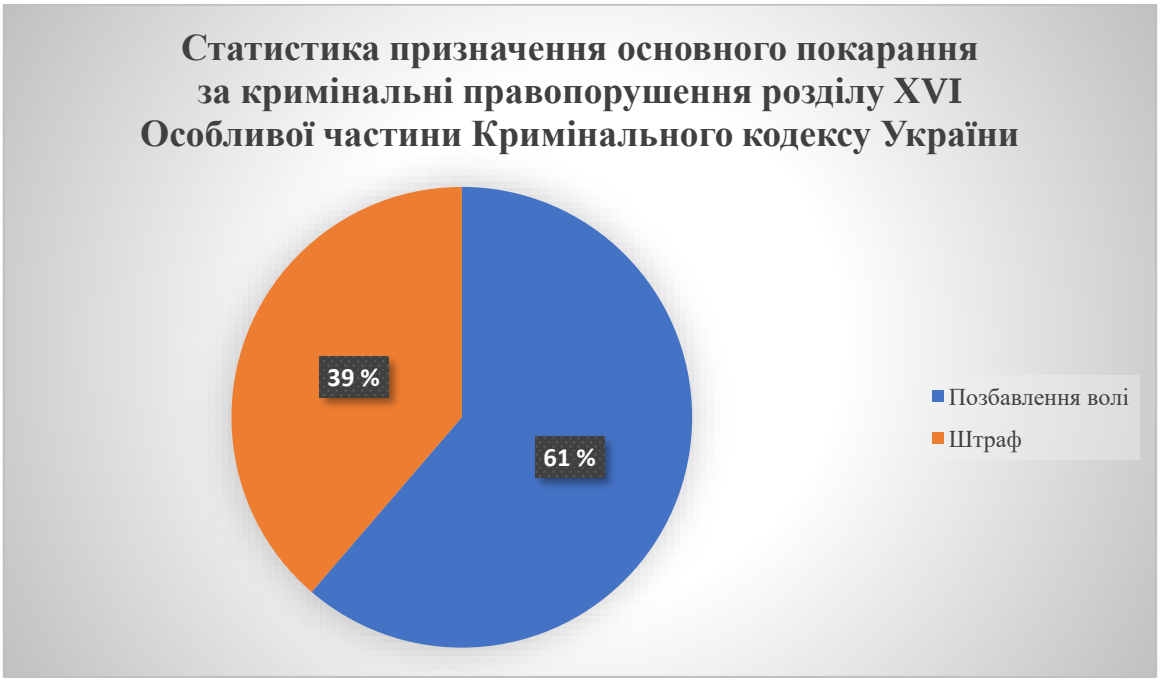

Рисунок 14 – Статистика призначення основного покарання за кримінальні правопорушення розділу XVI Особливої частини Кримінального кодексу України

Проте, незважаючи на фактичну рівномірність призначених покарань у вигляді штрафу та позбавлення волі, відбування покарання у вигляді позбавлення волі одержали лише 3 % засуджених. Зауважимо, що в разі

призначення покарання у вигляді позбавлення волі на певний строк у 98 % випадків відповідно до статті 75 Загальної частини Кримінального кодексу України особа, яка вчинила кримінальне правопорушення, звільнялася від відбування покарання з випробуванням.

Наприклад, вироком Франківського районного суду міста Львова було встановлено визнати Особу 1 винною у вчиненні кримінального правопорушення, передбаченого частиною 2 статті 361 Особливої частини Кримінального кодексу України, й призначити покарання у вигляді позбавлення волі строком на 3 роки. Водночас на підставі статті 75 Загальної частини Кримінального кодексу України було встановлено звільнити Особу 1 від відбування покарання з випробуванням і призначити їй випробувальний термін тривалістю 1 рік [370].

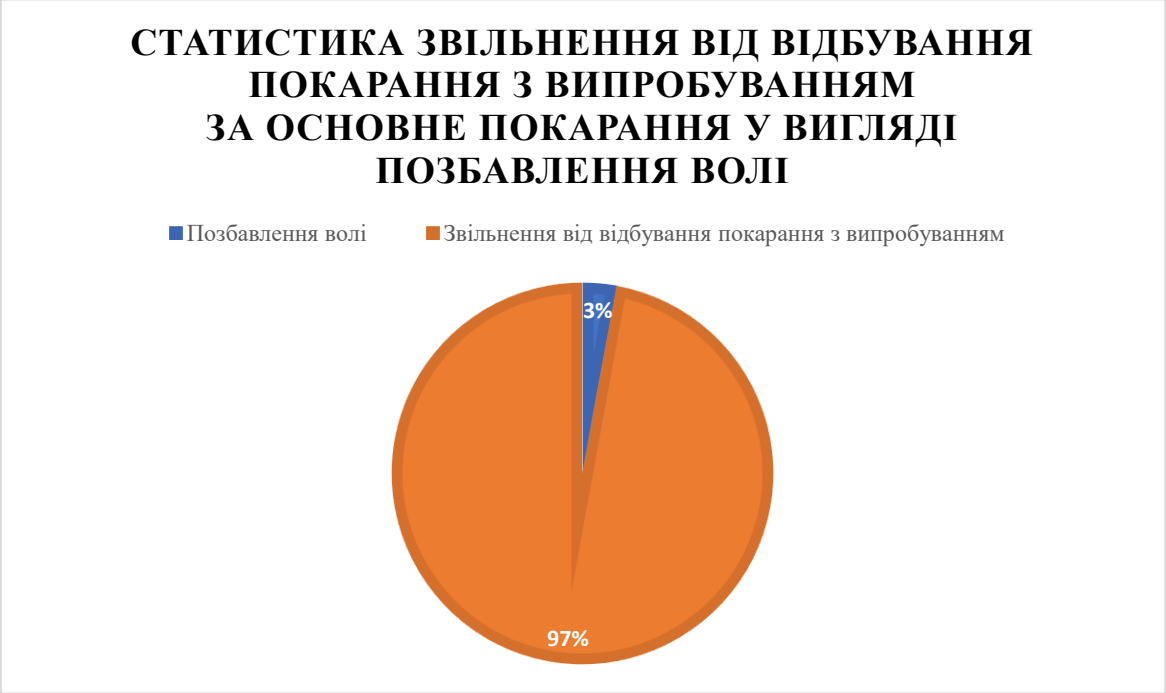

Рисунок 15 – Статистика звільнення від відбування покарання з випробувальним терміном за основне покарання у вигляді позбавлення волі

Базуючись на зазначеній статистиці, вважаємо, що фактично за 60 % вчинених суспільно небезпечних діянь особа, яка їх вчинила, не понесла достатнього покарання.

З огляду на індивідуалізацію покарання за кримінальні правопорушення, передбачені розділом XVI Особливої частини Кримінального кодексу України, варто брати до уваги, що такі суспільно небезпечні діяння завжди вчиняються з використанням інформаційно-телекомунікаційних технологій у формі цифрових пристроїв. Зважаючи на це, потрібно розглядати конфіскацію як можливість покарання. Варто зауважити, що в чинному Кримінальному кодексі України за кіберзалежні кримінальні правопорушення конфіскація майна як додатковий вид покарання не застосовується з 10 листопада 2015 року. Законом України «Про внесення змін до Кримінального кодексу України щодо вдосконалення інституту спеціальної конфіскації з метою усунення корупційних ризиків при її застосуванні» з частин 1 та 2 статті 361 Особливої частини Кримінального кодексу України було виключено норму, що визначала конфіскацію майна як додаткове покарання [371].

Відповідно до частини 1 статті 59 Загальної частини Кримінального кодексу України покарання у вигляді конфіскації майна полягає в примусовому безоплатному вилученні у власність держави всього або частини майна, що є власністю засудженого. Якщо конфіскується частина майна, суд повинен зазначити, яка саме частина майна конфіскується, або навести предмети, що конфіскуються. Крім того, відповідно до частини 2 статті 59 Загальної частини Кримінального кодексу України конфіскація майна встановлюється за тяжкі й особливо тяжкі корисливі злочини, а також за злочини проти основ національної безпеки України та громадської безпеки незалежно від ступеня їх тяжкості та може бути призначена лише у

випадках, спеціально передбачених в Особливій частині Кримінального кодексу України [14].

Незважаючи на виключення норми, що встановлювала додаткове покарання у вигляді конфіскації майна особи, яка вчинила кримінальне правопорушення, в судовій практиці широко застосовується спеціальна конфіскація. Відповідно до статті 96-2 Загальної частини Кримінального кодексу України спеціальна конфіскація застосовується, якщо гроші, цінності та інше майно: 1) одержані внаслідок вчинення кримінального правопорушення та/або є доходами від такого майна; 2) призначалися (використовувалися) для схиляння особи до вчинення кримінального правопорушення, фінансування та/або матеріального забезпечення кримінального правопорушення чи винагороди за його вчинення; 3) були предметом кримінального правопорушення, крім тих, що повертаються власникові (законному володільцю), а якщо його не встановлено, переходять у власність держави; 4) були підшукані, виготовлені, пристосовані або використані як засоби чи знаряддя вчинення кримінального правопорушення, крім тих, що повертаються власникові (законному володільцю), який не знав і не міг знати про їх незаконне використання [14].

Проте варто зауважити, що під час призначення покарання спеціальної конфіскації спостерігається відсутність єдиного підходу. Зокрема, фактично ідентичні справи з подібними методами вчинення вирішуються судами по-різному. Загалом, як ми вже зазначали, засобом вчинення будь-якого кримінального правопорушення, передбаченого розділом XVI Особливої частини Кримінального кодексу України, будуть інформаційно-телекомунікаційні технології у формі цифрових пристроїв або програмного коду. У таблиці 4 ми висвітлили три вироки суду, в яких було ухвалено три абсолютно різні питання щодо долі речових доказів.

Таблиця 4 – Рішення суду в кримінальних справах щодо долі речових доказів

Номер судової справи	Вчинене кримінальне правопорушення	Речові докази по справі	Рішення щодо долі доказів
Справа № 308/11741/20	Частина 1 статті 361 («Несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж») та частин 1, 2 статі 361-1 («Створення з метою протиправного використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут») Особливої частини Кримінального кодексу України	Системний блок персонального комп'ютера в корпусі «Logic Power»; роутер марки «tp-linc», мобільний телефон марки «Iphone» IMEI № 3 із сім-карткою оператора зв`язку Київстар № 4; ноутбук марки «Asus» (серійний номер: J7NOCVOT765F) із зарядним пристроєм; ноутбук марки «Samsung» (серійний номер: J9M791ND200008R) із зарядним пристроєм; три носії інформації: «Maxell», «San Disk», «TAB»	Конфіскація в дохід держави
Справа № 161/18959/20	Стаття 361-1 («Створення з метою протиправного використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут») Особливої частини Кримінального кодексу України	Жорсткий диск, s/n: WFLOQTM7, на якому наявне шкідливе програмне забезпечення під назвою «Encryption»	Знищити
Справа № 592/4316/20	Стаття 361-1 («Створення з метою протиправного використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут») Особливої частини Кримінального кодексу України	Ноутбук MSI s/n K1607N0061779	Повернути особі, заздалегідь знищивши шкідливі програми на жорсткому диску шляхом його форматування тощо

Зауважимо, що в першому та другому випадках судом було призначено покарання у вигляді позбавлення волі строком на 2 роки, у третьому випадку – покарання у вигдялі штрафу 500 неоподатковуваних мінімумів доходів громадян. Проте з об'єктивної сторони всі три кримінальні правопорушення вчинялися шляхом збуту або розповсюдження шкідливого програмного коду, що давав особі, яка вчинила кримінальне правопорушення, несанкціонований доступ до цифрового пристрою потерпілої особи. Водночас лише в першому випадку суд кваліфікував зазначені суспільно небезпечні діяння додатково як несанкціоноване втручання. В усіх трьох випадках суд призначив спеціальну конфіскацію з огляду на своє внутрішнє переконання. Проте, якщо в другому та третьому випадках було встановлено одиничне вчинення кримінального правопорушення у формі збуту або розповсюдження шкідливого програмного коду, то в першому випадку маємо ознаки повторності такого суспільно небезпечного діяння. Можемо припустити, що саме внаслідок вчинення кримінального правопорушення особою повторно було зумовлено рішення про спеціальну конфіскацію засобів вчинення кримінального правопорушення. Ураховуючи той факт, що цифрові пристрої є обов'язковим і фактично єдиним елементом вчинення кримінальних правопорушень, передбачених розділом XVI Особливої частини Кримінального кодексу України, можливість запровадження судами ухвали про спеціальну конфіскацію знаряддя вчинення за кримінальні правопорушення, які вчиняються повторно, в співучасті або спрямовані на інформаційно-телекомунікаційні технології, системи та мережі держави, є цілком обумовленою [375].

Щодо призначення такого виду покарання, як позбавлення права обіймати певні посади або займатися певною діяльністю, то статистика свідчить про те, що воно становить близько 15 % від загальної кількості винесених вироків. Найчастіше таке покарання застосовується до осіб, які

вчинили кримінальне правопорушення, передбачене статтею 362 Особливої частини Кримінального кодексу України.

Розглянувши основні покарання, що призначаються судом за кримінальні правопорушення, передбачені розділом XVI Особливої частини Кримінального кодексу України, хочемо розглянути основні проблеми під час їх призначення.

Зауважимо, що ми є прихильними застосування штрафу як основного виду покарання за більшість кримінальних правопорушень, передбачених розділом XVI Особливої частини Кримінального кодексу України, крім тих, які спричинили тяжкі наслідки, були вчинені повторно або спрямовані на інформаційно-телекомунікаційну інфраструктуру держави.

Проте в цьому разі є низка певних факторів, що дає змогу повністю забезпечити покарання у вигляді штрафу. Такі фактори зумовлені насамперед самою специфікою кримінальних правопорушень у кіберпросторі.

Першим фактором, що ми виділяємо, є вчинення декількох суспільно небезпечних діянь, передбачених Особливою частиною Кримінального кодексу України, для досягнення одного злочинного результату та власне призначення покарання за сукупністю кримінальних правопорушень. Загалом хочемо констатувати факт, що відповідно до аналізованої статистики судових рішень у формі вироків за кримінальні правопорушення, передбачені статтями 361, 361-1, 361-2 Особливої частини Кримінального кодексу України, у 57 % випадків вироки призначалися за сукупністю кримінальних правопорушень.

Наприклад, для несанкціонованого втручання в інформаційно-телекомунікаційну мережу, здійснюваного віддалено, особі, яка вчиняє кримінальне правопорушення, передусім необхідно одержати дані для доступу до такої системи. Такий доступ особа, яка вчиняє кримінальне правопорушення, може одержати шляхом використання шкідливого

програмного забезпечення та його фактичної інсталяції на цифровий пристрій жертви з подальшим отриманням усіх цифрових файлів, що зберігаються на такому пристрої. Отже, маємо ситуацію, за якої особа фактично вчинила суспільно небезпечне діяння, передбачене статтею 361-1 Особливої частини Кримінального кодексу України, що фактично буде визначатися як підготовче з подальшим одержанням несанкціонованого доступу, і як результат – втручання в роботу інформаційно-телекомунікаційної мережі, тобто діяння, передбачене статтею 361 Особливої частини Кримінального кодексу України. Зауважимо, що, оскільки мінімальна санкція статті 361 Особливої частини Кримінального кодексу України вища за мінімальну санкцію статті Особливої частини Кримінального кодексу України, особі за сукупністю кримінальних правопорушень і в результаті поглинання мерш суворого покарання більш суворим буде призначене покарання у вигляді штрафу від 2 000 неоподатковуваних мінімумів доходів громадян. Отже, на нашу думку, посягання на первісний об’єкт втрачає свою змістовність.

На рисунку 16 ми навели статистику кримінальних правопорушень, передбачених розділом XVI Особливої частини Кримінального кодексу України, що найчастіше вчиняються в сукупності з іншими кримінальними правопорушеннями інших розділів Особливої частини Кримінального кодексу України.

Проаналізувавши низку судових рішень у формі вироків, у яких простежується багатооб’єктність кримінальних правопорушень у кіберпросторі, ми дійшли висновку, що, незважаючи на те, що основним об’єктом під час вчинення кримінальних правопорушень були відносини у сфері власності й господарські відносини, остаточне покарання за сукупністю кримінальних правопорушень та в результаті поглинання менш суворого покарання більш суворим визначалося саме за суспільно небезпечні діяння, передбачені розділом XVI Особливої частини

Кримінального кодексу України. Це лише підтверджує нагальність запропонованих нами змін до відповідних статей Особливої частини Кримінального кодексу України [376; 377; 378; 379; 380; 381].

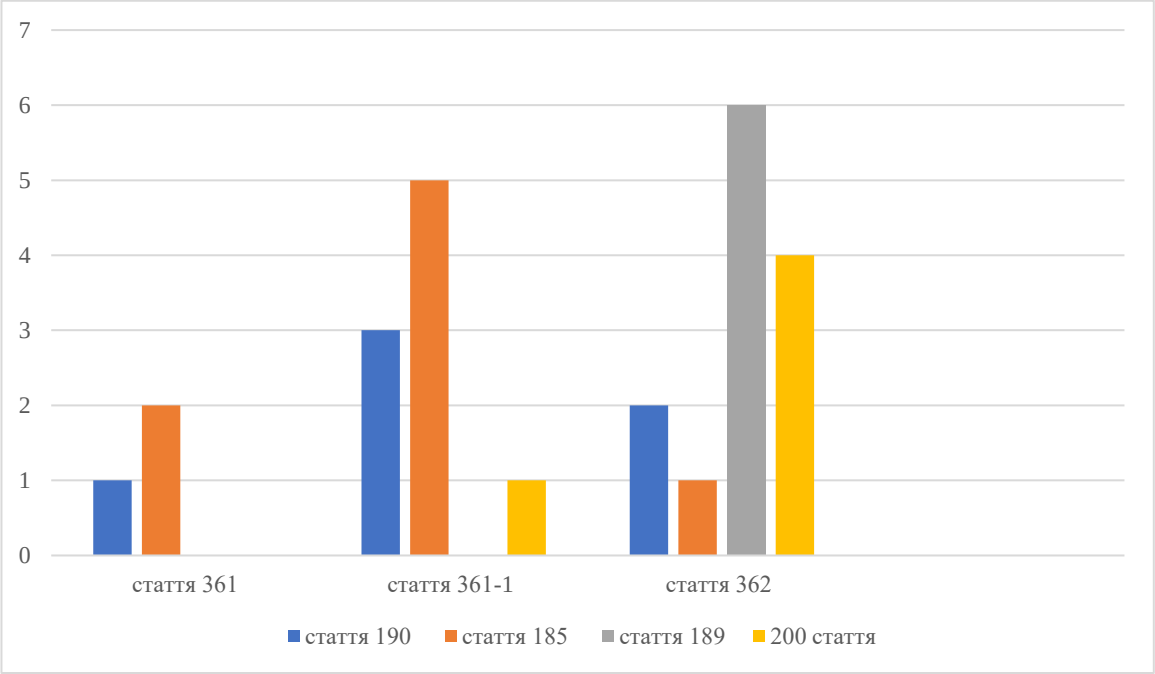

Рисунок 16 – Правопорушення, передбачені розділом XVI Особливої частини Кримінального кодексу України, що найчастіше вчиняються в сукупності з іншими суспільно небезпечними діяннями, передбаченими іншими розділами Особливої частини Кримінального кодексу України

Ще один фактор – вчинення таких кримінальних правопорушень неповнолітніми особами. У своїй науковій праці щодо аналізу особистості особи, яка вчиняє кримінальне правопорушення, Ю. Піцик зазначає, що 38 % осіб, які вчиняли кримінальні правопорушення в кіберпросторі, були студентами технікумів або закладів вищої освіти, водночас більшість із них була студентами першого курсу. Тобто фактично можемо говорити, що вік 30 % осіб, які вчиняють кримінальні правопорушення, передбачені

розділом XVI Особливої частини Кримінального кодексу України, – від 15 до 18 років [382].

Відповідно до статті 99 Загальної частини Кримінального кодексу України штраф застосовується лише до неповнолітніх, які мають самостійний дохід, власні кошти або майно, на яке може бути звернене стягнення. Згідно з даними Міжнародної організації праці в Україні на 2020 рік працювало близько 600 тисяч дітей віком від 16 до 18 років, тобто 28 % з усіх дітей віком від 16 до 18 років [383].

Незважаючи на закріплення в Законі України «Про вищу освіту» норми щодо індивідуального плану навчання, більшість закладів вищої освіти не дозволяє його оформлювати як студентам перших та других курсів, так і студентам технікумів та коледжів [384].

Ураховуючи це, можемо зробити висновок про відсутність у неповнолітньої особи самостійного доходу, а отже, неможливість застосування штрафу як основного виду покарання за кримінальні правопорушення, передбачені розділом XVI Особливої частини Кримінального кодексу України. У 2020 році згідно зі статистикою Генеральної прокуратури України було обліковано 2 498 кримінальних правопорушень, передбачених розділом XVI Особливої частини Кримінального кодексу України, 1 675 особам вручено підозру, з яких 175 – неповнолітні. Також акцентуємо увагу, що 49 кримінальних правопорушень цього виду були скоєні особами до 16 років, тобто такими, які не підпадають під кримінальну відповідальність [385].

Підсумовуючи вищевикладене, хочемо наголосити, що, незважаючи на доволі розгалужену систему покарань, які призначаються судом за вчинення кримінальних правопорушень, передбачених розділом XVI Особливої частини Кримінального кодексу України, найбільш поширеними є позбавлення волі на певний строк та штраф. На нашу думку, з огляду на застосування судами норми статті 75 Загальної частини Кримінального

кодексу України (звільнення від покарання з випробуванням) повністю нівелюються самі засади призначення покарання. Особливості вчинення кримінальних правопорушень у кіберпросторі, зокрема сукупності різних суспільно небезпечних діянь, спрямованих на досягнення одного злочинного результату, не дозволяють застосувати штраф як основне покарання у більшості випадків, у яких це є нагальним та обумовленим. Визначення ступеня тяжкості вчиненого кримінального правопорушення й призначення справедливого та достатнього покарання за нього є певним каталізатором упровадження певних єдиних уніфікованих правил, якими б керувалися судді під час призначення покарання за зазначені суспільно небезпечні діяння.

3.3. Кримінально-правова характеристика обставин, що обтяжують покарання за кримінальні правопорушення в кіберпросторі

Характер і спрямованість політики держави в кримінальному праві багато в чому визначає таку специфіку діяльності суду, як призначення покарання. Саме від правильного, всебічного оцінювання вчиненого особою суспільно небезпечного діяння залежить призначення справедливої міри покарання, що сприяє встановленню соціальної справедливості, виправленню засудженого, попередженню нових кримінальних правопорушень і, зрештою, зміцненню авторитету й поваги до держави та суду [386].

У сучасному світі інформаційно-телекомунікаційні технології, системи й мережі є необхідною складовою життєдіяльності держави та суспільства. Зростання їх ролі призвело до збільшення кількості кримінальних правопорушень у кіберпросторі. Зважаючи на це, дослідження проблеми кримінально-правової характеристики обставин, що

обтяжують покарання за кримінальні правопорушення в кіберпросторі за вчинення цих суспільно небезпечних діянь, є надзвичайно актуальним.

Насамперед нагадаємо, що кримінальні правопорушення в кіберпросторі можуть бути різноманітними: від неправомірного втручання в роботу інформаційно-телекомунікаційних технологій, систем або мереж і до кібертероризму.

По-друге, для кваліфікації кримінальних правопорушень у кіберпросторі застосовується кримінальний закон, що містить відповідні норми, які передбачають певні види покарань, а також обставини, що обтяжують покарання за кримінальні правопорушення, передбачені статтею 67 Загальної частини Кримінального кодексу України [14].

Пропонуємо розглянути кожну з цих обставин у розрізі кримінальних правопорушень у кіберпросторі. Умовно їх можна поділити на дві групи.

Обставини, що обтяжують покарання, які суд за їх наявності у справі враховує під час призначення покарання

1. Вчинення кримінального правопорушення групою осіб за попередньою змовою. Незважаючи на те, в результаті аналізу судової практики щодо вчинення кримінальних правопорушень у кіберпросторі нами було визначено переважно одноосібне вчинення таких суспільно небезпечних діянь, якщо ми говоримо про вчинення складних кібератак або шахрайських схем з інвестуванням у віртуальні активи, то такі діяння не можуть вчинятися одноосібно з огляду на складність та специфіку.

Вчинення кримінальних правопорушень у кіберпросторі у співучасті здебільшого характеризується чітким розподілом ролей, переважно всі учасники кримінального правопорушення діють як співвиконавці. Найчастіше у співучасті вчиняються кримінальні правопорушення проти власності, про що свідчить статистика підозр Департаменту кіберполіції Національної поліції України [387; 388].

Варто наголосити, що на відміну від традиційних кримінальних правопорушень, за яких визначення співучасників є очевидним, суспільно небезпечні діяння в кіберпросторі характеризуються значною прихованістю. Особа, яка здійснює неправомірний доступ до інформаційно-телекомунікаційної технології за допомогою шкідливого програмного забезпечення, здебільшого навіть не є його розробником. Так само шкідливе програмне забезпечення може бути створене не однією особою, а декількома, зокрема коли кожний співучасник розробляє свою частину цифрового коду, що відповідає за здійснення одної функції шкідливого програмного забезпечення. Зазвичай у такому разі слідству вдається встановити лише особу виконавця, який безпосередньо здійснив несанкціоноване втручання, у той час як інші співучасники не понесуть кримінального переслідування. Зауважимо, що сфера кіберпростору дає змогу особам бути учасниками відразу декількох злочинних груп або вчиняти декілька кримінальних правопорушень у співучасті.

На нашу думку, для більш повного розуміння форми співучасті правоохоронним органам варто зосередити увагу на дослідженні й характеристиці таких елементів вчинення кримінального правопорушення:

– електронних слідів (виявлення проміжків часу, упродовж яких було здійснено певні дії, що могли вчинятися лише із залученням кількох осіб);

– зв’язків (дослідження соціальних мереж, електронної пошти, будь-яких інших повідомлень, що свідчать про взаємозв’язок між кількома підозрюваними особами);

– стилю дій злочинця. Аналіз стилю дій вчинення кримінального правопорушення в кіберпросторі дає змогу дізнатися, наприклад, скільки осіб було причетно до кримінального правопорушення, зазвичай кожна особа має індивідуальний підхід до написання коду або порядку вчинення окремих дій;

– фізичних доказів (у результаті аналізу аудіо-, відеозаписів, показання свідків можна виявити, вчинено злочин групою осіб чи за попередньою змовою).

2. Вчинення кримінального правопорушення щодо особи похилого віку, особи з інвалідністю або особи, яка перебуває в безпорадному стані, або особи, яка страждає на психічний розлад, зокрема недоумство, має вади розумового розвитку, а також вчинення кримінального правопорушення щодо малолітньої дитини або в присутності дитини.

Беручи до уваги зазначену норму Загальної частини Кримінального кодексу України, можна стверджувати, що досить часто кримінальні правопорушення в кіберпросторі вчиняються щодо осіб похилого віку, а саме:

– виманювання даних платіжних карток та інших банківських реквізитів із метою їх подальшого використання й викрадення з них коштів;

– застосування інструментів соціальної інженерії шляхом маніпуляції для вчинення певних дій, зазвичай переказування коштів зловмисникові тощо.

3. Вчинення кримінального правопорушення щодо жінки, яка завідомо для винного перебувала у стані вагітності.

Питання застосування цієї обставини, що обтяжує покарання за кримінальні правопорушення, в кіберпросторі навряд чи має своє застосування, оскільки характерними ознаками кіберзлочинності є анонімність і відсутність особистого контакту між злочинцем та потерпілим, тому довести, що правопорушник знав або міг знати, що він вчинив кримінальне правопорушення щодо жінки, яка завідомо для нього перебувала в стані вагітності, досить складно або зовсім неможливо.

4. Вчинення кримінального правопорушення з використанням малолітнього або особи, яка страждає психічним захворюванням чи недоумством.

Подібні злочини зазвичай вчиняються з використанням малолітнього, що одночасно може містити й ознаки втягнення його в злочинну діяльність, а щодо питання використання особи, яка страждає психічним захворюванням чи недоумством, то таких осіб використовують як «приманку», тобто використовують їх персональні дані або, можливо, їх фотографії, лікарські висновки тощо для подальшого використання в злочинній діяльності.

5. Вчинення злочину з особливою жорстокістю. Ця обставина не буде застосовуватися до кримінальних правопорушень у кіберпросторі, оскільки особлива жорстокість вчиненого злочину належить до так званих оцінкових ознак, наявність якої пов'язується насамперед із використанням певного способу вчинення злочину, за якого винний усвідомлює, що заподіює потерпілому особливі фізичні чи моральні страждання шляхом завдання великої кількості тілесних ушкоджень, знущань, катувань, мордувань, мучень із використанням, зокрема, вогню, електроструму, кислоти, лугу, болісподійної отрути, тривалого позбавлення їжі, води, тепла тощо.

Проте про особливу жорстокість злочину може свідчити не лише спосіб його вчинення, а й інші обставини справи, зокрема прагнення винного заподіяти особливі моральні страждання, водночас не лише самому потерпілому, а й близьким йому особам [389, с. 433].

6. Вчинення злочину загальнонебезпечним способом. Визнається обставиною, що обтяжує покарання, зважаючи на те, що такий спосіб вчинення злочину створює реальну небезпеку (загрозу) заподіяння шкоди (чи фактично її заподіює) не лише безпосередньо вибраному винним об'єкту посягання, а й іншим правоохоронюваним інтересам.

Кримінальні правопорушення в кіберпросторі, вчинювані загальнонебезпечним способом, можуть призвести до значної шкоди для громадської й національної безпеки, економіки та інших аспектів життя.

Прикладами зазначених кримінальних правопорушень є такі:

– розповсюдження вірусів, шкідливих програм, що можуть призвести до вимкнення важливих систем, таких як лікарня, банки, енергетичні компанії та інші критичні інфраструктурні об’єкти;

– цілеспрямовані атаки на критичну інфраструктуру, таку як електричні мережі, транспортні та інші системи, які є життєво важливими для функціонування суспільства. Це може призвести до масового вимкнення електроенергії, перебоїв у роботі транспорту та інших катастрофічних наслідків;

– кібертероризм, атаки на органи державної влади, військові та інші критичні інфраструктурні об’єкти з метою спричинити найбільше ураження країні й суспільству. Злам системи авіасполучення, яка контролює рух повітряних суден, що може призвести до серйозних наслідків і є дуже небезпечним для багатьох людей.

7. Вчинення злочину з використанням умов воєнного або надзвичайного стану, інших надзвичайних подій.

Містить три обставини, за яких винний свідомо (умисно) використовує для вчинення злочину особливу (надзвичайну) обстановку, що склалася в країні або її окремих регіонах: а) воєнний стан; б) надзвичайний стан; в) інші надзвичайні події [389, с. 454].

Ця обставина є неабияк актуальною в умовах сьогодення. Україна вже більше року перебуває в умовах воєнного стану, а саме: з 24 лютого 2022 року. Наразі відбуваються безліч зборів на допомогу Збройним силам України, Територіальній обороні та іншим підрозділам, задіяним в обороні країни, цивільним особам, які постраждали під час війни, військовим, що проходять реабілітацію після поранень тощо. І деякі особи вводять в оману людей, які хочу допомогти, та привласнюють собі кошти, цілеспрямовано зібрані на допомогу, що за своєю суттю є шахрайством із використанням мережі Інтернет.

Іншими кримінальними правопорушеннями, що вчиняються в умовах воєнного стану є:

– кібершпигунство, за якого злочинець використовує віруси, шкідливі програми або інші технічні засоби, щоб одержати доступ до конфіденційної інформації або державної таємниці. В умовах воєнного або надзвичайного стану такий злочин може бути особливо небезпечним, оскільки зловмисники можуть одержати важливу військову або дипломатичну інформацію та згодом використовувати її у військово-політичних цілях;

– кібертероризм, за якого злочинець використовує інформаційно-телекомунікаційні технології, системи й мережі для завдання шкоди цивільній, військовій інфраструктурі або іншим системам, що можуть бути важливими для безпеки країни та населення;

– кібератаки, застосовувані за допомогою інформаційно-телекомунікаційних технологій, систем і мереж для завдання шкоди комп'ютерним мережам, вебсайтам, інформаційним системам тощо. В умовах воєнного або надзвичайного стану такий злочин може бути особливо небезпечним, оскільки може призвести до тимчасового вимкнення Інтернету або важливих систем зв'язку та комунікації, що може спричинити значні проблеми для зв'язку військових підрозділів та органів управління;

– розповсюдження дезінформації або фейків шляхом використання соціальних мереж, медіа- та інтернет-ресурсів для поширення неправдивої інформації, що може підривати національну безпеку, єдність і спокій нації тощо. В умовах воєнного або надзвичайного стану такі види злочинів можуть бути особливо небезпечним, оскільки злочинці можуть використовувати дезінформацію, щоб спричинити паніку серед населення або змусити владу ухвалити некоректні рішення.

Обставини, що суд залежно від характеру вчиненого злочину вправі не визнати такими, що обтяжують покарання

1. Вчинення злочину особою повторно та рецидив злочинів. Ця обставина буде застосована, якщо особа, яка вчинила кримінальне правопорушення, вже вчиняла подібні кримінальні правопорушення в кіберпросторі або регулярно вчиняє такі правопорушення. Варто наголосити, що кіберпростір та вчинення суспільно небезпечних діянь у ньому пролонгують повторність такого вчинення. Наприклад, застосування вірусів або інших шкідливих програм на вебсайтах, вчинення DDoS-атак тощо.

2. Вчинення кримінального правопорушення на підґрунті расової, національної, релігійної ворожнечі чи розбрату або статевої належності. Ця обставина застосовується в разі виявлення таких ознак:

– кібербулінгу, або систематичного приниження, залякування людей через Інтернет на підставі їх раси, національності, релігії, гендерної належності або орієнтації [390];

– нелегального доступу до комп'ютерних систем, що може бути спрямованим на одержання конфіденційної інформації про людей, які належать до певної расової, національної, релігійної або іншої групи;

– розповсюдження вірусного програмного забезпечення, яке може застосовуватися для завдання шкоди на підставі расової, національної або релігійної належності;

– кібератак на вебсайти, які належать до певних расових, національних або релігійних груп, що може призвести до обмеження, внеможливлення доступу до цих сайтів або завдання іншої шкоди, наприклад у вигляді репутаційних наслідків;

– онлайн-шахрайства, в якому злочинці можуть вчиняти злочинні дії щодо людей на підставі їх расової, національної або релігійної належності, застосовуючи методи соціальної інженерії.

3. Вчинення кримінального правопорушення у зв’язку з виконанням потерпілим службового або громадського обов’язку. Прикладами застосування цієї обставини є виявлення таких ознак кримінальних правопорушень:

– порушення конфіденційності даних, за якого злочинці одержують доступ до інформації, зібраної у зв’язку з виконанням потерпілим службового або громадського обов’язку, шляхом використання шкідливих програм, підміни ідентифікатора або зламу пароля тощо;

– шантажу й вимагання викупу у вигляді грошових коштів або інших послуг в обмін на повернення контролю над службовими або громадськими системами потерпілого, що так само може призвести до негативних наслідків, зокрема призупинення функціонування установи або організації, порушення їх законної діяльності;

– розповсюдження шкідливих програм, вірусів для одержання доступу до систем, які належать установі або організації, в якій працює потерпілий, що спричинить порушення конфіденційності інформації та роботи системи;

– атак на вебсайти та інші ресурси, які можуть спричинити відмову їх обслуговування або навіть зниження рейтингу, що негативно вплине на роботу установи або організації;

– застосування фішингу для одержання конфіденційної інформації про потерпілого, зібраної в рамках його службових або громадських обов’язків, якщо особа стала «жертвою» фішингових листів або сайтів;

– викрадення та використання ідентифікаційних даних потерпілого для одержання доступу до систем, що належать установі або організації, в якій він працює.

4. Тяжкі наслідки, завдані злочином, як обставина, що обтяжує кримінальне покарання, належить до так званих оцінкових понять, зміст та обсяг якого залежать від особливостей конкретної справи, тому щоразу

встановлюються судом з урахуванням усіх обставин. У разі віднесення наслідків до тяжких варто враховувати важливість (соціальну цінність) тих суспільних відносин, яким злочином заподіюється шкода, а також ступінь заподіяння цієї шкоди, що залежить від характеру (змісту) і розміру (обсягу) спричинених наслідків.

До тяжких наслідків здебільшого належать загибель людей, заподіяння тяжкої шкоди здоров'ю людини, великий матеріальний збиток, порушення основних конституційних прав і свобод людини та громадянина, дезорганізація діяльності органів державної влади й місцевого самоврядування, перешкоджання роботі підприємств, установ та організацій тощо. Серед загальновідомих прикладів варто виділити такі:

– атаку «WannaCry». У 2017 році шкідлива програма «WannaCry» атакувала більше ніж 200 000 комп'ютерів приблизно в 100 країнах світу. Це призвело до призупинення роботи банків, компаній та установ, що використовували застарілі операційні системи без установлення необхідних оновлень. Потерпілі компанії зазнали великих збитків і впродовж тривалого часу відновлювали свої системи [391];

– атаку «Equifax». У 2017 році «Equifax» – одне з найбільших кредитних бюро в США – було атаковане хакерами, що спричинило крадіжку більше ніж 140 мільйонів ідентифікаційних даних клієнтів, зокрема соціальних страхових номерів, дат народження та іншої конфіденційної інформації. Ця атака призвела до втрати довіри клієнтів і порушення вимог до захисту конфіденційної інформації [392];

– атаку на «Sony Pictures». У 2014 році хакери, яких пов'язують із КНДР, атакували «Sony Pictures» і зламали їх систему, що спричинило крадіжку більше ніж 100 терабайт конфіденційної інформації, зокрема електронних листів, фільмів та іншої приватної інформації. Ця атака зумовила міжнародний скандал і вплинула на відносини між США та КНДР [393];

– атаки на інфраструктуру України. У 2015–2017 роках і за час повномасштабного вторгнення Росії в Україну російські хакери атакували українську енергетичну, транспортну та інші інфраструктури, що призвело до вимкнення електроенергії й збоїв у транспорті. Унаслідок цих атак тисячі людей залишилися без світла й газу на тривалий час, що істотно ускладнило їх повсякденне життя [394], [395], [396];

– атаки на установи охорони здоров'я під час пандемії COVID – 19. У 2020 році хакери проводили кібератаки на лікарні та інші установи охорони здоров'я, щоб одержати доступ до медичної інформації про пацієнтів та вимагати викуп. Ці атаки погіршили стан пандемії й завдали шкоди лікарням, що вже працювали в напруженому режимі [397; 398];

– атаки на мережу «Twitter». Хакери зламали систему безпеки соціальної мережі «Twitter», використовуючи здобуті дані для зміни повідомлень відомих користувачів, таких як Ілон Маск, Джо Байден, Джеф Безос тощо, закликаючи до відправки криптовалюти в шахрайський електронний гаманець. Ця атака призвела до викрадення електронних адрес понад 200 млн користувачів цієї мережі, втрати великої кількості коштів та порушення довіри до неї [399], [400].

5. Вчинення кримінального правопорушення щодо подружжя чи колишнього подружжя або іншої особи, з якою винний перебуває (перебував) у сімейних або близьких відносинах. Ця обставина щодо кримінальних правопорушень у кіберпросторі малозастосовна, проте в теорії є цілком можливою, наприклад, якщо один із подружжя або колишнього подружжя знав певні конфіденційні дані. Зокрема, маючи паролі від онлайн-банкінгу, один із членів подружжя може вчинити крадіжку грошових коштів іншого. Маючи паролі від соціальних мереж, можна одержати особисту переписку члена подружжя, тим самим порушуючи право на приватність. Ще частіше можуть бути використані

фотографії інтимного характеру одного з членів колишнього подружжя з подальшим вимаганням грошових коштів за її неоприлюднення.

6. Вчинення кримінального правопорушення щодо особи, яка перебуває в матеріальній, службовій чи іншій залежності від винного. Ця обставина є такою, що обтяжує покарання, тому що, з одного боку, винний використовує залежне від нього становище потерпілого для вчинення щодо нього злочину, а з іншого – потерпілий через таку залежність від винного повністю позбавлений або істотно обмежений у можливості уникнути посягання чи чинити йому ефективний опір. Прикладами подібних правопорушень можуть бути:

– шантаж у кіберпросторі, тобто вимагання коштів, послуг або інформації від особи, яка перебуває в службовій залежності;

– вимагання або викрадення ідентифікаційних або інших персональних даних із метою їх подальшого використання в злочинних діяннях;

– відслідковування й постійний контроль особи за допомогою програмного забезпечення віддаленого доступу до комп'ютера чи мобільного телефона особи, яка перебуває в залежності, що порушує недоторканність приватного життя особи;

– «кібернасильство», що полягає в завданні шкоди за допомогою електронних форм спілкування й контакту, та може виражатися в поширенні неправдивої інформації, чуток, пліток, образ, погроз щодо особи, залякуванні з метою контролювання її дій та поведінки або без такої.

7. Вчинення кримінального правопорушення особою, яка перебуває в стані алкогольного сп'яніння або стані, спричиненому вживанням наркотичних або інших одурманюючих засобів, припускає, що під час нього винний перебував у певному фізіологічному стані, викликаному дією на його організм речовин, зазначених у пункті 13 частини 1 статті 67

Загальної частини Кримінального кодексу України, що певною мірою спровокувало вчинення ним суспільно небезпечного діяння [14].

Водночас оцінювання обставини, передбаченої в пункті 13 частини 1 статті 67 Загальної частини Кримінального кодексу України як такої, що обтяжує покарання, можливе лише за умови, що вживання зазначених засобів:

а) призвело до особливого фізіологічного, а не патологічного стану організму винного, тому що інакше особа може бути визнана неосудною;

б) було добровільним, тому що насильницьке введення в організм особи таких засобів (речовин) або доведення її до стану одурманення шляхом обману не може визнаватися обставиною, що обтяжує покарання.

Проте об’єктивне обґрунтування такої обставини дасть змогу дійти висновку, що вчинення кримінального правопорушення в кіберпросторі в стані алкогольного або наркотичного сп’яніння є малоймовірним, оскільки зазвичай такі дії потребують пильної уважності, високого рівня використання технічних засобів і технологічних інструментів.

Водночас варто зауважити, що доведення вчинення кримінального правопорушення в кіберпросторі в стані алкогольного або наркотичного сп’яніння є майже неможливим, крім випадків, коли наявні прямі докази цього.

Одним із ключових завдань у боротьбі з кіберзлочинністю є підвищення ефективності правового регулювання в цій сфері. Для цього необхідно не лише змінити законодавство з урахуванням специфіки кіберпростору, а й забезпечити його ефективне застосування. Важливим питанням, що стоїть перед правоохоронними органами та законодавцями, є запровадження нових обставин, які обтяжують покарання за вчинення кримінальних правопорушень у кіберпросторі.

Питання кібербезпеки є одним із найбільш актуальних у сучасному світі. В умовах усе більшого застосування інформаційних технологій і

зростання кількості кібератак у різних сферах життєдіяльності захист інформації й комп'ютерних систем стає надзвичайно важливим завданням для будь-якої держави. Тому необхідно розглянути питання державної інформації та державних комп'ютерів.

Державні комп'ютери відіграють надзвичайно важливу роль у забезпеченні кібербезпеки держави. Вони забезпечують захист державних інформаційних ресурсів від зламів і вірусів, а також контролюють доступ до державної таємниці й конфіденційної інформації. Крім того, державні комп'ютери використовують для виявлення та блокування кібератак на державні інформаційні системи. Також державні комп'ютери дають змогу проводити ретельну моніторингову роботу в кіберпросторі, що допомагає у виявленні нових загроз і швидкому реагуванні на них.

Інформація, що становить державну таємницю, також є важливою складовою забезпечення кібербезпеки держави. Державна таємниця охоплює інформацію, що стосується національної безпеки, оборони, зовнішньої політики, економічних інтересів та інших сфер, які не підлягають розголошенню.

Однією з основних причин захисту державної таємниці є запобігання витоку конфіденційної інформації, що може призвести до порушення національних інтересів та збільшення ризику кібератак на державні системи та інфраструктуру.

Для захисту державної таємниці від кіберзагроз держава проводить різноманітні технічні й організаційні заходи. Зокрема, державні органи встановлюють системи доступу до державної таємниці, шифрують дані, використовують захист від вірусів та інших загроз. Крім того, вони проводять аудит інформаційної безпеки й надають відповідні рекомендації з метою покращання захисту такої інформації.

Проте зберігання державної таємниці також може стати об'єктом кіберзагроз, тим паче враховуючи, що зараз Україна перебуває в умовах

війни, що збільшує можливі ризики таких загроз. Тому варто розглянути питання кримінальних правопорушень із використанням державної таємниці та державного комп'ютера в кіберпросторі, що може впливати на кримінальну відповідальність осіб, які зловживають цими ресурсами.

Тобто виникає необхідність у виділенні додаткової обставини в Кримінальному кодексі України, що обтяжує покарання. Кримінальні правопорушення в кіберпросторі, що можуть бути вчинені з використанням державного комп'ютера або державної таємниці, можуть бути різноманітними й залежать від того, як саме їх використовують. Ось декілька прикладів таких злочинів:

– використання державного комп'ютера або державної таємниці для здійснення кібератаки на іншу систему або викрадення конфіденційної інформації;

– використання державної таємниці або державного комп'ютера з метою особистої вигоди. Наприклад, якщо особа використовує державний комп'ютер для здійснення фінансового шахрайства або одержання незаконного доступу до захищеної інформації;

– використання державної таємниці або державного комп'ютера для підготовки або здійснення терористичного акту. Наприклад, якщо особа використовує державний комп'ютер для планування теракту або поширення матеріалів, що сприяють тероризму, розповсюдженню будь-якої пропаганди, яка становить загрозу національній безпеці;

– використання державної інформації або державного комп'ютера з метою впливу на результати виборів. Наприклад, якщо особа використовує державний комп'ютер для підготовки фальшивих голосів або поширення дезінформації з метою впливу на виборчий процес;

– розповсюдження шкідливого програмного забезпечення або вірусів через державну інформаційну систему. Наприклад, зловмисник може використати державний комп'ютер для створення й розповсюдження

шкідливого програмного забезпечення, що може спричинити збій комп'ютерних систем і втрату інформації, яка в них зберігається;

– незаконний доступ до комп'ютерних систем державних органів або баз даних, що містять конфіденційну інформацію. Наприклад, під час такого злочину зловмисник може зламати паролі, використовуючи державний комп'ютер, одержати доступ до персональних даних громадян, фінансових даних та іншої важливої інформації;

– спам або фішинг – використання державної інформаційної системи, для масового розсилання спаму, фішингу та інших видів небажаних повідомлень, які містять шкідливі посилання, що може стати причиною витоку інформації;

– кримінальні правопорушення, пов'язані з електронними фінансовими операціями, що вчиняються з використанням державної таємниці. Наприклад, зловмисник може використати державну інформацію для крадіжки фінансових даних, підробки фінансових документів, відкриття фіктивних рахунків тощо.

Зазначені приклади показують, що використання державної таємниці та державних комп'ютерів може бути дуже небезпечним і стати причиною вчинення різних кіберзлочинів. Тому в разі виявлення порушень, пов'язаних із використанням державної інформації, необхідно вживати відповідних заходів для запобігання подібним випадкам у майбутньому.

Особи, які використовують державні ресурси для вчинення кримінальних правопорушень у кіберпросторі, повинні нести за це належну відповідальність, а враховуючи питання вразливості державної інформаційної безпеки, ризиків підкупу державних службовців або інших осіб, які мають доступ до державних комп'ютерів та державної таємниці, вважаємо необхідним доповнити частину 1 статті 67 Кримінального кодексу України пунктом 14: «вчинення кримінального правопорушення

особою з використанням державного комп'ютера та/або державної таємниці».

У світі, де кібератаки стають все більшими й складнішими, захист інформації та комп'ютерних систем є надзвичайно важливим завданням для будь-якої держави. Тому державна таємниця й державні ресурси є пріорітетними елементами в забезпеченні кібербезпеки держави та захисті її інформаційних ресурсів. Вони допомагають виявляти й аналізувати нові загрози, захищати державні інформаційні системи від кібератак і контролювати доступ до державної таємниці.

Використання державної таємниці та державного комп'ютера для злочинних цілей може мати серйозні наслідки для особи, яка зловживає цими ресурсами. Такі обставини повинні бути використані як додаткові під час розгляду кримінальної справи й привести до підвищення рівня кримінальної відповідальності за такий злочин.

Підбиваючи підсумки вищевикладеного, хочемо зазначити, що обставини, які обтяжують кримінальне покарання в разі їх реалізації в розрізі кіберпростору, мають свою специфічну та нетрадиційну характеристики. Не всі обставини, явизначені в частині 1 статті 67 Загальної частини Кримінального кодексу України, можуть буду застосовані до суспільно небезпечних діянь, що вчиняються в кіберпросторі. Серед основних обставин, що обтяжують кримінальне покарання, ми виділили такі: 1) вчинення кримінального правопорушення групою осіб за попередньою змовою; 2) вчинення злочину з використанням умов воєнного або надзвичайного стану, інших надзвичайних подій; 3) вчинення кримінального правопорушення щодо особи похилого віку, особи з інвалідністю або особи, яка перебуває в безпорадному стані, або особи, яка страждає на психічний розлад, зокрема недоумство, має вади розумового розвитку, а також вчинення кримінального правопорушення щодо малолітньої дитини або в присутності дитини. Водночас, на нашу думку,

необхідно доповнити систему обставин, 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 вчинення кримінального правопорушення є цифрова інформація, яка має ознаки державної таємниці.

РОЗДІЛ 4.
МІЖНАРОДНО-ПРАВОВІ ЗАХОДИ ТА ЗАРУБІЖНИЙ ДОСВІД КРИМІНАЛЬНО-ПРАВОВОЇ ОХОРОНИ КІБЕРПРОСТОРУ

4.1. Теоретико-правові аспекти застосування норм і принципів міжнародного права до регулювання відносин у кіберпросторі в Україні

Сьогодні життєдіяльність нашого суспільства неосяжними кроками переноситься в кібернетичний простір, водночас кіберзагрози стали цілком реальними й архінебезпечними не лише для окремих громадян, держав та корпорацій, а й для системи нормального функціонування міжнародних відносин. Хочемо наголосити, що розвиток і вдосконалення системи міжнародного публічного права потребують урахування стану розвитку інформаційно-телекомунікаційних технологій з одночасним адаптуванням міжнародно-правового регулювання до сучасного інформаційно-комунікаційного середовища. Не можна не погодитися з думкою С. Задорожної, яка наголошує, що відносини, які склалися в кіберпросторі, можуть бути складовою частиною міжнародних відносин. У такому разі на відносини в кіберпросторі поширюються норми міжнародного права [401, с. 51].

Принципи міжнародного права – це історично обумовлені основоположні загальновизнані норми, що мають вищу юридичну силу, виражають головний зміст міжнародного права, є правовою основною всіх міжнародних договорів, виражають їх характерні риси та володіють вищою імперативною юридичною силою [402].

Основні принципи міжнародного права закріплені відразу в декількох документах, зокрема мова йде про: 1) Статут Організації Об’єднаних Націй

[403]; 2) Підсумковий акт Організації з безпеки і співробітництва в Європі [404]; 3) Декларацію про міжнародні принципи відповідно до Статуту Організації Об'єднаних Націй [405].

Варто наголосити, що принципи, закріплені в зазначених документах, деяким чином збігаються, але водночас мають різну змістовність. На нашу думку, Підсумковий акт Організації з безпеки і співробітництва в Європі містить найбільш розширений перелік принципів міжнародного права. Зважаючи на це, аналіз принципів міжнародного права щодо діяльності в кіберпросторі ми будемо робити відповідно до нього.

Основними принципами регулювання міжнародних відносин у рамках кіберпростору, на нашу думку, є такі: 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 й основних свобод, зокрема свободи совісті, релігії та переконань; 8) принцип невтручання у внутрішні справи; 9) принцип непорушності кордонів.

Пропонуємо розглянути зазначені принципи в розрізі їх реалізації в кібернетичному просторі [406].

Принцип суверенної рівності держав є основоположним принципом міжнародних відносин загалом і відносин у кіберпросторі зокрема. Основна суть цього принципу полягає в повазі до суверенітету держав та правової рівноправності в міжнародних відносинах. Принцип суверенної рівності проголошено в пункті 1 статті 2 Статуту ООН: «Організацію засновано на принципі суверенної рівності всіх її членів» [407; 403].

Характеризуючи принцип суверенної рівності держав у рамках кіберпростору, варто наголосити, що є дві концепції державного кібернетичного суверенітету.

Відповідно до першої концепції кібернетичний простір є централізованим та фактично регулюється відповідно до комплексного підходу всіма країнами – членами світового товариства, а не кожною країною окремо. З огляду на цю концепцію роль окремої держави щодо регулювання відносин у кіберпросторі фактично нівелюється. Ми є прихильниками такої концепції, але, на нашу думку, сьогодні фактично немає міжнародної нормативної бази щодо регулювання відносин у кіберпросторі. Водночас локальна політика держав щодо спроб регулювання таких відносин здебільшого обмежується лише регулюванням відносин, пов'язаних із кібербезпекою та правопорушеннями в цій сфері. На нашу думку, створення єдиної уніфікованої нормативної бази щодо міжнародного регулювання питань, пов'язаних із кібернетичним простором, із подальшою імплементацією в законодавства держав-ратифікантів повинно стати пріоритетним завданням міжнародної спільноти цього десятиліття [408].

Відповідно до другої концепції кібернетичний простір має певний імунітет від державного суверенітету. Як уже було зазначено, ми є прихильниками контролю за відносинами в кіберпросторі. Саме з огляду на це вважаємо, що кіберпростір не може мати імунітету від державного суверенітету й поширення на нього державної влади. Д. Голдшміт у своїй праці «Хто контролює Інтернет» зазначив, що: 1) кіберпростір потребує державного контролю, незважаючи на належність суб'єкта в кіберпросторі, його діяльність повинна регулюватися відповідно до законодавства держави, в якій така діяльність здійснюється; 2) відносини фінансового характеру, які складаються в кіберпросторі, потребують державного регулювання, в іншому разі учасники таких відносин будуть юридично незахищеними; 3) цифрова інформація, що існує в кіберпросторі й має нематеріальний характер, прямо впливає на відносини, суб'єкти та об'єкти,

які складаються в матеріальному світі; 4) захист національної безпеки держави від кіберзагроз [409].

Ураховуючи неможливість використання зброї в кіберпросторі в її класичному розумінні, принцип незастосування сили або погрози силою набуває свого специфічного втілення. Передусім мова йде про кібератаки та погрози їх вчинення. Незважаючи на відсутність матеріальної складової під час кібератак, наслідки від них є цілком матеріальними, завдані збитки сягають мільярдів доларів. Ураховуючи той факт, що наразі системи управління об'єктами життєзабезпечення, банківської сфери, енергетики, водопостачання в розвинених країнах світу керуються й багато в чому залежать від інформаційно-телекомунікаційних технологій, систем і мереж, кібератаки на такі об'єкти є прямим застосуванням сили в її фізичному розумінні.

Сьогодні Російська Федерація здійснює багато кібератак на сектор національної оборони нашої держави, урядовий і фінансовий сектори. Крім того, не можемо не звернути увагу на кібератаки з боку Російської Федерації на пострадянські країни, зокрема Литву, Латвію, Молдову, Естонію [410; 411].

Хочемо зауважити, 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 невілює можливості міжнародно-правового захисту держав від вчинення кібератак із боку інших держав або окремих осіб за сприяння конкретних держав.

Отже, можемо стверджувати, 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 [412].

Інший принцип, що ми хочемо охарактеризувати в розрізі кіберпростору, – принцип співробітництва держав. Оскільки більшість питань, пов'язаних із діяльністю в кіберпросторі, є неврегульованою, принцип співробітництва держав набуває основоположного значення. Ми переконані, що лише шляхом співробітництва держав і міжнародних організацій на міжнародній арені у сфері регулювання кіберпростору можна досягти певних успіхів та вирішити зазначену проблему.

На нашу думку, основної реалізації цей принцип набув у 2001 році, коли результатом співробітництва держав стало підписання Будапештської Конвенції «Про кіберзлочинність». Уже в 2003 році було підписано Додатковий протокол до Конвенції «Про кіберзлочинність». Крім того, під час 42-го саміту «Великої Сімки» 26 травня в підсумковій Декларації держави-учасниці визнали кіберпростір відкритим, доступним, надійним, взаємозв'язаним і безпечним середовищем та основою економічного процвітання й зростання [413].

Незважаючи на співробітництво держав у рамках регулювання відносин, що виникають у кіберпросторі, та ухвалення декількох міжнародних нормативних актів, жодний із зазначених документів повністю не врегульовує питання ані кіберпростору, ані кібербезпеки. Зазначені міжнародні нормативні акти здебільшого зосереджують увагу саме на формах вчинення суспільно небезпечних діянь у кіберпросторі. Ми вважаємо, що сьогодні виникає нагальна потреба в уніфікованому міжнародному нормативному акті, у якому визначалися б поняття «кримінальне правопорушення в кіберпросторі», «кіберпростір», «кібертероризм», «кіберзагроза», «кібератака», «кіберзброя». Водночас у такому акті повинно бути врегульоване питання щодо притягнення до

відповідальності за кібератаки, превентивні кібератаки й кібератаки у відповідь.

Реалізація принципу невтручання у внутрішні справи держави в розрізі кіберпростору вбачається через заборону втручання однієї держави в інформаційну складову іншої. На нашу думку, цей принцип тісно пов'язаний із принципом суверенної рівності держав як предикатного порушення інформаційної діяльності держави. У наш час зазначений принцип міжнародного права в контексті регулювання кіберпростору виражається в здійсненні ворожої пропаганди [414].

Під ворожою пропагандою в кіберпросторі варто розуміти використання будь-якої цифрової інформації, що є неправдивою, зміненою, перекрученою, з метою вплинути на суспільну думку населення іншої держави, тим самим схилити на бік ворога.

Ми вважаємо, що основним завданням кіберпростору є комунікаційна складова в різних її проявах. Тобто можемо стверджувати, що процес порушення комунікації між суб'єктами однієї чи декількох держав між собою буде прямим втручання. Це може проявлятися в перехопленні конфіденційної інформації шляхом розміщення серверу передавання такої цифрової інформації на території країни, що її перехоплює.

У контексті принципу мирного врегулювання спорів пропонуємо звернути увагу на Стратегію міжнародного співробітництва в кіберпросторі, розроблену Міністерством закордонних справ Китаю спільно з Адміністрацією кіберпростору Китаю. Відповідно до зазначеної стратегії міжнародне співтовариство повинно дотримуватися цілей і принципів, закріпленних у Статуті Організації Об'єднаних Націй, зокрема незастосування сили й мирного врегулювання спорів для забезпечення миру та безпеки в рамках кіберпростору. Також у Стратегії закріплено, що всі держави повинні протидіяти агресії й запобігати її нарощуванню в

кіберпросторі, а всі конфліктні питання врегульовувати мирним шляхом [415].

Фактично, не маючи жодної юридичної сили, сьогодні ця Стратегія є єдиним проявом визнання державами необхідності в мирному вирішенні конфліктів, що виникають у кіберпросторі.

Архіважливе значення для регулювання відносин у кіберпросторі має принцип рівноправ'я та право народів розпоряджатися своєю долею. Будь-які дії, що мають характер пропаганди й спрямовані на викривлення реальних фактів та впливають на самовизначеність окремої спільноти, є неправомірними. Відповідно ніхто не може неправомірно втручатися в інформаційно-телекомунікаційні технології, системи й мережі чи здійснювати пропаганду з метою порушення цього принципу.

Базуючись на тому, що принцип непорушності кордонів та територіальної цілісності держав нерозривно пов'язаний із матеріальною складовою, застосувати його до відносин у кібепросторі неможливо. На нашу думку, цей принцип тісно пов'язаний із принципом суверенітету держави й до нього можна застосувати відносини в кіберпросторі, які виникли з приводу діяльності інформаційних систем, що контролюються органами іншої держави.

Останній принцип, що ми хочемо охарактеризувати, – принцип поважання прав людини й основних свобод, зокрема свободи совісті, релігії та переконань. На нашу думку, головною особливістю цього принципу є те, що він повинен застосовуватися незалежно від того, де виникають відносини: у реальному (матеріальному) світі чи кіберпросторі. Відповідно до статті 12 Загальної декларації прав людини ніхто не може зазнавати безпідставного втручання в його особисте й сімейне життя, безпідставного посягання на недоторканність його житла, таємницю його кореспонденції або його честь і репутацію. Кожна людина має право на захист закону від такого втручання або таких посягань [416].

Сьогодні шляхом використання інформаційно-телекомунікаційних технологій зловмисники можуть одержати доступ до будь-яких персональних даних особи у вигляді цифрової інформації, збереженої та оброблюваної в інформаційно-телекомунікаційних технологіях, системах і мережах, порушуючи зазначений принцип. Водночас у ситуації, за якої правопорушення спрямоване на державу як суб'єкта міжнародного права порушуються права всіх її громадян та інших осіб, цифрова інформація яких стала об'єктом витоку.

Варто констатувати факт, що неврегульованість цього питання на міжнародному рівні спричиняє невпевненість громадян у захищеності цифрової інформації від стороннього втручання.

Розглянувши загальні принципи міжнародного права щодо регулювання відносин у кіберпросторі, закріплені в міжнародних нормативних актах, можемо зробити висновок, що більшість із них мають пряме застосування до відносин у кіберпросторі. Проте, враховуючи специфіку кіберпростору, доцільним є розроблення системи спеціальних принципів міжнародного права, які будуть застосовуватися винятково до відносин, що виникли в кіберпросторі.

А. Василенко виділяє такі спеціальні міжнародно-правові принципи використання кіберпростору: 1) принцип автономності й незалежності кіберпростору; 2) принцип визнання відсутності кордонів кіберпростору; 3) принцип невтручання в державний сектор кіберпростору; 4) принцип співвідношення міжнародного та державного регулювання кіберпростору; 5) принцип нейтралітету кіберпростору й запобігання міжнародним конфліктам у ньому; 6) принцип пропорційності необхідної самооборони в конфліктах, що виникають у кіберпросторі; 7) принцип відповідальності держав за порушення вимог щодо заборони ведення злочинної пропаганди; 8) принцип створення глобальної системи міжнародної кібербезпеки; 9) принцип обміну інформацією про кіберзагрози; 10) принцип координації

між державами в кіберпросторі; 11) принцип заборони торгівлі інформацією про приватних осіб; 12) принцип захисту права на доступ до інтернет-мережі [417].

Проаналізувавши загальні й спеціальні міжнародно правові принципи використання кіберпростору, хочемо проаналізувати основні міжнародні нормативні акти, що визначають правове регулювання кримінальних правопорушень у ньому.

Історично першим нормативним актом, присвяченим питанням регулювання кримінальних правопорушень у кіберпросторі, була Рекомендація № R89 (9) Комітету Міністрів країн – членів Ради Європи «Про злочини, пов'язані з комп'ютерами» від 13 вересня 1989 року [418].

Відповідно до цього документа державам – членам Ради Європи під час розроблення національного законодавства щодо встановлення кримінальної відповідальності за діяння, що вчиняються в кіберпросторі, необхідно було взяти до уваги Звіт Європейського комітету про проблеми злочинності в разі використання комп'ютерної техніки. У розрізі цього Звіту Комітет із проблем злочинності оцінив таке явище, як комп'ютерна злочинність. Водночас він надав керівні вказівки й рекомендації для криміналізації суспільно небезпечних, протиправних діянь у законодавстві країн-учасниць [419].

Ухвалення зазначеної рекомендації стало першим етапом в уніфікації боротьби з кримінальними правопорушеннями, що вчиняються з використанням комп'ютерної техніки на міжнародному рівні.

Відповідно до Звіту «Про кримінальні правопорушення з використанням комп'ютерної техніки» всі кримінальні правопорушення цього типу були поділені на дві групи: 1) мінімально необхідні до імплементації в національне законодавство країн-учасниць; 2) додаткові.

До мінімально необхідних кримінальних правопорушень у кіберпросторі, що необхідно імплементувати в національні законодавства країн-учасниць належать наведені далі.

1. Комп'ютерне шахрайство, яке визначається як уведення, зміна або видалення даних чи програм комп'ютера або інше втручання в процеси оброблення даних, що впливає на його підсумки, завдає економічних збитків або призводить до знищення власності іншої особи та чиниться з метою отримання незаконним шляхом економічної вигоди для себе чи іншої особи [420, с. 66].

2. Комп'ютерний саботаж: уведення, зміна або видалення даних чи програм комп'ютера або створення перешкод комп'ютерним системам із метою перешкоджання роботі комп'ютера чи телекомунікаційної системи.

3. Завдання шкоди комп'ютерним даним або програмам, тобто незаконне видалення, заподіяння шкоди або погіршення якості даних чи програм комп'ютера [421, с. 55].

4. Несанкціонований доступ, що являє собою неправомірний доступ до системи чи комп'ютерної мережі шляхом порушення заходів охорони.

5. Несанкціоноване перехоплення, тобто неправомірне та здійснене із застосуванням технічних засобів перехоплення повідомлень, спрямованих у систему або мережу комп'ютерів, що виходять із системи або мережі комп'ютерів і переданих у межах системи чи мережі комп'ютерів [422].

6. Несанкціоноване відтворення комп'ютерної програми, охоронюваної авторським правом. Під ним розуміється досконале неправомірне поширення, відтворення або передавання в громадське користування комп'ютерної програми, що охороняється законом [423, с. 17].

7. Комп'ютерна фальсифікація, тобто введення, зміна або видалення даних (програм) комп'ютера або інше втручання в процес оброблення даних, вчинене способом або за умов, установлених нормами

національного законодавства, якими ці дії кваліфікуються як фальсифікації, і скоєні щодо традиційного об’єкта правопорушення [424].

8. Несанкціоноване відтворення мікросхеми, тобто досконале неправомірне відтворення мікросхеми виробу на напівпровідниках, якщо вона охороняється законом, або неправомірне використання чи імпорт у комерційних цілях мікросхеми або виготовленого із застосуванням виробу на напівпровідниках.

Так само додатковий перелік кримінальних правопорушень відповідно до Звіту «Про кримінальні правопорушення за використання комп’ютерної техніки» охоплює такі склади кримінально протиправних діянь: 1) неправомірну зміну даних або програм на комп’ютері; 2) комп’ютерне шпигунство; 3) несанкціоноване використання комп’ютера; 4) несанкціоноване використання комп’ютерної програми.

Д. Говіл на основі ознак, наданих у Рекомендації, визначив комп’ютерне шпигунство як одержання незаконними способами, розкриття, передавання або використання торгової чи комерційної таємниці особою, яка не має на це права, з метою заподіяння економічної шкоди особі, яка має доступ до цієї таємниці, або отримання незаконної економічної вигоди для себе чи третьої особи [425].

Несанкціоноване використання комп’ютерної програми – це незаконні та неправомірні дії щодо використання комп’ютерної програми, що охороняється законодавством, вчинені з метою отримання незаконного прибутку для зловмисника чи третіх осіб або заподіяння правовласникові шкоди [426].

А. Паткі визначив ознаки несанкціонованого використання комп’ютера та що саме можна класифікувати до таких дій, зокрема: 1) особою, яка має право доступу до використання комп’ютера, з усвідомленням нею, що такі дії можуть завдати шкоди комп’ютерній системі або значно вплинути на процес її функціонування; 2) будь-якою

особою з метою заподіяти шкоду правомірному користувачеві комп'ютерної системи; 3) будь-якою особою з фактичним заподіянням шкоди комп'ютерній системі загалом [427].

Варто зауважити, що Рада Європи розробила низку інструментів для гармонізації законодавства у сфері кримінальних правопорушень у кіберпросторі, і, попри те, що такі Рекомендації не були обов'язковими, їх положення можна грамотно використати в чинному кримінальному законі. На нашу думку, незважаючи на те, що зазначені Рекомендації були ухвалені більше ніж 30 років тому, вони містять той спектр кримінальних правопорушень у кіберпросторі, що сьогодні мають дуже високий ступінь суспільної небезпеки. Зокрема, мова йде про такі кримінальні правопорушення, як фальсифікація цифрових даних і цифрове шпигунство. Водночас, на нашу думку, більшість кримінальних правопорушень, визначених Рекомендацією, переважно дублюються, адже мають одне й те саме змістове значення.

Іншим історичним документом, зміст якого наголошував на спрямуванні зусиль міжнародної спільноти на злагодженість роботи зі створення безпечного й вільного від злочинності кіберпростору, була Окінавська хартія. Вона визначала необхідність закріплення в рамках міжнародного права принципів безпеки інформаційно-телекомунікаційних технологій у боротьбі з кримінальними правопорушеннями в кіберпросторі [428].

Необхідність криміналізації суспільно небезпечних діянь, вчинених у кіберпросторі, також є одним із пунктів Рамкового рішення Ради Європейського Союзу «Про боротьбу з шахрайством і підробкою безготівкових платіжних засобів», відповідно до якого кожна держава-учасниця повинна вжити всіх можливих заходів, щоб кримінальним правопорушенням визнавалися умисні дії особи, спрямовані на завдання збитків володільцеві майна шляхом неправомірного введення, видалення,

модифікації цифрової інформації або несанкціонованого втручання у функціонування цифрового пристрою чи програмного забезпечення [429].

Основоположним документом у досліджуваній сфері, на нашу думку, є Конвенція Ради Європи «Про кіберзлочинність». Вона містить норми матеріального кримінального права, що регламентують кримінальні правопорушення, пов'язані з використанням інформаційно-телекомунікаційних технологій, систем та мереж. Відповідно до Конвенції держави-учасниці повинні імплементувати норми у вітчизняні законодавства й гармонізувати їх [430].

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

Україна ратифікувала Конвенцію «Про кіберзлочинність» 7 вересня 2005 року, а вже 1 липня вона набрала чинності.

Конвенція містить перелік основних видів комп'ютерних правопорушень, що розкриває їх дефініції, та встановлює заходи відповідальності за їх вчинення, які варто внести до національного законодавства [431, с. 95].

Закріплені в Конвенції склади поділені на чотири групи відповідно до об'єкта посягання: 1) правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем; 2) правопорушення, пов'язані з комп'ютерами; 3) правопорушення, пов'язані зі змістом; 4) правопорушення, пов'язані з порушенням авторських та суміжних прав [18].

Відповідно кожна із закріплених у Конвенції груп містить у собі певні ознаки кримінальних правопорушень, що необхідно закріпити в національних законодавствах країн-учасниць.

Зокрема, до кримінальних правопорушень проти конфіденційності, цілісності та доступності комп'ютерних даних і систем відповідно до Конвенції належать такі суспільно небезпечні діяння: 1) незаконний доступ, тобто навмисний, без права на нього доступ до інформаційно-телекомунікаційних технологій, систем або мереж, з'єднаних з іншим комп'ютером, що порушує заходи безпеки й вчинений із метою заволодіти цифровими даними чи іншим злим наміром; 2) нелегальне перехоплення, під яким розуміється здійснене з використанням цифрових технічних засобів та навмисно, без права на нього перехоплення даних, що передаються в інформаційно-телекомунікаційну систему або з неї, або всередині такої системи, або цифрових даних, якщо вони не призначені для загального користування.

Предмет аналізованого кримінального правопорушення може охоплювати весь спектр інформаційно-телекомунікаційних технологій, систем та мереж. Водночас варто зауважити, що відповідно до Конвенції за зазначене діяння особа буде нести кримінальну відповідальність, лише якщо воно скоєне щодо комп'ютерної системи, з'єднаної з іншою комп'ютерною системою або буде встановлено злий намір [432].

Діяння у формі втручання в дані являє собою псування цифрових даних різними способами, вчинене умисно й без права на нього. Г. Родерік визначає, що саме можна вважати псуванням цифрових даних. На його думку, це зміна, пошкодження, видалення, блокування, погіршення цифрових даних, збережених в інформаційно-телекомунікаційній системі [433, с. 418].

Ще одним протиправним діянням є втручання у функціонування системи, тобто створення серйозних перешкод роботі інформаційно-телекомунікаційної системи.

Останнім суспільно небезпечним діянням аналізованої групи є зловживання цифровими пристроями.

Відповідно до Конвенції необхідно встановити відповідальність за придбання для використання, володіння, виробництво, продаж, оптовий продаж, імпорт та інші способи надання в користування пристроїв, за допомогою яких можна здійснювати кримінальні правопорушення в кіберпросторі. До них належать пристрої та програми, спеціально розроблені або адаптовані для цілей вчинення правопорушень, а також дані (паролі або коди доступу), за допомогою яких зловмисник може одержати доступ до інформаційно-телекомунікаційної системи або її частини й використовувати її для скоєння правопорушення [434, с. 12].

До кримінальних правопорушень, пов'язаних із комп'ютерами, Конвенція класифікує підробку та шахрайство, пов'язані з комп'ютером.

Водночас підробка, пов'язана з комп'ютером, визначається як блокування, стирання, зміна або введення комп'ютерних даних, якщо воно відбувається з наміром, щоб змінені (з порушенням автентичності) дані використовувалися або розглядалися як автентичні в юридичних цілях. Під комп'ютерним шахрайством розуміються суспільно небезпечні дії, спрямовані на позбавлення іншої особи власності, вчинені умисно з шахрайським чи іншим нечесним наміром, орієнтованим на неправомірне одержання економічної вигоди для зловмисника чи третьої особи. Таке діяння може бути скоєно шляхом будь-якого втручання у функціонування комп'ютерної системи, наприклад уведення, видалення, зміни або блокування комп'ютерних даних та інших дій.

До групи правопорушень, пов'язаних зі змістом даних, на підставі положень Конвенції належить лише одне діяння – правопорушення,

пов’язане з дитячою порнографією, яке, проте, охоплює комплекс протиправних, суспільно небезпечних дій. До нього належать: 1) виробництво дитячої порнографічної продукції, здійснюване несанкціоновано та навмисно з метою подальшого поширення у комп’ютерній системі; 2) пропозиція чи надання в користування дитячої порнографії через комп’ютерну систему; 3) придбання через комп’ютерну систему дитячої порнографії для особистого використання або третіх осіб; 4) володіння дитячою порнографією як збереженою на комп’ютерних носіях і розміщеної в комп’ютерній системі [435].

Під дитячою порнографією в цьому разі розуміють порнографічні матеріали, що зображують: участь неповнолітньої особи у відвертій сексуальній дії; участь особи, яка здається неповнолітньою, у відвертих сексуальних діях; реалістичні зображення неповнолітньої особи, яка бере участь у відвертій сексуальній дії. Як можемо помітити, це визначення теж не закріплює конкретних ознак належності порнографічних матеріалів до дитячої порнографії, залишаючи особливості правової регламентації національному законодавству країн-учасниць Конвенції [436].

Остання група правопорушень, що, проте, не закріпленна в Конвенції, – правопорушення, пов’язані з порушенням авторського права та суміжних прав. Положення статті 10 Конвенції мають відсильний характер і покладають на країн-учасниць Конвенції зобов’язання щодо криміналізації зазначеного діяння в нормах національних кримінальних законодавств, але якщо такі дії здійснюються за допомогою інформаційно-телекомунікаційних технологій та умисно [437].

Зауважимо, що в 2003 році Рада Європи підписала Додатковий протокол до Конвенції «Про кіберзлочинність», відповідно до якого держави-учасниці повинні були криміналізувати у своїх законодавствах суспільно небезпечні діяння, що стосувалися дій расистського й

ксенофобного характеру, які були вчинені через інформаційно-телекомунікаційні мережі.

Крім того, норми Конвенції зобов'язують країн-учасниць кваліфікувати як кримінально протиправні дії, що полягають у підбурюванні до скоєння будь-якого з вищедосліджених кримінальних правопорушень, співучасть у них або замах. Водночас установлення відповідальності за підбурювання та співучасть є обов'язком держави-підписанта Конвенції, а криміналізація замаху – правом [438].

Зауважимо, що відповідно до статті 12 Конвенції держави-учасниці повинні вжити таких заходів, що давали б змогу юридичній особі нести кримінальну відповідальність за весь спектр протиправних дій, передбачених Конвенцією.

Проаналізувавши основні норми Конвенції «Про кіберзлочинність», хочемо наголосити, що, незважаючи на різноманітність закріплення в ній норм, вона містить лише загальні положення регламентації відповідальності за кримінальні правопорушення з використанням інформаційно-телекомунікаційних технологій, систем і мереж. На нашу думку, це потребує істотного доповнення й уточнення в рамках національних законодавств держав-учасниць.

Водночас не можемо не звернути увагу на певні норми Конвенції, з якими ми категорично не погоджуємося. Однією з таких норм є пункт «b» статті 32, який містить положення, відповідно до якого Сторона 1 може без згоди Сторони 2 одержувати через інформаційно-телекомунікаційну систему, яка знаходиться на її території, доступ до цифрових даних, зебережених на території іншої Сторони 2, або одержати їх, якщо ця Сторона 2 має законну й добровільну згоду особи, яка має законні повноваження розкривати ці дані через таку інформаційно-телекомунікаційну систему. Отже, положення Конвенції фактично

закріплюють повноваження правоохоронних органів держав-учасниць вчиняти зазначені дії в юрисдикції іншої держави без її дозволу.

Хочемо провести аналіз норм Конвенції «Про кіберзлочинність» на предмет імплементації в кримінальне законодавство України. Наш аналіз ми будемо робити в розрізі співвідношення норм Конвенції та норм Кримінального кодексу України, одночасно визначаючи їх позитивні й негативні моменти.

Стаття 2 Конвенції закріплює необхідність криміналізації суспільно небезпечного діяння у формі незаконного доступу. У Кримінальному кодексі України зазначене суспільно небезпечне діяння криміналізоване в рамках статті 361 Особливої частини Кримінального кодексу України «Несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж».

Стаття 3 Конвенції закріплює відповідальність за незаконне перехоплення цифрової інформації, що передається через інформаційно-телекомунікаційні технології. Зазначена норма, на жаль, не набула криміналізації в рамках Кримінального кодексу України відповідно до змістовності, визначеної в Конвенції. Проте частина 2 статті 362 Особливої частини Кримінального кодексу України «Несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї» визначає як одну з форм дії об'єктивної сторони таке діяння, як перехоплення. Проблематику в цьому разі становить те, що суб'єкт такого кримінального правопорушення є спеціальним. Варто зауважити, що, незважаючи на відсутність у чинному Кримінальному кодексі України норм щодо перехоплення, можна виділити низку кримінальних

правопорушень, за яких діяння у формі перехоплення може буди основним під час вчинення правопорушення. Наприклад, залежно від характеру цифрової інформації таке діяння може кваліфікуватися за статтями 111, 114, 163 Особливої частини Кримінального кодексу України.

Стаття 4 Конвенції передбачає необхідність кваліфікувати як кримінальне правопорушення умисне створення серйозних перешкод функціонуванню комп'ютерної системи шляхом маніпуляцій із цифровими даними. Зазначені діяння підпадають під склад кримінального правопорушення, передбачений статтею 361 Особливої частини Кримінального кодексу України.

Стаття 5 Конвенції, що наголошує на криміналізації суспільно небезпечних дій у формі втручання в систему, виражена відразу у двох статтях Особливої частини Кримінального кодексу України, а саме: 361 та 363-1.

Стаття 6 Конвенції зобов'язує кваліфікувати як злочини такі дії: виробництво, продаж, придбання для використання, імпорт, оптовий продаж або інші форми надання в користування пристроїв, зокрема комп'ютерних програм, розроблених та адаптованих для цілей скоєння будь-якого з правопорушень, передбачених статтями 2–5 Конвенції; комп'ютерних паролей, кодів доступу чи інших аналогічних даних, за допомогою яких може бути одержаний доступ до комп'ютерної системи чи її частини.

В Україні відповідальність за таке суспільно небезпечне діяння можливе в рамках статті 359 Особливої частини Кримінального кодексу України «Незаконні придбання, збут або використання спеціальних технічних засобів отримання інформації».

Щодо комп'ютерних паролів, кодів доступу чи інших аналогічних даних, за допомогою яких може бути одержаний доступ до комп'ютерної

системи чи її частини, то в рамках системи кримінального права України відповідальність може наставати за статтею 361-1 Особливої частини Кримінального кодексу України «Створення з метою протиправного використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут».

Стаття 7 Конвенції передбачає встановлення відповідальності за підробку, пов'язану з комп'ютером. Зазначена стаття доволі широко охоплює коло суспільно небезпечних діянь, передбачених Кримінальним кодексом України. Проте залежно від ознак вчиненого особою суспільно небезпечного діяння її дії можуть кваліфікуватися за такими статтям Особливої частини Кримінального кодексу України: 1) незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, електронними грошима, обладнанням для їх виготовлення (стаття 200); 2) незаконне виготовлення, підробка, використання чи збут підроблених документів на отримання наркотичних засобів, психотропних речовин або прекурсорів (стаття 318); 3) підробка документів, печаток, штампів та бланків, збут чи використання підроблених документів, печаток, штампів (стаття 358); 4) службова підробка (стаття 366).

Стаття 8 Конвенції передбачає відповідальність за комп'ютерне шахрайство. Незважаючи на наявність кваліфікаційної ознаки в статті 190 Особливої частини Кримінального кодексу України, широкий спектр діянь, визначених Конвенцією, залишається поза правовим регулюванням.

Правопорушення, пов'язані з дитячою порнографією, визначаються в статті 9 Конвенції, одночасно такі норми закріплено в статті 301-1 Особливої частини Кримінального кодексу України під назвою «Одержання доступу до дитячої порнографії, її придбання, зберігання,

ввезення, перевезення чи інше переміщення, виготовлення, збут і розповсюдження».

Останній вид кримінального правопорушення наведений у статті 10 Конвенції й передбачає відповідальність за порушення авторського права та суміжних прав. У Кримінальному кодексі України, зміст діянь, розглянутих у статті 10 Конвенції, передбачає кримінальну відповідальність за декількома статтями Особливої частини Кримінального кодексу України, зокрема: 1) порушення авторського права та суміжних прав (стаття 176); 2) порушення прав на винахід, корисну модель, промисловий зразок, топографію інтегральної мікросхеми, сорт рослин, раціоналізаторську пропозицію (стаття 177).

Поширення расистського й ксенофобного матеріалів через комп'ютерні системи, передбачене статтею 3 Додаткового протоколу до Конвенції «Про кіберзлочинність», також закріплене в кримінальному законі України, зокрема статтях 161, 300, 442 Особливої частини Кримінального кодексу України.

На нашу думку, незважаючи на те, що всі кримінальні правопорушення, передбачені Конвенцією «Про кіберзлочинність», закріплені в статтях Особливої частини Кримінального кодексу України, більшість із них не визначає вчинення кримінальних правопорушень шляхом використання інформаційно-телекомунікаційних технологій, систем або мереж як таких, що мають підвищений ступінь суспільної небезпеки, як рекомендує Конвенція. У таблиці 5 ми навели співвідношення норм Конвенції «Про кіберзлочинність» і Кримінального кодексу України в розрізі використання елементів інформаційно-телекомунікаційних технологій під час вчинення кримінального правопорушення та його закріплення як кваліфікаційної ознаки або прямо передбаченого в статті.

Таблиця 5 – Результат імплементації норм Конвенції «Про кіберзлочинність» у законодавство України

Конвенція «Про кіберзлочинність»	**Кримінальний кодекс України**	**Реалізація**
1	**2**	**3**
Стаття 2 «Незаконний доступ»	Стаття 361 «Несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж»	Виконано та реалізується в чинному Кримінальному кодексі України через установлення кримінальної відповідальності за несанкціоноване втручання в роботу інформаційно-телекомунікаційних технологій, систем та мереж
Стаття 3 «Нелегальне перехоплення»	Частина 2 статті 362 «Несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї»	Виконано лише в частині встановлення відповідальності щодо спеціального суб'єкта такого кримінального правопорушення, але саме діяння у формі перехоплення в його загальному розумінні не криміналізоване, а самі подібні діяння кваліфікуються за частиною 3 статті 361 Особливої частини кримінального Кодексу як діяння у формі порушення процесу маршрутизації цифрової інформації
Стаття 4 «Втручання у дані»	Частина 3 статті 361 «Несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж»	Виконано та вчиняється у формі несанкціонованого втручання в роботу інформаційно-телекомунікаційних технологій, систем та мереж, яке призвело до однієї або кількох альтернативних дій, зокрема витоку, втрати, підробки, блокування цифрової інформації, спотворення процесу її оброблення або порушення встановленого порядку її маршрутизації

Продовження таблиці 5

1	2	3
Стаття 5 «Втручання у систему»	Стаття 361 «Несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж. Стаття 361-1 «Створення з метою протиправного використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут»	Виконано
Стаття 6 «Зловживання пристроями»	Стаття 361-1 «Створення з метою протиправного використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут». Стаття 359 «Незаконні придбання, збут або використання спеціальних технічних засобів отримання інформації»	Виконано

Продовження таблиці 5

1	2	3
Стаття 7 «Підробка, пов'язана з комп'ютерами»	Стаття 200 «Незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, електронними грошима, обладнанням для їх виготовлення»	Незважаючи на наявність статті 200 Особливої частини Кримінального кодексу України, загалом вважаємо, що підробка у сфері цифрової інформації на сьогодні фактично не криміналізована. Крім того, предметом будь-якої підробки згідно з чинним кримінальним законом не може бути цифрова інформація
Стаття 8 «Шахрайство, пов'язане з комп'ютерами»	Частина 3 статті 190 «Шахрайство»	Незважаючи на наявність у чинному кримінальному законі кваліфікаційної ознаки шахрайства, вчиненого шляхом незаконних операцій із використанням електронно-обчислювальної техніки, суспільно небезпечні діяння з огляду на особливості статті 190 Особливої частини Кримінального кодексу України не можуть бути кваліфіковані як діяння, вчинені обманом або зловживанням довірою шляхом будь-якого втручання в інформаційно-телекомунікаційну технологію, мережу чи систему
Стаття 9 «Правопорушення, пов'язані з дитячою порнографією»	Стаття 301-1 «Одержання доступу до дитячої порнографії, її придбання, зберігання, ввезення, перевезення чи інше переміщення, виготовлення, збут і розповсюдження»	Не спостерігається виділення як кваліфікувальної ознаки вчинення кримінального правопорушення шляхом використання інформаційно-телекомунікаційних технологій, систем та мереж

Продовження таблиці 5

1	2	3
Стаття 10 «Правопорушення, пов'язані з порушенням авторських та суміжних прав»	Стаття 177 «Порушення авторського права і суміжних прав»	Не спостерігається виділення як кваліфікаційної ознаки вчинення кримінального правопорушення шляхом використання інформаційно-телекомунікаційних технологій, систем та мереж
Стаття 3 (Додатковий протокол до Конвенції «Про кіберзлочинність»)	Стаття 161«Порушення рівноправності громадян залежно від їх расової, національної, регіональної належності, релігійних переконань, інвалідності та за іншими ознаками». Стаття 300 «Ввезення, виготовлення або розповсюдження творів, що пропагують культ насильства і жорстокості, расову, національну чи релігійну нетерпимість та дискримінацію». Стаття 442 «Геноцид»	Не спостерігається виділення як кваліфікаційної ознаки вчинення кримінального правопорушення шляхом використання інформаційно-телекомунікаційних технологій, систем та мереж

Отже, підбиваючи підсумки вищевикладеного, хочемо зазначити, що незважаючи на можливості застосування загальних принципів міжнародного права до регулювання відносин у кіберпросторі, сьогодні (в епоху цифрової трансформації) уніфікація спеціальних принципів міжнародного права щодо відносин у кіберпросторі є нагальною потребою міжнародної спільноти. Попри швидку трансформацію кіберпростору й похідного від нього інтернет-простору та адаптацію кіберзлочинців до реалій суспільства, єдиним чинним міжнародним актом щодо встановлення кримінальної відповідальності за кримінальні правопорушення в кіберпросторі залишається Конвенція «Про кіберзлочинність». Як уже зазначалося, поява нових видів кримінальних правопорушень у кіберпросторі йде одночасно з появою нових інноваційних технологій, що зумовлює вдосконалення норм Конвенції «Про кіберзлочинність».

4.2. Порівняльно-правовий аналіз кримінальної відповідальності за вчинення кримінальних правопорушень у кіберпросторі за законодавством зарубіжних держав

Аналізуючи проблематику кримінально правової відповідальності за кримінальні правопорушення, вчинені в кіберпросторі, не можна залишити поза увагою зарубіжний досвід регулювання цього суспільно небезпечного феномену. Кримінальна відповідальність за правопорушення в кіберпросторі передбачена в більшості країн світу, водночас криміналізація цих протиправних, суспільно небезпечних діянь здійснюється впорядковано та методично в рамках злагодженої державної політики, спрямованої на протидію кримінальним правопорушенням у кіберпросторі.

Транснаціональний характер кримінальних правопорушень у кіберпросторі зумовлює взаємодію з правовими системами й правоохоронними органами інших держав. Зауважимо, що така співпраця можлива лише в разі чіткого розуміння національних особливостей установлення та реалізації кримінальної відповідальності за кримінальні правопорушення в кіберпросторі. На нашу думку, порівняльно-правовий аналіз загалом дає змогу по-іншому поглянути на національний кримінальний закон, тим самим виявивши його слабкі та сильні сторони й зробивши пропозиції щодо його подальшого якісного реформування [439].

Аналіз і використання зарубіжного досвіду правового регулювання кримінальної відповідальності за вчинення кримінальних правопорушень у кіберпросторі стає дедалі актуальнішим з урахуванням того факту, що в багатьох державах процес криміналізації правопорушень у кіберпросторі почався набагато раніше, ніж в Україні.

Варто наголосити, що процес криміналізації складів кримінальних правопорушень у кіберпросторі в різних державах не проходив рівномірно. Наприклад, Сполучені Штати Америки, низка країн Європейського Союзу,

Японія почали розроблення свого законодавства щодо боротьби з кримінальними правопорушеннями в кіберпросторі значно раніше за інші держави [440, с. 46].

На нашу думку, такий швидкий процес адаптації до кіберзагроз насамперед пояснюється високим рівнем розвитку зазначених держав, зокрема в технологічному плані, що зумовило появу перших злочинних кіберугрупувань і вчинення перших кримінальних правопорушень у кіберпросторі, як наслідок – ранній сплеск кіберзлочинності та одночасного усвідомлення негайного правового регулювання цього суспільно небезпечного явища [441].

Ураховуючи той факт, що Сполучені Штати Америки та країни Європейського Союзу мають значний досвід щодо криміналізації кримінальних правопорушень у кіберпросторі, аналіз якого допоможе найкраще протидіяти цьому суспільно небезпечному явищу як у матеріальному, так і в процесуальному аспекті, пропонуємо зосередити увагу саме на їх досвіді в питаннях регулювання кримінальної відповідальності за вчинення кримінальних правопорушень у кіберпросторі. Крім того, ми проаналізуємо досвід інших країн, зокрема країн Латинської Америки, Азії та пострадянської системи.

Аналізуючи принципи кримінальної відповідальності за вчинення кримінальних правопорушень у кіберпросторі, можемо стверджувати, що вони істотно відрізняються в країнах романо-германської та англо-саксонської правових сімей. Водночас у країнах із прецедентним правом акцент здійснюється на визнанні кримінально протиправним діяння в кожному конкретному судовому рішенні, як результат – уведення в законодавство таких держав загальних формулювань із подальшим широким оцінюванням таких суспільно небезпечних діянь. Навпаки, країни романо-германської правової сім’ї намагаються створити чітке уніфіковане

правове регулювання в рамках законодавчих актів для кожного конкретного виду кримінальних правопорушень у кіберпросторі [442].

Варто зауважити, що, незважаючи на відмінності у правовому регулюванні встановлення кримінальної відповідальності між різними країнами, спільним для всіх країн є факт загрози таких суспільно небезпечних діянь з урахуванням їх пріоритету правового регулювання. Сьогодні ми з упевненістю можемо зазначити, що правове регулювання встановлення кримінальної відповідальності за кримінальні правопорушення в кіберпросторі на рівні окремих країн має тенденцію до уніфікації на рівні або окремих законодавчих, або кодифікованих актів. Водночас нормативні акти, ухвалювані країнами у сфері встановлення кримінальної відповідальності за зазначені суспільно небезпечні діяння, здебільшого копіюють один одного, але фактично кожна країна має свою специфіку в регулюванні зазначеної проблеми.

Професор Вашингтонського державного університету А. Кігерл пояснює це тим, що кримінальні правопорушення в кіберпросторі мають здебільшого транскордонний характер і для їх ефективного розслідування правоохоронні органи різних країн світу повинні користуватися єдиним понятійним апаратом. Зауважимо, що в більшості країн світу національне законодавство в частині встановлення кримінальної відповідальності за вчинення кримінальних правопорушень у кіберпросторі має конвенціальний характер. Як ми зазначали в попередньому підрозділі, міжнародні нормативні акти регламентують кримінальну відповідальність за вчинення кримінальних правопорушень у кіберпросторі, зокрема Конвенція «Про кіберзлочини» наголошує на необхідності зведення національних законодавств країн-учасниць до одноманітності [443].

Для вироблення рекомендацій щодо вдосконалення правового регулювання вчинення кримінальних правопорушень у кіберпросторі в Україні вважаємо необхідним провести порівняльний аналіз конкретних

способів правового регулювання відповідальності за вчинення цих суспільно небезпечних діянь у законодавстві інших країн.

На нашу думку, найбільш розробленим законодавством у сфері правового регулювання встановлення кримінальної відповідальності за вчинення кримінальних правопорушень у кіберпросторі є Сполучені Штати Америки. Зауважимо, що саме Сполучені Штати Америки можна вважати першою країною, в якій було вчинене кримінальне правопорушення в кіберпросторі, і з того часу вектор кібербезпеки для Сполучених Штатів Америки став одним із найпріоритетніших. Зауважимо, що саме в цій країні були ухвалені нормативні акти щодо регулювання питання боротьби з кримінальними правопорушеннями в кіберпросторі. Зокрема, першою спробою встановлення кримінальної відповідальності за вчинення кримінальних правопорушень у кіберпросторі варто вважати ухвалений у 1986 році Акт «Про комп'ютерне шахрайство та зловживання». На той момент цей Акт вважався основним нормативно-правовим актом, що встановлював відповідальність за вчинення кримінальних правопорушень шляхом використання інформаційно-телекомунікаційних технологій [444].

Зауважимо, що цей нормативний документ неодноразово доповнювався, останні поправки до нього були ухвалені в 1996 році. Саме правові положення цього Акту стали основою для розроблення законодавства щодо встановлення кримінальної відповідальності за вчинення кримінальних правопорушень шляхом використання інформаційно-телекомунікаційних технологій на рівні окремих штатів [445].

Акт «Про комп'ютерне шахрайство» надає такий перелік кримінальних правопорушень, що можуть вчинятися шляхом використання інформаційно-телекомунікаційних технологій: 1) умисне одержання або зміна повідомлень, збережених у пам'яті комп'ютера, а також створення перешкод для законного доступу до таких повідомлень; 2) комп'ютерне

шпигунство; 3) шахрайство з використанням комп'ютера; 4) шахрайство під час торгівлі комп'ютерними паролями; 5) загрози, здирство, шантаж за допомогою комп'ютера; 6) порушення конфіденційності електронної пошти та голосових повідомлень; 7) перехоплення й розголошення повідомлень, що передаються по телеграфу, усно чи електронним способом; 8) торгівля викраденими або підробленими пристроями доступу, які можуть бути використані для отримання грошей, товарів чи послуг; 9) умисне пошкодження обладнання, ліній і систем зв'язку; 10) несанкціонований доступ до інформації, що знаходиться у використовуваному урядом комп'ютері; 11) пошкодження або порушення урядового комп'ютера [446].

Перелік кримінальних правопорушень, що вчиняються в кіберпросторі, доволі широкий, водночас спостерігається певне дублювання діянь, що, проте, вчиняються різними способами. Зауважимо, що кримінальна відповідальність за вчинення цих суспільно небезпечних діянь і власне санкція залежать від багатьох факторів, зокрема рецидиву, кримінологічної характеристики особи, яка вчинила правопорушення, розміру завданих збитків, тяжкості діяння та спричинених наслідків [447, с. 461].

Крім того, законодавство Сполучених Штатів Америки закріплює спеціальний понятійний апарат щодо встановлення кримінальної відповідальності за вчинення кримінальних правопорушень у кіберпросторі, зокрема «захищений комп'ютер», під яким розуміється комп'ютер, що знаходиться у винятковому користуванні фінансової установи або уряду США або використовуваний у роботі для них [448, с. 24].

Водночас протиправні суспільно небезпечні дії, спрямовані на «захищений комп'ютер», підлягають застосуванню заходів кримінально-

правового впливу згідно з Актом «Про комп'ютерне шахрайство», відповідальність за які значно суворіша.

Цікавим є досвід Сполучених Штатів Америки щодо формулювання поняття «одержання інформації», що, крім копіювання й переміщення цифрової інформації, також охоплює процес самого «читання», тобто ознайомлення з цифровою інформацією без подальшого вчинення будь-яких дій щодо неї. Саме таке формулювання ми пропонуємо внести до частини 1 статті 361 Особливої частини Кримінального кодексу України, що дасть змогу правильніше кваліфікувати суспільно небезпечні діяння за відсутності наслідків, передбачених частиною 3 зазначеної статті. На нашу думку, таке розширене тлумачення дозволить притягнути до відповідальності осіб, які вчиняють кримінальні правопорушення, без фактичної зміни первинного знаходження джерела цифрової інформації.

Не можна не звернути увагу на застосований в Акті «Про комп'ютерне шахрайство» термін «збитки», що означає будь-яке пошкодження цілісності та доступності цифрових даних, програм, систем або цифрової інформації. На нашу думку, такий підхід на законодавчому рівні дав би змогу вносити рішення про розмір і характер збитків у кожному випадку індивідуально, ураховуючи всі обставини справи [449, с. 691].

Як уже було зазначено, Акт «Про комп'ютерне шахрайство» став відправною точкою для формування відповідальності за кримінальні правопорушення в кіберпросторі окремих штатів, пропонуємо розглянути на прикладах. Питання врегульованості встановлення кримінальної відповідальності за вчинення окремих видів цих суспільно небезпечних діянь, зокрема шахрайства, вчиненого шляхом використання інформаційно-телекомунікаційних технологій, систем та мереж.

Відповідно до Закону штату Арканзас, підрозділу 4 «Кримінальні правопорушення проти власності» розділу 5 «Кримінальні правопорушення»

глави 41 «Кримінальні правопорушення, пов'язані з комп'ютером» параграфу 5-41-103 «Комп'ютерне шахрайство» особа вважається такою, яка вчинила «комп'ютерне шахрайство», якщо вона, використовуючи доступ до комп'ютера, комп'ютерної системи або мережі, викрала грошові кошти або інше майно шляхом обману або зловживання довірою. Зазначимо, що відповідно до Законів штату Арканзас це кримінальне правопорушення належить до класу D, за який передбачає покарання у вигляді позбавлення волі на строк до 6 років [450].

На відміну від штату Арканзас штат Вірджинія, урегульовуючи питання кримінальної відповідальності за вчинення «комп'ютерного шахрайства» як основний вид покарання запровадило штраф. Зокрема, відповідно до кримінального законодавства штату воно карається штрафом до 10 000 доларів Сполучених Штатів Америки або позбавленням волі на строк до 10 років. У параграфі 18.2-152.3 «Комп'ютерне шахрайство» Основного кримінального закону штату Вірджинія визначається: 1) якщо вартість викраденого майна не перевищує 200 доларів, правопорушення варто відносити до 1-го класу категорії D, покарання за яке передбачає штраф до 2 500 доларів або позбавлення волі на строк до одного року (водночас можуть бути застосовані відразу два основних покарання); 2) якщо збитки від зазначеного діяння перевищують 200 доларів, то кримінальне правопорушення варто відносити до 5-го класу категорії D, покарання за яке передбачає позбавлення волі на строк від одного до десяти років з одночасним штрафом до 2 500 доларів [451].

Звід законів штату Луїзіана передбачає кримінальну відповідальність за комп'ютерне шахрайство в параграфі 73.5. Водночас відповідно до зазначеного параграфу надаються ознаки складу кримінального правопорушення, зокрема використання особою комп'ютера, телекомунікаційної мережі або системи та обман. Відповідно до законодавства штату Луїзіана відповідальність за вчинення комп'ютерного

шахрайства має два альтернативні покарання: штраф розміром до 10 000 доларів або позбавленням волі на строк до 5 років. Як і в попередньому варіанті, законодавство дозволяє одночасне застосування обох видів покарання. Цікавим є досвід запровадження як кваліфікаційної ознаки в разі вчинення зазначеного кримінального правопорушення інтернет-мережі. Зокрема, якщо, особа яка вчиняє комп'ютерне шахрайство, робить це з використанням Інтернету, встановлюється додаткове покарання у вигляді позбавлення волі строком не менше за один рік [452].

Відповідно до Зводу законів штату Іллінойс комп'ютерне шахрайство визначається як суспільно небезпечні дії, спрямовані на неправомірне заволодіння чужим майном, шляхом обману або інших дій щодо копіювання захищеної цифрової інформації, блокування, ураження або знищення цифрових даних і так само виведення з ладу телекомунікаційних цифрових пристроїв, систем або мереж. Варто зауважити, що кримінальне законодавство штату Іллінойс має найбільш диференційовану систему покарань з-поміж інших штатів. Зокрема, відповідальність за вчинення комп'ютерного шахрайства в цьому штаті передбачає п'ять класів і два альтернативні покарання: штраф розміром від 1 000 до 50 000 доларів та позбавлення волі строком від 1 до 7 років [453].

Варто зазначити, що окремо законодавство штату Іллінойс виділяє посягання на власність, здійснюване в режимі онлайн.

Поряд з установленням кримінальної відповідальності за збут у мережі Інтернет майна, здобутого злочинним шляхом, у статті 16J-15 сформульовано склад інтернет-крадіжки шляхом обману, зміст якої пов'язаний з учиненням винним дій щодо оплати товарів чи послуг в інтернет-мережі з використанням недостовірних даних (передбачається: даних вигаданої чи іншої особи). Як і в статті про комп'ютерне шахрайство,

відповідальність за вчинення цього кримінального правопорушення диференціюється залежно від розміру викраденого майна [454].

Не можна не звернути увагу на досвід криміналізації суспільно небезпечних діянь проти власності штату Джорджія. На відміну від інших штатів у своєму Зводі законів він використовує категорію не комп'ютерного шахрайства, а крадіжки за допомогою комп'ютера. У розділі, присвяченому комп'ютерним кримінальним правопорушенням, у параграфі 16-9-93 передбачено, що будь-яка особа визнається винною в скоєнні комп'ютерної крадіжки, якщо вона використовує комп'ютер або комп'ютерну мережу з усвідомленням того, що таке використання є неправомірним, із метою: 1) вилучення чи присвоєння майна іншої особи; 2) одержання права на майно будь-яким обманним способом; 3) перетворення власності на порушення договору чи іншого юридичного зобов'язання.

Відповідно до пункту «h» цієї статті це кримінальне правопорушення карається або штрафом до 50 тисяч доларів, або позбавленням волі на строк до 15 років, або обома цими видами покарання.

Згідно зі статистичними даними фірми з кібербезпеки «Check point» серед усіх вчинених на території Сполучених Штатів Америки кримінальних правопорушень у кіберпросторі частка кібершахрайств найбільша [455]. Незважаючи на цей факт, деякі штати не мають спеціальних норм щодо комп'ютерного шахрайства. Одним із них є штат Невада, згідно із законодавством якого кримінальна відповідальність за подібні дії передбачена загальною нормою про неправомірний доступ до цифрової інформації, що охороняється законом [456].

Розглядаючи питання врегулювання кримінальної відповідальності за вчинення кримінальних правопорушень у кіберпросторі країн англо-саксонської правової сім'ї, не можемо не звернути увагу на досвід Великої Британії. Варто зазначити, що правове регулювання встановлення

кримінальної відповідальності за кримінальні правопорушення, які вчиняються шляхом використання інформаційно-телекомунікаційних технологій, систем або мереж, спираються на прецедентне право.

Водночас основним нормативним актом у сфері регламентації встановлення кримінальної відповідальності за кримінальні правопорушення в кіберпросторі є Акт «Про комп'ютерні зловживання» 1990 року [457].

Зазначений нормативний акт закріплює відповідальність за «неправомірний доступ», під яким варто розуміти використання комп'ютера з наміром одержати доступ, якщо особа, яка вчиняє кримінальне правопорушення, заздалегідь усвідомлює неправомірність і незаконність такого доступу [458].

Неправомірний доступ у рамках Акту «Про комп'ютерні зловживання» поділено на: 1) доступ до цифрової інформації, що зберігається на комп'ютері, коли метою особи, яка вчиняє кримінальне правопорушення, є викрадення збережених на комп'ютері цифрових даних; 2) доступ із наміром вчинити інше кримінальне правопорушення, за якого комп'ютер використовується як засіб здійснення іншого протиправного діяння [459, с. 607].

Також кримінальним правопорушенням визнається неправомірна модифікація комп'ютерних даних, тобто зміна змісту цифрового програмного коду, що зберігається в комп'ютері. Варто зазначити, що, крім формальних ознак складу кримінального правопорушення, визначених в Акті «Про комп'ютерні зловживання», суд під час призначення покарання обов'язково повинен з'ясувати дві обставини: 1) умисел особи, яка вчинила кримінальне правопорушення, передбачене відповідною статтею, щодо неправомірного доступу, зміни цифрової інформації тощо; 2) поінформованість особи, яка вчинила кримінальне правопорушення, що

внесені нею зміни до цифрової інформації в телекомунікаційному пристрої є несанкціонованими.

Крім того, відповідно до бланкетних норм Закону «Про захист дітей» [460] 1978 року та Закону «Про сексуальні злочини» [461] 1956 року особи можуть підлягати кримінальній відповідальності за виготовлення й розповсюдження порнографічних зображень дітей віком до 16 років, здійснювані з використанням інформаційно-телекомунікаційних технологій, систем і мереж. Так само Закон «Про тероризм» 2000 року [462] закріплює, що неправомірний доступ до цифрової інформації, яка 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.

На нашу думку, запозичення позитивного досвіду Великої Британії в рамках боротьби та встановлення кримінальної відповідальності за кібертероризм є обов'язковим кроком у рамках становлення стратегії кібербезпеки держави й тих кібернетичних загроз, що ми маємо сьогодні з боку Російської Федерації.

Не можна не акцентувати увагу на досвіді Ірландії в становленні кримінальної відповідальності за правопорушення в кіберпросторі. Актом «Про кримінальну шкоду» 1991 року визначено, що використання інформаційно-телекомунікаційної технології з метою одержання неправомірного доступу до цифрових даних є кримінальним правопорушенням. Цікавим є момент установлення винної особи. Зокрема, за законодавством Ірландії винною у вчиненні кримінального правопорушення буде як та особа, яка перебуває на території Ірландії або за її межами, так і особа, яка перебуває в іншій країні, але об'єктом

посягання є відносини, що охороняються законодавством Ірландії. У цьому разі така особа визнається винною незалежно від успішності своїх дій [463].

Використання інформаційно-телекомунікаційних технологій для отримання неправомірної вигоди на користь особи, яка вчинила кримінальне правопорушення, або третіх осіб, або з метою заподіяння майнової шкоди, карається позбавленням волі на строк до 10 років. Варто зауважити, що ця норма, регламентована Актом «Про шахрайство», має нечітке формулювання, унаслідок чого може застосовуватися до широкого кола кримінальних правопорушень у кіберпросторі [464].

Кримінальний кодекс Канади в статті 403 встановлює відповідальність за використання персональних даних із метою розкрадання чужого майна. Відповідно до санкції цієї статті особа, визнана винною у вчиненні такого кримінального правопорушення, підлягає покаранню у вигляді позбавлення волі строком до 10 років. Одночасно з цим у статті 402.1 надається поняття персональних даних, зокрема під персональними даними особи розуміється така цифрова інформація: відбитки пальців, ім’я, адреса, дата народження, власноручний підпис, електронний підпис, цифровий підпис, ім’я користувача, номер кредитної картки, номер дебетової картки, номер фінансового рахунку, номер паспорта, номер полісу соціального страхування, номер медичного страхування, номер водійського посвідчення чи пароль [465].

На відміну від кримінального законодавства вищерозглянутих країн кримінальний закон Нової Зеландії передбачає окремий розділ у рамках чинного Кримінального кодексу країни, що встановлює відповідальність за кримінальні правопорушення в кіберпросторі. Зокрема, відповідно до Кримінального кодексу Нової Зеландії криміналізовано такі кримінальні правопорушення: 1) доступ до інформаційно-телекомунікаційної технології шляхом обману; 2) пошкодження або втручання в роботу інформаційно-телекомунікаційної технології; 3) виготовлення, продаж, розповсюдження

або володіння програмним забезпеченням для вчинення кримінального правопорушення; 4) доступ до інформаційно-телекомунікаційної системи без авторизації [466].

Примітним є той факт, що кримінальна відповідальність за суспільно небезпечні діяння, що вчиняються шляхом використання інформаційно-телекомунікаційних технологій, передбачає лише позбавлення волі з максимальним строком до 10 років. Не можемо не звернути увагу, що, на противагу всім країнам англо-саксонської правової сім'ї, кримінальне законодавство Нової Зеландії виділяє кримінальні норми щодо вчинення шахрайства шляхом використання інформаційно-телекомунікаційних технологій саме в групу «комп'ютерних кримінальних правопорушень», а не в групу «кримінальних правопорушень проти власності».

Розглянувши аспекти встановлення кримінальної відповідальності в країнах англо-саксонської правової сім'ї, пропонуємо перейти до аналізу кримінальних законодавств романо-германської правової сім'ї, до якої належить Україна. Водночас вважаємо необхідним зосередити увагу саме на країнах Європейського Союзу.

Найбільше складів кримінальних правопорушень шляхом використання інформаційно-телекомунікаційних технологій серед країн Європейського Союзу передбачено в Кримінальному кодексі Нідерландів, водночас у ньому немає окремої глави «Кримінальні правопорушення з використанням інформаційно-телекомунікаційних технологій, систем або мереж». У цьому разі склади окремих суспільно небезпечних діянь у кіберпросторі розміщені відповідно до об'єкта посягання. Зазначимо, що такий досвід застосовується більшою частиною країн Європейського Союзу й має дещо спільне з Кримінальним кодексом України в розрізі імплементації норм Конвенції «Про кіберзлочинність».

Наприклад, стаття 138a, що регламентує кримінальну відповідальність за «несанкціоноване втручання в цифровий пристрій або систему

збереження», наведена в розділі V «Кримінальні правопорушення проти громадського порядку». У цьому самому розділі розміщено норми, що регламентують кримінальну відповідальність за «використання технічних засобів, призначених для перехоплення або запису цифрових даних, які обробляються в інформаційно-телекомунікаційних системах». Кримінальна відповідальність за «неправомірне перехоплення або копіювання цифрових даних» та «використання цифрових даних, отриманих злочинним шляхом» також розглянута в розділі V Кримінального кодексу Нідерландів. Варто звернути увагу на систему й розмір покарань аналізованої країни. З упевненістю можемо говорити, що кримінальне законодавство Нідерландів у частині встановлення кримінальної відповідальності за суспільно небезпечні діяння в кіберпросторі має доволі лояльний характер. Основним покаранням за зазначені кримінальні правопорушення є позбавлення волі, але строк покарання встановлюється до одного року [467].

Аналізуючи кримінальне законодавство Нідерландів, ми звернули увагу на той факт, що в ньому не використовується звична нам термінологія, така як «вірус» і «шкідливе програмне забезпечення». Замість цього законодавчому регулюванню підлягає встановлення кримінальної відповідальності за «дії у формі розповсюдження цифрових даних, спрямовані на заподіяння шкоди, шляхом їх подальшого самокопіювання в інформаційно-телекомунікаційній технології або системі».

На думку Е. Рудгера, загальний аспект такого формулювання фактично є певною заготовкою на майбутнє, що дасть змогу відмежувати кримінальне законодавство країни від подальшого реформування та в разі появи нових технологічних новинок, які не підлягатимуть дії «суворих норм права». Ми погоджуємося з позицією науковця й вважаємо, що такий досвід у формулюванні протиправного діяння міг би бути застосований у рамках національного законодавства, оскільки сфера кримінальних

правопорушень у кіберпросторі має тенденцію до швидкого розвитку [468, с. 6].

Відповідальність за вчинення кримінальних правопорушень у кіберпросторі також передбачена в Кримінальному кодексі Франції, зокрема в розділі III «Посягання на систему автоматизованого оброблення даних». Водночас звернімо увагу, що норми кримінального закону Франції захищають власне не відносини в кіберпросторі, а інформаційно-телекомунікаційні технології, системи та мережі, а також програмне забезпечення як об'єкти власності [469].

Кримінальний кодекс Іспанії регламентує відповідальність за кримінальні правопорушення в кіберпросторі в розділі X. Особливість установлення кримінальної відповідальності за кримінальні правопорушення в кіберпросторі відповідно до кримінального законодавства Іспанії полягає у відсутності спеціалізованих складів цього типу суспільно небезпечних діянь Водночас Іспанське кримінальне законодавство має дуже розгалужену систему кваліфікаційних ознак. Наприклад, відповідно до частини 2 статті 249 Кримінального кодексу Іспанії шахрайство – це діяння, вчинене шляхом знищення або модифікації цифрової інформації або цифрового документа будь-якого виду. Цікавим є досвід установлення кваліфікаційної ознаки «шляхом використання інформаційно-телекомунікаційних технологій» у таких кримінальних правопорушеннях: 1) порушення таємниці листування; 2) порушення авторського права; 3) тероризм. Вважаємо запозичення такого підходу щодо встановлення кваліфікаційних ознак, що регламентували б кримінальні правопорушення в кіберпросторі у вітчизняне законодавство України, цілком виправданим, ураховуючи підвищений ступінь суспільної небезпеки [117].

Розглянемо досвід Данії в установленні кримінальної відповідальності за шахрайські дії, вчинені в кіберпросторі.

Статтею 279 «а» комп'ютерне шахрайство визначається як незаконна зміна, доповнення або видалення цифрової інформації чи програмного коду, використовуваних для цифрового автоматизованого оброблення даних із метою одержання для себе або третіх осіб незаконної вигоди. На нашу думку, саме таке формулювання шахрайства шляхом використання інформаційно-телекомунікаційних технологій допомогло б вирішити проблеми співвідношення суспільно небезпечних дій, що мають ознаки як крадіжки, так і шахрайства [470].

Науковий інтерес для нашого дослідження також становить закріплення кримінальної відповідальності за вчинення кримінальних правопорушень шляхом використання інформаційно-телекомунікаційних технологій, систем та мереж у законодавстві Німеччини. Як і в багатьох країнах Європейського Союзу, в Кримінальному кодексі Німеччини відсутній спеціалізований розділ, який присвячувався б кримінальній відповідальності за кримінальні правопорушення в кіберпросторі. Основними кримінальними правопорушеннями в кіберпросторі, передбаченими Кримінальним кодексом Німеччини, є такі: 1) шпигунство (стаття 202 а); 2) модифікація даних (стаття 303 а); 3) комп'ютерний саботаж (стаття 303 б); 4) комп'ютерне шахрайство (стаття 203 а); 5) підробка цифрових даних, необхідних для отримання доказів (стаття 269); 6) порушення телекомунікаційної таємниці [115].

Німеччина також пішла шляхом установлення кримінальної відповідальності за кримінальні правопорушення в кіберпросторі, визначаючи кваліфікаційні ознаки, зокрема «шляхом використання комп'ютера». Ми підтримуємо позицію німецького кримінального законодавства з приводу тлумачення норм установлення кримінальної відповідальності за «комп'ютерне шахрайство». Шахрайство може визнаватися комп'ютерним лише тоді, коли обманутою є не фізична особа (шляхом уведення або модифікації цифрової інформації), а коли за

допомогою введення чи модифікації цифрової інформації в оману ввели саме інформаційно-телекомунікаційну технологію, що видала потрібний злочинний результат особі, яка вчинила кримінальне правопорушення. Зазначене тлумачення комп'ютерного шахрайства, закріплене в Кримінальному кодексі Німеччини, відрізняється від суспільно небезпечних діянь цього типу, передбачених кримінальними законодавствами інших країн, зокрема України.

Серед інших особливостей правового регулювання кримінальної відповідальності за кримінальні правопорушення в кіберпросторі є те, що відповідно до пункту 1 статті 23 Кримінального кодексу Німеччини будь-який замах на вчинення кримінального правопорушення караний. Тобто, незважаючи на те, чи досягла особа свого злочинного результату, у будь-якому разі вона буде нести кримінальну відповідальність за загальними правилами [471].

Зауважимо, що Німеччина не є ратифікантом Конвенції «Про кіберзлочинність», але широко використовує рекомендації обов'язкового й необов'язкового списків кримінальних правопорушень № 89 (9) Ради Європи. Крім того, в кримінальному законодавстві Німеччини використовується власний категоріальний апарат. Зокрема, в пункті 2 статті 202 а Кримінального кодексу Німеччини дається визначення поняття «дані», під яким розуміються цифрові дані, що збираються й передаються електронним, магнітним або іншим способом, яким не сприймаються у фізичному вимірі [472].

Несанкціонований доступ особи до спеціально захищених комп'ютерних даних, здійснюваний із метою одержання вигоди для себе або третіх осіб, тягне за собою покарання у вигляді позбавлення волі строком до трьох років. Анулювання, знищення, приведення в непридатність або зміна цифрових даних, оброблюваних в інформаційно-телекомунікаційній системі або мережі, караються штрафом чи

позбавленням волі до двох років. Пунктом 1 статті 303 б Кримінального кодексу Німеччини встановлено відповідальність за «комп'ютерний саботаж», тобто порушення процесу оброблення цифрових даних, що мають істотне значення національного характеру, якщо він призвів до: 1) непридатності або зміни комп'ютерної програми; 2) пошкодження процесу оброблення цифрових даних або носія таких даних. Зазначені дії караються позбавленням волі терміном до п'яти років або штрафом. Варто зазначити, що відповідно до розглянутої правової норми спрямованість умислу особи, яка вчиняє кримінальне правопорушення, на пошкодження носія даних кваліфікується як комп'ютерне кримінальне правопорушення, тоді як відповідно до статті 194 Особливої частини Кримінального кодексу України таке діяння належить до кримінальних правопорушень проти власності й має специфічний порядок кваліфікації [473].

Інша група країн, досвід у регулюванні кримінальних правопорушень у кіберпросторі яких ми хочемо розглянути, обумовлена історично, а саме: радянським минулим. Першою країною, аналіз якої ми хочемо зробити в контексті встановлення кримінальної відповідальності за суспільно небезпечні діяння в кіберпросторі, є Азербайджан. Варто зауважити, що особливістю кримінального законодавства пострадянських країн є регламентація норм, що визначають відповідальність за кримінальні правопорушення в кіберпросторі в окремому розділі. Не є винятком і Азербайджан, у якому кримінальні правопорушення в кіберпросторі передбачені розділом XIII Кримінального кодексу Азербайджану «Кіберзлочини».

Нормами цього розділу криміналізовані такі суспільно небезпечні дії: 1) неправомірний доступ до комп'ютерної системи (стаття 271), тобто навмисний вхід до комп'ютерної системи без права доступу або з порушенням заходів захисту; 2) неправомірне заволодіння комп'ютерною інформацією (стаття 272, відповідно до якої криміналізована норма щодо

заволодіння комп'ютерною інформацією, не призначеною для публічного користування); 3) неправомірне втручання в комп'ютерну систему або комп'ютерну інформацію (стаття 273), що закріплює відповідальність за неправомірне пошкодження, знищення, псування чи зміну комп'ютерної інформації; 4) оборот коштів, виготовлених для скоєння кіберзлочинів (стаття 273-1, яка встановлює відповідальність за виробництво пристроїв або комп'ютерних програм); 5) фальсифікація комп'ютерних даних (стаття 273-2), тобто несанкціоноване навмисне запровадження, зміна, знищення або блокування комп'ютерних даних із метою видати сфальсифіковані дані за автентичні [474].

Зауважимо, що зазначені статті за змістом подібні до закріплених у розділі XVI Особливої частини Кримінального кодексу України.

Кримінальний кодекс Республіки Казахстан містить дві статті, що регламентують відповідальність за скоєння кримінальних правопорушень із використанням інформаційно-телекомунікаційних технологій: 1) неправомірний доступ до комп'ютерної інформації, створення, використання та поширення шкідливих програм для ЕОМ (стаття 227); 2) неправомірна зміна ідентифікаційного коду абонентського пристрою стільникового зв'язку, пристрою ідентифікації абонента, а також створення, використання, розповсюдження програм для зміни ідентифікаційного коду абонентського пристрою (стаття 227-1).

Незважаючи на доволі однотипні законодавства Республіки Казахстан та Азербайджану, норми щодо встановлення кримінальної відповідальності за кримінальні правопорушення в кіберпросторі не виділені в окремий розділ, а розміщуються в главі 7 кодексу «Кримінальні правопорушення у сфері економічної діяльності» [475].

На нашу думку, не можна не звернути увагу на досвід Естонії в питаннях регулювання встановлення кримінальної відповідальності за вчинення кримінальних правопорушень шляхом використання

інформаційно-телекомунікаційних технологій, систем або мереж. Зазначимо, що в Кримінальному кодексі Естонії такі кримінальні правопорушення виділені в окремий розділ «Кримінальні правопорушення у сфері комп'ютерної інформації та оброблення даних». Цікавим є рішення законодавства Естонії щодо розміщення в зазначеному розділі такого кримінального правопорушення, як «комп'ютерне шахрайство», на відміну від більшості країн пострадянського простору, де спеціальний склад правопорушення «шахрайство» наведений у розділі «Кримінальні правопорушення проти власності». Загалом перелік кримінальних правопорушень, передбачених Кримінальним кодексом Естонії, доволі значний: 1) комп'ютерне шахрайство (стаття 268); 2) знищення комп'ютерної інформації або комп'ютерних програм (стаття 269); 3) комп'ютерний саботаж (стаття 270); 4) незаконне використання комп'ютерів, систем та мереж (стаття 271); 5) незаконне порушення або блокування зв'язку в комп'ютерній мережі (стаття 272); 6) протизаконне розповсюдження комп'ютерних вірусів (стаття 273); 7) незаконне передавання захисних паролів до комп'ютера (стаття 273); 8) пред'явлення державним установам недостовірних цифрових даних (стаття 274); 9) незаконна видача даних із державного або муніципального банку даних (стаття 275) [111].

Варто зауважити, що особливій кримінально-правовій охороні піддаються відносини у сфері захисту об'єктів державної інформаційно-телекомунікаційної структури, але на відміну від більшості країн такі відносини не закріплені в рамках окремого розділу, який визначав би кримінальну відповідальність за кримінальні правопорушення проти основ національної безпеки. Кримінальне законодавство Естонії пішло шляхом виділення підвищеної охорони та, як результат, суворішого покарання в рамках кваліфікаційних ознак. Зокрема, до кваліфікаційних ознак кримінальних правопорушень, що вчиняються шляхом використання

інформаційно-телекомунікаційних технологій, систем і мереж, належать: 1) вчинення дій, передбачених відповідною статтею Кримінального кодексу Естонії та спрямованих на державні цифрові регістри; 2) вчинення дій, передбачених відповідною статтею Кримінального кодексу Естонії й спрямованих на створення перебоїв у функціонуванні державних установ; 3) вчинення дій, передбачених відповідною статтею Кримінального кодексу Естонії, щодо інформації, яка має характер державної таємниці чи таємниці національного характеру; 4) вчинення дій, передбачених відповідною статтею Кримінального кодексу Естонії, з метою розповсюдження шкідливого програмного коду в державних інформаційно-телекомунікаційних системах і мережах.

Завершуючи аналіз установлення кримінальної відповідальності за кримінальні правопорушення в кіберпросторі, хочемо в рамках порівняльної таблиці 6 визначити окремі позитивні аспекти й можливості їх імплементації в кримінальний закон України.

Таблиця 6 – Можливості запровадження позитивного досвіду зарубіжних країн щодо встановлення кримінальної відповідальності за кримінальні правопорушення в кіберпросторі

Країна	**Позитивний досвід**	**Можливості та шляхи впровадження в кримінальний закон України**
1	**2**	**3**
Естонія	Підвищена кримінально-правова охорона об’єктів і суспільних відносин у рамках державної діяльності в кіберпросторі	На нашу думку, визначення в рамках кваліфікаційних ознак до статей розділу XVI Особливої частини Кримінального кодексу України відносин, які складаються в інформаційному, цифровому державному секторі, пропонуємо в рамках статтей: 1) 361 – закріпити «дії, передбачені частинами 1–3, якщо вони вчиненні щодо державної інформаційно-телекомунікаційної технології, системи чи мережі»;

Продовження таблиці 6

1	2	3
		2) 361-1 – «дії, передбачені частинами 1–2, шляхом розповсюдження шкідливого програмного коду в державну інформаційно-телекомунікаційну технологію, систему або мережу»; 3) 362-2 – «дії, передбачені частинами 1–2, щодо інформації, яка містить державну, військову таємницю»; 4) 363-1 – «дії, передбачені частинами 1–2, спрямовані на порушення функціонування роботи інформаційно-телекомунікаційної технології, системи або мережі державного значення»
Сполучені Штати Америки	Криміналізація в рамках кримінального законодавства Сполучених Штатів Америки суспільно небезпечного діяння у формі «несанкціонованого одержання цифрової інформації»	Ураховуючи фактичну прогалину в частині 1 статті 361 Особливої частини Кримінального кодексу України щодо відсутності формулювання зазначених дій, вважаємо за необхідне закріпити в рамках частини 1 статті 361 Особливої частини Кримінального кодексу України «несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж, якщо вони спричинили наслідки у формі витоку цифрової інформації», одночасно виключити з частини 3 статті 361 Особливої частини Кримінального кодексу України «наслідки у формі витоку інформації». Водночас пропонуємо в примітці до цієї статті визначити поняття «витік цифрової інформації». Також вважаємо потрібним навести форми витоку цифрової інформації, зокрема ознайомлення, читання

Продовження таблиці 6

1	2	3
Данія	Визначення складу кримінального правопорушення «комп'ютерне шахрайство» як незаконної зміни, доповнення або видалення цифрової інформації чи програмного коду, використовуваних для цифрової автоматизованої оброблення даних, із метою одержання для себе або третіх осіб незаконної вигоди	Проблеми кваліфікації відповідно до частини 3 статті 190 Особливої частини Кримінального кодексу України викликають потребу правильного формулювання й тлумачення суспільно небезпечних дій у формі незаконних операцій із використанням електронно-обчислювальної техніки. Формулювання, запропоноване кримінальним законодавством Данііневілює всі питання, пов'язані, по-перше, зі способом вчинення кримінального правопорушення, по-друге, з матеріальним складом предмета кримінального правопорушення і, по-третє, додаткову кваліфікацію за відповідною статтею розділу XVI Особливої частини Кримінального кодексу України

З урахуванням проведеного аналізу можна зробити висновок, що законодавство з правового регулювання відповідальності за вчинення кримінальних правопорушень шляхом використання інформаційно-телекомунікаційних технологій, систем та мереж у різних країнах розвивається по-різному.

Країни, що належать до англо-саксонської правової сім'ї, крім нормативного регулювання, широко застосовують систему судових прецедентів. Правова регламентація встановлення 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 дуже 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 в 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 шляхом використання інформаційно-телекомунікаційних технологій, систем та мереж, виділені в окремий розділ.

ВИСНОВОК

У результаті проведення комплексного дослідження ми дали кримінально-правову оцінку кримінальним правопорушенням, що вчиняються в кіберпросторі, та зробили свої висновки щодо стану чинного законодавства, спрямованого на встановлення кримінальної відповідальності за вчинення суспільно небезпечних діянь у кіберпросторі. У нашому досліджені було сформовано низку пропозицій щодо вдосконалення чинного законодавства щодо кримінально-правової охорони кіберпростору й запропоновано практичні рекомендації щодо реалізації виокремлених нами змін.

На основі дослідження ми дійшли до таких висновків.

1. Запропоновано виділяти шість етапів становлення кримінальної відповідальності на теренах України, зокрема: 1) початковий (характеризується правовим вакуумом у регулюванні кримінально-правової охорони кіберпростору з безкарністю кримінальних правопорушень у ньому); 2) зародження (ухвалення Кримінального кодексу України, який визначав три види кримінально караних діянь у кіберпросторі та активне використання зловмисниками у своїй кримінально протиправній діяльності різноманітних IRC-клієнтів для вчинення шахрайств у кіберпросторі); 3) імплементаційний (ратифікація Україною Конвенції про кіберзлочинність, що визначала 23 кримінальні правопорушення в кіберпросторі та фактичну імплементацію частини норм Конвенції про кіберзлочинність у законодавство України); 4) економічний (характеризується появою віртуальних валют і розвитком економічних кримінальних правопорушень у кіберпросторі); 5) нормотворчий (створення спеціалізованого правоохоронного – органу Департаменту кіберполіції Національної Поліції України, ухвалення Закону України «Про основні засади забезпечення кібербезпеки України»); 6) сучасний

(карантинні обмеження, спричинені пандемією COVID – 19, та збройна агресія Російської Федерації дали новий поштовх у розвитку кримінально протиправних діянь у кіберпросторі, зокрема з'явилися нові види кримінальних правопорушень у ньому, а їх кількість стрімко збільшується).

2. Визначено, що поняття «кіберпростір» ширше за поняття «інтернет-простір», але вужче від «інформаційного» та «віртуального простору» та фактично є його частиною. Ми пропонуємо розглядати кіберпростір у трьох аспектах: філософському, легальному й доктринальному. У доктринальному аспекті кіберпростір може розглядатися в інформаційному (кіберпростір – це система функціонування децентралізованих інформаційних потоків, створена на основі інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем, учасники якої створюють, розповсюджують, зберігають інформацію), віртуальному (кіберпростір – це віртуальний простір, який виникає в результаті взаємодії користувачів мережевих технологій) і соціальному (кіберпростір – це соціальний феномен, наповнений людьми, проєкції яких породжені текстовими символами, які взаємодіють між собою у віртуальному середовищі шляхом спроб конструювання цифрової особистості) аспектах. Основними характеристикиками кіберпростору є такі: віртуальна складова, мережева належність, середовище взаємодії, динамічність, комунікативність, поєднання територіалізації та детеритиоріалізації. Основні принципи, що забезпечують стабільність функціонування кіберпростору: принцип своєчасного втручання, принцип дотримання прав і свобод людини й громадянина, принцип дисципліни, принцип відповідальності.

3. Наголошено, що використання інформаційно-телекомунікаційних технологій, систем та мереж під час вчинення кримінальних правопорушень є різновидом суспільно небезпечної й протиправної діяльності, що в сучасних умовах має тенденцію до збільшення як у рамках

національних масштабів, так і в глобальному плані. Кримінальним правопорушенням у кіберпросторі характерні специфічні ознаки, що роблять його більш суспільно небезпечним серед інших суспільно небезпечних діянь, зокрема високий рівень латентності, транснанціональність, дистанційність, кваліфікація осіб, які вчиняють кримінальні правопорушення цього виду.

4. Було визначено, що категорійний апарат, використовуваний для характеризування зазначених кримінальних правопорушень, є застарілим, тому виникає нагальна потреба в його зведенні відповідно до сучасних тенденцій науки та техніки. Зокрема, на нашу думку, термін «електронно-обчислювальна машина (комп'ютер)» повністю не відображає весь спектр засобів, використовуваних особами, які вчиняють кримінальні правопорушення в кіберпросторі. Зважаючи на це, ми пропонуємо термін «цифровий пристрій». Крім того, вважаємо необхідним розглядати поняття «інформаційні (автоматизовані), електронні комунікаційні, інформаційно-комунікаційні системи, електронні комунікаційні мережі» комплексно й у сукупності як «інформаційно-телекомунікаційні технології, системи та мережі».

5. Основна характеристика кримінальних правопорушень у кіберпросторі була здійснена на основі їх типологізаційних ознак, а саме: за сутністю кримінальних правопорушень у кіберпросторі. У рамках цієї ознаки ми виділили кіберзалежні й кіберутворювальні кримінальні правопорушення.

6. Детально проаналізовані елементи складів кримінальних правопорушень, передбачених розділом XVI Особливої частини Кримінального кодексу України. Визначено, що більшість кримінальних правопорушень цього типу є предикатними. На основі аналізу судової практики виявлені проблеми, що виникають під час кваліфікації окремих кримінальних правопорушень цієї групи. Розглянуті найпоширеніші типи

шкідливого програмного забезпечення, зокрема: 1) віруси; 2) комп'ютерні хробаки; 3) бекдор (backdoor); 4) викрадач інформації (stealer); 5) руткіт (rootkit); 6) залякувальне програмне забезпечення (scareware); 7) кілогер (keylogger); 8) вірус-вимагач (ransomware); 9) кліпери (clippers); 10) майнери (miners).

7. Запропоновано дематеріалізувати предмет кримінального правопорушення, передбаченого статтею 185 Особливої частини Кримінального кодексу України, та одночасне запровадження спеціального складу крадіжки, а саме: крадіжки у сфері обігу безготівкових або електронних грошей та віртуальних активів. У статті 189 Особливої частини Кримінального кодексу України запропоновано ввести кваліфікаційну ознаку «погроза блокування, видалення, знищення, модифікації або іншого несанкціонованого втручання в роботу інформаційно-телекомунікаційних технологій, систем та мереж, що може завдати шкоди правам та інтересам потерпілої особи».

8. Досліджено основні міжнародні нормативні акти у сфері встановлення відповідальності за кримінальні правопорушення в кіберпросторі. На основі аналізу визначено, що фактично Конвенція «Про кіберзлочинність» була базисом для становлення кримінальної відповідальності за суспільно небезпечні діяння, вчинені в кіберпросторі. Установлено, що Україна як держава – учасниця Конвенції «Про кіберзлочинність» повністю імплементувала в національне законодавство норми, визначені Конвенцією, але водночас на інформаційно-телекомунікаційних технологіях як знарядді вчинення кіберутворювальних кримінальних правопорушень у чинному Кримінальному кодексі України не наголошено.

9. Проведено аналіз законодавства зарубіжних країн щодо встановлення кримінальної відповідальності за кримінальні правопорушення в кіберпросторі. З урахуванням проведеного аналізу

можна зробити висновок, що законодавство з правового регулювання відповідальності за вчинення кримінальних правопорушень шляхом використання інформаційно-телекомунікаційних технологій, систем та мереж у різних країнах розвивається по-різному.

10. Доведено, що відсутність єдиної міжнародної нормативної правової бази, істотні відмінності в національних законодавствах країн, об'єднаних ідеєю спільної боротьби з кримінальними правопорушеннями в кіберпросторі, та відсутність єдиного підходу до визначення понятійного апарату аналізованої сукупності суспільно небезпечних діянь суттєво ускладнюють ефективну протидію використанню інформаційно-телекомунікаційних технологій, систем і мереж під час скоєння кримінальних правопорушень.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Encyclopedia Britannica. Phreaking. URL: https://www.britannica.com/topic/phreaking.

2. Дзюндзюк В. Б. Поява і розвиток кіберзлочинності. *Державне будівництво.* 2013. № 1. URL: http://nbuv.gov.ua/UJRN/DeBu_2013_1_3.

3. Кушнерьов О. С. Безпека інформації : конспект лекцій. Сумський державний університет, 2021. URL: https://essuir.sumdu.edu.ua/bitstream-download/123456789/85989/3/Kushnerov.pdf;jsessionid=A1C640C968B01096CBBB800BC0B30DD1.

4. Cohen F. Computer Viruses: Theory and Experiments. *Computers & Security*. 1987. № 6. С. 22–35. https://doi.org/10.1016/0167-4048(87)90122-2.

5. Computer Fraud and Abuse Act of 1986. URL: http://www.wipo.int/wipolex/ru/text.jsp?file_id=179619.

6. James A. Lewis. Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats. Center for Strategic and International Studies. URL: https://www.researchgate.net/publication/245508226_Assessing_the_Risks_of_Cyber_Terrorism_Cyber_War_and_Other_Cyber_Threats.

7. Krapp P. Terror and Play, or What Was Hacktivism?. *The MIT Press Journals.* URL: https://clck.ru/K5gJj.

8. Корченко О. Г. Кібертероризм, комп’ютерний тероризм. *Енциклопедія Сучасної України*. НАН України, НТШ. Київ : Інститут енциклопедичних досліджень НАН України. 2013. URL: https://esu.com.ua/article-6747.

9. Habr. Делаем deface сайта с помощью XSS : вебсайт. URL: https://habr.com/ru/post/328276/.

10. PricewaterhouseCoopers : вебсайт URL: http://surl.li/ibsdf.

11. Кравцова М. О. Сучасний стан і напрями протидії кіберзлочинності в Україні. *Вісник Кримінологічної асоціації України*. 2018. № 2 (19). С. 155–166.

12. На темной стороне Интернета: Что такое Dark Web и Deep Web?. *DGL.RU.* URL: https://clck.ru/K5gLD.

13. Ржевська Н. Ф. Кіберзлочинність як виклик державній інформаційній політиці : дипломна робота. 2020. С. 34–35. URL: https://er.nau.edu.ua/bitstream/NAU/42039/1/%D0%A5%D0%B0%D1%80%D0%B8%D0%BD_%D0%94%D0%B8%D0%BF%D0%BB%D0%BE%D0%BC.pdf.

14. Кримінальний кодекс України від 5.04.2001 р. № 2341-III ; ред. станом на 12.09.2020 р. *Відомості Верховної Ради України.* 2001. № 25–26. Ст. 131.

15. Біленчук П. Д., Зубань М. А. Комп'ютерні злочини: соціально-правові та кримінолого-криміналістичні аспекти. Українська академія внутрішніх справ, 1994. С. 6. URL: http://surl.li/ibsdk.

16. Батурин Ю. М., Жодзишский А. М. Компьютерная преступность и компьютерная безопасность. Юрид. лит-ра, 1991. 160 с. URL: http://lawlibrary.ru/izdanie14201.html.

17. Судова практика розгляду справ про злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), автоматизованих систем та комп'ютерних мереж і мереж електрозв'язку. *Офіційний вебсайт Верховного суду України.* URL: https://www.viaduk.net/clients/vsu/vsu.nsf/(documents)/AFB1E90622E4446FC2257B7C00499C02.

18. Конвенція Ради Європи «Про кіберзлочинність» від 21.11.2001 р. URL: http://zakon.rada.gov.ua/laws/show/994_575.

19. Пушкаренко П. І. Кіберзлочинність як новітній феномен тіньової економіки. URL: https://clck.ru/K5g9r.

20. Кіберзахист, що рятує: як нам посилити опір агресії Росії. *Економічна правда* : вебсайт. URL: https://www.epravda.com.ua/columns/2017/06/1/625543/.

21. Русецький В. І. Теоретико-правовий аналіз понять «кіберзлочин» і «кіберзлочинність». *Право і безпека*. 2017. № 1 (64). С. 74–78.

22. Що таке фішинг?. *Вікіпедія* : вебсайт. URL: https://uk.wikipedia.org/wiki/Фішинг.

23. Большинство киберпреступлений в Беларуси – это кража денег с банковских карт. *Минск новости* : веб-сайт. URL: https://minsknews.by/bolshinstvo- kiberprestupleniy-v-belarusi-eto-krazha-deneg-s-bankovskih-kart/.

24. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 р. № 2163 VIII. URL: http://surl.li/ajfjh.

25. Бохенко В. М. Кримінологічні ризики обігу криптовалют. *Юридичний науковий електронний журнал.* № 12/2021. С. 327. DOI: https://doi.org/10.32782/2524-0374/2021-12/82.

26. За останні роки в Україні зросли кіберзлочини. *Дивись Інфо* : вебсайт. URL: https://dyvys.info/2020/09/25/za-ostanni-roky-v-ukrayini-zrosly-kiberzlochyny/.

27. Маклюэн М. Понимание медиа: внешние расширения человека. 2003. С. 400. URL: http://surl.li/avaiz.

28. Півняк Г. Г., Бусигін Б. С., Дівізінюк М. М. *Тлумачний словник з інформатики.* Дніпро : Нац. гірнич. ун-т, 2010. 600 с. URL: http://www.programmer.dp.ua/download/tlumachniy-slovnik-z-informatiki.pdf.

29. Дубняк К. А. Інформаційний простір: структура та функціональні параметри. 2015. № 4 (24). С. 21–24. (Серія: Соціальні комунікації).

30. Дубас О. П. Інформаційно-комунікаційний простір: поняття, сутність, структура. URL: http://dspace.nbuv.gov.ua/bitstream/handle/123456789/26693/22-Dubas.pdf.

31. Семенов А. Захист національного інформаційного простору Великої Британії. *Матеріали міжнародної конференції «Політична праксеологія: безпека, технології, комунікації»* / за ред. В. Бебика. Київ : ВАПН, 2016. 117 с.

32. Біловус Л. Український інформаційний простір: сьогодення та перспективи. URL: http://ijimv.knukim.edu.ua/zbirnyk/1_1/bilovus_l_i_ukrayinskyy_informatsiynyy_prostir.pdf.

33. Тлумачний словник он-лайн. URL: https://ua.opentran.net/dictionary/D0%B2%D1%96%D1%80%D1%82%D1%83%D0%B0%D0%BB%D1%8C%D0%BD%D0%B8%D0%B9.html.

34. Носов Н. А. Виртуальный человек : очерки по виртуальной психологии детства. РАН, Ин-т человека. Минск : Магистр, 1997. 192 с.

35. Алексєєва О. Р. Інтернет-простір та медіазасоби як чинники впливу на процеси соціалізації й соціального виховання особистості. *Вісник ЛНУ імені Тараса Шевченка*. 2015. № 2 (291). С. 8. URL: http://dspace.luguniv.edu.ua/xmlui/bitstream/handle/123456789/589/Alekseeva.pdf?sequence=1&isAllowed=y.

36. Lukin S. Modern aspects of digitalization of public spaces. *Public Administration Aspects.* 2020. № 8 (1 SI). P. 9193. URL: https://doi.org/10.15421/152049.

37. Терешкун. О., Ілюшкін О. Соціальні мережі у сучасному суспільстві: психологічний аналіз. *Соціальна психологія* : український науковий журнал. 2011. № 5. С. 86–95.

38. Лазаренко Н. Л. Комунікація в інтернет-просторі: психологічний аспект. *Information Technologies and Learning Tools*. 2018. DOI: 10.33407/itlt.v65i3.2036.

39. Uche Mbanaso. The Cyberspace: Redefining A New World. Developing Cyber Warfare Capability and Capacity in AfricaBi-Annual Cyber

Abuja Conference Centre for Cyber Space Studies. 2015. DOI: 10.9790/0661-17361724.

40. Богач О. В. Кіберпростір і перспектива соціалізації особистості старшокласників. *Психологічні перспективи. Спеціальний випуск: Проблеми кібераґресії.* Київ : Інститут соціальної та політичної психології НАПН України. 2012. Т. 1. С. 158–167.

41. Oxford dictionary of English. Oxford. URL: https://www.oxfordreference.com/display/10.1093/acref/9780199571123.001.0001/acref9780199571123;jsessionid=3230C69E7D1037479D75F4779A2A3CED.

42. Колодюк О. В. Національні стратегії інформаційного суспільства: необхідність, переваги та стан щодо запровадження в Україні. *Информационное общество : вебсайт.* URL: http: //www.isu.org.ua/viewarticale/publications/117?new_lang=u.

43. Винер Н. Кибернетика, или управление и связь в животном и машине. Москва, 1983. 412 с.

44. Lewis A. J. Securing Cyberspace for the 44th Presidency. *Centre for Strategic and International Studies*. 2008. URL: http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44 .pdf.

45. Gibson W. Burning. Chrome. Omni, 1982. URL: http://www.williamflew.com/omni46b.html.

46. Gibson W. Neuromancer. New York, 1984.

47. Barlow J. P. A Declaration of the Independence of Cyberspace. URL: https://www.eff.org/cyberspace-independence.

48. National Military Strategy for Cyberspace Operations. *Department of Defense.* URL: http://www.dod.gov/pubs/foi/ojcs/07-F-2105doc1.pdf.

49. National Security Strategy. White House. URL: https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/national_security_strategy.pdf.

50. Liepman M. James. Cyberspace: The Third Domain. *Homeland security digital library.* URL: https://www.hsdl.org/?view&doc=89385&coll=public.

51. The Comprehensive National Cybersecurity Initiative. URL: https://obamawhitehouse.archives.gov/sites/default/files/cybersecurity.pdf.

52. National security presidential directive – 54 / White House. URL: https://irp.fas.org/offdocs/nspd/nspd-54.pdf.

53. National security presidential directive – 23 / White House. URL: https://irp.fas.org/offdocs/nspd/nspd-54.pdf.

54. Computer Security Act of 1987. H.R.145. URL: https://www.congress.gov/bill/100th-congress/house-bill/145.

55. Janet Reno. Attorney general of the united states, et al., appellants v. american civil liberties union et al. *Supreme court of the united states.* URL: https://www.ciec.org/SC_appeal/opinion.shtml.

56. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 р. № 2163VIII. *Верховна Рада України* : офіційний вебсайт. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text.

57. John Suler. Department of Psychology. Lawrenceville : Rider University. URL: http://users.rider.edu/~suler/psycyber/suler.html.

58. Чепелевой Н. В. Проблемы психологической герменевтики : монография / под ред. Н. В. Чепелевой. – Киев : Изд-во Национального педагогического университета им. Н. П. Драгоманова, 2009. 382 с.

59. Katsh E. Law in a Digital World: Computer Networks and Cyberspace. *Villanova Law Review.* 1993. Vol. 38, Iss 2. P. 403–486.

60. Beer Sijpesteijn. Describing Cyberspace. URL: https://www.academia.edu/8234339/Describing_Cyberspace.

61. Thackrah J. R. Dictionary of Terrorism. *Taylor & Francis.* 2004. 318 p.

62. Woolley P. Defining Cyberspace as a United States Air Force Mission. *Air Force Institute of technology*. URL: http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA453972& Location=U2&doc=GetTRDoc.pdf.

63. Kramer F. D. Cyberpower and National Security : Policy Recommendations for a Strategic Cyberpower and National Security. Washington D. C. : *National Defense University Press*. 2009. URL: https://ndupress.ndu.edu/Portals/68/Documents/Books/CTBSPExports/Cyberpower/Cyberpower-I-Chap-01.pdf?ver=2017-06-16-115055-617.

64. Гахов С. О. Кіберпростір як основна категорія науки кібернетика. *Сучасний захист інформації.* 2017. № 1. С. 53–57. URL: http://nbuv.gov.ua/UJRN/szi_2017_1_11.

65. K. Darbik. Cyberspace in a risk society. 2022. DOI: 10.35467/cal/151808.

66. Рибка С. В. Кіберпростір, управління інфраструктурою, кібербезпека. *Стратегічна панорама.* 2015. № 1. С. 126–134. URL: http://nbuv.gov.ua/UJRN/Stpa_2015_1_17.

67. Дубов Д. В. Кіберпростір як новий вимір геополітичного суперництва : монографія. Київ : НІСД, 2014. 328 с.

68. Wasilewski J. Zarys definicyjny cyberprzestrzeni. *Przegląd Bezpieczeństwa Wewnętrznego*. 2013. № 9. P. 227.

69. Гавловський В. Інформаційна безпека: захист інформації в автоматизованих системах (організаційно-правовий аспект). *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні.* Київ : 2000. С. 50–53.

70. Голубєв В. О. Боротьба з комп'ютерними злочинами – проблема транснаціонального масштабу. URL: http://surl.li/ibsgb.

71. Warf B. Borders in Cyberspace. *Invisible Borders in a Bordered World*. DOI: 10.4324/9780429352515-15.

72. Хилдрет С. А. Кибертерроризм и кибервойна. *Материалы Исследовательской службы Конгресса. Доклад Исследовательской службы Конгресса.* URL: http://www.infousa.ru/information/bt-1028.htm.

73. Фурашев В. М. Кіберпростір та інформаційний простір, кібербезпека та інформаційна безпека: сутність, визначення, відмінності. *Інформація і право*. 2012. № 2 (5). С. 163–164. URL: http://surl.li/ibsgf.

74. Бурячок В. Л. Інформаційна та кібербезпека: соціотехнічний аспект : підручник / за заг. ред. В. Б. Толубка. Київ : ДУТ. 2015. 288 с.

75. Гнатюк С. О. Кібертероризм: історія розвитку, сучасні тенденції та контрзаходи. *Безпека інформації*. 2013. Т. 19. № 2. С. 118–129.

76. Targowski A. The Evolution of Cyberspace. *IRMA International Conference, IT Management and OrganizationalInnovations*. 1996. P. 333–338. URL: https://www.academia.edu/17334683/The_Cyberspace_Redefining_A_New_World.

77. Манжай О. Використання кіберпростору в оперативно-розшуковій діяльності. *Special investigation activity systems of the world, particularly cybercrime fighting systems.* URL: http://surl.li/hyvnn.

78. Поняття і характеристика кіберпростору. URL: http://www.elbib.in.ua/ponyattya-i-harakteristika-kiberprostoru-sotsiologiya-internetu.html.

79. Мягка М. М. Кіберпростір у вимірі комунікативного впливу. *Науковий вісник Міжнародного гуманітарного університету.* 2017. № 30 (2). С. 141–142. URL: http://surl.li/hyvqw. (Серія: Філологія).

80. Самойленко О. А. Природа кіберпростору як об’єкта криміналістичного дослідження. *Криміналістика і судова експертиза.* 2018. № 63 (1). С. 174–184. URL: http://nbuv.gov.ua/UJRN/krise_2018_63(1)__21.

81. Stevens B. Cyberspace and the state: towards a strategy for cyberpower. Abington : Routledge. URL: http://surl.li/hyvsf.

82. Kohl U. Jurisdiction in cyberspace. *Research handbook on international law and cyberspace* / ed. by N. Tsagourias, R. Buchan. Cheltenham ; Northampton : Edward Elgar publ., 2015. P. 49–51.

83. Official Documents System of the United Nations. URL: http://surl.li/hyvue.

84. Швиданенко Г. Диджиталізація – сучасний напрямок розвитку інноваційного підприємництва. URL: https://core.ac.uk/download/pdf/197269051.pdf.

85. Офіційний вебсайт Інтерполу. URL: https://www.interpol.int/News-and-Events.

86. Шемчук В. В. Кіберзлочинність як перешкода розвитку інформаційного суспільства в Україні. *Вчені записки ТНУ ім. В. І. Вернадського.* 2018. Том 29 (68). № 6. С. 121–123. URL: https://doi.org/10.32838/TNU-2707-0581/2018.6/21. (Серія: Юридичні науки).

87. Про рішення ради національної безпеки і оборони України : Указ Президента «Про хід реформування системи кримінальної юстиції та правоохоронних органів» від 15.02.2008 р. URL: https://zakon.rada.gov.ua/laws/show/311/2008#Text.

88. Макарчук Д. Поняття кримінально караного діяння у Конституціях України, Франції та ФРН. *Підприємництво, господарство і право.* 2019. № 5. С. 244–249.

89. Конвенція про захист прав людини і основоположних свобод від 04.11.1950 р. *Офіційний вісник України*. 1998. № 13. С. 270–302.

90. Конституція України станом на 01.01.2023 р. / Верховна Рада України. Харків : Право, 2020. 82 с.

91. Крайник Г. С. Поняття та ознаки злочину за кримінальним законодавством України. *Молодий вчений*. 2016. № 11 (38). С. 309–312. URL: http://molodyvcheny.in.ua/files/journal/2016/11/72.pdf.

92. Українське Кримінальне право : підручник. URL: https://pidru4niki.com/1705100856179/pravo/zlochin_diyannya.

93. Філей Ю. В. Соціальна сутність суспільної небезпеки. *Кримінальне право: традиції та новації* : матеріали міжнародного круглого столу, присвяченого 90-літтю з дня народження видатного вченого, героя України, академіка В. В. Сташиса (Полтава, 9–10 липня 2015 р.). Харків, 2015. С. 98–103.

94. Ghelerter D. Cybercrime in the Developing World. *KSU conference on cybersecurity education, research and practice – 2022*. DOI: 10.32727/28.2023.10.

95. Волонець Д. Ф. Суб'єктивна сторона кримінальних правопорушень, передбачених статтями 366-2, 366-3 КК України. *Держава та регіони*. 2021. № 3 (73). С. 115–117. URL: http://surl.li/hywcd.

96. Шульга А. М. Теоретичні проблеми визначення та практичне застосування поняття злочину проти земельних ресурсів України. *Юридичний науковий електронний журнал.* 2020. № 1 С. 235–237. DOI: https://doi.org/10.32782/2524-0374/2020-1/56.

97. Литвинова О. М. *Кримінальне право України. Загальна частина* : підручник / за заг. ред. О. М. Литвинова. Харків : Нац. ун-т внутр. справ, 2020. 428 с.

98. Фріс П. Л. Кримінальне право України. Загальна частина : підручник. Київ : Атіка, 2004. 488с.

99. Пащенко О. О. Закон про кримінальну відповідальність та кримінально-правові норми: питання соціальної обумовленості. *Вісник Луганського державного університету внутрішніх справ ім. Е. О. Дідоренка*. 2017. № 4 (80). С. 104–111. URL: http://surl.li/hywln.

100. Войтко Б. С. Соціальна інженерія як інструмент для проникнення в інформаційну систему підприємства : збірник тез

доповідей (Секція: Прикладні аспекти використання інформаційних систем і технологій). URL: https://jait.donnu.edu.ua/article/view/9023.

101. David Wall. Particularly confusing is the tendency to regard almost any offence that involves a computer as a ‘cybercrime. *The centre for crime and justice studies.* 2004. № 58. P. 20. ULR: http://surl.li/hywnr.

102. Офіційний вебсайт Массачусетського Технологічного Університету. URL: https://news.mit.edu/.

103. Lyadskiy V. V. Crimes in the field of computer information. *Electronic Bulletin of the Rostov Socio-Economic Institute.* 2014. № 6. P. 122 URL: https://cyberleninka.ru/article/n/prestupleniya-v-sfere-kompyuternoy-informatsii.

104. Неділько Я. В. Поняття кіберзлочинів та їх види. *Науковий часопис Національної академії прокуратури України.* 2018. № 4. С. 49–58. ULR: http://www.chasopysnapu.gp.gov.ua/chasopys/ua/pdf/4-2018/nedilko.pdf.

105. Кримінальний кодекс Індії від 06.10.1862 р. URL: https://wipolex.wipo.int/ru/legislation/details/7668.

106. Armenia Criminal Code. URL: http://surl.li/hywpq.

107. Criminal code of Georgia. URL: http://surl.li/hywqc.

108. Criminal Code of the Azerbaijan Republic. URL: http://surl.li/hywqq.

109. Criminal code of Turkmenistan. URL: http://surl.li/hzdpi.

110. Estonia Penal Code. URL: http://surl.li/hyxak.

111. Latvia Criminal Code. URL: http://surl.li/hyxax.

112. Criminal code of the Republic of Tajikistan. URL: https://cis-legislation.com/document.fwx?rgn=2324.

113. Austria Criminal Code. URL: http://surl.li/hzcez.

114. Germany Criminal Code. URL: https://www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html.

115. Portugal Criminal Code. URL: http://surl.li/hzcuq.

116. Spain Criminal Code. URL: http://surl.li/hzdvw.

117. Fraud and related activity in connection with computers. *18 U.S. Code № 1030*. URL: http://surl.li/hzdwf.

118. UK Public General Acts. *Computer Misuse Act 1990*. URL: https://www.legislation.gov.uk/ukpga/1990/18/contents.

119. Азаров Д. В. Злочини у сфері комп'ютерної інформації: кримінально-правове дослідження : монографія. Київ : *Атіка*, 2007. С. 304.

120. Карчевский Н. В. Киберпреступление или преступление в сфере использования информационных технологий? *Кібербезпека в Україні: правові та організаційні питання :* матеріали Всеукр. наук.-практ. конф. Одеса : ОДУВС, 2016. С. 10–15.

121. Васильковський І. І. Поняття, класифікація та характеристика окремих видів кіберзлочинів. *Прикарпатський юридичний вісник*. 2017. Вип. 1 (16), том 2. С. 196–201.

122. Ставер А. В. Загальні вразливості банківських карт і способи їх усунення. *Протидія кіберзлочинності в фінансово-банківській сфері* : матеріали Всеукр. наук.-практ. конф. Харків : ХНУВС, 2013. С. 144–147.

123. Простосердов М. А. Проблемы квалификации компьютерных преступлений. *Российское правосудие*. 2012. № 6 (74). С. 106–108.

124. Амелін О. В. Визначення кіберзлочинів у національному законодавстві. *Науковий часопис Національної академії прокуратури України*. 2016. № 3. С. 1–10.

125. Буз С. И. Киберпреступления: понятие, сущность и общая характеристика. *Юристъ – Правоведъ*. 2019. № 4 (91). С. 78–82.

126. German hospital hacked, patient taken to another city dies. *AP NEWS* : вебсайт. URL: https://apnews.com/article/technology-hacking-europe-cf8f8eee1adcec69bcc864f2c4308c94

127. Mohamed A., Geir M. K. Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks. *Journal of CyberSecurity*. 2015. № 4. P. 65–88.

128. Болгов В. М., Гадіон Н. М., Гладун О. З. Організаційно-правове забезпечення протидії кримінальним правопорушенням, що вчиняються з використанням інформаційних технологій : наук.-практ. посіб. Київ : Національна академія прокуратури України. 2015. С. 202.

129. Вехов В. Б. Криминалистическая характеристика и совершенствование практики расследования и предупреждения преступлений, совершаемых с использованием компьютерной техники : автореф. дисс. ... канд. юрид. наук. Волгоград, 2012. С. 13–33

130. Довженко О. Поняття кіберзлочину з криміналістичної позиції. *Трибуна молодого вченого* : юридичний вісник. 2018. № 3. С 79–83.

131. Бєлєнький В. Відповідальність за кіберзлочини за кримінальним правом США, Великобританії та України : автореф. дис. … канд. юрид. наук : 12.00.08. Київ. 2016. 19 с.

132. Sabillon R. Cybercrime and Cybercriminals: A Comprehensive Study. *International Journal of Computer Networks and Communications Security*. URL: https://www.researchgate.net/publication/304822458_Cybercrime_and_Cybercriminals_A_Comprehensive_Study.

133. Бельський Ю. Щодо визначення поняття кіберзлочину. *Юридичний вісник.* 2014. № 6. С. 414–418.

134. Васильковський І. І. Поняття «кіберзлочинність» та «кіберзлочини»: стан та співвідношення. *Міжнародний юридичний вісник: актуальні проблеми сучасності (теорія та практика).* 2018. № 1. С. 276– 282.

135. Савчук Н. В. Кіберзлочинність: зміст та методи боротьби. *Теоретичні та прикладні питання економіки* : зб. наук. праць. Київ : Видавничо-поліграфічний центр «Київський університет», 2009. Вип. 19. С. 338–342.

136. Тарасюк К. В. Прокурорський нагляд при розслідуванні комп'ютерних злочинів. *Комп'ютерно інтегровані технології: освіта, наука, виробництво.* 2012. № 10. С. 178–181.

137. Тропина Т. Л. Киберпреступность: понятие, состояние, уголовноправовые меры борьбы : дисс. ... канд. юрид. наук : 12.00.08. Владивосток, 2005. 235 с.

138. Wall D. S. Cybercrime: The transformation of crime in the information age. Oxford : Polity. URL: http://surl.li/iamhw.

139. Словник термінів з кібербезпеки / за заг. ред. О. В. Копана, Є. Д. Скулиша. Київ : ВБ «АванпостПрим», 2012. 214 с.

140. Definition of Cyber Crime. *LawPage.* URL: https://lawpage.in/cyber_laws/crime/definition-of-cyber-crime.

141. Ahmmed F. Meaning and Nature of Cyber Crime. URL: https://www.academia.edu/41411512/Meaning_and_Nature_of_Cyber_Crime.

142. Користін О. Є. Протидія кіберзлочинності в Україні: правові та організаційні засади : навч. посіб. Київ : Скіф, 2012. 728 с.

143. Гаркуша Ю. Теоретико-правовий аналіз понять «кіберзлочин» і «кіберзлочинність». *Право і безпека*. 2017. № 1 (64). С. 74–78.

144. Сіренко О. В. Поняття кіберзлочинів та особливості методики їх розслідування. *Кібербезпека в Україні: правові та організаційні питання* : матер. ІІ Всеукр. наук.-практ. конф. Одеса : ОДУВС, 2017. С. 48–49.

145. A. Završnik. Cybercrime definitional challenges and criminological particularities. *Masaryk University Journal of Law and Technology*. P. 27. URL: https://core.ac.uk/download/pdf/230601102.pdf.

146. Столяр О. Міжнародно-правові проблеми визначення та класифікації «кіберзлочинів». *In: Jurnalul juridic national: teorie şi practică.* 2017. № 4 (26). С. 185–188.

147. Дуленко В. А., Мамлеев Р. Р., Пестриков В. А. Використання високих технологій в кримінальному середовищі. *Боротьба зі злочинами у сфері комп'ютерної інформації* : навч. допомога. Київ, 2007.

148. Чекунов І. Г. Сучасні кіберзагрози. Кримінально-правова та крімінологічна класифікація і кваліфікація кіберзлочинів. *Право і кібербезпека.* 2012. № 2. С. 9–22.

149. Курушин В. Д., Мінаєв В. А. Комп'ютерні злочини та інформаційна безпека. *Новий юрист*. 1998. С. 14–21.

150. Яцишин М. Ю. Використання сили у кіберпросторі в рамках міжнародного права. *Інформація і право*. 2018. № 4 (27). С. 22–31.

151. Адамова О. С. Поняття правової класифікації. *Часопис цивілістики.* 2015. № 18. С. 19–24.

152. Яковенко А. В. Типологізація правових систем: галузевий аспект. *Наука та суспільне життя України в епоху глобальних викликів людства у цифрову еру* : матеріали Міжнар. наук.-практ. конф. Одеса : Видавничий дім «Гельветика», 2021. Т. 2. С. 244–246.

153. Бондаренко О. С. Концепція кримінально-правової протидії корупції : монографія. Суми : Сумський державний університет. 2021. 472 с.

154. Люликова М. Protiv pravosudia. URL: https://www.academia.edu/24627410/Protiv_pravosudia_2015_1_.

155. Štitilis D. Kai kurie neteisėtos prieigos prie kompiuterinės informacijos kriminalizavimo aspektai. *Jurisprudencija*. 2003. № 47 (39). P. 61.

156. Антипов В. І., Антипов В. В. Пропорційність покарань та їх значення для класифікації злочинів. *Фіскальна політика: теоретичні та практичні аспекти юридичної науки* : зб. тез доповідей Міжнар. наук.-практ. конф. Вінниця : Нілан-ЛТД, 2017. С. 332–334.

157. Дудоров О. О. Поняття злочину. Класифікація злочинів. *Вісник Асоціації кримінального права України.* 2013. № 1 (1). С. 84–102.

158. Ахтырская Н. Цели, задачи, функции криминалистической классификации. *Уголовное право*. 2002. № 2. С. 88–89.

159. Хахановський В. Г. Тлумачення та класифікація кримінальних правопорушень як кіберзлочинів. *Інформація і право.* 2020. № 2. С. 99–104.

160. Кундеус В. Г. Поняття та види кіберзлочинів. *Держава і злочинність: нові виклики в епоху постмодерну*. 2020. № 4. С. 44–46.

161. Протидія кіберзлочинності в Україні: правові та організаційні засади : навч. Посіб / О. Є. Користін, В. М. Бутузов, В. В. Василевич та ін. Київ : Скіф, 2012. 728 с.

162. Міщук Н. Кіберзлочинність як загроза інформаційному суспільству. *Вісник Львівського університету*. 2014. № 51. С. 173–179. (Серія: Економічна).

163. Голіна В. В., Головкін Б. М. Кримінологія: Загальна та Особлива частини : навч. посіб. Харків : Право, 2014. 513 с.

164. Дзюндзюк В. Б., Дзюндзюк Б. В. Поява і розвиток кіберзлочинності. *Державне будівництво*. 2013. № 1. 12 с. URL: http://nbuv.gov.ua/j-pdf/DeBu_2013_1_3.pdf.

165. Rusetskyi A. A., Kutsolabskyi D. A. Theoretical and legal analysis of the concepts of «cybercrimes» and «cybercrime». *Pravo i Bezpeka*. №. 1. P. 74–78.

166. Bajaj S. Cyber fraud: a digital crime. *International Conference Information Systems* 2008. P. 147–153. URL: http://surl.li/iampj.

167. Singh S., Silakari S. A. Survey of Cyber Attack Detection Systems. *International Journal of Computer Science and Network Security*. Vol. 9, № 5. P. 1–10. URL: http://paper.ijcsns.org/07_book/200905/20090501.pdf.

168. Altowaijri S. Reducing Cybersecurity Risks in Cloud Computing Using A Distributed Key Mechanism. *International Journal of Computer Science and Network Security*. 2021. № 21 (9). URL: http://surl.li/iamqp.

169. Matveev V. Cybercrime in the Economic Space: Psychological Motivation and Semantic-Terminological Specifics. *International Journal of Computer Science and Network Security*. 2021. Vol. 21, № 11. URL: https://doi.org/10.22937/IJCSNS.2021.21.11.18.

170. Про національну безпеку України : Закон України від 21.06.2018 р. № 2469-VIII. *Верховна Рада України* : офіційний вебсайт. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text.

171. Про рішення Ради національної безпеки і оборони України : Указ Президента України від 14.05.2021 р. : Про Стратегію кібербезпеки України. URL: http://surl.li/iamtt.

172. Буряк М. В. Злочини проти основ національної безпеки України у політичній сфері. URL: http://surl.li/iamuj.

173. Polianskyi A., Polianskyi O. Criminal liability for crimes against national security. *Archives of Criminology and Forensic Sciences*. 2021. № 3. P. 72–88. https://doi.org/10.32353/acfs.3.2021.08.

174. Матвійчук В. К. Злочини проти основ національної безпеки: поняття та загальна характеристика. *Юридична наука*. 2013. № 9. С. 80–87. URL: http://surl.li/iamvq.

175. Служба безпеки затримала шпигунку ФСБ, яка намагалася проникнути в СБУ і стати «подвійним агентом». *Служба безпеки України* : вебсайт. URL: http://surl.li/iamwb.

176. Вирок Вінницького міського суду у справі № 127/13877/22. URL: https://reyestr.court.gov.ua/Review/105190434.

177. СБУ затримала агента РФ, який збирав дані для обстрілів на півдні Одещини. *Служба безпеки України* : вебсайт. URL: http://surl.li/iamxa.

178. Судовий Вирок у справі № 554/7741/22. ULR: https://reyestr. court.gov.ua/Review/106573069.

179. Служба безпеки України затримала адміністратора телеграм-каналу, який зняв та опублікував обстріл Брушниьскої ТЕС. *Одеса онлайн* : вебсайт. URL: https://odessa.online/sbu-zaderzhala-administratora-telegram-kanala-kotoryj-snyal-i-opublikoval-obstrel-burshtynskoj-tes/.

180. Українські діти можуть «здавати» окупантам позицій ЗСУ за грошову винагороду. *Судово-юридична газета* : вебсайт. URL: http://surl.li/iamyw.

181. Окупанти пропонують неповнолітнім за гроші здавати позиції ЗСУ. URL: http://surl.li/iamyw.

182. Ставер А. В. Загальні вразливості банківських карт і способи їх усунення. *Протидія кіберзлочинності в фінансово-банківській сфері* : матеріали Всеукр. наук.-практ. конф. Харків : ХНУВС, 2013. С. 144–147.

183. Клапків Л. М., Клапків Ю. М., Свірський В. С. Фінансові ризики в діяльності страхових компаній: теоретичні засади, сучасні реалії та прагматизм управління : монографія. Івано-Франківськ : Кушнір Г. М., 2020. 171 с.

184. Гавловський В. Д. Теоретичні засади відстеження деструктивних процесів у соціальних мережах. *Боротьба з організованою злочинністю і корупцією (теорія і практика)*. Київ : МНДЦ, 2012. № 1. 247–258.

185. Обережно! З’явилася нова шахрайська схема – виплата допомоги від НБУ. Дебет-кредит : вебсайт. URL: http://surl.li/ianaz.

186. Марков В. В. До питання щодо зарубіжного досвіду протидії кіберзлочинності. *Право і безпека*. 2015. № 2 (57). С. 107–113.

187. Науково-практичний коментар до розділу XVII Особливої частини Кримінального кодексу України. URL: https://ips.ligazakon.net/document/KK004886.

188. Шинкарецька Г. Г., Берман А. М. Цифровізація та проблема забезпечення національної безпеки. *Освіта і право*. 2020. № 5. С. 254–260.

189. Вікторія Л. В. Вина як кримінально-правова категорія та її вплив на кваліфікацію злочину. *Молодий вчений*. 2021. № 6 (94). С. 22–25.

190. Науково-практичний коментар до Кримінального кодексу України / за заг. ред. О. М. Джужі, А. В. Савченка, В. В. Чернєя. Київ : Юрінком Інтер, 2016. 1064 с.

191. Савченко А. В. Корупційні злочини (кримінально-правова характеристика) : навч. посіб. Київ : Центр учбової літератури, 2016. 168 с.

192. Абдул С. В., Андрусенко С. В. Злочини у сфері обігу наркотичних засобів, психотропних речовин, їх аналогів або прекурсорів: тактика проведення окремих слідчих (розшукових) та негласних слідчих (розшукових) дій : метод. рек. Одеса : ОДУВС, 2018. 100 с.

193. Шевчук Т. А. Розповсюдження наркотичних засобів, психотропних речовин або їх аналогів через мережу Інтернет. URL: http://surl.li/ianbv.

194. Про практику розгляду судами кримінальних справ про злочини, вчинені стійкими злочинними об'єднаннями. Постанова Пленуму Верховного Суду України № 13 від 23.12.2005 р. URL: http://surl.li/bvuha.

195. Правоохоронці викрили учасників двох злочинних організацій у привласненні 10 млн грн з банківських карток громадян. *Мультимедійна платформа іномовлення України* : вебсайт. URL: https://www.ukrinform.ua/rubric-society/3556513-sahrai-vikrali-z-bankivskih-kartok-10-miljoniv-obicauci-socviplati.html.

196. Додатковий протокол до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи, від 28.01.2003 р. URL: https://zakon.rada.gov.ua/laws/show/994_687#Text.

197. Чокас Ю. С. Кіберзлочини проти власності: кримінально-правова та кримінологічна характеристика. URL: http://surl.li/iandg.

198. Вирок Соснівського районого суду м. Черкаси у справі № 712/6176/20. ULR: https://reyestr.court.gov.ua/Review/92814657.

199. McGuire Dr. M., Dowling S. Cybercrime: A review of the evidence Summary of key findings and implications. *Home Office Research Report 75*. University of Surrey, 2013. P. 29–46.

200. Комп'ютерна злочинність : навчальний посібник / за ред. П. Д. Біленчук, Б. В. Романюк, В. С. Цимбалюк та ін. Київ : Атіка, 2012. 240 с.

201. Селюк А. В. Розслідування комп'ютерних злочинів : наук.-метод. посіб / за ред. А. В. Селюк. Київ : Вид-во НА СБУ, 2010. 24 с.

202. Дердюк Б. М. Поняття та теоретичні основи криміналістичної класифікації комп'ютерних злочинів. *Прикарпатський юридичний вісник.* Вип. 3, № 6. 2014. С. 225–233. URL: http://surl.li/ianij.

203. Про затвердження Правил охорони праці під час експлуатації електронно-обчислювальних машин : Наказ Міністерства праці та соціальної політики України Комітету по нагляду за охороною праці України від 10.02.1999 р. № 21. URL: http://surl.li/ianiu.

204. Про затвердження Вимог щодо безпеки та захисту здоров'я працівників під час роботи з екранними пристроями : Наказ Міністерства Соціальної політики України від 14.02.2018 р. № 207. URL: https://zakon. rada.gov.ua/laws/show/z0508-18#Text.

205. Про захист інформації в інформаційно-комунікаційних системах : Закон України від 05.07.1994 р. № 80/94-ВР. URL: https://zakon.rada. gov.ua/laws/show/80/94-%D0%B2%D1%80#Text.

206. Про авторське право і суміжні права : Закон України від 23.12.1993 р. № 3792-XII. URL: https://zakon.rada.gov.ua/laws/show/3792-12 #Text.

207. Науково-практичний коментар до КК України. URL: http://pravoznavec.com/ua/books/162/12264/28/.

208. Науково-практичний коментар до Кримінального кодексу України / за заг. ред. І. М. Копотуна. Київ : К Н Т, 2023. 932 с.

209. Рішення Деснянського районного суду м. Чернігова у справі № 750/4468/19. URL: https://reyestr.court.gov.ua/Review/82055604.

210. Про захист інформації в інформаційно-комунікаційних системах : Закон України від 05.06.1994 р. № 80/94-ВР. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text.

211. Кримінальне право (Особлива частина) : підручник / за ред. О. О. Дудорова, Є. О. Письменського. Київ : ВД «Дакор», 2013. 606 с.

212. Кібератака вірусу Petya: що відомо. URL: http://surl.li/avmrp.

213. Узагальнення практики розгляду справ за обвинуваченням осіб у вчиненні злочинів, передбачених розділом XVI Кримінального кодексу України «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» (ст. 361–363-1). URL: http://surl.li/iannu.

214. M. Siponen. Unauthorized copying of software and levels of moral development: A literature analysis and its implications for research and practice. *Information Systems Journal*. 2004. № 14 (4). P. 387–407. DOI: 10.1111/j.1365-2575.2004.00179.x/.

215. Кримінальне право. Особлива частина : підручник. URL: https://pidru4niki.com/1584072059860/pravo/kriminalne_pravo_.

216. Науково-практичний коментар Кримінального кодексу України / за заг. ред. О. М. Джужі, А. В. Савченка, В. В. Чернєя. Київ : Юрінком Інтер, 2016. 1064 с.

217. Карчевський М. В. Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. URL: http://it-crime.at.ua/index/tezi_lekcij/0-31.

218. Апеляційний суд Харківської області. Узагальнення судової практики кримінальних справ та кримінальних проваджень про злочини у

сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку за період 2012–2014 роки. URL: http://surl.li/ianpx.

219. Дмитрук М. М. Типові наслідки «несанкціонованого втручання в роботу ЕОМ, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку». URL: http://surl.li/ianqd.

220. Генеральна прокуратура України : вебсайт. URL: http://surl.li/ianqs.

221. Що таке кодграббер і чи можна від нього захистити свій автомобіль. *Про авто* : вебсайт. URL: http://autopark.pp.ua/7934-scho-take-kodgrabber-chi-mozhna-vd-nogo-zahistiti-svy-avtomobl-pro-avto.html.

222. Що таке скімінг?. URL: http://surl.li/ianrj.

223. Карткове шахрайство в Україні: шахраї змінюють способи роботи. URL: http://surl.li/ianrl.

224. Supply Chain Risk – the «Cyber Attack» URL: https://www.isg-one.com/industries/consumergoods/articles/supply-chain-risk-the-cyber-attack.

225. Szor P. The Art of Computer Virus Research and Defense. *Addison-Wesley Professional* : Annotated edition. 2005. P. 742. URL: https://www.amazon.de/-/en/Peter-Szor/dp/0321304543.

226. Website Security Statistics Report. *WhiteHat Security*. 2019. 30 p. URL: https://info.whitehatsec.com/Website-Stats-Report-2019.html.

227. Staniford V. P., Weaver N. How to own the Internet in your spare time. *In Proceedings of the 11th USENIX Security Symposium*. URL: https://www.usenix.org/legacy/events/sec02/full_papers/staniford/staniford_html/index.html.

228. Karresand M. Separating Trojan horses, viruses, and worms – a proposed taxonomy of software weapons a proposed taxonomy of software weapons. *Information Assurance Workshop «IEEE Systems, Man and Cybernetics Society»* (2003). DOI: 10.1109/SMCSIA.2003.1232411.

229. Загальні рекомендації щодо зменшення наслідків від впливу шкідливого програмного забезпечення. *Sert-ua* : вебсайт. URL: https://cert.gov.ua/recommendation/2502.

230. Лефтеров Л. В. Шкідливе програмне забезпечення як знаряддя кіберзлочинності. URL: http://surl.li/iantv.

231. Sikorski M. Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software. *No Starch Press*. 1st edition. 2012. URL: https://www.amazon.de/-/en/Michael-Sikorski/dp/1593272901.

232. Cuff P. Distributed channel synthesis. *Trans. Inf. Theory*. 2013. Vol. 59, № 11. P. 7071–7096

233. Створення та використання шкідливих програм. URL: http://surl.li/fepzp.

234. Боровик А. В. Кіберзлочини в Україні (кримінально-правова характеристика) : навч. посіб. / за ред. А. В. Боровик, І. М. Копотун. Луцьк : Волиньполіграф, 2019. 314 с.

235. Шкідливі програмні та технічні засоби : вебсайт. URL: https://it-crime.at.ua/index/shkidlivi_programni_ta_tekhnichni_zasobi/0-34.

236. Що таке шкідливе програмне забезпечення?. URL: https://www.microsoft.com/de-de/.

237. Науково-практичний коментар до Кримінального кодексу України он-лайн. Т. 2. URL: http://mego.info/.

238. Про інформацію: Закон України від 02.10.1992 р. № 2657-XII. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text.

239. Про доступ до публічної інформації : Закон України від 13.01.2011 р. № 2939-VI. URL: https://zakon.rada.gov.ua/laws/show/2939-17#Text.

240. Про адвокатуру та адвокатську діяльність : Закон України від 05.07.2012 р. № 5076-VI. URL: https://zakon.rada.gov.ua/laws/show/5076-17#Text.

241. Про нотаріат : Закон України від 02.09.1993 р. № 3425-XII. URL: https://zakon.rada.gov.ua/laws/show/3425-12#Text.

242. Про банки і банківську діяльність : Закон України від 07.12.2000 р. № 2121-III. URL: https://zakon.rada.gov.ua/laws/show/2121-14#Text.

243. Плугатир М. В. Кримінальна відповідальність за несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка оброблюється в державних електронних інформаційних ресурсах. *Право і суспільство.* 2014. № 1.2. С. 256–258. URL: http://nbuv.gov.ua/UJRN/Pis_2014_1.2_62.

244. Про захист інформації в інформаційно-комунікаційних системах : Закон України від 05.07.1994 р. № 80/94-ВР. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text.

245. Науково-практичний коментар до Кримінального кодексу України. *Юрист-консульт: народний портал* : вебсайт. URL: https://legalexpert.in.ua/komkodeks/uk.html.

246. Кримінальна відповідальність за «СПАМ». URL: http://surl.li/ianzt.

247. Що таке DDoS-атака? *Офіційний сайт державної служби спеціального зв'язку та захисту інформації України*. URL: https://cip.gov.ua/ua/faqs/sho-take-ddos-ataka.

248. Что такое DDoS-Booter / IP-стрессер? Инструменты для DDoS-атак. URL: https://www.cloudflare.com/ru-ru/learning/ddos/ddos-attack-tools/ddos-booter-ip-stresser/.

249. Нацполіція відкрила провадження за фактом DDoS-атак на українські сайти. *Суспільне* : вебсайт. URL: http://surl.li/iaoab.

250. У 2020 році до кіберполіції надійшло понад 30 тисяч звернень щодо шахрайства в Інтернеті. *Департамент кіберполіції Національної поліції України* : вебсайт. URL: http://surl.li/gocxq.

251. Кіберполіція розкрила статистику інтернет-злочинності з початку року. *Finance ua* : вебсайт. URL: https://news.finance.ua/ua/news/-/483006/kiberpolitsiya-rozkryla-statystyku-internet-zlochynnosti-z-pochatku-roku.

252. 2021 Report on CSIRT-Law Enforcement Cooperation / European Union agency for cybersecurity. URL: http://surl.li/iaoas.

253. Шапочка С. В. Класифікація шахрайства, що вчиняється з використанням комп'ютерних мереж (кібершахрайства). *Наука і правоохорона.* 2015. № 1. С. 159–165.

254. Grigaitytė U. Nusikaltimai virtualioje erdvėje – šiuolaikiniai Iššūkiai ir prevencijos galimybės. *Vilnius University Open Series*. DOI: 10.15388/OS.TMP.2020.13.

255. K. Wan Fei Ma. COVID-19 and Cyber Fraud: Emerging Threats During the Pandemic. DOI: 10.13140/RG.2.2.18540.39042.

256. Про зареєстровані кримінальні правопорушення та результати їх досудового розслідування. *Офіс генерального прокурора* : вебсайт. URL: https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogo-rozsliduvannya-2.

257. Financial crime and fraud in the age of cybersecurity. URL: http://surl.li/iaobj.

258. Фейкові COVID-сертифікати в Україні: як каратимуть шахраїв?. URL: https://www.dw.com/uk/feikovi-covid-sertyfikaty-v-ukraini-yaka-vidpovidalnist-zahrozhuie-shakhraiam/a-59626047.

259. Департамент кіберполіції Національної поліції України : вебсайт. URL: https://cyberpolice.gov.ua/news/prodavav-neisnuyuchi-generatory-kiberpolicziya-vykryla-zlovmysnyka-u-shaxrajstvi-3765/.

260. Що таке послуга OLX Доставка?. *Olx* : вебсайт. URL: http://surl.li/ovqo.

261. Як не «влетіти» на гроші в OLX: найпопулярніша схема шахраїв-покупців. URL: https://te.20minut.ua/Groshi/yak-ne-vletiti-na-groshi-v-olx-naypopulyarnisha-shema-shahrayiv-pokupt-11296224.html.

262. Прудка Л. М. Психологічні особливості шахрайства в мережі Інтернет. *Південно-український правничий часопис*. 2018. URL: http://www.sulj.oduvs.od.ua/archive/2018/2/10.pdf.

263. Goldman Z. K. Deterring Financially Motivated Cybercrime. Economic espionage. URL: http://surl.li/iavym.

264. Breen C. F. ALarge-Scale Measurement of Cybercrime Against Individuals. URL: http://surl.li/iavyy.

265. Булатов А. С. Кримінальне маніпулювання під час шахрайства. *Юридична психологія*. 2015. № 2. С. 203–213. URL: http://surl.li/iavzf.

266. Ваш родич потрапив у ДТП: у поліції розповіли про найпоширеніші шахрайські схеми. *Суспільне* : вебсайт. URL: http://surl.li/iavzr.

267. Національна поліція України : офіційний вебсайт Національної поліції України у Львівській області. URL: http://surl.li/iawas.

268. Financial Crime Guide: A firm's guide to countering financial crime risks (FCG). URL: https://www.handbook.fca.org.uk/handbook/FCG.pdf.

269. Каже, що військовий: шахрай намагається видурити гроші в лучан. *Інформаційне агентство «Конкурент»* : вебсайт. URL: http://surl.li/iawbn.

270. Шахраї взяли на ваше ім'я онлайн-кредит: що робити?. *Liga Zakon* : вебсайт. URL: https://jurliga.ligazakon.net/news/208174_shakhra-vzyali-na-vashe-mya-onlayn-kredit-shcho-robiti.

271. Не ставай дропом! – безкоштовний сир буває тільки в мишоловці. *Департамент кіберполіції Національної поліції України* : вебсайт. URL: https://www.cyberpolice.gov.ua/article/ne-stavaj-dropom-198/.

272. Про роботу банківської системи в період запровадження воєнного стану : Постанова Правління Національного банку України від 24.02.2022 р. № 18. URL: http://surl.li/bumgr.

273. Кіберполіція викрила мережу фейкових вебобмінників / Інформаційне агенство Інтерфакс Україна. *Інтерфакс* : вебсайт. URL: https://interfax.com.ua/news/general/512564.html.

274. Кіберполіція викрила учасників транснаціональної шахрайської групи у привласненні грошей сотень тисяч осіб по всьому світу. *Департамент кіберполіції Національної поліції України* : вебсайт. URL: http://surl.li/iawev.

275. Рішення Ковельського міськрайонного суду у справі № 159/2149/17. URL: https://youcontrol.com.ua/ru/catalog/court-document/67836018/

276. Кіберполіція викрила організаторів шахрайського call-центру, які ошукали близько 18 тисяч іноземців. *Департамент кіберполіції Національної поліції України* : вебсайт. URL: http://surl.li/iaxfm.

277. Кіберполіція провела загальнонаціональну операцію з припинення діяльності ворожих ботоферм. *Департамент кіберполіції Національної поліції України* : вебсайт. URL: http://surl.li/iaxgx.

278. На Житомирщині правоохоронці оголосили підозру злочинній групі у шахрайстві за схемою «друг просить у борг». *Департамент кіберполіції Національної поліції України* : вебсайт. URL: http://surl.li/iaxhk

279. Продавав неіснуючі генератори: кіберполіція викрила зловмисника у шахрайстві. *Департамент кіберполіції Національної поліції України* : вебсайт. URL: http://surl.li/iaxhv.

280. Рішення когелії суддів Першої судової палати Касаційного кримінального суду Верховного Суду у справі № 755/5898/16-к. URL: http://iplex.com.ua/doc.php?regnum=103132841&red=10000394d1745bb3879ae81ebf20669127b714&d=5.

281. Узагальнення судової практики розгляду справ про адміністративні корупційні правопорушення та деякі злочини, передбачені розділом XVII Кримінального кодексу України. URL: http://surl.li/iaxin.

282. Фішинг на платформі оголошень – викрили зловмисника. URL: http://surl.li/iaxiy.

283. Аколов Д. Фішинг, хто і як маніпулює вашим вибором. URL: https://kniga.biz.ua/pdf/7451-Fishing.pdf.

284. Предмет крадіжки. URL: https://crimpravo.com/pitannya-ta-vidpovidi/predmet-kradizhky.html.

285. Соломко А. Г. Особливості кримінальної відповідальності за крадіжку. URL: https://conf.ztu.edu.ua/wp-content/uploads/2022/11/227.pdf.

286. Антифрод. *Wikipedia* : вебсайт. URL: http://surl.li/iaxka.

287. Що таке лог-файли. *Hostiq* : вебсайт. URL: http://surl.li/iaxlf.

288. Міщук В. В. Відмінність вимагання від подібних складів злочинів за кримінальним законодавством України. *Економіка і право*. 2013. № 23 С. 158–163. URL: http://surl.li/iaxmi.

289. Найпоширеніші схеми кіберзлочинців та способи захисту від них. *Навчально-науковий центр інформаційних технологій* : вебсайт. URL: http://surl.li/iaxow.

290. У жінки вимагали гроші, погрожуючи розповсюдити в Інтернеті її інтимні фото. *Тижневик «Ехо»* : вебсайт. URL: https://exo.in.ua/news/41358.

291. Злиті фото знаменитостей з icloud. URL: https://vk-spy.ru/uk/money/slitye-znamenitostei-iz-icloud-hakery-opublikovali-intimnye-foto-znamenitostei/.

292. Гринчак А. А. Протидія расизму, ксенофобії та екстремізму : навч. посіб. Харків, 2018. 248 с.

293. Расизм і ксенофобія в Україні: реальність та вигадки. *Харківська правозахисна група* / за ред. Б. Є. Захарова. Харків : Права людини, 2009. 192 с.

294. Кондратов Д. Ю. Кваліфікуючі ознаки порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв'язку або через комп'ютер. *Вісник кримінологічної асоціації України.* 2019. № 2 (21). С. 43–53.

295. Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/.

296. Про платіжні системи та переказ коштів в Україні : Закон України від 05.04.2001 р. № 2346-III. URL: http://surl.li/jris.

297. Скрипник В. Речі, обмежені в цивільному обороті, як об'єкти цивільних прав. *Підприємство, господарство і право*. 2018. № 1. С. 36–40.

298. Крупина Я. В. Кримінальна відповідальність за незаконні дії з документами на переказ, платіжними картками й іншими засобами доступу до банківських рахунків, електронними грошима, обладнанням для їх виготовлення за законодавством зарубіжних країн. URL: http://elar.naiau.kiev.ua/handle/123456789/13936.

299. Науково-практичний коментар до Кримінального кодексу України. URL: http://mego.info/.

300. Про затвердження Положення про порядок здійснення операцій з чеками в іноземній валюті на території України : Постанова Правління Національного банку України від 29.12.2000 р. № 520. URL: https://zakon.rada.gov.ua/laws/show/z0152-01#Text.

301. Аналіз статті 209 Кримінального кодексу України доступний для ознайомлення. *Академія фінансового моніторингу* : вебсайт. URL: http://surl.li/ibgqu.

302. Цивільний кодекс україни від 06.01.2003 р. № 435-IV. URL: https://zakon.rada.gov.ua/laws/show/435-15.

303. Про валюту і валютні операції : Закон України від 21.05.2018 р. № 2473-VIII. URL: https://zakon.rada.gov.ua/laws/show/2473-19#Text.

304. Habib A. ACFCS Special Contributor Report: Crowdfunding – An unorthodox way of Money Laundering? Definitely maybe. URL: http://surl.li/ibgrt.

305. Seagrave S. Lords of the Rim: the invisible empire of the overseas. URL: http://surl.li/ibgsi.

306. Gakunu P. Reforming the Financial System in Sub-Saharan Africa: the (long) Way Ahead. Finance & Bien Commun, 2007. № 28. P. 139–146.

307. Казначева Д. В. Основні види злочинів, що вчиняються із застосуванням криптовалюти. URL: http://surl.li/ibgtc/.

308. History of virtual assets of Ukraine or something in the crypt. URL: http://surl.li/ibgtr.

309. Конференция BlockchainUA. URL: http://surl.li/ibgua.

310. Sitthipon T. A Review of Cryptocurrency in the Digital Economy. DOI: 10.25147/ijcsr.2017.001.1.124.

311. Dilanchiev A. Factors Influencing Cryptocurrency Adoption in Georgia. *Journal of Business*. Vol. 11, № 2. 2022. DOI: 10.5281/zenodo.7628008.

312. Gonak I. Cryptocurrency as an object of investment. URL: http://surl.li/ibgvt.

313. Овчаренко А. С. Правове регулювання віртуальних активів та криптовалют в Україні: сучасний стан і перспективи. *Юридичний науковий електронний журнал*. 2020. № 4. С. 200–201.

314. Про обіг криптовалют : Проєкт Закону від 06.10.2017 р. № 7183. *Верховна Рада України* : вебсайт. URL: http://surl.li/boqu/.

315. Про віртуальні активи : Пропозиції Президента до Закону від 11.06.2020 р. URL: http://surl.li/ibhac.

316. Про віртуальні активи : Пропозиції Президента до Закону від 17.02.2022 р. № 2074-IX. URL: http://surl.li/gtzs.

317. Рішення Конституційного Суду України у справі за конституційним зверненням відкритого акціонерного товариства «Всеукраїнський Акціонерний Банк» щодо офіційного тлумачення положень пункту 22 частини першої статті 92 Конституції України, частин першої, третьої статті 2, частини першої статті 38 Кодексу України про адміністративні правопорушення (справа про відповідальність юридичних осіб) від 30 травня 2001 року. Справа № 1-22/2001.

318. Рішення Конституційного суду України у справі за конституційним поданням Уповноваженого Верховної Ради України з прав людини щодо відповідності Конституції України (конституційності) положенням третього речення частини першої статті 13 Закону України «Про психіатричну допомогу» (справа про судовий контроль за госпіталізацією недієздатних осіб до психіатричного закладу) від 1.06.2016 р. Справа № 1-1/2016.

319. Levin R. B. A day late and a digital dollar short: Central bank digital currencies. *GLI – Blockchain & Cryptocurrency Regulation 2022*. *4th Edition.* URL: http://surl.li/ibhdp.

320. Angel J. The Ethics of Payments: Paper, Plastic, or Bitcoin?. *Journal of Business Ethics*. *Innovations in payment technologies and the emergence of digital currencies.* 2014. № 3. P. 603–611.

321. Gervais A. Is Bitcoin a Decentralized Currency. *Security & Privacy.* 2014. № 12. P. 256–270.

322. Berentsen A. The Case for Central Bank Electronic Money and the Non-case for Central Bank Cryptocurrencies. *Federal Reserve Bank of St. Louis* : вебсайт. URL: http://surl.li/ibhki.

323. Верес І. Електронні гроші та криптовалюта як засоби розрахунків у сфері електронної комерції. *Підприємництво і право*. 2018. № 11. С. 10–15.

324. Carstens A. Money in the Digital Age: What Role Central Banks?. 2018. URL: https://www.bis.org/speeches/sp180206.htm.

325. Polyakova Y. A., Vorobyova O., Chertakova E. Revisiting the formation of the legal status of cryptocurrency in the Russian legislation. *Amazonia Investiga*. 2019. № 28 (22). P. 711–718. URL: https://www.amazonia investiga.info/index.php/amazonia/article/view/824.

326. Volosovych S. Cryptocurrency market transformation during the pandemic Covid – 19. *Financial and Credit Activity Problems of Theory and Practice*. 2023. № 1 (48). P. 114–126. DOI: 10.55643/fcaptp.1.48.2023.3949.

327. Грекова І. В. Окремі аспекти криміналістичної характеристики крадіжок автотранспортних засобів. *Південно-український правничий часопис.* 2015. № 4. С. 122–125.

328. Payments System Board Annual Report 2022. *Reserve bank of Australia* : website. URL: http://surl.li/ibhop.

329. Australia Income Tax Assessment Act (1997), № 40 (2022) and Act № 75 (2022). URL: https://www.legislation.gov.au/Details/C2022C00307.

330. Crypto And Tax In Australia: Everything You Need To Know. *Forbes* : вебсайт. URL: http://surl.li/ibhpf.

331. Tina van der Linden. Markets in crypto-assets regulation: Does itprovide legal certainty and increase adoptionof crypto-assets?. *Financial Innovatio.* 2023. DOI: 10.1186/s40854-022-00432-8.

332. Canada Has Been Experimenting With A Digital Fiat Currency Called CAD-COIN. *Forbes* : вебсайт. URL: http://surl.li/ibhqa.

333. Про Національний банк України : Закон України від 20.05.1999 р. № 679-XIV. URL: https://zakon.rada.gov.ua/laws/show/679-14# Text.

334. Лист Національного банку України від 08.12.2014 р. № 29-208/72889. URL: https://zakon.rada.gov.ua/laws/show/v2889500-14# Text.

335. Лист Національного банку України від 22.03.2018 р. № 40-0006/16290. URL: https://zakononline.com.ua/documents/show/374117_374182.

336. НБУ заборонив купувати криптовалюту за гривні. *Delj.ua* : вебсайт. URL: http://surl.li/ibhrq/.

337. Що в Україні можна купити за криптовалюту. *Финансовий портал Минфин* : вебсайт. URL: http://surl.li/hmhjk.

338. Thomas W. Etablir la sécurité juridique concernant le bitcoin. URL: http://surl.li/ibhud.

339. Ante L. The Influence of Stablecoin Issuances on Cryptocurrency Markets. URL: http://surl.li/ibitn.

340. Про віртуальні активи : Закон України від 17.02.2022 р. № 2074-IX. URL: https://zakon.rada.gov.ua/laws/show/2074-20#Text.

341. Калініна А. В. Криптовалюта – цифровий актив злочинності. URL: http://surl.li/ibiui.

342. 20-річному українцю загрожує 8 років в'язниці за крадіжку криптовалюти. *Obozrevatel* : вебсайт. URL: http://surl.li/ibiuo.

343. Що таке токен на блокчейні. *Bankchart* : вебсайт. URL: http://surl.li/ibivi.

344. Binance : вебсайт. URL: http://surl.li/bnjlr.

345. Uniswap : вебсайт.URL: https://uniswap.org/.

346. Pancakeswap : вебсайт. URL: https://pancakeswap.finance//.

347. Biswap : вебсайт. URL: https://biswap.org//.

348. Шахрайство під виглядом інвестування у криптовалюту – у Києві викрито злочинну групу. *Офіс генерального прокурора* : вебсайт. URL: http://surl.li/ibiyt.

349. The Financial Action Task Force. URL: https://www.fatf-gafi.org/.

350. O'Leary R. R. Europol Warns Zcash, Monero and Ether Playing Growing Role in Cybercrime. *Coindesk* : вебсайт. URL: http://surl.li/ibjda.

351. Exchange rates. *Best exchange* : вебсайт. URL: https://www.bestchange.com/.

352. Bitcoin ATM Map. *CoinATMRadar* : вебсайт. URL: https://coinatmradar.com/.

353. Марисюк К. До питання про поняття загальних засад призначення покарання. *Науковий вісник Дніпропетровського державного університету внутрішніх справ.* 2020. № 3. С.114–118. DOI: 10.31733/2078-3566-2020-3-114-118.

354. Сахарук. Т. Загальні засади призначення покарання за кримінальним правом України та зарубіжних країн: порівняльний аналіз : автореф. дис. … канд. юрид. наук : 12.00.08. Київ, 2006. 18 с.

355. Музика А. Інститут призначення покарання: поняття і загальна характеристика. *Право України.* 2011. № 9. С. 174–183.

356. Омельчук О. Загальні засади призначення покарання: законодавче регулювання та практика застосування. *Університетські наукові записки.* 2013. № 4. С. 360–366.

357. Васильєв А. А., Пироженко О. С. Про деякі проблеми застосування кримінального покарання у виді штрафу: аналіз законодавчих новел. *Вісник Вищої ради юстиції.* 2013. № 1 (13). С. 80.

358. Денисова Т. А. Основні тенденції діяльності держави у сфері застосування кримінальних покарань. *Вісник Львівського Університету.* 2010. № 50. С. 260–265. (Серія: Юридична).

359. Бабанли Р. Ш. Призначення покарання в Україні: теоретико-прикладні засади. Чернігів : Десна Поліграф, 2019. 488 с.

360. Спронюк О. Поняття санкції у теорії права. *Історико-правовий часопис.* 2016. № 1 (7). С. 234–240.

361. Бражник А. А. Абсолютно-визначені покарання за злочини проти статевої свободи та статевої недоторканості. URL: https://dspace.nlu.edu.ua/bitstream/123456789/18281/1/Brazhnik_81-84.pdf.

362. Щур К. В. Призначення штрафу як додаткового виду покарання. *Кримінально-правові та кримінологічні заходи протидії злочинності* : матеріали Всеукраїнської науково-практичної конференції. Одеса : ОДУВС, 2015.

363. Попрас В. О. Штраф як вид покарання за кримінальним правом України : монографія. Харків : Право, 2009. 224 с.

364. Смирнов А. А. Штраф у кримінальному праві України. *Право і безпека.* 2005. № 4. С. 168–172.

365. Попович А. Г. Теоретичний аспект поняття штрафу як юридичної категорії. *Новітні кримінально-правові дослідження* : зб. наук. пр. Миколаїв : Іліон, 2017. С. 141–144.

366. Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану : Закон України від 24.03.2022 р. № 2149-IX. URL: https://zakon.rada.gov.ua/laws/show/2149-20/ed20220403#n6.

367. Кріпак А. А. Покарання у вигляді позбавлення волі у законодавстві України та окремих країн західної Європи. *Вісник Пенітенціарної асоціації України*. 2018. № 1. С. 105–114. URL: https://visnykpau.com/index.php/journal/article/view/131.

368. Рішення Франківського районного суду м. Львова № 465/2391/19. URL: https://reyestr.court.gov.ua/Review/85733514.

369. Про внесення змін до Кримінального кодексу України щодо вдосконалення інституту спеціальної конфіскації з метою усунення корупційних ризиків при її застосуванні : Закон України від 10.11.2015 р. № 770-VIII. URL: https://zakon.rada.gov.ua/laws/show/770-19/ed20151126#n29.

370. Рішення Ужгородського міськрайонного суду у справі № 308/11741/20. URL: https://reyestr.court.gov.ua/Review/93903445.

371. Рішення Луцького міськарайонного суду у справі № 161/18959/20. URL: https://reyestr.court.gov.ua/Review/93155890.

372. Рішення Ковпаківського районного суду у справі № 592/4316/20. URL: https://reyestr.court.gov.ua/Review/89242851.

373. Рішення суду у справі № 676/1984/21. URL: https://reyestr.court.gov.ua/Review/96443215.

374. Рішення Кіровського суду у справі № 404/4975/21 URL: https://reyestr.court.gov.ua/Review/103688801.

375. Рішення Арбузинського районного суду у справі № 467/1069/21. URL: https://reyestr.court.gov.ua/Review/102133515.

376. Рішення Кам'янець-Подільського міськрайонного суду у справі № 676/4712/21. URL: https://reyestr.court.gov.ua/Review/101616341.

377. Рішення Хмельницького міськрайонного суду у справі № 686/26099/21. URL: https://reyestr.court.gov.ua/Review/101623083.

378. Вирок суду у справі № 1-кп/711/173/20. URL: https://reyestr.court.gov.ua/Review/99816224.

379. Рішення Ужгородського міськрайонного суду у справі № 308/4477/21. URL: https://reyestr.court.gov.ua/Review/99768721.

380. Піцик Ю. М. Аналіз особистості кіберзлочинця, який вчиняє злочини проти власності у кіберпросторі. URL: http://www.vestnik-pravo.mgu.od.ua/archive/juspradenc26/28.pdf.

381. Діти та робота: особливості працевлаштування неповнолітніх. *Безоплатна правова допомога* : вебсайт. URL: http://surl.li/ibjuk.

382. Про вищу освіту : Закон України від 01.07.2014 р. № 1556-VII. URL: https://zakon.rada.gov.ua/laws/show/1556-18#Text.

383. Єдиний звіт про осіб, які вчинили кримінальні правопорушення за серпень 2020 року. URL: http://surl.li/ibjwv.

384. Федорчук І. М. Обставини, які обтяжують покарання за кримінальним правом України : монографія. Львів : ЛьвДУВС, 2017. 240 с. URL: http://surl.li/ibpsw.

385. Кіберполіція викрила злочинну групу, яка оформлювала кредити на зниклих безвісти і полонених військовослужбовців. *Департамент кіберполіції Національної поліції України* : вебсайт. URL: https://cyberpolice.gov.ua/news/kiberpolicziya-vykryla-zlochynnu-grupu-yaka-oformlyuvala-kredyty-na-znyklyx-bezvisty-i-polonenyx-vijskovosluzhbovcziv-8913/.

386. Поліцейські Києва викрили групу шахраїв, які під приводом продажу техніки ошукали близько 300 громадян. *Департамент кіберполіції Національної поліції України* : вебсайт. URL: https://cyberpolice.gov.ua/news/policzejski-kyyeva-vykryly-grupu-shaxrayiv-yaki-pid-pryvodom-prodazhu-texniky-oshukaly-blyzko--gromadyan-4330/.

387. Кримінальний кодекс України. Науково-практичний коментар / за заг. ред. В. Я. Тація, В. П. Пшонки, В. І. Борисова, В. І. Тютюгіна. Харків : Право, 2013.

388. Градова Ю. В. Кібербулінг як загроза психологічному здоров'ю підлітків. URL: https://univd.edu.ua/general/publishing/konf/26_11_2019/pdf/18.pdf.

389. Вірус WannaCry пошкодив комп'ютери у 99 країнах світу. URL: https://www.bbc.com/ukrainian/features-39907984.

390. How 4 Chinese Hackers Allegedly Took Down Equifax. URL: https://www.wired.com/story/equifax-hack-china/.

391. Sony Hackers Have Flashed A 'Disturbing' New Warning On Staff Computers. URL: https://web.archive.org/web/20150708173853/http://www.businessinsider.com/sony-hackers-new-warning-on-computers-2014-12.

392. У Кремлі підгоряє. Російські хакери посилили атаки на інфраструктуру України. *Фокус* : вебсайт. URL: https://focus.ua/uk/digital/55

3817-v-kremle-podgoraet-russkie-hakery-uzhestochili-ataki-na-infrastrukturu-ukrainy.

393. Кібератаки, артилерія, пропаганда. загальний огляд вимірів російської агресії : вебсайт. URL: https://cip.gov.ua/ua/news/kiberataki-artileriya-propaganda-zagalnii-oglyad-vimiriv-rosiiskoyi-agresiyi.

394. Analysis of the Cyber Attack on the Ukrainian. *Power Grid* : website. URL: https://web.archive.org/web/20180401121206/https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf.

395. Час перевірити рівень кібербезпеки в медицині. URL: https://datami.ua/kiberbezpeka-v-meditsini/.

396. Огляд подій у сфері кібербезпеки, січень 2023. URL: https://www.rnbo.gov.ua/files/2023/NKCK/Cyber%20digest_january_2023_fin.pdf.

397. Twitter зазнав хакерської атаки. У мережу потрапили дані 200 млн користувачів. *Forbes* : вебсайт. URL: http://surl.li/ibpxj.

398. Хакери зламали твітер-акаунти Гейтса, Маска, Байдена і закликали перевести біткойни. *Радіосвобода* : вебсайт. URL: http://surl.li/ibpzj.

399. Задорожна С. М. Природно-правовий характер принципів міжнародного права. *Науковий вісник Чернівецького університету* : зб. наук. пр. 2013. Вип. 660. С. 49–56. (Серія: Правознавство).

400. Конспект лекцій з дисципліни міжнародне право. URL: http://surl.li/gwwwa.

401. Статут Організації Об’єднаних Націй. URL: https://unic.un.org/aroundworld/unics/common/documents/publications/uncharter/UN%20Charter_Ukrainian.pdf.

402. Декларація про принципи міжнародного права, що стосуються дружніх відношень та співробітництва між державами у відповідності зі

Статутом Організації Об’єднаних Націй. *Liga 360* : вебсайт. URL: http://surl.li/ibpzz.

403. Заключний акт НБСЄ в Хельсінкі від 01.08.1975 р. URL: http://kimo.univ.kiev.ua/MVZP/75.htm.

404. Final stage of the Conference on Security and Cooperation in Europe Helsinki, 30 July – 1 August 1975. URL: http://surl.li/ibqah.

405. Войціховський А. В. Міжнародне право : навч. посіб. Харків : 2020. 544 с. URL: http://surl.li/ibqaj.

406. Patrick W. Franzese. Sovereignty in cyberspace: can it exist?. *Air Force Law Review*. Vol. 64. URL: http://surl.li/ibqam.

407. Goldsmith J., Wu T. Who Controls the Internet?: Illusions of a Borderless World. *Faculty Books*. 2006. P. 175. URL: http://surl.li/ibqax.

408. Війна Росії проти України: хронологія кібератак. URL: https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI(2022)733549_XL.pdf.

409. Естонія зазнала масштабної російської кібератаки після демонтажу радянського пам’ятника. *Радіо «Свобода»* : вебсайт. URL: http://surl.li/ibqbi.

410. Anahit P. Cyberwar. URL: https://www.academia.edu/35526558/Cyberwar_Anahit_Parzyan_pdf.

411. G7 Ise-Shima Leaders’ Declaration. URL: https://www.mofa.go.jp/files/000160266.pdf.

412. Туранський М. В. Пропагандистська кампанія Росії у підготовці до анексії кримського півострова. URL: http://surl.li/ibqcb.

413. International strategy of cooperation on cyberspace. URL: https://www.chinadaily.com.cn/kindle/2017-03/02/content_28409210.htm.

414. Загальна декларація прав людини ООН : Міжнародний документ від 10.12.1948 р. URL: http://surl.li/umvi.

415. Василенко А. І. Теоретичні аспекти застосування норм і принципів міжнародного права до регулювання відносин в кіберпросторі. Одеса, 2018. 33 с.

416. Council of Europe. Committee of Misisters. Recommendation № 9 (89) on 13 September 1989. URL: http://surl.li/ibqcq.

417. The existing Council of Europe Convention on the Protection of Environment through Criminal Law. ETS № 172. 1998. URL: https://www.coe.int/en/web/cdpc.

418. Abdul Raheem Fathima Shafana. Predictive Data Mining for Phishing Websites: A Rule Based Approach. *Journal of Information Systems & Information Technology*. Vol. 5, № 2. 2020. P. 61–71. URL: http://surl.li/ibqcx.

419. Gagandeep Kaur Rosha. E-Crime Behaviour of Internet Users. *International Journal on Future Revolution in Computer Science & Communication Engineering.* Vol. 3, № 11. P. 23–337. URL: http://surl.li/ibqdg.

420. Golyatina S. M. Problems of electronic funds theft investigation. *SHS Web of Conferences 108, 04008 IX Baltic Legal Forum 2020.* URL: https://www.researchgate.net/publication/351997834_Problems_of_electronic_funds_theft_investigation.

421. Prithivi Raj. Analysis of legal measures to control and prevent cyber crimes. *International Journal of Multidisciplinary Research and Development.* 2021. Vol. 8, № 4. P. 16–19. URL: http://surl.li/ibqdu.

422. Silviu Jîrlăianu. Computer Related Forgery, Between Concept And Reality. *International conference knowledge-based organization.* 2015. № 21 (2). URL: http://surl.li/ibqfz.

423. Govil J. Ramifications of cyber crime suggestive. *Preventive measure Electro / Information Technology*. 2007. URL: http://surl.li/ibqgc.

424. Kweku K. A., Martin S. O, Hein S. V. Considerations Towards a Cyber CrimeProfiling System. 2008. URL: http://surl.li/ibqgv.

425. Patki A. B. Cyber Crime Information System for Cyberethics Awareness. *Department of Information Technology, Government of India*. 2003. URL: http://surl.li/ibqdg.

426. Окінавська хартія глобального інформаційного суспільства. URL: https://studies.in.ua/inform-pravo-shporu/2201-oknavska-hartya-global nogo-nformacynogo-susplstva.html.

427. Directive 2014/42/eu of the European Parliament and of the Council of 3 april 2014 on the freezing and confiscation of instrumentalities and proceeds of crime in the European Union. URL: http://surl.li/ibqhy.

428. Online Police Station : a state-of-the-art Italian SemanticTechnology against cybercrime / Federico Neri, Paolo Geraci, Gianluca Sanna, Liviana Lotti. URL: http://surl.li/ibqih.

429. Скулиш Є. Д. Міжнародно-правове співробітництво у сфері подолання кіберзлочинності. *Інформація і право*. 2014. № 1 (10). С. 93–100.

430. Gregory B. W. The Community Cyber SecurityMaturity Model. 2007. URL: https://ieeexplore.ieee.org/abstract/document/4076571.

431. Roderic G. B. Developments in the global law enforcement of cybercrime. *Policing: An International Journal of Police Strategies and Management.* 2021. *№* 29 (2). P. 408–433. URL: http://surl.li/ibqjm.

432. Osman Goni. Cyber Crime and Its Classification. *Int. J. Of Electronics Engineering and Applications*. 2020. № 1. P. 01–17. DOI: 10.30696/IJEEA.X.I.2021.01-17.

433. Alin Teodorus Drăgan. Child Pornography and Child Abuse in Cyberspace. *Journal of legal studies*. 2018. Vol. 21, № 35. P. 52–60. URL: https://www.researchgate.net/publication/326401361_Child_Pornography_and_ Child_Abuse_in_Cyberspace.

434. Farina K. Cyber Crime: Identity Theft. URL: https://www.research gate.net/publication/304188885_Cyber_Crime_Identity_Theft.

435. Shrimati Das. Cyber Crime and Cyber Ethics: Staying Safeand Enabled in the Cyber Space Quest. *Multidisciplinary Journal of Humanities and Social Sciences*. URL: http://surl.li/ibqkz.

436. Kurt Saunders. Counteracting Identity Fraud in the Information Age: The Identitiy Theft and Assumption Deterrence Act. URL: https://www.researchgate.net/publication/228189021_Counteracting_Identity_Fraud_in_the_Information_Age_The_Identitiy_Theft_and_Assumption_Deterrence_Act.

437. Harmen van der Wilt. Chapter 1: Legal responses to transnational and international crimes: towards an integrative approach? : Monograph. URL: http://surl.li/ibqln.

438. Сідак В. С. Забезпечення інформаційної безпеки в країнах НАТО та ЄС : навч. посіб. Київ : КНТ, 2007. 160 с.

439. 16 Latest Cybercrime Trends & Predictions for 2022 / 2023 and Beyond. URL: https://financesonline.com/cybercrime-trends/.

440. Potokin Y. N. The influence of roman law on the formation and development of the romano-germanic legal family. URL: http://surl.li/ibrpv.

441. Kigerl A. Cyber crime nation typologies: K-Means clustering of countries based on cyber crime rates. URL: https://www.academia.edu/29440896/Cyber_Crime_Nation_Typologies_K_Means_Clustering_of_Countries_Based_on_Cyber_Crime_Rates.

442. Computer Fraud and Abuse Act (CFAA) in 1986. URL: https://www.nacdl.org/Landing/ComputerFraudandAbuseAct.

443. Goldman L. Interpreting the Computer Fraud and Abuse Act. URL: https://www.researchgate.net/publication/305850068_Interpreting_the_Computer_Fraud_and_Abuse_Act.

444. Greer B. J. The Growth of Cybercrime in the United States. URL: https://www.researchgate.net/publication/320781855_The_Growth_of_Cybercrime_in_the_United_States.

445. Barringer T., Roberts B. S. The Credit Card Fraud Act of 1984 Clarification, or Further Confusion, of the Law of Credit Card Fraud?. *American Business Law Journal*. № 24 (3). P. 449–466. URL: https://doi.org/10.1111/j.1744-1714.1986.tb00506.x.

446. Aïmeur E., Schonfeld D. The ultimate invasion of privacy: Identity theft. *9thAnnual International Conference on Privacy, Security and Trust*. 2011. P. 24–31. https://doi.org/10.1109/PST.2011.5971959.

447. Bagchi K., Udo G. An analysis of the growth of computer and Internet securitybreaches. *Communications of the Association for Information Systems*. 2013. № 12 (1). P. 684–701.

448. Arkansas Code Title 5 «Criminal Offenses» Subtitle 4 «Offenses Against Property» Chapter 41 «Computers, Computer Systems, and Networks». URL: https://law.justia.com/codes/arkansas/2017/title-5/subtitle-4/chapter-41/.

449. Code of Virginia Title 18.2 «Crimes and Offenses Generally». URL: https://law.lis.virginia.gov/vacode/title18.2/.

450. Louisiana Laws Revised Statutes Title 14 «Criminal Law». URL: https://law.justia.com/codes/louisiana/2021/revised-statutes/title-14/.

451. Illinois Compiled Statutes Chapter 720 «Criminal offenses 720 ILCS 5» – Criminal Code of 2012. URL: https://law.justia.com/codes/illinois/2021/chapter-720/act-720-ilcs-5/.

452. Maria Tcherni-Buzzeo. The Dark Figure of Online Property Crime: Is Cyberspace Hiding a Crime Wave?. URL: https://www.researchgate.net/publication/273104024_The_Dark_Figure_of_Online_Property_Crime_Is_Cyberspace_Hiding_a_Crime_Wave.

453. Chek Point. Cyber security report 2021. URL: http://surl.li/ibrrs.

454. Table of titles and chapters Nevada revised statutes. Title 52 : Trade regulations and practices. Chapter 603 : Computers. URL: https://www.leg.state.nv.us/Division/Legal/LawLibrary/NRS/index.html.

455. Computer Misuse Act. Removed a redundant sentence / some formatting corrected – 05.02.2020. Legal Guidance, Cyber : online crime, Youth crime. URL: https://www.cps.gov.uk/legal-guidance/computer-misuse-act.

456. Niloufer Selvadurai. Unauthorised access to wireless local area networks: The limitations of the present Australian laws. *Computer Law & Security Review*. 2009. № 25 (6). P. 536–542. DOI: 10.1016/j.clsr.2009.09.003.

457. Data mining for creditcard fraud: A comparative study / S. Bhattacharyya, S. Jha, K. Tharakunnel, J. C. Westland. *Decision Support Systems*. 2011. № 50 (3). P. 602–613. https://doi.org/10.1016/j.dss.2010.08.008.

458. Protection of Children Act 1978. *UK Public General Acts*. URL: https://www.legislation.gov.uk/ukpga/1978/37/body.

459. Sexual Offences Act 1956. *UK Public General Acts*. URL: https://www.legislation.gov.uk/ukpga/Eliz2/4-5/69.

460. Terrorism Act 2000. *UK Public General Acts.* URL: https://www.legislation.gov.uk/ukpga/2000/11/contents.

461. Criminal Damage Act, 1991. № 31 of 1991. URL: https://www.irishstatutebook.ie/eli/1991/act/31/enacted/en/print.

462. Criminal justice (theft and fraud offences) Act, 2001. № 50 of 2001. URL: https://www.irishstatutebook.ie/eli/2001/act/50/enacted/en/pdf.

463. Criminal Code of Canada (R. S. C., 1985, c. C-46). URL: https://laws-lois.justice.gc.ca/eng/acts/c-46/.

464. New Zeland Crimes Act 1961. Public Act 1961 № 43. URL: https://www.legislation.govt.nz/act/public/1961/0043/latest/DLM327382.html.

465. Penal Code of the Netherlands in 1881-03-03. URL: https://sherloc.unodc.org/cld/document/nld/1881/penal_code_of_the_netherlands.html.

466. Eric Rutger Leukfeldt. High Volume Cyber Crime and the Organization of the Police: The results of two empirical studies in the

Netherlands. *International Journal of Cyber Criminology*. 2013. Vol. 7, № 1. P. 1–17. URL: http://surl.li/ibrtw.

467. France Criminal Code. URL: https://www.equalrightstrust.org/ert documentbank/french_penal_code_33.pdf.

468. The Criminal Code of Danish. Order № 909 of September 27, 2005, as amended by Act Nos. 1389 and 1400 of December 21, 2005. URL: https://www.globalwps.org/data/DNK/files/Danish%20Criminal%20Code.pdf.

469. Johannes Kaspar. Legal and empirical aspects of cybercrime in Germany. URL: http://surl.li/ibruf.

470. Criminal Code in the version published on 13 November 1998 (Federal Law Gazette I, p. 3 322), as last amended by Article 2 of the Act of 22 November 2021 (Federal Law Gazette I, p. 4 906). URL: https://www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html.

471. Julia Hörnle. 5 Jurisdiction of the Criminal Courts in Cybercrime Cases in Germany and England. 2021. P. 101–115. URL: http://surl.li/ibrul.

Наукове видання

Думчиков Михайло Олександрович

КОНЦЕПТУАЛЬНІ ЗАСАДИ КРИМІНАЛЬНО-ПРАВОВОЇ ОХОРОНИ КІБЕРПРОСТОРУ В УКРАЇНІ

Монографія

Художнє оформлення обкладинки М. О. Думчикова
Редактор О. В. Федяй
Комп’ютерне верстання М. О. Думчикова

Формат 60×84/16. Ум. друк. арк. 24,06. Обл.-вид. арк. 25,74. Тираж 300 пр. Зам. №

Видавець і виготовлювач
Сумський державний університет,
вул. Римського-Корсакова, 2, м. Суми, 40007
Свідоцтво суб’єкта видавничої справи ДК № 3062 від 17.12.2007.