СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
ДНІПРОВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ВНУТРІШНІХ СПРАВ

Кваліфікаційна наукова
праця на правах рукопису

ДУМЧИКОВ МИХАЙЛО ОЛЕКСАНДРОВИЧ

УДК 343.3:004.056:007(477)

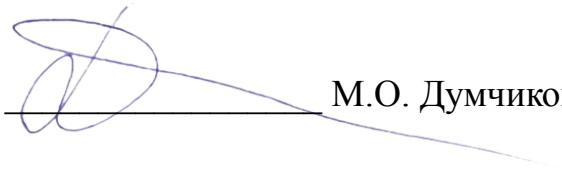
ДИСЕРТАЦІЯ

КОНЦЕПТУАЛЬНІ ЗАСАДИ КРИМІНАЛЬНО-ПРАВОВОЇ ОХОРОНИ КІБЕРПРОСТОРУ В УКРАЇНІ

12.00.08 – кримінальне право та кримінологія;
кримінально-виконавче право

Подається на здобуття наукового ступеня доктора юридичних наук

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело



_____ М.О. Думчиков

Науковий консультант —
Бондаренко Ольга Сергіївна,
доктор юридичних наук, доцент

Дніпро – 2024

АНОТАЦІЯ

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

Дисертація на здобуття наукового ступеня доктора юридичних наук за спеціальністю 12.00.08 «Кримінальне право та кримінологія; кримінально-виконавче право» (081 – Право). – Сумський державний університет, Суми, 2024. – Дніпровський державний університет внутрішніх справ, Дніпро, 2024.

У дисертації наведено теоретичне узагальнення й запропоновано нове вирішення наукової проблеми, яке полягало у розробленні на основі аналізу існуючих наукових підходів, чинного вітчизняного та зарубіжного законодавства і практики їх реалізації, комплексних науково та практично обґрунтованих концептуальних засад кримінально-правової охорони кіберпростору в Україні.

Об’єктом дослідження є суспільні відносини, що виникають у процесі кримінально-правової охорони кіберпростору та встановлення кримінальної відповідальності за вчинення кримінальних правопорушень у кіберпросторі. Предметом дослідження є концептуальні засади кримінально-правової охорони кіберпростору в Україні.

Ретроспективно узагальнено та систематизовано наукові дослідження присвячені кримінально-правовій охороні кіберпростору. Наголошено, що беззаперечним елементом успіху наукового дослідження є використання правильної методології, як б у повній мірі забезпечувала системність та комплексність наукового дослідження та одночасно дозволила б розробити висновки та рекомендації, які б відображали вагоме та змістовне значення, як для наукової так і для практичної діяльності. Зокрема, було використано: метод аналізу, емпіричний метод, метод контент-аналізу, метод кейс-студії, порівняльно-правовий метод, метод системного аналізу, які застосовувалися у

взаємозв’язку й взаємозалежності, що також забезпечило повноту та об’єктивність цього дослідження.

Визначено шість етапів становлення кримінальної відповідальності за кримінальні правопорушення у кіберпросторі на теренах України:
1) початковий; 2) зародження; 3) імплементаційний; 4) економічний;
5) нормотворчий; 6) сучасний. Здійснено співвідношення понять «кіберпростір», «інформаційний-простір», «віртуальний-простір» та «інтернет-простір». Водночас, визначено, що, поняття «кіберпростір» є вужчим за змістом від понять «інформаційний» та «віртуальний» простір, проте ширше за поняття «інтернет-простір».

Констатовано, що, традиційно виділяють три підходи до формування сутності поняття «кіберпростір»: легальний, доктринальний й філософський. На основі аналізу зазначених підходів, зокрема доктринального, запропоновано розглядати кіберпростір в інформаційному, віртуальному та соціальному ракур

Сформульовано основні характеристики та принципи організації кіберпростору, зокрема, серед основних характеристик було виділено віртуальність, мережеву приналежність, середовище взаємодії, динамічність, комунікативність та поєднання територіалізації та територіалізації. Серед принципів, що забезпечують стабільність функціонування кіберпростору нами було виділені: принцип дисципліни, принцип відповідальності, принцип дотримання прав та свобод людини і громадянина та принцип своєчасного втручання. Розмежовано поняття «кримінальне правопорушення у кіберпросторі», «кримінальне правопорушення у сфері комп’ютерної інформації» та «комп’ютерне кримінальне правопорушення».

Визначено та удосконалено основні характеристики кримінальних правопорушень у кіберпросторі: 1) інтелектуальний характер;
2) транснаціональний характер; 3) латентність; 4) використання навичок соціальної інженерії; 5) суб’єктна складова; 6) дистанційність; 7) доступність матеріалів необхідних для скоєння кримінального правопорушення у

кіберпросторі; 8) анонімність.

Акцентовано увагу на доцільності узгодження термінології, закріпленої у Законі України «Про основні засади забезпечення кібербезпеки України» з положеннями та нормами чинного Кримінального кодексу України, зокрема, щодо впровадження та використання терміну «кримінальне правопорушення у кіберпросторі», під яким пропонуємо розуміти суспільно небезпечне, протиправне, винне, каране діяння, що посягає та заподіює шкоду різним суспільним відносинам шляхом використання інформаційно-телекомунікаційних технологій, інформаційно-телекомунікаційних систем та мереж та створюваного ними кіберпростору.

Виділено кілька підстав для типологізації кримінальних правопорушень у кіберпросторі: за родовом об’єктом, за кількістю посягань, за спрямованістю, за ціллю використання інформаційно-телекомунікаційних технологій, систем і мереж, за видами кримінальних правопорушень передбачених в Конвенції «Про кіберзлочинність».

Наголошено, що кримінальні правопорушення в кіберпросторі, є соціально небезпечним, протиправним явищем, яке становить загрозу не тільки національним, але й міжнародним інтересам, а боротьба з ними є однією з головних завдань правоохоронних органів, як національного так і міжнародного рівня.

Акцентовано увагу на тому, що кримінальні правопорушення які вчиняються в кіберпросторі, в сфері обігу цифрової інформації та функціонування інформаційно-телекомунікаційних технологій не є ідентичними за своєю сутністю з кримінальними правопорушеннями в сфері використання інформаційно-телекомунікаційних технологій. На підставі цього визначено, що перші варто називати кіберзалежні, а інші кіберутворювальні кримінальними правопорушеннями. Зокрема, кіберзалежні кримінальні правопорушення прийнято вважати кіберзалежними, тобто основним предметом цього типу кримінальних

правопорушень у кіберпросторі виступає цифрова інформація в сфері цифрових технологій, інформаційно-телекомунікаційних системах та мережах. Кіберутворювальні кримінальні правопорушенням є класичними кримінальними правопорушеннями, які внаслідок використання інформаційно телекомунікаційних технологій «перейшли» у кіберпростір.

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

Акцентовано на необхідності законодавчого закріплення поняття «несанкціоноване втручання», під яким пропонуємо розуміти, одержання можливості для ознайомлення та (або) використання цифрової інформації, шляхом проникнення в інформаційно-телекомунікаційні системи та мережі з використанням спеціальних технічних засобів та (або) спеціального програмного забезпечення, особою яка не має права доступу до такої інформації та (або) роботи з нею.

Запропоновано авторську типологізацію шкідливих технічних, за процесом створення: 1) шкідливі технічні засоби, які створені спеціально для вчинення певної категорії кримінальних правопорушень, і не можуть бути застосовані для іншої роботи; 2) традиційні технічні засоби, які внаслідок модифікації застосовуються для вчинення кримінальних правопорушень;
3) традиційні технічні засоби, які можуть використовуватися для вчинення кримінальних правопорушень.

Установлено, що переважна більшість науковців під шахрайством з використанням інформаційно-телекомунікаційних технологій розуміє

«фішинг», 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 190 статтею Особливої частини Кримінального кодексу України. Доведено, що суспільно небезпечні діяння у формі «фішингу», необхідно кваліфікувати за частиною 3 статті 361 Особливої частини Кримінального кодексу України, з причини специфічного предмета такого кримінального правопорушення, зокрема цифрової інформації. У випадку «фішингу» обман виступає лише як спосіб отримання персональних даних у вигляді цифрової інформації. Визначено основні способи легалізації майна отриманого злочинним шляхом у кіберпросторі: 1) легалізація майна отриманого злочинним шляхом за допомогою вже існуючої Інтернет інфраструктури (маркетплейси, сайти оголошень, соціальні мережі, Інтернет аукціони, краудфандінг); 2) легалізація майна отриманого злочинним шляхом, шляхом створення нової веб – інфраструктури (Інтернет – магазин);
3) легалізація майна отриманого злочинним шляхом використання обмінників та цифрової (електронної) валюти; 4) легалізація майна отриманого злочинним за допомогою віртуальних активів.

Визначено та надано характеристику основним ознакам віртуальних активів: 1) децентралізованість; 2) транснаціональність; 3) конфіденційність операцій; 4) цифровізація; 5) майновий характер; 6) анонімність. Надано визначення поняття «віртуальний актив», під яким пропонується розуміти цифрову валюту (віртуальну, без фізичної форми), створення і контроль за якою базується на криптографічних методах, щодо якої встановлена повна децентралізація, що гарантує коректність операцій в системі в тому числі відсутності можливості впливати на транзакції учасників криптосистеми.

Узагальнено та систематизовано зарубіжний досвід правового регулювання віртуальних активів. На основі розглянутого досвіду та визначеної специфіки віртуальних активів. Наголошено, що віртаульні активи

варто розглядати у трьох аспектах, а саме як: 1)інформацію; 2) валюту;
3) інше нематеріальне благо. Наголошено, що сьогодні віртуальні активи як предмет кримінального правопорушення за законодавством України можуть виступати лише, як елемент цифрової інформації. Водночас пропонується розширити предмет крадіжки, включивши до нього цифровий інформаційний продукт.

Акцентовано увагу на тому, що кіберзалежні кримінальні правопорушення характеризуються вчиненням декількох суспільно небезпечних діянь, які передбачені Особливою частиною Кримінального кодексу України для досягнення одного злочинного результату, та власне призначення покарання за сукупністю кримінальних правопорушень.

Визначені та проаналізовані основні обставини, що обтяжують покарання за кримінальні правопорушення у кіберпросторі з врахуванням специфічних особливостей вчинення таких суспільно-небезпечних діянь. Наголошено на необхідності введення додаткової обставини, що обтяжує кримінальні правопорушення у кіберпросторі: 1) заподіяння шкоди інформаційно-телекомунікаційній технології, системи або мережі державного значення, яке має ознаки критичної інфраструктури; 2) предметом кримінального правопорушення виступає цифрова інформація, яка має ознаки державної таємниці.

Наголошено, 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 та фактично невілює можливості міжнародно-правового захисту держав від вчинення кібератак з боку інших держав, або окремих осіб за сприянням конкретних держав.

Акцентовано, що міжнародні нормативні акти здебільшого зосереджують увагу саме на формах вчинення суспільно небезпечних діянь у кіберпросторі. Узагальнено та систематизовано зарубіжний досвід правового

регулювання відповідальності за вчинення кримінальних правопорушень шляхом використання інформаційно-телекомунікаційних технологій. З'ясовано, що країни, які відносяться до англо–саксонської правової сім'ї, окрім нормативного регулювання, широко застосовують систему судових прецедентів, при цьому правова регламентація встановлення кримінальної відповідальності за кримінальні правопорушення в кіберпросторі, переважно розміщена в окремих нормативних актах, при цьому така країна, як Сполучені Штати Америки, крім загального регулювання відносин щодо встановлення кримінальної відповідальності за кримінальні правопорушення у кіберпросторі, застосовує регулювання на рівні окремих штатів, яке дуже різниться між собою. Країни романо–германської правової сім'ї навпаки характеризуються уніфікацією своєї правової регламентації, щодо кримінальної відповідальності за кримінальні правопорушення у кіберпросторі. Однак, незважаючи, на приналежність до одної правової сім'ї, кримінальне законодавство цих країн суттєво різниться між собою. Так, країни західної та центральної Європи не виділяють в окремий розділ кримінальні правопорушення у кіберпросторі, а кримінальна відповідальність за них передбачені різними розділами їх Кримінальних кодексів, в свою чергу у країнах північної Європи, кримінальна відповідальність за суспільно небезпечні діяння, шляхом використання інформаційно – телекомунікаційних технологій, систем та мереж виділені в окремий розділ.

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

SUMMARY

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

The dissertation for obtaining the scientific degree the Doctor of Law on a specialty 12.00.08. – Criminal Law and Criminology; Criminal Executive Law. – Dnipro State University of Internal Affairs, Dnipro, 2023.

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

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

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

The study identifies six stages of criminal liability for offenses committed in

cyberspace within the borders of Ukraine: 1) initial stage; 2) formation stage; 3) implementation stage; 4) economic stage; 5) legislative stage; 6) contemporary stage.

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

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

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

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

Emphasis is placed on the desirability of aligning the terminology outlined in the Law of Ukraine on the Fundamental Principles of Ensuring Cybersecurity in Ukraine with the provisions and norms of the existing Criminal Code of Ukraine. This pertains specifically to the incorporation and utilization of the term criminal offense in cyberspace, which is proposed to encompass socially perilous, illicit,

blameworthy acts that infringe upon and disrupt various social relationships through the use of information and telecommunication technologies, information and telecommunication systems, and the corresponding cyberspace they engender.

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

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

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

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

Attention is drawn to the necessity of introducing legislation for the concept

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

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

The primary methods for legitimizing criminally obtained assets in cyberspace are outlined: 1) using existing internet infrastructure (marketplaces, classifieds, social networks, internet auctions, crowdfunding); 2) establishing new web infrastructure (online stores);

3) using exchanges and digital currency for asset laundering; 4) employing virtual assets for laundering obtained property.

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

A summary and categorization of foreign practices concerning the legal

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

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

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

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

The predominant focus of international normative acts centers on the modes of committing socially perilous acts in cyberspace. The foreign practices in legal regulations pertaining to liability for committing criminal offenses through the utilization of information and communication technologies are summarized and categorized. Countries belonging to the Anglo-Saxon legal tradition widely employ

both normative regulations and a system of legal precedents. In contrast, the establishment of criminal liability for offenses in cyberspace is primarily relegated to separate normative enactments. The United States, for instance, applies both general and state-specific regulations. In the Romano-Germanic legal tradition, countries display unified regulations for criminal liability concerning offenses in cyberspace. However, even within this legal framework, substantial differences exist among these countries. For instance, countries in Western and Central Europe do not isolate offenses in cyberspace into a distinct section, incorporating their liability into various sections of their Criminal Codes. Conversely, Northern European countries segregate criminal liability for socially perilous actions using information and communication technologies, systems, and networks into a separate section.

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

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Монографії

1. Dumchikov M., Bondarenko O., Peculiarities of criminal legal protection of cyberspace and combating cybercrimes : monograph. Germany : AP Lambert Academic Publishing GmbH & Co. KG, 2023. 73 p. (*Особистий внесок здобувача: проаналізовано нові форми вчинення кримінальних правопорушень у кіберпросторі, зокрема, крадіжку з платіжних карт – «кардинг», повернення оплати за отриманий товар «рефандинг», та основні форми вчинення суспільно небезпечних діянь у кіберпросторі, предметом яких є віртуальні активи).*

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

Статті у фахових виданнях України категорії «Б»

3. Думчиков М. О. Процеси диджиталізації і криміналістика: ретроспективний аналіз. *Збірник «Криміналістика і судова експертиза.* 2020. Вип. 65. С. 100–108. DOI: https://doi.org/10.33994/kndise.2020.65.11.

4. Думчиков М. О., Рєпін Д. А. Легалізація доходів, отриманих злочинним шляхом, за допомогою використання віртуальної валюти (криптовалюти): кримінологічний та кримінально-правовий аспект. *Журнал східноєвропейського права*. 2020. № 82. С. 32–37. (*Особистий внесок здобувача: досліджено поняття «віртуальний актив» та надано його авторське визначення, окреслено й проаналізовано основні ознаки віртуальних активів, визначено, що саме підпадає під категорію віртуальних активів*).

5. Думчиков М. О., Пахомов В. В., Бондаренко О. С. Криміналістичні проблемні аспекти боротьби зі злочинами у кіберсфері.

Збірник «Криміналістика і судова експертиза. 2020. № 1. С. 18–22. (*Особистий внесок здобувача: надано рекомендації щодо вдосконалення нормативно-правової бази з питань забезпечення кібербезпеки, здійснено розмежування понять «комп'ютерний злочин» і «кіберзлочин», здійснено криміналістичну типологізацію кримінальних правопорушень у кіберпросторі*).

6. Dumchykov M. O., Bondarenko O. S. Criminological aspects of combatting money laundering in cyberspace. *Legal Horizons*. 2021. № 14. P. 105–110. (*Особистий внесок здобувача: проведено аналіз криміналістичної характеристики легалізації відмивання злочинних доходів у кіберпросторі, зазначено основні способи легалізації майна, отриманого злочинним шляхом, за допомогою віртуальних активів*).

7. Думчиков М. О., Бондаренко О. С. Кримінологічні аспекти протидії легалізації корупційних доходів у кіберпросторі. *Правові горизонти*. 2021. № 14. С. 105–110. (*Особистий внесок здобувача: названо основні напрями вдосконалення методів забезпечення у сфері протидії й попередження легалізації прибутків, пов'язаних із злочинністю в кіберпросторі, виокремлено та проаналізовано основні способи легалізації злочинних доходів за допомогою віртуальних активів*).

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

9. Думчиков М. О., Шевцов Я. А. До проблеми визначення поняття та ознак кіберзлочинів. *Журнал східноєвропейського права*. 2022. № 104. С. 12–22. (*Особистий внесок здобувача: визначено специфічні ознаки кримінальних правопорушень у кіберпросторі, детально проаналізовано такі ознаки, як анонімність і територіальна складова*).

10. Думчиков М. О. Особливості кваліфікації шахрайства в кіберпросторі, засобом вчинення якого є віртуальні активи.

Науково-інформаційний вісник Івано-Франківського університету права імені Короля Данила Галицького. Серія Право. 2022. № 14 (26). С. 159–165. DOI: 10.33098/2078-6670.2022.14.26.149-155.

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

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

13. Думчиков М. О., Каріх І. В. Становлення та генеза кримінальної відповідальності за кримінальні правопорушення у кіберпросторі на теренах України. *Юридичний науковий електронний журнал*. 2022. № 5. С. 476–478. DOI: https://doi.org/10.32782/2524-0374/2022-5/113. (*Особистий внесок здобувача: проаналізовано основні етапи становлення злочинності в кіберпросторі на теренах України*).

14. Думчиков М. О., Малетов Д. В. Загальна характеристика та види розкрадань шляхом використання інформаційних технологій як одного з найпоширеніших видів кримінальних правопорушень у кіберпросторі. *Юридичний науковий електронний журнал*. 2022. № 7. С. 278–28. DOI: https://doi.org/10.32782/2524-0374/2022-8/60. (*Особистий внесок здобувача: дослідження можливості комп'ютерно-технічної експертизи як важливої допомоги в розкритті та розслідуванні кримінальних правопорушень, пов'язаних із розкраданнями коштів із банківських карт, розкрито сутність «кардингу» як найпопулярнішого кримінального правопорушення, пов'язаного з викраденням безготівкових коштів*).

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

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

17. Думчиков М. О. Поняття та ознаки кіберпростору, які роблять його привабливим для вчинення кримінальних правопорушень в сфері комп'ютерної інформації. *Юридичний науковий електронний журнал*. 2022. № 3. С. 195–197. DOI: https://doi.org/10.32782/2524-0374/2022-3/44.

18. Думчиков М. О., Каріх І. В. Зарубіжний досвід протидії кримінальним правопорушенням проти власності, вчиненим із використанням інформаційно-телекомунікаційних технологій. *Прикарпатський юридичний вісник*. 2023. № 2. С. 55-61. (*Особистий внесок здобувача: окреслено основні підходи до встановлення кримінальної відповідальності за вчинення кримінальних правопорушень у кіберпросторі проти власності за законодавством зарубіжних держав, виокремлено позитивний досвід кримінально-правової охорони кіберпростору зарубіжних держав від зовнішніх та внутрішніх посягань*).

19. Думчиков М. О., Каріх І. В. Неправомірний вплив на інформаційну інфраструктуру України. *Юридичний науковий електронний журнал*. 2023. № 5. С. 111–116. (*Особистий внесок здобувача: визначено основні фактори та загрози державній інформаційній інфраструктурі, що може бути об'єктом учинення суспільно небезпечного діяння, запропоновано підходи до вдосконалення нормативно-правової системи кримінально-правової охорони державної інфраструктури України*).

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

Статті в зарубіжних періодичних наукових виданнях юридичного напряму

21. Pakhomov V., Bondarenko O., Dumchikov M. Criminal legal characteristic of social engineering as a way of committing fraud. *Legea si Viata*. 2019. № 4/2. P. 149–153. (*Особистий внесок здобувача: визначено значення соціальної інженерії під час учинення кримінальних правопорушень у кіберпросторі, проаналізовано основні суспільно небезпечні діяння, вчинювані в кіберпросторі за допомогою методів соціальної інженерії*).

22. Думчиков М. О., Пахомов В. В. Кіберзлочинність як новітній феномен та джерело високого рівня суспільної небезпеки. *Visegrad Journal on Human Rights*. 2021. № 2. С. 333–340. (*Особистий внесок здобувача: здійснено аналіз кримінальних правопорушень, регламентованих XVI розділом Особливої частини Кримінального кодексу України, визначено їх специфічні характеристики, запропоновано криміналізувати нові види кримінальних правопорушень у кіберпросторі).*

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

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

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

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

26. Dumchikov M., Kononenko N., Batsenko L., Halenin R., Hlushchenko N. Issues of regulating cryptocurrency and control over its turnover:

international experience. 2020, 10–20 July. Vol. 9. Issue 31. DOI: https://doi.org/10.34069/AI/2020.31.07.1. (**WoS**). *(Особистий внесок здобувача: надане авторське розуміння поняття криптовалюта, визначено основні схеми використання криптовалюти в протиправній діяльності, окреслено та охарактеризовано основні ознаки криптовалюти, проаналізовано зарубіжні підходи до регулювання криптовалют у зарубіжних державах*).

27. Dumchikov M., Yunin O., Nestor N., Borko A., Yermenchuk O. Criminological and forensic characteristics of forms of embezzlement committed through the use of information technology. *Amazonia Investiga*. 2021. № 10. P. 131–140. DOI: https://doi.org/10.34069/AI/2021.41.05.13. (**WoS**). (*Особистий внесок здобувача: визначено та проаналізовано кримінальні правопорушення, які можуть вчиняти за допомогою інформаційних технологій, як засіб учинення кримінального правопорушення, порівняно системи кримінально-правової охорони кіберпростору України та зарубіжних держав, зокрема, країн Європейського Союзу та Сполучених Штатів Америки*).

28. Dumchikov Mykhailo, Bondarenko Olha, Utkina Maryna. Cybercrime as a Threat to the National Security of the Baltic States and Ukraine: The Comparative Analysis. *International Journal of Safety and Security Engineering*. 2022. № 4. P. 10. DOI: https://doi.org/10.18280/ijsse.120409. (**Scopus**). (*Особистий внесок здобувача: визначено основні загрози для України та країн Балтії у сфері забезпечення кібербезпеки, запропоновано варіанти протидії наявним кіберзагрозам, на підставі аналізування позитивного досвіду країн Балтії запропоноване вдосконалення системи кримінально-правової охорони кіберпростору*).

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

здобувача: здійснено класифікацію кримінальних правопорушень у кіберпросторі, проаналізовано найбільш суспільно небезпечні кримінальні правопорушення, які вчиняються у світі, на основі позитивного зарубіжного досвіду, запропоновано зміни до низки статей Особливої частини Кримінального кодексу України).

30. Dumchikov M., Horobets N., Honcharuk V., Dehtiar R. Digital Currency as a Subject of Economic Criminal Offenses. *Law, State and Telecommunications Review*. 2022. Vol. 14, No. 1. P. 20–30. DOI: 10.26512/lstr.v14i1.38676. (**Scopus**). (*Особистий внесок здобувача: окреслено поняття «віртуальний актив», проаналізовано кримінальні правопорушення, де віртуальні активи можуть бути предметом кримінального посягання, виокремлено та проаналізовано способи легалізації майна, отриманого злочинним шляхом, за допомогою цифрової валюти*).

31. Dumchikov M. Reznik O. Bondarenko O. Peculiarities of countering legalization of criminal income with the help of virtual assets: legislative regulation and practical implementation. Journal of Money Laundering Control. 2022. DOI: 10.1108/JMLC-12-2021-0135. **(Scopus та WoS).** (Особистий внесок здобувача: визначено та охарактеризовано основні способи легалізації злочинних доходів за допомогою віртуальних активів, проаналізовано нормативні підходи до вдосконалення системи протидії легалізації майна, отриманого злочинним шляхом, за допомогою віртуальних активів).

Тези наукових доповідей

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

33. Думчиков М. О. Кримінально-правова характеристика телефонного скамінгу як одного з видів соціальної інженерії. *Die wichtigsten*

Vektoren für die Entwicklung der Wissenschaft im Jahr 2020: der Sammlung wissenschaftlicher Arbeiten «ΛΌГОΣ» zu den Materialien der internationalen wissenschaftlich-praktischen Konferenz : тези доповідей. Europäische : Duchy of Luxembourg, 2020. С. 68-70.

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

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

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

37. Думчиков М. О. Інтернет-шахрайство у сфері комп'ютерної інформації як об'єкт криміналістичного аналізу. *Актуальні питання судової експертології, криміналістики та кримінального процесу* : тези доповідей. Київ : Ліра-К, 2021. С. 108–111.

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

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

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

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

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

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

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

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

державний університет, 2022. С. 257-260.

46. Думчиков М. О. Кіберзлочини в сфері комп’ютерної інформації: поняття та види. *Актуальні питання юридичної науки та практики : зб. наук. праць студ. та молодих вчених* : тези доповідей. Хмельницький : Вид-во МАУП, 2022. С. 73-77.

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

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

ЗМІСТ

ВСТУП

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

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

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

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

В умовах повномасштабного вторгнення кіберпростір став однією з

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

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

Вищезазначене засвідчує необхідність здійснення глибокого та змістовного наукового вивчення суспільно небезпечних діянь, вчинюваних у кіберпросторі для з’ясування основних проблемних аспектів установлення кримінальної відповідальності за їх учинення, і розроблення основних заходів, необхідних для їх усунення.

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

Зокрема, це такі вчені, як Д. Азаров, О. Алексєєва, О. Амелін, Ю. Батурин, Ю. Бельський, П. Біленчук, Л. Біловус, О. Богач, В. Болгов, А. Боровик, О. Тихонова В. Бохенко, А. Булатов, М. Буряк, В. Бурячок, А. Василенко, І. Васильковський, І. Верес, Б. Войтко, В. Гавловський, Ю. Гаркуша, С. Гахов, С. Гнатюк, В. Голубєв, Ю. Градова, І. Грекова, А. Гринчак, Б. Дердюк, А. Клочко М. Дмитрук, О. Довженко, О. Дубас,

К. Дубняк, В. Дуленко, Д. Казначева, А. Калініна, М. *Карчевський, Л.* Клапків, О. Колодюк, Д. Кондратов, О. Користін, О. Корченко, М. Кравцова, Г. Крайник, А. Кріпак, Я. Крупіна, В. Кундеус, В. Курушин, О. Кушнерьов, Н. Лазаренко, О. Литвинова, О. Манжай, І. Коптун, К. Марисюк, В. Марков, В. Матвійчук, В. Міщук, Н. Міщук, М. Мягка, А. Овчаренко, О. Омельчук, М. Панов, О. Пащенко, Ю. Піцик, М. Плугатир, Л. Прудка, П. Пушкаренко, О. Кирбят'єв Н. Ржевська, В. Русецький, Н. Савчук, О. Самойленко, А. Селюк, А. Семенов, В. Сідак, О. Сіренко, Є. Скулиш, А. Соломко, А. Ставер, О. Столяр, К. Тарасюк, О. Терешкун, М. Туранський, Ю. Філей, Т. Філіпенко, В. Фурашев, В. Хахановський, І. Чекунов, Ю. Чокас, С. Шапочка, Г. Швиданенко, В. Шемчук, Г. Шинкарецька, М. Яцишин.

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

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

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

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

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

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

Ця наукова праця є спробою запропонувати оновлений підхід до кримінально-правової охорони кіберпростору в Україні та встановлення

кримінальної відповідальності за вчинення кримінальних правопорушень у кіберпросторі.

Зв'язок роботи з науковими програмами, планами, темами, грантами. Дисертація виконана відповідно до Стратегії розвитку наукових досліджень Національної академії правових наук України на 2021–2025 роки, а також у межах науково-дослідних тем Навчально-наукового інституту права Сумського державного університету «Концептуальні засади реформування системи правоохоронних органів в сучасних умовах трансформації нагляду і контролю щодо забезпечення економічної безпеки України» (номер державної реєстрації 0120U100474), «Корупція в умовах воєнного стану та післявоєнної відбудови: оптимальна модель протидії» (номер державної реєстрації 0124U000556), «Національна безпека України через запобігання фінансовим шахрайствам та легалізації брудних грошей: воєнні та післявоєнні виклики» (номер державної реєстрації 0123U101945), «Кібербезпекові та цифрові трансформації економіки країни воєнного часу: боротьба із кіберзлочинами, корупцією та тіньовим сектором» (номер державної реєстрації 0124U000544), «Засади діяльності правоохоронних органів у сфері контролю за системою залучення і використання МТД: глобалізаційний вимір» (номер державної реєстрації 0124U000635), Програма ERASMUS+ Модуль Жана Моне «Досвід ЄС щодо захисту персональних даних у кіберпросторі» (2023-2026 – EUEPPDC – 101125350 – ERASMUS-JMO-2023-MODULE).

Мета та завдання дослідження. Мета дисертаційного дослідження полягає в розробленні на основі аналізування наявних наукових підходів, чинного вітчизняного та зарубіжного законодавств і практики їх реалізації комплексних науково й практично обґрунтованих концептуальних засад кримінально-правової охорони кіберпростору в Україні.

Для досягнення зазначеної мети були вирішені такі завдання:

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

- охарактеризувати методологічні засади дослідження кримінально-правової охорони кіберпростору в Україні;
- проаналізувати теоретико-правові підходи до тлумачення поняття «кіберпростір;
- сформувати поняття та ознаки кримінальних правопорушень у кіберпросторі;
- здійснити теоретико-прикладну типологізацію кримінальних правопорушень у кіберпросторі;
- надати кримінально-правову характеристику кіберзалежних та кіберутворювальних кримінальних правопорушень;
- визначити особливості кримінально-правової кваліфікації кримінальних правопорушень у кіберпросторі, предметом та засобом учинення яких є віртуальні активи;
- визначити особливості призначення покарання за вчинення кримінальних правопорушень у кіберпросторі;
- здійснити кримінально-правову характеристику обставин, що обтяжують покарання за кримінальні правопорушення в кіберпросторі;
- охарактеризувати особливості застосування норм і принципів міжнародного права у сфері кіберпростору в Україні;
- здійснити порівняльно-правовий аналіз кримінальної відповідальності за вчинення кримінальних правопорушень у кіберпросторі;
- запропонувати напрями вдосконалення Кримінального кодексу України.

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

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

Методи дослідження. Методологічною основою дослідження стала сукупність методів наукового пізнання. З філософських методів ми використали *метод концептуального аналізу* під час аналізування

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

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

Інформаційною та емпіричною основою дослідження були:

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

Наукова новизна одержаних результатів полягає в тому, що подане дисертаційне дослідження є однією з перших спроб комплексно на монографічному рівні на основі використання комплексного й системного підходів розробити галузево-профільовані та ефективні концептуальні засади кримінально-правової охорони кіберпростору в Україні з урахуванням останніх наукових досягнень, положень міжнародно-правових актів, що визначають кримінальну відповідальність за кримінальні правопорушення в кіберпросторі, положень національного законодавства та позитивних рис зарубіжного досвіду. На підставі проведеного дослідження сформульовано низку нових концептуальних наукових положень та висновків, запропонованих особисто здобувачем.

уперше:

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

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

- запропоновано виділити принципи, що забезпечують функціонування кіберпростору: дисципліну, відповідальність, додержання

прав і свобод людини та громадянина й своєчасне втручання;

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

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

- запропоновано авторську типологізацію шкідливих технічних засобів, зокрема, за процесом створення: 1) шкідливі технічні засоби, що створені спеціально для вчинення певної категорії кримінальних правопорушень і не можуть бути застосовані для іншої роботи; 2) традиційні технічні засоби, які внаслідок модифікації застосовують для вчинення кримінальних правопорушень; 3) традиційні технічні засоби, які можна використовувати для вчинення кримінальних правопорушень;

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

- запропоновано виділення в межах кваліфікуючої ознаки статті

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

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

удосконалено:

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

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

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

- поняття віртуального активу для потреб Закону України «Про віртуальні активи», під яким пропонується розуміти цифрову валюту (віртуальну, без фізичної форми), створення й контроль за якою базуються на криптографічних методах, щодо якої встановлена повна децентралізація, що

гарантує коректність операцій у системі, зокрема, відсутність можливості впливати на транзакції учасників криптосистеми;

набули подальшого розвитку:

- характеристика теоретико-прикладних підходів до типологізації кримінальних правопорушень у кіберпросторі;
- підстави розмежування понять «кримінальне правопорушення в кіберпросторі», «кримінальне правопорушення у сфері комп'ютерної інформації» та «комп'ютерне кримінальне правопорушення»;
- модель вчинення кримінального правопорушення в кіберпросторі;
- види обставин, що обтяжують покарання за вчинення суспільно небезпечних діянь у кіберпросторі.

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

У науковій статті «Становлення та генеза кримінальної відповідальності за кримінальні правопорушення в кіберпросторі на теренах України», підготовленій разом із І. Каріхом, особисто здійснений аналіз основних етапів становлення злочинності в кіберпросторі на теренах України. У науковій статті «Загальна характеристика та види розкрадань шляхом використання інформаційних технологій як одного з найпоширеніших видів кримінальних правопорушень у кіберпросторі» в

співавторстві з Д. Малетовим дисертант дослідив можливості комп'ютерно-технічної експертизи як важливої допомоги в розкритті та розслідуванні кримінальних правопорушень, пов'язаних із розкраданнями коштів із банківських карт, розкрив сутність «кардингу» як найпопулярнішого кримінального правопорушення, пов'язаного з викраденням безготівкових коштів.

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

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

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

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

кримінально-правової охорони кіберпростору.

У науковій статті «The essence and classification of cybercrime in the field of computer information» у співавторстві з В. Пахомовим дисертант здійснив класифікацію кримінальних правопорушень у кіберпросторі, проаналізував найбільш суспільно небезпечні кримінальні правопорушення, які вчиняються у світі, на основі позитивного зарубіжного досвіду запропонував зміни до низки статей Особливої частини Кримінального кодексу України. У науковій статті «Digital Currency as a Subject of Economic Criminal Offenses» у співавторстві з Н. Горобець і Р. Дегтяр здобувач окреслив поняття «віртуальний актив», проаналізував кримінальні правопорушення, де віртуальні активи можуть бути предметом кримінального посягання, виокремив та проаналізував окремі способи легалізації майна, отриманого злочинним шляхом за допомогою цифрової валюти. У науковій статті «Peculiarities of countering legalization of criminal income with the help of virtual assets: legislative regulation and practical implementation» у співавторстві з О. Рєзніком та О. Бондаренко особистий внесок здобувача полягає у визначенні основних способів легалізації злочинних доходів за допомогою віртуальних активів та наданні їх характеристики, а також проаналізовано нормативні підходи щодо вдосконалення системи протидії легалізації майна, отриманого злочинним шляхом за допомогою віртуальних активів.

У науковій статті «Criminological and forensic characteristics of forms of embezzlement committed through the use of information technology» у співавторстві з О. Юніним, Н. Нестор, А. Борко, О. Єрменчук дисертант визначив та проаналізував кримінальні правопорушення, що можуть вчинятися за допомогою інформаційних технологій, як засіб учинення кримінального правопорушення, порівняв системи кримінально-правової охорони кіберпростору України та зарубіжних держав, зокрема, країн Європейського Союзу та Сполучених Штатів Америки. У науковій статті «Issues of regulating cryptocurrency and control over its turnover: international experience» у співавторстві з Н. Кононенко, Л. Басенко, Р. Халеніним та

Н. Глущенко особистий внесок дисертанта полягає в наданні авторського визначення поняття «криптовалюта», визначенні основних схем використання криптовалюти в протиправній діяльності, окресленні й охарактеризуванні основних ознак «криптовалюти», аналізуванні зарубіжних підходів щодо регулювання «криптовалют» у зарубіжних державах.

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

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

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

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

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

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

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

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

РОЗДІЛ 1
ІСТОРИЧНІ ТА ТЕОРЕТИКО–МЕТОДОЛОГІЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ В КІБЕРПРОСТОРІ

1.1. Становлення та генеза кримінальної відповідальності за кримінальні правопорушення в кіберпросторі в Україні

Характеризуючи ґенезу кримінальної відповідальності за правопорушення в кіберпросторі, доцільно розпочати з ретроспективного розвитку злочинності як явища. Варто відмітити, що більшість кримінально-протиправних діянь з'явилася досить давно і з часом просто набула нових рис, способів вчинення, з'явилися нові знаряддя й засоби їх вчинення. Поза тим 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 Інтернету.

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 у 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, дозволяє проникнути у вуличні телефони, з подальшим одержанням доступу до управління телефонними мережами за допомогою навичок соціальної інженерії [364].

Зародження феномену фрикінгу часто пов’язують з діяльністю Д. Енгресса, видатного телефонного хакера, який зумів майстерно імітувати сигнали телефонних дзвінків за допомогою звичайного свисту. Ця навичка у поєднанні з умілим впливом на технічних працівників, які обслуговували телефонні лінії, давала йому можливість здійснювати міжнародні дзвінки без сплати вартості. Хоча Енгресс не використовував телефонні мережі для особистого збагачення, його методи швидко набули популярності серед молодих техніків та неповнолітніх хакерів, які створювали власні пристрої для генерації необхідних телефонних сигналів [127].

Фрикінг як практика почався, як технічний виклик і хакерський експеримент, але швидко перетворився на серйозний інструмент кіберзлочинності. Початкові інтенції, можливо, і були невинними або науковими у своїй основі, проте згодом деякі технічні навички, розвинуті в рамках фрикінгу, стали основою для розвитку методів соціальної інженерії в кіберзлочинності. Енгресс, несвідомо чи свідомо, продемонстрував, що зловмисники можуть маніпулювати технологіями на дуже глибокому рівні, обходячи традиційні заходи безпеки. Це виявило вразливості у системі телефонного зв’язку, які потім були використані іншими злочинцями для створення складних схем шахрайства.

Цей історичний приклад вказує на важливість розуміння того, як технологічні інновації можуть бути використані як для позитивного, так і для негативного впливу на суспільство. Вивчення фрикінгу допомагає краще зрозуміти, як кіберзлочинці адаптуються до нових технологій і як можна покращити методи захисту інформації.

Отже початок 70-х років можна назвати певною відправною точкою в історії кримінальних правопорушень у кіберпросторі. З цього моменту почав активно розвиватися 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 із Мілуокі (Сполучені Штати Америки) здійснили перше зафіксоване інтернет-проникнення. Ці підлітки зламали 60 комп'ютерів за дев'ять днів, зокрема комп'ютери в лабораторії округу 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» [340].

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 три види інформації: 1) інформацію, що належить фінансовим установам, а саме: інформацію про кредитні картки та рахунки, дані, що належать державним установам; 2) інформацію від міжнародних та урядових організацій. Тому це можна назвати першим заходом проти кримінальних правопорушень у кіберпросторі [342].

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 у кіберпросторі, після чого особи, які вчиняють кримінальні правопорушення в мережі, починають ділитися вміннями та навичками, навіть серед хакерів формується певна ієрархія, в 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 у кіберпросторі [67, с. 13].

Водночас кримінальні правопорушення в кіберпросторі перестають бути якимось 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 незвичним явищем через те, що вони постійно розвивалися як кримінальна індустрія, зокрема через її масштаби та транснаціональну спрямованість [483].

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 отримала доступ до комп'ютеризованої системи контролю води на греблі Теодора Рузвельта в Арізоні. Це дало їй змогу вільно відкрити шлюзи і 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» [399].

Наприкінці XX століття кібератаки все більше набували масовості та транснаціонального характеру. Масовий характер кримінальних правопорушень у кіберпросторі супроводжувався розвитком інформаційних технологій державних структур, які здійснюють свою діяльність. Одним із напрямом такої діяльності виступав кібернетичний простір. Зокрема, створюються різноманітні державні сайти та сервіси, які були розпорядниками великого обсягу інформації та мали доступ до інтернет-мережі, вебресурси з новинами, вебресурси національних закладів освіти та міжнародні сервіси онлайн-торгівлі. Велика кількість та різноманітність вебресурсів у мережі Інтернет породила нові види кримінальних правопорушень у кіберпросторі та привернула увагу зловмисників у цій сфері, тим самим зародивши так званий «Хактивізм». Зазначимо, що хактивізм проявлявся у двох основних спрямуваннях діяльності: розповсюдження інформації шляхом її незаконного поширення на різних вебресурсах у мережі Інтернет та перешкоджання роботі таких ресурсів загалом [499].

Наприклад, перша така акція задля 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 з сайтів, через що система перевантажувалась і таким чином було виведено з ладу відразу кілька таких сайтів. Шляхом завдання різних збитків планувалося привернути увагу до позиції противників такої політики уряду [113].

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 та здобували контроль над різними сайтами з метою заміни розміщеної на них інформації, тобто встановлювали «дефейс». Усі ці дії були спрямовані на засудження воєнних дій Югославії й НАТО. Крім того, також законними шляхами, було поширено багато інформації стосовно небезпеки війни. Такі акції мали чимало суспільно-політичних наслідків [392].

Проте не всі хакери керуються політичними ідеями, дуже велика кількість має саме комерційні інтереси в 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 з 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 [67].

Тож до початку XXI століття сформувалися всі основні тенденції, напрями 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 у кіберпросторі та поява субкультури хактивізму; 3) набуття кримінально-протиправною діяльністю у 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 [392].

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 «множитися», і процес цей неймовірно швидкий, адже відбувається в міжнародних масштабах, тому загальна статистика з цього питання залишається невтішною [446].

Зараз жертвами зловмисників, які здійснюють свою діяльність 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, тим самим посівши друге місце серед економічних кримінальних правопорушень у світі, залишивши позаду кримінальні правопорушення, пов'язані з легалізацією грошових коштів, отриманих незаконним шляхом, та різні корупційні кримінальні правопорушення [458].

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 [114, с. 159].

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, тут же існують 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 [359].

Проте зазначена статистика не повністю відповідає дійсності, адже кримінальні правопорушення в кіберпросторі є одними з найлатентніших видів кримінальних правопорушень, а, отже, реальна картина та статистичні дані значно більші. Передусім це зумовлено відсутністю чітких методів та прийомів збирання даних про скоєння 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 складали 78 584 карбованці. Цей факт був занесений у міжнародний реєстр правопорушень подібного роду і став своєрідним початком розвитку нового виду кримінальних правопорушень у колишньому СРСР [217, с. 87].

Цей інцидент є значним, оскільки він відзначає перехід злочинності до нової технологічної ери у радянському суспільстві. Вперше комп'ютерні технології були використані не лише для поліпшення ефективності адміністративних процесів, а й стали інструментом у скоєнні злочинів. Вільнюський випадок відкрив двері для подальшого розвитку кіберзлочинності, показавши потенціал комп'ютерних мереж як засобу для незаконного збагачення. Осмислення цього інциденту важливе для розуміння, як технічний прогрес може впливати на кримінальні схеми, а також нарощування зусиль у сфері кібербезпеки для захисту від подібних загроз.

Проаналізувавши наукові джерела, ми пропонуємо власний авторський підхід ретроспективного розвитку кримінальної відповідальності за правопорушення в кіберпросторі на теренах України. На нашу думку, варто виділити 6 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 рік – сьогодні).

Пропонуємо почати з першого етапу становлення й генези кримінальної відповідальності на теренах України, який ми окреслили як початковий, основний період якого припав на початок незалежності України. Парадокс розвитку людства полягає в тому, що протягом 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 [215, с. 34].

Ефективна система боротьби з банківськими злочинами може забезпечити стабільність банківського сектору України. Розробка такої системи вимагає аналізу інструментів інституціональної політики для протидії загрозам стабільності банківської системи [314].

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 різного типу шахрайства в мережах електрозв'язку стають відправною точкою історії кримінальних правопорушень у кіберпросторі на теренах нашої держави [93].

Основною характеристикою другого етапу, який припадає на 2001 рік, є набрання 5 квітня 2001 року чинності Кримінальним кодексом України.

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) [121].

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 деякі науковці трактують доктринальне поняття кримінального правопорушення, вчиненого у кіберпросторі, зокрема, 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 виступають суспільні відносини у сфері цифрової інформації, а комп'ютер може виступати 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 [19].

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 та комп'ютерних мереж і мереж електрозв'язку трактувала електронно-обчислювальну техніку як комплекс електронних технічних засобів, побудованих на основі мікропроцесорів та призначених для автоматичного оброблення інформації при вирішенні обчислювальних та інформаційних завдань [255].

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, однак через брак спеціальних знань в органах внутрішніх справ такі посягання залишалися нерозкритими. 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 й динамічний розвиток комп'ютерних мереж й 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 та швидкому

співробітництві в кримінальних питаннях.

Основною метою 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 у кіберпросторі; 5) ефективна міжнародна співпраця 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 види кримінальних правопорушень у кіберпросторі, зокрема:
1) правопорушення проти конфіденційності; 2) правопорушення, пов'язані з комп'ютером; 3) правопорушення, пов'язані зі змістом; 4) порушення, пов'язані з авторськими та суміжними правами [107].

Зокрема, правопорушення проти конфіденційності охоплювали: незаконний доступ, нелегальне перехоплення, втручання в дані, втручання в систему та зловживання пристроями. Фактично правопорушення проти конфіденційності, закріплені в Конвенції, відображені в главі XVI Особливої частини Кримінального кодексу України. До таких кримінальних правопорушень належали різного типу 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, поділяються на підробку,

пов’язану з комп’ютером, та шахрайство, пов’язане з комп’ютером. Такі правопорушення знайшли відображення в Кримінальному кодексі України в статтях 200, 358 та 190. Зокрема, до них належать будь-які види віртуального шахрайства, «скам», «фішинг», підроблення електронних документів для отримання кредитів, підроблення документів для відкриття рахунків в електронних платіжних системах тощо.

Стаття 9 Конвенції про кіберзлочинність визначає як правопорушення вироблення, пропонування, розповсюдження, здобуття й володіння дитячою порнографією. Зокрема, стаття 301 Конвенції про кіберзлочинність встановлює відповідальність за одержання доступу до дитячої порнографії, її придбання, зберігання, ввезення, перевезення чи інше переміщення, виготовлення, збут і розповсюдження. Так само зазначено, що одержання доступу до дитячої порнографії з використанням інформаційно-телекомунікаційних систем або технологій слід вважати умисним, якщо доведено, що особа усвідомлювала, що у такий спосіб вона одержить доступ до дитячої порнографії [121].

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-обчислювальних машин, систем та комп’ютерних мереж і мереж електрозв’язку належать: 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, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації. Такі несанкціоновані дії з інформацією передбачають, що вони вчинені особою, яка не мала на це права, а також що доступ до інформації 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 велику 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 у статті 363, усі дії пов'язані з порушенням правил експлуатації, але стаття 363-1 окремо виділяє конкретні дії, які спрямовані на перешкоджання функціонуванню інших комп'ютерних приладів, їх систем і мереж.

Статтею 176 Кримінального кодексу України встановлюється 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 кримінального правопорушення, виду вчинення й предмета кримінального правопорушення. На нашу думку, при кваліфікації кримінальних правопорушень, вчинених у кіберпросторі, акцентується увага на визначенні наведених факультативних ознак.

Розглядаючи четвертий етап, який припадає на 2009 – 2015 роки, варто наголосити, що в цей період спостерігається динаміка росту 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 для попередніх етапів було характерне 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 та причин таких правопорушень. Ураховуючи той факт, що певні кримінальні правопорушення 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 та 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 у всій системі тіньової економіки. І як результат – можливість анонімно здійснювати різноманітні операції економічного характеру, що не можуть бути контрольовані державою. Поступово інтернет-мережа починає бути каналом фінансування тероризму [213].

Кіберпростір дозволяє 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 [96].

Стають популярними такі кримінальні правопорушення, як кардинг, скамінг, фішинг і чорний рефаундінг. Кардинг – це використання в операціях реквізитів платіжних карт, отриманих зі зламаних серверів інтернет-магазинів, платіжних і розрахункових систем, а також із персональних комп’ютерів (безпосередньо або через програми віддаленого доступу, «трояни», «боти») [233, 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 з переказу або обміну валюти, інтернет-магазинів тощо [302].

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 покупцю, 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 приклад, що в 2010 році співробітники Міністерства внутрішніх справ затримали групу білорусів, які викрадали гроші з іноземних карт-рахунків. Для переведення в готівку вони купували через Інтернет дорогі турпутівки в країни Азії та інші країни й перепродавали їх за пів ціни. У 2012 році більшість цих людей відпустили, оскільки вони відшкодували збитки розміром понад 330 тис. доларів [23].

П'ятий етап характеризується чотирма визначальними факторами. По-перше, створенням спеціалізованого правоохоронного органу –«Департаменту кіберполіції Національної поліції України» 5 жовтня 2015 року, по-друге, ухваленням Закону України «Про основні засади забезпечення кібербезпеки України», по-третє, ухваленням рішення «Про Стратегію кібербезпеки України» та, по-четверте, стрімким розвитком криптоактивів.

Законом України «Про основні засади забезпечення кібербезпеки України» установлено основні поняття, такі як кіберпростір, кібербезпека, кіберзлочин, кібератака, кіберзагроза та інші. Зокрема, під кіберпростором

варто розуміти 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. Відповідно до законодавчого визначення кіберпростору можемо відмітити певні характерні йому ознаки: 1) віртуальний характер; 2) є комунікативним середовищем; 3) утворюється за допомогою електронних комунікацій та мережі Інтернет [203].

Кримінальне правопорушення в кіберпросторі (комп'ютерне кримінальне правопорушення) законодавець визначає як суспільно небезпечне діяння в кіберпросторі, 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, які 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: 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 набуває особливо значущого та суміжного феномену в рамках кіберпростору. Вона виступає різновидом електронних грошових коштів, алгоритми діяльності яких базується та функціонує на основі механізму асиметричного шифрування [26, с. 327].

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

Таблиця 1. Переваги та недоліки криптовалюти

Перевага	**Недолік**
Простота користування гаманцем	Певні держави можуть заборонити криптоплатежі на своїй території (а деякі вже заборонили: певні райони Китаю, Ісландія, Таїланд, Киргизія, Болівія та ін.)
Доступність. Дозволяє 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 здатність призводять до незворотної втрати всієї накопиченої валюти
Має децентралізований характер, відсутність єдиного цифрового банку	Ненадійність (криптовалюта може як упасти, так і піднятися в ціні за короткий період часу)
Анонімність – детальна інформація щодо власника криптогаманця відсутня	Виникає загроза для економічного й фінансового життя держави та суспільства, в разі неможливості регулювати, контролювати криптовалюту (через відсутність або недостатність відповідного законодавства, спеціалістів та 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 та поповнення електронних гаманців, а також цілодобова доступність і швидкісні проведення транзакцій (протягом декількох секунд). Криптогаманець фізичної особи найчастіше має прив'язку до електронної пошти або номера мобільного телефона. Тож 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 противоправних 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 вчинили кримінальні правопорушення в кіберпросторі, почали використовувати цю вразливість у своїх інтересах. Усе більше як державних, так і приватних послуг почали надавати онлайн, розпочало створюватися електронне державне урядування. Спостерігається поступове витиснення 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, вчинені в кіберпросторі, відбуваються щохвилини й завдають 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 [80]. Простота вчинення кримінальних правопорушень. Безліч доступних форумів та чатів, де можна знайти способи та методи скоєння того чи іншого правопорушення: починаючи від «кардингу» – до методів ведення інформаційної війни та кібертероризму.

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

3. 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 скоєння кримінальних правопорушень, а також заходи безпеки для осіб, які вчиняють кримінальні правопорушення у кіберпросторі.

Актуальні тренди породили нові види кримінальних правопорушень у

кіберпросторі та сприяли 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 правопорушенньь**	**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
1	2	3
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 [135, 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 кіберпросторі, усе більше можливостей для реалізації своїх незаконних намірів. З огляду на це ми вважаємо необхідним побудувати нову національну модель забезпечення кібербезпеки держави загалом та кожного громадянина, компанії й організації зокрема. Така модель має ґрунтуватися на чіткій координації між правоохоронними органами, органами фінансового нагляду та судовими системами, а також на їх задовільній кадровій, матеріально-технічній підтримці.

Сучасний стан кіберзлочинності несе великі загрози для суспільства, і з кожним роком кількість кримінальних правопорушень у кіберпросторі зростає, що поглинає усе більше коштів. Злочинність у кіберпросторі становить глобальну небезпеку 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, а це дає йому змогу існувати протягом такого тривалого періоду часу.

Підсумовуючи вищевикладене, зазначаємо, що початок розвитку кримінальної відповідальності за кримінальні правопорушення в кіберпросторі датують початком 70-х років XX століття. 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 та 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. Методологічні засади дослідження кримінальних правопорушень у кіберпросторі

Існує багато способів визначення дослідження. Простіше кажучи, дослідження включає збір, упорядкування та впровадження інформації, щоб зрозуміти, пояснити або довести теорію чи тему. Незважаючи на те, що дослідження є життєво важливими як у науковій, так і в ненауковій сферах, одним із найбільш відповідних і всебічних типів досліджень є наукове дослідження.

Якщо б ми обговорювали історію наукових досліджень, то повинні були б повернутися до витоків науки та самих досліджень. Найдавніші розробки цих двох термінів можна простежити до Стародавнього Єгипту та Месопотамії, десь від 3000 до 1200 років до нашої ери. Сучасна ера наукових досліджень бачила дивовижні успіхи та досягнення лише за останні кілька століть, і в найближчому майбутньому вони лише продовжуватимуть зростати.

Наукові дослідження використовують різноманітні наукові моделі,

теорії та колекції даних, щоб знайти пояснення того, чому певні явища відбуваються в реальному світі. Через експерименти, тематичні дослідження чи фокус-групи наукові дослідження можна проводити багатьма різними способами. Кінцевою метою наукових досліджень є розширення людських знань.

Наукові дослідження важливі, оскільки вони допомагають нам зрозуміти, як все працює. Крім того, вони далі розвивають різні галузі. Саме наукові дослідження допомагають вирішити існуючі проблеми та нові, які можуть виникнути в майбутньому. Завдяки науковим дослідженням прості спостереження та теорії можна перетворити на практичне навчання та встановлені факти [513].

Дослідники організовують своє дослідження шляхом формулювання та визначення проблеми дослідження. Це допомагає їм зосередити дослідницький процес, щоб вони могли зробити висновки, що найкращим чином відображають реальний світ. У дослідженні гіпотеза – це запропоноване пояснення явища. Нульова гіпотеза – це гіпотеза, яку дослідник намагається спростувати. Зазвичай нульова гіпотеза представляє поточний погляд/пояснення аспекту світу, який дослідник хоче оскаржити.

Юридичне наукове дослідження має свої особливості, які відрізняють його від досліджень у інших наукових галузях. Ось кілька особливостей юридичного наукового дослідження. Насамперед юридичне дослідження зосереджене на вивченні права, його принципів, норм та інститутів. Воно має на меті розкриття юридичної сутності об'єкта дослідження і визначення його місця в правовій системі.

Юридичне дослідження базується на законодавчих нормах, міжнародних договорах, прецедентах та інших джерелах права. Воно вимагає аналізу та інтерпретації нормативних актів та розробки висновків на їх основі. Тому юридичне дослідження включає правовий аналіз, який полягає в систематичному дослідженні та інтерпретації правових норм, розгляді практики їх застосування та вивченні відповідних судових рішень.

Юридичне дослідження використовує нормативно-правовий метод, що передбачає аналіз текстів нормативних актів, їх порівняння, класифікацію та систематизацію.

Юридичне дослідження підпорядковується специфічній юридичній логіці. Воно потребує аргументованості, логічної послідовності та дотримання принципів юридичного мислення.

Також юридичне дослідження часто відбувається у формі дискусій та наукових обговорень. Воно підтримується обміном думками, аргументацією позицій та переглядом наукових доказів.

Юридичне дослідження має високі вимоги до правової доведеності та обґрунтованості висновків. Це означає, що дослідження повинне базуватися на об'єктивних доказах, юридичній літературі, судовій практиці та інших авторитетних джерелах.

Ці особливості роблять юридичне наукове дослідження унікальним і вимагають від дослідників глибоких знань у галузі права, вміння застосовувати правові методи та дотримання високих стандартів наукової обґрунтованості.

Методологія юридичного дослідження передбачає висунення дослідником альтернативної гіпотези, гіпотези дослідження, як альтернативного способу пояснення явища.

Дослідник перевіряє гіпотезу, щоб спростувати нульову гіпотезу, не тому, що йому/їй подобається дослідницька гіпотеза, а тому, що це означало б наблизитися до пошуку відповіді на конкретну проблему. Дослідницька гіпотеза часто базується на спостереженнях, які викликають підозру, що нульова гіпотеза не завжди правильна [414].

Методологія дослідження має на меті зробити дослідника систематичним у його мисленні, пропозиціях та дослідженнях, вільним від інтелектуального застою та орієнтованим на творчість, оновлення, критику та систематичний та організований аналіз, а також уникнення будь-яких довільних суджень дослідника або впадання в наукову наївність, засновану

від ступеня його озброєності науковою методологією та методами і прийомами дослідження. Під підходом розуміється шлях або шлях (у сфері мови), і він визначається як: шлях, який веде до розкриття істини в науках за допомогою набору загальних правил, які домінують у функціонуванні розуму та визначають його операції, поки не буде досягнуто відомого результату. Методологія – це розділ епістемології, який займається вивченням навчальних програм або методів, які дозволяють отримати доступ до наукового знання про речі та явища [429].

У пошуковій методології дослідження, наприклад у деяких якісних дослідженнях незалежні та залежні змінні, можуть бути не визначені заздалегідь. Вони можуть бути не вказані, тому що дослідник ще не має чіткого уявлення про те, що насправді відбувається.

Змішані змінні – це змінні зі значним впливом на залежну змінну, які дослідник не зміг контролювати або усунути, – іноді через те, що дослідник не усвідомлює ефекту змішуючої змінної. Головне – виявити можливі змінні, що змішують, і якось спробувати їх усунути або контролювати.

Вибір методу дослідження має вирішальне значення для того, які висновки ви можете зробити про явище. Це впливає на те, що ви можете сказати про причину і фактори, що впливають на явище.

Також важливо вибрати метод дослідження, який буде в межах можливостей дослідника. Час, гроші, здійсненність, етика та доступність для правильного вимірювання явища є прикладами проблем, які стримують дослідження [414].

Існує багато видів методів дослідження. Залежно від типу дослідження використовуються різні методи. Методи дослідження в науці базуються на так званому науковому методі. Науковий метод – це основний процес, якого дотримуються всі дослідники, досліджуючи певну тему. Ці методи важливі, оскільки переконання людини можуть впливати на те, як вона інтерпретує певні явища. Використовуючи ці специфічні методи, дослідники можуть зменшити помилки, засновані на власних упередженнях [462].

Усі методи дослідження базуються на науковому методі. Термін «науковий метод» відноситься до тієї інтелектуальної структури, в якій діє розум дослідника, тоді як слово «метод дослідження» означає застосовані кроки для цієї інтелектуальної структури, і ця різниця не означає, що ці два терміни, тобто. конфлікт між ними. І метод, але ця відмінність призначена для уточнення та тлумачення. У будь-якому науковому дослідженні розумові процеси в свідомості дослідника мають інтегровану структуру та організацію, яка спрямовує його практичні кроки. Тому бажано, щоб кожен термін розглядався з одного боку, з двох, щоб слово «метод» використовувалося для позначення прикладного аспекту дослідницьких кроків. Щоб прояснити це докладніше, репрезентація залежить від уявлення про існування проблеми, з якою стикаються двоє людей, перший плутається, намагається і робить помилки, поки не прийде до вирішення цієї проблеми, яке може бути правильним або неправильним, але в обох випадках він не вважається науковим дослідником, оскільки він не вирішив її відповідно до розумової організації, яка може. Що стосується другого, він має справу з проблемою науковим шляхом, тобто він приступив до її вирішення певним інтелектуальним шляхом. Кроки, які вчені називають «кроками наукового мислення», є результатами його дослідження та перевірки. Що стосується кроків наукового методу мислення, вони майже такі ж, як кроки будь-якого методу дослідження, але з деякими деталями, які відрізняються залежно від різних методів дослідження. Однак інтелектуальний метод – це те, що організовує будь-який метод дослідження [472].

Науковий метод складається з чотирьох основних компонентів. Процес починається з базового спостереження та опису явища. Спостереження змушують дослідників розглядати питання про те, чому відбуваються певні явища. Потім дослідники висувають гіпотезу або передбачення того, що станеться або яким буде результат певних явищ. Згодом вони проводять певні типи експериментів, щоб підтвердити або спростувати це передбачення [462].

Кількісні методи дослідження різноманітні; однак вони чітко

дотримуються наукового методу. Ці методи стосуються проведення експериментів з метою дослідження конкретної гіпотези. Гіпотеза – це передбачення щодо явища, яке стверджує, як дві речі пов'язані між собою. Вони називаються незалежними та залежними змінними. Експерименти вивчають взаємозв’язки між цими змінними з метою виявлення причини цих явищ.

На відміну від кількісних методів, якісні методи не ґрунтуються на передбаченні між двома змінними. Натомість якісні методи використовуються для відкритого дослідження певної теми. Ці методи особливо корисні для розгляду тем, про які мало відомо, і для розуміння суб’єктивної інформації, наприклад, досвіду окремих людей. Тематичні дослідження, спостереження за учасниками, опитування та інтерв’ю – все це методи якісного дослідження.

Хоча в багатьох дослідженнях використовується лише один метод дослідження, існує багато способів поєднання методів. Наприклад, дизайн змішаних методів – це спосіб поєднання якісних і кількісних методів дослідження для глибшого розуміння явища. У цих типах проєктів використовується як традиційна наукова методологія, як-от проведення експерименту з більш дослідницькими методами, як-от тематичне дослідження. Хоча ці проєкти можуть бути дорогими та обтяжливими для дослідника, вони також можуть створити надійне дослідження, об’єднавши сильні сторони обох методів [462].

Проєктування методології дослідження для вивчення кримінально-правової охорони кіберпростору має кілька важливих переваг. Воно забезпечує ефективність розслідування шляхом створення структурованого та систематичного підходу, що дозволяє уникнути пропусків та забезпечує більш точне та ефективне дослідження. Крім того, така методологія гарантує надійність та достовірність дослідження з чітко визначеними кроками та процедурами, які дозволяють збирати, зберігати та аналізувати докази відповідно до встановлених стандартів. Врахування вимог кримінального законодавства забезпечує юридичну відповідність

дослідження, яке є предметом законності та прийнятності доказів у судових процесах. Також методологія співпраці та координації між різними структурами забезпечує взаємодію між правоохоронними органами, експертами з компаніями з кібербезпеки та іншими зацікавленими сторонами, які отримали обмін інформацією та результативність дослідження.

Крім того, розробка такої методології сприяє професійному розвитку фахівців у цій галузі, вдосконалює їхні навички, знання та покращує розробку нової техніки та підходи до дослідження і розслідування кримінальних правопорушень у кіберпросторі. Загалом методологія проєктування дослідження відіграє ключову роль у забезпеченні ефективного, надійного та юридично відповідного розслідування кримінальних правопорушень у кіберпросторі, що сприяє покращенню кібербезпеки та захисту прав потерпілих сторін.

Дослідження кримінально-правової охорони кіберпростору в Україні було проведене за допомогою різних методів. Пропонуємо зосередити увагу на характеристиці кожного із цих методів.

Метод аналізу правових актів включає дослідження законодавчих актів, які регулюють кіберкримінальну відповідальність в Україні. Дослідник може аналізувати Кримінальний кодекс України, законодавство у сфері кібербезпеки та інші відповідні нормативні акти, щоб визначити становлення та еволюцію правового регулювання кримінальної відповідальності за кримінальні правопорушення у кіберпросторі.

Емпіричний метод включає збір та аналіз емпіричних даних, таких як статистика злочинності у кіберпросторі, судові рішення, звіти правоохоронних органів та інші джерела. Шляхом вивчення цих даних можна розкрити тенденції та зміни в кримінальній відповідальності за кримінальні правопорушення у кіберпросторі протягом певного періоду.

Метод контент-аналізу передбачає систематичний аналіз текстового або медійного контенту, що стосується кримінальної відповідальності за кримінальні правопорушення у кіберпросторі. Дослідник може аналізувати

законодавчі документи, судові рішення, наукові статті, засоби масової інформації та інші джерела, щоб зрозуміти еволюцію підходів до кримінальної відповідальності у кіберпросторі.

Метод кейс-студії включає детальне вивчення конкретних випадків вчинення кримінальних правопорушень у кіберпросторі в Україні. Дослідник може аналізувати судові процеси, методи розслідування, способи збору доказів та прийняття судових рішень, щоб з'ясувати, яким чином формується кримінальна відповідальність за кримінальних правопорушень у кіберпросторі в Україні та як вона змінюється з часом.

Порівняльно-правовий метод передбачає порівняння кримінально-правової характеристики кримінальних правопорушень у кіберпросторі у різних країнах або регіонах. Так можна аналізувати законодавство, судову практику та політику щодо кримінальних правопорушень у кіберпросторі у різних юрисдикціях, щоб встановити схожість та відмінності, а також ідентифікувати кращі практики.

Метод концептуального аналізу передбачає аналіз понять, теоретичних моделей та концепцій, пов'язаних з кримінальними правопорушеннями у кіберпросторі. Так, дослідник може вивчати різні теоретичні підходи до визначення та пояснення кримінальними правопорушеннями у кіберпросторі, аналізувати концепції кібербезпеки, кримінального поведінки та інші концептуальні рамки для формулювання кримінально-правової характеристики.

Використання системного аналізу дозволяє розглянути кіберпростір як складну систему, включаючи взаємодію різних суб'єктів, процесів та факторів. Це допомагає виявити взаємозв'язки та впливові фактори, що впливають на кримінальну кваліфікацію та призначення покарання у кіберпросторі.

Залучення експертів, які мають досвід у кібербезпеці, правознавстві або інших відповідних галузях, може допомогти у формуванні кваліфікаційних критеріїв та розумінні особливостей призначення покарання за вчинення

кримінальних правопорушень у кіберпросторі.

Застосування соціологічних методів, таких як анкетування, інтерв'ювання або спостереження, може допомогти вивчити погляди, думки та переконання учасників кримінального правопорушення у кіберпросторі, а також фактори, які впливають на їхнє рішення вчиняти злочини та підбирати покарання. Для потреб цього дослідження ми використовували: метод аналізу; емпіричний метод; метод контент-аналізу; метод кейс-студії; порівняльно-правовий метод; метод системного аналізу.

Комбінування різних методів у науковому дослідженні про кримінально-правову охорону кіберпростору має важливість з декількох причин. Воно дозволяє охопити різноманітні аспекти проблеми, збільшити обсяг дослідження і отримати більш повне розуміння проблеми. Комбінування різних методів також сприяє забезпеченню достовірності отриманих результатів, оскільки кожен метод має свої обмеження і може призвести до помилок. Використання декількох незалежних методів дозволяє перевірити й підтвердити отримані результати, підвищуючи надійність дослідження. Комбінування різних методів також дозволяє застосовувати комплексний підхід до аналізу проблеми кримінально-правової охорони кіберпростору. Наприклад, соціологічні методи можуть доповнювати правовий аналіз, а технічні методи можуть допомогти виявити технічні уразливості кіберпростору. Комбінування різних методів дослідження також сприяє отриманню ширшого розуміння проблеми кримінально-правової охорони кіберпростору, оскільки різні методи дозволяють досліджувати проблему з різних перспектив і аналізувати її з різних точок зору. Тому компонування різних методів дослідження у науковому дослідженні про кримінально-правову охорону кіберпростору є важливим для розширення обсягу дослідження, забезпечення достовірності результатів, застосування комплексного підходу і отримання глибшого розуміння проблеми.

1.3. Теоретико-правові підходи 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 призвело сучасних мислителів до висновку, що людське суспільство зазнало справді серйозних якісних змін. Характер цих змін дозволяє констатувати початок нової ери в розвитку історії людства – ери мережевого панування [431].

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 призвів до появи мережевого суспільства, що характеризується складністю та структурним дисбалансом [135, 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 та 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 несуть шкоду значному колу приватних, державних і корпоративних інтересів [363].

Інтеграція держави у всесвітній інформаційний простір, розвиток інформаційного суспільства та глобальна діджиталізація призвели до виникнення нових загроз національним інтересам України в кіберпросторі.

Основними тенденціями розвитку загроз є: 1) збільшення кількості

атак, багато з яких призводять до великих збитків; 2) підвищення складності атак, що охоплюють кілька етапів і можуть передбачити спеціальні методи захисту від можливих контрзаходів; 3) вплив майже на всі електронні (цифрові) пристрої, серед яких останнім часом усе більшого значення (та найбільше піддаються ризикам у сфері інформаційної безпеки) набувають 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 методів кібератак на інші країни [468].

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, інша друкована продукція, телефонія, Інтернет [463].

Розглядаючи поняття «інформаційного простору» з точки зору інформаційної безпеки, словник термінів і визначень у галузі інформаційної безпеки визначив інформаційний простір як сукупність інформації та інформаційної інфраструктури; сферу діяльності, пов'язану із створенням, перетворенням і використанням інформації, зокрема індивідуального й суспільного створення, інформаційно-телекомунікаційну інфраструктуру та власну інформацію [171].

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 здійснює обробку, зберігання,

використання й передачу інформації за допомогою різного типу технічних засобів та інших технологічних рішень. За такого підходу інформаційному простору властива обмеженість і прихильність до каналів поширення даних [333].

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. Дзялошинський 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 [73, 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» [72, 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: 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 [240, с 117].

Л. Білоусов зазначає, що створення, передача, накопичення та зберігання інформації відбувається за допомогою певних суб'єктів інформаційного середовища, а сам інформаційний простір визначає як коло інтересів інформаційної взаємодії чи впливу; інформація, призначена для використання суб'єктами інформаційної сфери; інформаційна інфраструктура, що забезпечує можливість обміну між суб'єктами; соціальні відносини, створювані через формування, передачу, розподіл і зберігання інформації, обмін інформацією всередині суспільства [20].

Тож 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, недоторканністю приватного життя, та конвенціональні межі. Інформаційний простір є ширшим за кіберпростір, тобто останній виступає його частиною.

Поняття «віртуальний простір» також є значно ширшим за «кіберпростір», оскільки «віртуальний», як синонім слова «уявний», охоплює більше коло відносин, ніж ті, що обмежені комп'ютерними технологіями [259].

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

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 із умонтованою точкою зору, технології спіндокторингу (управління новинами та медіа-подіями) 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 [8, с. 8].

Віртуальний простір можна розглядати як середовище, створене комп'ютерними технологіями, що породжує аудіовізуальну реальність публічного простору, дозволяє людям взаємодіяти одна з одною й з репрезентованими в ньому об'єктами, організаційно-методологічні умови та сукупність технічних умов, містить програмне забезпечення для зберігання, оброблення та передавання інформації [425, с. 92].

Х. Мерітедж вважає, що сьогодні основними особливостями функціонування віртуального простору є: 1) медіатизація, що характеризується сукупністю масових явищ інформаційного впливу та взаємодії; 2) масова комунікація найважливіший інструмент проєктування та самопостановки віртуального простору; 3) використання практики електронної демократії 4) застосування smart-технологій [434].

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 інформаційно-телекомунікаційних мереж.

Розвиток віртуального простору породжує формування різноманітних форм і методів спілкування між користувачами. Віртуальність є більш досконалим та ефективним інструментом взаємодії й взаємовпливу [160]. Водночас Інтернет сприяє інтенсифікації комунікаційних процесів, що є

результатом стрімкого прогресу комп'ютерних технологій в усіх сферах суспільного життя. Таким чином створюється віртуальний публічний простір, який формує нові можливості та реалії спілкування, стає найбільш динамічною, технологічною й культурною економікою сучасності, соціальним і політичним явищем нашого часу [412].

На противагу «інформаційному простору» та «віртуальному простору», «інтернет-простір», навпаки, є надто вузьким поняттям, тому що на відміну від інтернет-мережі існують інші інформаційно-телекомунікаційні мережі, такі як FidoNet, Cren, Top, Freenet, Ants P2P та ін. Крім того, враховуючи структурні елементи Інтернету, можливо, у майбутньому його замінять міжнародною інформаційно-телекомунікаційною мережею 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 інформації 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 [258, 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; підтримка екологічно орієнтованих

інтернет-ініціатив щодо гуманного поводження з людьми в Інтернеті, що можуть не відразу окупитися; проєктування технологічних інтернет-інновацій та інтернет-комунікацій у сфері гармонізації процесу розвитку сучасної особистості з новими соціальними інфраструктурами, що виникають в інтернет-середовищі [128].

З початку появи інтернет-мережі майже кожна людина одержала можливість швидкого та оперативного доступу до інформації. Саме з огляду на інтенсивний розвиток інтернет-мережі стало можливим 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 вимові термін «кіберпростір» закріпився як один із широко використовуваних синонімів для мережі Інтернет, але варто пам'ятати, що поняття «кіберпростір» та «Інтернет» не є тотожними [505].

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 розмитості зазначеного феномену обумовлюють його недостатню вивченість, проте вже існують загальні, принципові положення, одержані в результаті сучасних напрацювань [21, 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 розглядає 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 в 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» у сенсі як «мистецтво рульового», як «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 [428].

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 та неперервність [104].

Еволюція кібердискурсу сприяла появі цілого нового набору термінів, що позначають появу нового світу, створеного поширенням комп'ютерно-опосередкованої комунікації (СМС). Сьогодні префікс «кібер-» використовують у словах, що позначають зв'язок з електронними мережами зв'язку й віртуальною реальністю [39].

Для формування конкретної дефініції поняття кіберпростір, а також

визначення його сутності спробуємо виокремити його специфічні ознаки. На думку А. Люіса, кіберпростір має наступні 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 жоден оператор зв'язку; 4) є простором, у якому будь-яка особа може вільно діяти, висловлюватися та навіть працювати [422].

Варто зауважити, що попри поширеність терміна «кіберпростір» у повсякденному житті, його сутність і специфіка не є чітко визначеними. У широкому розумінні кіберпростір ототожнють 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.

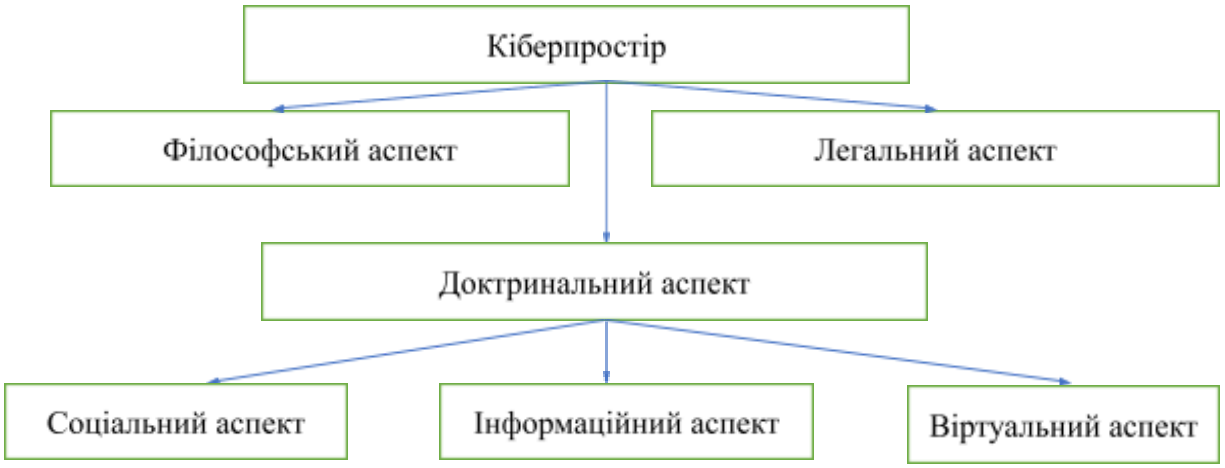


Рис. 1 – Аспекти кіберпростору

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 [431].

Канадський письменник-фантаст В. Гібсон уперше написав про кіберпростір у «пророчому» оповіданні Burning Chrome, опублікованому в липневому номері журналу Omni за 1982 рік, як «штучний інтелект», «віртуальна реальність», «транснаціональні корпорації», «матриця» [380].

Роман В. Гібсона 1984 року «Нейромант», у якому автор визначає кіберпростір, як середовище «сенсорних галюцинацій», що щодня

відчувають мільярди операторів з усіх націй, зокрема діти, набув особливої популярності в цьому контексті [381].

Графічне репрезентування комп'ютерних даних осіб. Неймовірна складність. Потоки світла, кластери й сузір'я інформації, упорядковані людським розумом. Зокрема, завдяки роботам 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 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» [325].

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 [437].

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 [440].

Тож в офіційному дискурсі безпеки Сполучених Штатів Америки кіберпростір розглядають саме як фізичний простір. Директор Національного центру біотехнологічної інформації Дж. Лімпан наголошував, що визначення такого відходу 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 [423].

Комплексний документ з оцінювання стану безпеки кіберпростору Сполучених Штатів Америки «Кібербезпековий огляд» від 2009 року визначає кіберпростір як інформаційну сферу, сукупність інформації, інформаційних систем, суб'єктів та об'єктів інформації, сайтів в інформаційно-телекомунікаційних мережах, мережі зв'язку, інформаційні технології.

Відповідно до визначення, запропонованого в президентській Директиві з національної безпеки, кіберпростір – це як 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 й як спеціальну структуру, що поєднує різних індивідуумів з усього світу: користувачів мережі, поширювачів інформації, сервіс-провайдерів та інших зацікавлених осіб [495].

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 складової, директива визначає інформаційну базу, що складається з потоків інформації, які люди передають один одному за допомогою мережевих засобів зв'язку. Директива визначає кіберпростір як 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 надаються за їх допомогою. Причому бути користувачем таких послуг лише за допомогою електронно-обчислювальних машин та засобів зв'язку комп'ютерної мережі [438].

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») [439].

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 [344].

Кіберпростір представляє собою віртуальне середовище, створене за допомогою інформаційно-телекомунікаційних мереж. У цьому середовищі користувачі мають можливість здійснювати широкий спектр взаємодій, включаючи адміністративні, цивільні та кримінальні правовідносини. Кіберпростір може бути частиною будь-якої інформаційної мережі, зокрема Інтернету, який слугує яскравим прикладом такого середовища. Проте важливо розуміти, що Інтернет сам по собі не є кіберпростором, але створює умови для його існування.

Водночас визначення кіберпростору як інформаційно-телекомунікаційного середовища важливе для розуміння його правового та соціального контексту. Це середовище не тільки дозволяє

користувачам взаємодіяти в різних правових полях, але й відкриває нові можливості для кіберзлочинності та вимагає посилення правових рамок для захисту цифрової інформації. На нашу думку, співставлення кіберпростору та Інтернет- простору, як його частини, допоможе зрозуміти структуру цифрового світу та необхідність адаптації правових норм для забезпечення безпеки та стабільності в цьому середовищі, що швидко змінюється.

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 [400].

Інтернет Верховний Суд США визначає 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». Тобто це 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 з використанням мережі Інтернет та/або інших глобальних мереж передавання даних [203].

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

З точки зору доктринального аспекту визначення поняття «кіберпростору» можна розглядати в соціальній, інформаційній та

віртуальній характеристиках [401; 484; 475].

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 [403].

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 відображення 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 [284, с. 311].

Розгляд і дослідження кіберпростору в контексті психологічної герменевтики й семіотики можливе 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 є можливість відкривати додаткові значення, конструювати нові. Процес семіотичного моделювання є основою для формування суб'єктивної реальності особистості [429].

У праці одного з перших дослідників проблем кіберпростору Е. Кетша зазначено, що концептуально це поняття пов'язано з розвиненою електронною культурою, яка дозволяє 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 [411, 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 полегшує та істотно прискорює розумову діяльність людей [327, 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, без організаційних, культурних, національних чи політичних кордонів збирання, зберігання й передавання даних та інформації між електронним обладнанням [494, с. 310].

За визначенням П. Воллі, кіберпростір – це принципово новий вид проєкційного середовища культури, який з'єднує реальність і сучасну технологічну сферу, полегшуючи й прискорюючи цим інтелектуальну діяльність людини [513].

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 їх груп, в Інтернеті також є електронні помічники (програми штучного інтелекту), яких навчають створювати й поширювати контент

самостійно [417].

С. Гахов, аналізуючи кіберпростір з точки зору соціальної діяльності, зазначає, що його зміст становлять соціальні відносини між власниками інформаційних систем, власниками інформації, споживачами (користувачами), спеціально уповноваженими державними органами, роботодавцями, працівниками, юридичними та фізичними особами. Зокрема, до таких він відносить: 1) виробників ІТ-продуктів та ІТ-послуг тощо;
2) правові норми, що регулюють відповідні суспільні відносини, що 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 [53,
с. 55].

Отже, кіберпростір – це соціальний феномен, оскільки він наповнений людьми, 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 складову людської реальності.

Очевидно, що кіберпростір і реальний простір 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 призвели 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, протікає 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 [406].

На думку С. Рибки, кіберпростір – це середовище, утворене організованою сукупністю інформаційних процесів (створення інформації, передавання, використання) за участю людини, зокрема на об'єктах критичної інфраструктури держави із застосуванням ресурсів складових частин національної інформаційно-комунікаційної інфраструктури [216, 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, через яку насправді кіберпростір є децентралізованим і не належить ні державі, ні конкретній особі.

Д. Дубов наголошує, що кіберпростір – середовище, створене організованою сукупністю інформаційних процесів на основі інформаційних, телекомунікаційних та інформаційно-телекомунікаційних систем, уніфікованих за загальними принципами та правилами незалежно від форми власності [74, с . 112].

Дж. Василевскіх наголошував, що термін кіберпростір використовують 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 [510, с. 227].

Очевидно, що кіберпростір є інформаційним простором.

На цьому акцентують увагу В. Гавловський [51, с. 51] і В. О. Голубєв, які у статті «Боротьба з комп'ютерними злочинами – проблема транснаціонального масштабу» описують термін «кіберпростір» як інформаційний простір, створений за допомогою комп'ютера, в якому необхідно позначити об'єкти або символічний прояв інформації-простір, де діють переміщення комп'ютерних програм і даних [58].

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 [322].

С. Хілдерт визначає кіберпростір як одну з багатьох форм віртуальної реальності, але наголошує: 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, що використовується для опису об'єктів, широко поширених у комп'ютерній мережі [280].

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 [277, с. 163].

В. Бурячок розуміє кіберпростір як віртуальне комунікаційне середовище, утворене системою зв'язків між користувачами та об'єктами інформаційної інфраструктури, такими як IP для передавання інформації, яка циркулює в них, з метою задоволення інформаційних потреб суспільства [31, с. 190].

С. Гнятюк пропонує визначати кіберпростір як віртуальний простір, що виникає в результаті взаємодії користувачів, програмно-апаратних засобів і мережевих технологій (зокрема Інтернету) для підтримки й управління процесами перетворення інформації (електронних інформаційних ресурсів) для задоволення інформаційних потреб для охоплення суспільства [56, с. 123].

Наступним етапом аналізу поняття «кіберпростір» є окреслення та детальне характеризування його сутнісних ознак. У наукових джерелах відсутня стала позиція 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 жоден оператор зв'язку; 4) є простором, у якому будь-яка особа може вільно діяти, висловлюватися та навіть працювати [492, с. 335].

К. Дарбік визначає такі ознаки кіберпростору: 1) випадковість;
2) неістотність; 3) необмеженість; 4) універсальність і поширеність;
5) інтерактивність; 6) динамічність; 7) гнучкість; 8) непередбачуваність;
9) ліберальність [406].

На думку А. Манжая, кіберпростір має три основні характеристики: це інформаційний простір, є комунікативним середовищем, утвореним за

допомогою технічних систем [136].

За С. Гаховим до основних характеристик кіберпростору належать його динамічність, функціональність, інформаційність та визначення його як середовища існування. Динамічність кіберпростору, на думку науковця, означає його постійно мінливий характер, а протяжність та обсяг кіберпростору 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 як 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 [53, 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. Тож 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, де 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 взаємопов'язаних комп'ютерних мереж. Отже, будь-яка зміна стану відповідних взаємопов'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. Інтернет складається з окремих комп'ютерів, серверів та інших технічних пристроїв, об'єднаних між собою провідним і бездротовим шляхом 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 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, наданими через Інтернет; 4) кіберпростір – це еволюційна складна динамічна система (system of systems), і тоді його передусім варто

розглядати саме так, незалежно від того, чи буде він проявляти свої технічні, інформаційні й соціальні аспекти [175].

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 кіберпростору, 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 володіння предметами (об'єкти інтелектуальної власності, платіжні продукти, матеріальні активи);

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

Як середовище взаємодії М. Мягка виділяє властиву кіберпростору специфіку:

- на відміну від реального світу кіберпростір не має кордону між країнами;
- кіберпростір не обмежений, кожний має свободу висловлення своєї думки;
- комунікація в кіберпросторі 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 [143, с. 141].

По-четверте, динамічність, кіберпростір не є чітко визначеним і конкретизованим. Зважаючи на це, його можна визначати 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 існує 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 [236, 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, які реалізовані в межах державних кордонів.

Як у вітчизняній, так і в іноземній науковій доктрині протягом усього інтегрування громадських та державних інститутів у кіберпростір звучали побоювання і щодо неефективності географічної територіальності в

міжнародному праві, і щодо відсутності збірних кордонів держав із межами реалізації їх влади [486, с. 177].

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

Сьогодні одночасно відбувається, 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 та 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 держави, щодо конкретної території та знаходження власності осіб у межах цієї території, і визначено, що перебування цих осіб та власності є цілком відомим. 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 [416, с. 50].

Тому можна визначити кіберпростір як частину інформаційного простору, який функціонує на основі інформаційно-комунікаційних технологій, що дозволяє 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: дисципліна, відповідальність, додержання прав та свобод людини й громадянина та своєчасного втручання.

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 додержуватися 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 подальшого їх використання для проведення широкомасштабних стабілізаційних заходів з підтримки безпечності кіберпростору.

Принцип дотримання 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 й свобод людини та громадянина. Так само приватні суб'єкти діяльності в кіберпросторі повинні враховувати й мінімізувати ризики порушення прав людини в інтернет-просторі та 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 попередження вчинення дій у сфері інформаційно-комунікаційних технологій, визнаних шкідливими або здатних створити загрозу міжнародному миру та безпеці. Проте варто зауважити, що така вимога фактично стосується лише урядових організацій і підприємств. Недержавні суб'єкти також можуть здійснювати атаки у відповідь на зловмисників, і подібні дії також можуть підірвати стабільність кіберпростору [445].

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, які є володільцями й розпорядниками інформації в хмарних сервісах, кожна людина тим чи іншим чином залучена до кіберпростору і 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 його можливостей (послуг, товарів отримання), і тому зацікавлені в належній політиці щодо охорони кіберпростору.

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 характеристикиками кіберпростору є такі: віртуальна складова, мережева належність, середовище взаємодії, динамічність, комунікативність, поєднання територіалізаії та детериторіалізації. Серед основних принципів, що забезпечують стабільність функціонування кіберпростору, варто виділити такі: принцип своєчасного втручання, принцип додержання прав і свобод людини й громадянина, принцип дисципліни, принцип відповідальності.

1.4. 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 століття поставило виклики перед загрозами не лише в реальному житті, а й у кіберпросторі.

На початку 2018 року було окреслено основні тенденції диджиталізації, зокрема: 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 [290].

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 [462].

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 [167].

Спостерігаємо, що в XXI столітті 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 мати здатність до обміну загалом або конкретної частини на інший товар в його матеріальному вигляді або 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 [485].

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 покращення інструментів їх вчинення створюють економічні загрози для глобальних інформаційних мереж [292, с. 122].

Розвиток кримінальних правопорушень у кіберпросторі одночасно відбувається у двох напрямах. 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» [472].

Крім того, використання інформаційно-телекомунікаційних систем дозволяє 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 у 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 [206].

Варто зауважити, що зазначена колізія кримінального законодавства виникла ще під час прийняття 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».

Тож 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 [134, с. 246].

У міжнародних нормативних актах і безпосередньо у 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 [106].

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 зазначених держав лише визначають його види. Виняток становить Кримінальний кодекс штату Канзас, у якому зазначено, що кримінальне правопорушення – це дія або бездіяльність, передбачені законодавством штату, за які може бути призначено покарання у вигляді позбавлення волі, смертної кари або штрафу [408].

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 з 1 січня 2020 року.

У 8 статті Конституції України закріплено, що в Україні визнається і діє принцип верховенства права, а нормативно-правові акти ухвалюють на основі Конституції України та повинні відповідати їй [110].

Одночасно спостерігаємо колізію в законодавстві про кримінальну відповідальність,у якій закріплено поняття «кримінального правопорушення»

та «кримінального проступку», що в Конституції України взагалі не згадані, 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 визначаються винятково законами України. Конституція України визначає засади цивільно-правової відповідальності, діяння, які визначаються як злочини, адміністративними й дисциплінарними правопорушеннями, та встановлює відповідальність за них.

Стаття 11 Кримінального кодексу України визначає 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 небезпечність, протиправність, винність і караність.

Перша з них – це суспільна небезпечність. Загалом суспільна небезпека кримінального правопорушення полягає в тому, що кримінальне правопорушення завдає або створює загрозу заподіяння шкоди суспільним відносинам, що охороняються законом про кримінальну відповідальність. Саме така ознака кримінального правопорушення, як суспільна небезпечність, 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 якої 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 та суб'єктивні ознаки кримінального правопорушення: його предмет, наслідки, характер, форма вини, мотив і мета є одними з основоположних категорій кримінального права, тому суспільна небезпека кримінального правопорушення повинна бути початковою й кінцевою точкою будь-якого кримінального розслідування [115, 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. Тож 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, у результаті якого правопорушник одержав доступ до даних браузера, об'єктом кримінального правопорушення будуть суспільні відносини у сфері нормального функціонування електронно-обчислювальних машин, а у 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 його 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 [269].

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 [273, 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 [110].

Отже навіть з положень Конституції випливає, що вина неодмінно є обов'язковим елементом будь-якого злочину або кримінального проступку, відсутність якого свідчить про відсутність самого складу кримінального правопорушення [48, с. 117].

Концепція вини як фундаментальної передумови кримінальної відповідальності відіграє вирішальну роль у правовій системі. Вона не лише забезпечує справедливість кримінального переслідування, але й слугує захистом від необгрунтованих звинувачень. Це утверджує необхідність чіткого розуміння правових норм та їх застосування в контексті захисту основних прав та свобод людини.

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 [357].

Повністю підтримуємо позицію, відповідно до якої емоційний стан є самостійною ознакою суб'єктивної сторони складу кримінального

правопорушення, адже, по-перше, він, 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) [48, с. 116].

Вину варто обговорювати у двох аспектах. По-перше, як ознаку кримінального правопорушення. По-друге, як складову суб'єктивної сторони кримінального правопорушення. Водночас необхідно зазначити, що будь-яке суспільно небезпечне діяння є актом добровільної і свідомої поведінки суб'єкта, а свідомість і воля є суб'єктивними критеріями такої поведінки [295, 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 таке діяння, вчинене винно, тому одним із складів вини є також здатність особи відчувати провину. Крім того, певний вплив на провину 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 [132, с. 350].

Стаття 23 Кримінального кодексу України визначає вину як психічне ставлення особи до своєї дії чи бездіяльності, а також до наслідків, передбачених законодавством, яке може мати форми умислу або необережності. Закон таким чином виділяє дві основні форми вини і поділяє їх на додаткові категорії. Визначення будь-якої форми вини завжди включає аналіз двох ключових аспектів: інтелектуального та вольового.

Ключ до розуміння вини у кримінальному праві в рамках теоретичного

дискусу полягає у визначенні, як особа ставиться до своїх дій та їх наслідків. Так, інтелектуальний аспект вини охоплює усвідомлення особою законності своїх дій або бездіяльності, тоді як вольовий аспект стосується бажання чи готовності особи діяти згідно з цим усвідомленням. Розрізнення між умислом та необережністю дозволяє правозастосовним органам точніше кваліфікувати дії особи, а також ефективніше застосовувати санкції, що відповідають ступеню її провини. Таке розуміння вини сприяє справедливості та законності в процесі кримінального переслідування.

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, обстановки, способу, знарядь), а також засобів вчинення злочину, коли ці ознаки були включені як конструктивні до складу конкретного злочину або кримінального правопорушення [276, с. 387].

Вивчення вини в кримінальному праві, особливо через призму думок П. Л. Фріса, дозволяє більш глибоко зрозуміти взаємозв'язок між усвідомленістю особи та її вольовими рішеннями в контексті вчинення кримінальних правопорушень. Інтелектуальний компонент підкреслює значення повної інформованості про елементи злочинної діяльності, а вольовий компонент оцінює ступінь контролю, який особа має над своїми діями та їх потенційними наслідками. Водночас, розрізняючи різні форми вини, правосуддя має змогу точніше визначати відповідальність та запобігати несправедливості, враховуючи ступінь усвідомлення та бажання особи щодо настання наслідків її дій.

При вчиненні кваліфікуючих або привілейованих кримінальних правопорушень, обставини, що їх характеризують, мають бути чітко усвідомлені особою. Також у випадках суспільно-небезпечних діянь, що включають матеріальні наслідки, особа має повністю розуміти потенційні наслідки своїх дій або бездіяльності. Вольовий аспект вини в цьому разі може виражатися через «бажання», «свідоме прийняття» наслідків або «легковажне

ставлення» до можливості їх запобігання. Визначальним є те, що вольовий компонент вини стосується виключно наслідків дій особи, що, своєю чергою, формує різні типи вини в залежності від ставлення до цих наслідків. Вольовий момент необережності характеризується тим, що особа або легковажно розраховувала на відвернення суспільно небезпечних наслідків (кримінальна протиправна самовпевненість), або повинна була й могла передбачити суспільно небезпечні наслідки (кримінальна протиправна недбалість) [49, 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, непередбаченого в ньому [110].

Деякі фахівці, які підтримують традиційне тлумачення протиправності у контексті кримінальних правопорушень, вказують на існування двох її форм. В. Борисов та О. Пащенко, аналізуючи протиправність як критерій вини в кримінальному праві, розрізняють пряму кримінальну протиправність, що означає непосередню заборону певної дії або бездіяльності за кримінальним законодавством, і змішану протиправність, що враховує визнання діяння протиправним також і за нормами інших галузей права. [170, с. 106].

Варто зауважити, що протиправність у кримінальному праві має значний вплив на судову практику і визначення відповідальності за кримінальні правопорушення. Співвідношення прямого та змішаного виду протиправності, на нашу думку, дозволить глибше проаналізувати юридичну природу суспільно небезпечних діянь, визначити межі їх регулювання різними галузями права. Пряма кримінальна протиправність підкреслює універсальність кримінального законодавства, тоді як змішана

протиправність вказує на взаємодію кримінального права з іншими правовими системами, забезпечуючи більш всебічний підхід до правопорушень.

Аналіз прямої та змішаної протиправності у кримінальному праві дозволяє глибше зрозуміти юридичну природу суспільно небезпечних діянь і визначити межі їх регулювання різними галузями права.

З такою ознакою, як протиправність, пов'язана і 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 зазначені в законодавчому визначенні поняття кримінального правопорушення, а випливають 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, що і є підставою вважати караність обов'язковою ознакою кримінального правопорушення. Крім того, варто зауважити, що караність пов'язана з такими ознаками кримінального правопорушення, як суспільна небезпечність, протиправність, винність, і є похідною від них [169].

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 кримінальних правопорушень у кіберпросторі; 2) анонімність кримінальних правопорушень у кіберпросторі; 3) транснаціональний характер кримінальних правопорушень у кіберпросторі; 4) латентність кримінальних правопорушень у кіберпросторі; 5) простір, у якому вчиняють кримінальні правопорушення; 6) застосування навичок соціальної інженерії; 7) суб'єктна складова; 8) дистанційність кримінальних правопорушень у кіберпросторі;

9) доступність матеріалів, необхідних для скоєння кримінального

правопорушення в кіберпросторі.

Надання специфічних характеристик кримінальних правопорушень у кіберпросторі, на нашу думку, доцільно почати саме з інтелектуальної характеристики. Інтелектуальний характер кримінальних правопорушень у кіберпросторі означає, що її вчинення вимагає певного набору навичок і знань як технологічного, так і комунікативного характеру. Крім того, залежно від виду кримінального правопорушення в кіберпросторі особа, яка його вчиняє, може володіти тими чи іншими специфічними навичками. Наприклад, особа яка здійснює кібершахрайство, повинна вміло 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 потребує характеристики, є анонімність. Анонімність як ознака кримінального правопорушення в кіберпросторі дозволяє 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, використання неправдивої інформації або взагалі «нікнеймів» створює в кримінального правопорушника певне відчуття безкарності та вседозволеності в кібернетичному просторі, оскільки ідентифікувати його надзвичайно складно. На нашу думку, саме анонімність як ознака кримінального правопорушення в кіберпросторі підштовхує користувачів інтернет-мережі до заняття кримінально-протиправною діяльністю 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 підкреслити, що 60 %

кримінальних правопорушень у кіберпросторі вчиняються організованими групами, учасники яких є громадянами різних держав і які перебувають на території різних країн. Саме така ознака, як транснаціональність, робить кримінальні правопорушення у кіберпросторі фактично недосяжними для правоохоронних органів різних держав світу саме на рівні локальної протидії зазначеним кримінальним правопорушенням. На нашу думку, варто зазначити, що незважаючи на те, що кіберпростір є транскордонним, не всі кримінальні правопорушення в ньому транснаціональні. Наприклад, якщо кримінальний правопорушник і жертва живуть в одній країні [441].

Кримінальні правопорушення в кіберпросторі наразі є одним із найбільш латентних кримінальних правопорушень серед усіх інших. Насамперед це зумовлено самим фактом незвернення осіб, які стали жертвами кримінальних правопорушень у кіберпросторі, до правоохоронних органів, до яких належить розслідування зазначеного виду кримінальних правопорушень. Також одним із визначальних факторів латентності кримінальних правопорушень у кіберпросторі варто виділити те, що жертви навіть не розуміють, щодо них скоїли кримінальне правопорушення [469].

Наприклад, у разі поширення вірусних програм або шкідливого програмного забезпечення жертва може ніколи не поміти некоректності роботи свого персонального комп’ютера, або під час викрадання даних із веббраузера жертви (реквізитів банківських карт), жертва не здогадається про скоєне, поки 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, яка вчиняє кримінальне правопорушення, заборонені товари, послуги, документи чи інформацію, тим самим скоївши протиправне діяння [414].

Зокрема, часто самі кредитні організації, банки, сервіси електронних переказів та 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 те, що збитки в них часто здаються незначними порівняно з витратами, необхідними для їх розслідування. Здебільшого процедура розслідування кримінальних правопорушень у кіберпросторі забирає дуже багато часу, але 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 вчиняється кримінальне правопорушення, є однією з його основних ознак. На нашу думку, обмежувати кримінальні правопорушення в кіберпросторі певними гаджетами, інтернет-мережею або комп'ютером неправильно, оскільки особа, яка вчиняє кримінальне правопорушення, використовує у своїй діяльності різноманітні інформаційно-телекомунікаційні мережі й технології для доступу в кібернетичний простір. Як результат, можемо наголосити, що кіберпростір є обов'язковим фактором скоєння кримінального правопорушення.

Наступною ознакою кримінальних правопорушень у кіберпросторі є застосування навичок соціальної інженерії для вчинення фактично половини кримінально протиправних діянь у кіберпросторі. Соціальна інженерія – це вид атаки, що спирається на взаємодію людей і часто супроводжується маніпулюванням ними з порушенням нормальної процедури безпеки та є передовою практикою з метою одержання доступу до систем, мереж або фінансової вигоди [46].

Така ознака, як суб'єктивна складова, характеризується зниженим віком осіб, які скоюють кримінальні правопорушення в кіберпросторі. Варто зазначити, що це внаслідок того, що кримінальні правопорушення в кіберпросторі, по-перше, дуже прибуткова форма зайнятості, а по-друге,

інформація щодо скоєння таких кримінальних правопорушень 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 невілювання матеріального аспекту діяльності кримінального правопорушника та взаємодії із жертвою.

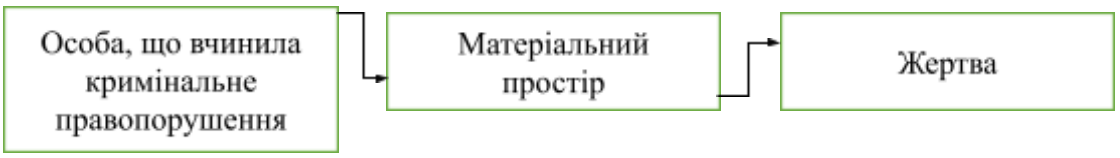


Рисунок 2 – Традиційна модель вчинення кримінального правопорушення

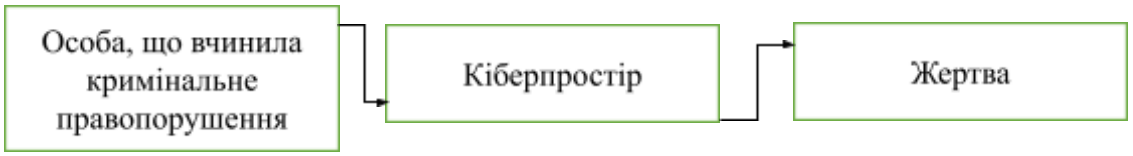


Рисунок 3 – Модель вчинення кримінального правопорушення у кіберпросторі

Д. Валл зазначає, що особа, яка вчинила кримінальне правопорушення

в кіберпросторі, не бачить свою жертву під час вчинення правопорушення, тому не може бачити 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 [357].

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 несе вагомих матеріальних збитків [168].

Зловмисники, які мають спеціальні знання про комп'ютерні мережі, можуть викрасти декілька мільйонів у банківському секторі, розвернути супутник на 180^{o}, вимкнути в лікарні систему життєзабезпечення пацієнтів, перебуваючи в будь-якому куточку світу й залишаючись непоміченим [426].

Доступність матеріалів, необхідних для скоєння кримінального правопорушення в кіберпросторі, є ще однією його ознакою. 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 поки що відсутня єдина точка зору стосовно цього питання. На нашу думку, основна проблема полягає в недосконалості чинного кримінального законодавства, у якому непередбачені 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 ньому використовують поняття «кіберзлочин (комп'ютерний злочин), що трактують як суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена Законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України [203].

Зауважимо, що в зазначеному законі поряд із поняттям «кіберзлочин» у дужках наведено «комп'ютерний злочин». Цей закон був прийнятий 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 і узгоджувати з чинним законодавством. Зокрема, наголошено на необхідності визначення співвідношення понять «комп'ютерні злочини» і «кіберзлочини». Також поняття «кіберзлочин» повинно 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» [159, с. 53].

Як вже зазначалося, з 1 січня 2020 року набрав чинності Закон України «Про внесення змін до деяких законодавчих актів України щодо спрощення досудового розслідування окремих категорій злочинів», де було запроваджено поняття «кримінального правопорушення», а отже необхідне узгодження інших нормативно-правових актів до положень Кримінального кодексу України, зокрема і Закону України «Про основні засади забезпечення кібербезпеки України». Тому вважаємо за необхідне вживання терміну «кримінальне правопорушення у кіберпросторі» замінити в статті 1 Закону України «Про основні засади забезпечення кібербезпеки України» термін «кіберзлочин (комп'ютерний злочин)» на «кримінальне правопорушення у 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. Сьогодні сфера правопорушень у кіберпросторі не є достатньо дослідженою та врегульованою на законодавчому рівні. І як
результат – 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 з використанням електронно-обчислювальних машин [120].

Кримінальні правопорушення в кіберпросторі – досить широке коло кримінальних правопорушень, що налічує більш 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 незакріпленими 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. Тому, 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 Кримінальний кодекс України є близьким за структурою.

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 «злочинів проти власності» [319].

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 [348].

Таку ж назву розділу має і XXX глава Кримінального кодексу Азербайджану [349].

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» [351].

Подібним чином 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 відносить не до кримінальних правопорушень проти власності, а саме до правопорушень у кіберпросторі [366].

У Кримінальному кодексі Литовської Республіки система кримінальних правопорушень у кіберпросторі згідно з главою XXX визначається як «злочини проти інформатики». В Кримінальному Законі Латвії немає окремого розділу, який би розглядав та визначав систему кримінальних правопорушень у кіберпросторі, самі кримінальні правопорушення в кіберпросторі наведені в XX розділі під назвою «кримінальні правопорушення проти безпеки та громадського порядку» [420].

На відміну від розглянутих вище систем кримінальних правопорушень в 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 кваліфікуючу ознаку «якщо таке діяння вчинене із заподіянням насилля» [350].

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 [378] 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» [321]. Така сама ситуація спостерігається і в Кримінальному кодексі Португалії, у якому визначений лише один вид кримінального правопорушення в кіберпросторі: стаття 193 «Зловживання комп'ютером» [456]. 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 [481].

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» установлена 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 ззовні; 2) перевищення рівня доступу до отримання 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 дозволяє одержати несанкціонований доступ, якщо така торгівля впливає на торговельні відносини між штатами;

8) вимагання, погрози, шантаж, вчинені з використанням

електронно-обчислювальної техніки [373].

Основним законом Сполученого Королівства, що визначає та регламентує кримінальну відповідальність за кримінальні правопорушення в кіберпросторі, є Закон «Про неправомірне використання комп'ютерних технологій», прийнятий 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 розділом 1–3 [506].

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 [433].

У доктринальних джерелах сьогодні відсутній єдиний підхід до розуміння поняття кримінального правопорушення в кіберпросторі. Одні науковці вважають поняття «кримінальних правопорушень у кіберпросторі» та «комп'ютерного кримінального правопорушення» синонімічними. Інші науковці визначають зазначені поняття, як подібні, однак не синонімічні. Водночас одні науковці вважають термін «комп'ютерних кримінальних правопорушень» ширшим за «кримінальні правопорушення в кіберпросторі», а інші, навпаки, що кримінальні правопорушення в кіберпросторі охоплюють комп'ютерні кримінальні правопорушення як один зі своїх видів [404; 515; 274; 382; 337].

Д. Азаров та А. Музика наголошують, що значна кількість науковців відмовляється 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 [7, 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 М. Карчевський пропонує використовувати поняття кримінального правопорушення у сфері використання інформаційних технологій і визначає його, як один з видів кримінальних правопорушень у сфері комп'ютерного кримінального правопорушення, що передбачені Кримінальним кодексом України. Це суспільно небезпечні, винні, вчинені суб'єктом кримінального правопорушення діяння, що заподіюють шкоду забезпеченим засобам обчислювальної техніки, відносинам у сфері реалізації інформаційної потреби. Ми не погоджуємося з думкою М. Карчевського, оскільки згідно з його визначенням комп'ютерні кримінальні правопорушення ширші 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 заподіює шкоди суспільним відносинам у сфері реалізації інформаційної потреби й не вчиняється за допомогою засобів електронно-обчислювальної техніки [92, с. 12].

І. Васильковський визначає 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'ютерного кримінального правопорушення є ширшим 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 отримання прав контролю над такою системою (наприклад, використання шкідливого програмного забезпечення, фальсифікація інформації про стан об'єкта у 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 [34, 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, які 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 відрізняються 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, з позиції автора залишається незрозуміло, 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, яка хоча формально і містить ознаки будь-якого діяння, передбаченого цим Кодексом, але через малозначність не становить суспільної небезпеки, тобто не заподіяла і не могла заподіяти істотної шкоди фізичній чи юридичній особі, суспільству або державі. Ураховуючи зазначене, можна дійти висновку, що крадіжка за частиною першою статті 185, вчинена на суму 150 гривень, не буде вважатися ані кіберзлочином, ані кіберпроступком, але шахрайство за частиною 3 статті 190, вчинене на 150 гривень, буде вважатися кримінальним правопорушенням у кіберпросторі, зокрема кіберзлочином, і особа нестиме покарання у вигляді позбавлення волі від 3 до 8 років [251, с. 145].

В. Поліщук висуває цікаву тезу, що комп'ютерні кримінальні правопорушення можуть мати місце як у реальному світі, так і в кіберпросторі, що звужує їх визначення порівняно з ширшим поняттям комп'ютерних злочинів. На нашу думку, кримінальні правопорушення в кіберпросторі мають певні специфічні ознаки та 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 [210].

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» [9, с. 8].

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 та смерті особи [377].

Подібне бачення й у А. Мохамеда: «На нашу думку, це поняття можна визначити як сукупність кримінальних правоворушень, що здійснюються за допомогою ІКТ (інформаційно-комунікаційних технологій) [436, с. 71].

Акцентуємо увагу на тому, що науковці, розглядаючи питання кримінально-правової охорони кіберпростору, наголошують, що поняття «кримінального правопорушення в кіберпросторі» є синонімічним до поняття «кримінальних правопорушень 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 [7].

В. Болгов вважає, що термін «кримінальні правопорушення, що вчиняються з використанням інформаційних технологій» є незручним для повсякденного використання. Замість цього він пропонує вживати коротший термін «кіберзлочини» [22, с. 122].

На наше переконання, запропонована В. Болговим термінологія, з одного боку, відображає еволюцію мови та потреби правової сфери у точнішій та доступнішій лексиці, що відповідає технологічному розвитку суспільства. Короткий термін «кіберзлочини» дозволяє швидше ідентифікувати специфіку злочинів, пов'язаних з інформаційними технологіями, та сприяє більш ефективному їх розумінню та протидії. Це особливо важливо в контексті глобальної кібербезпеки, де швидкість реагування та ясність термінів мають вирішальне значення для захисту інформаційних активів. Водночас, з іншого боку, як ми вже зазначали, використання терміну «кримінальне правопорушення у кіберпросторі»

відповідає більш сучасному стану науки і техніки.

Аналізуючи інший підхід до розуміння поняття «кримінального правопорушення в кіберпросторі», підкреслимо, що А. Вейц пропонує таке визначення кримінального правопорушення в кіберпросторі: це суспільно небезпечне діяння, передбачене кримінальним законом, що здійснюється з використанням електронно-обчислювальної техніки (комп'ютерів). Водночас немає 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 та 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 й кіберпроступками залежно від використання такої техніки [38, 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 він пов’язує кримінальні правопорушення в кіберпросторі з правопорушеннями, вчинюваними в електронних мережах. Відповідно до другого підходу кримінальними правопорушеннями в кіберпросторі є протиправні, винні діяння, вчинювані за допомогою комп’ютерного й мобільного зв’язку в Інтернет-мережі [70, 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, здійснені 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 [18].

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 інші. Водночас вважаємо потрібним виокремити підвид кримінальних правопорушень у кіберпросторі – «кримінальні правопорушення у сфері комп'ютерної інформації», і зазначити, що вони охоплюють більш вузьке коло кримінальних правопорушень, зокрема 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: як суспільно небезпечне діяння, вчинюване з використанням засобів комп'ютерної техніки щодо інформації, оброблюваної та використовуваної в
інтернет-мережі. На нашу думку, таке визначення, навпаки, надто вузьке, оскільки, по-перше, на відміну від інтернет-мережі 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) [466].

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 [112].

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 кваліфікуючою ознакою вчинення злочину (наприклад, комп'ютерне шахрайство або кібертероризм) [17, 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» [35, с. 278]. Проте негативні наслідки вчинення кіберзлочину не завжди мають економічний характер.

Н. Савчук дає таке визначення поняття «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 [235, 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 та розслідування, складність доказування в суді подібних справ, володіє транснаціональна складова здебільшого з використанням інформаційної мережі Інтернет, високим збитком навіть від одиничного кримінального правопорушення [257, с. 180].

В. Тітова пропонує визначати кримінальне правопорушення в кіберпросторі, як сукупність злочинів, передбачених Кримінальним кодексом України, що здійснюються в кіберпросторі, де основними безпосередніми об'єктами злочинного посягання виступають конституційні права і свободи людини і громадянина, суспільні відносини у сфері комп'ютерної інформації та інформаційних технологій, суспільні відносини у сфері економіки і економічної діяльності, суспільні відносини у сфері державної влади, суспільні відносини у сфері охорони здоров'я населення і суспільної моралі та інші охоронювані кримінальним законом об’єкти [260].

Звернімо увагу, що науковець оперує саме термінами «комп’ютери» 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, яка є інформаційною, глобальною та мережевою, і його варто відрізняти від кримінальних правопорушень, у яких просто використовують комп’ютери. Кримінальні правопорушення у 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 з метою одержання прибутку. Вони можуть бути розбиті на кримінальні правопорушення, які пов’язані з цілісністю системи, кримінальні правопорушення, в яких мережеві комп’ютери використовуються для сприяння вчиненню кримінального правопорушення, та кримінальні правопорушення, що стосуються саме комп’ютерів [509].

Словник термінів із кібербезпеки за редакцією О. Копана надає два визначення поняття кримінального правопорушення в кіберпросторі. Водночас автори розділяють 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 управляючою 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 існуючих 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 [245].

3. 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) [258].

4. Професор Ф. Ахмед дав три визначення поняттю «кримінальне правопорушення в кіберпросторі»: 1) будь-яка протиправна дія, в 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 отримав або міг би отримати вигоду; 3) зловживання комп’ютером розглядається як будь-яка протиправна, неетична чи несанкціонована поведінка, пов’язана з

автоматичним обробленням та передаванням даних [310; 112, с. 341].

5. 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 та яке може створити особисту небезпеку громадянинові, загрозу національній безпеці держави й світовій безпеці [52, 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, наслідком якого стало 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 [22, 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 яке передбачено кримінальну відповідальність» [242, 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 небезпечності та шкоди, що вони завдають суспільству й державі.

А. Завршник підкреслює, 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 [514].

Тому можемо констатувати той факт, що поняття кримінального правопорушення в кіберпросторі є ширшим за своїм змістом поняттям, ніж «кримінальні правопорушення у сфері комп'ютерної інформації» та «комп'ютерні кримінальні правопорушення».

І як підкреслює 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 [254].

Зважаючи на це, ми можемо стверджувати, що саме найменування «кримінальне правопорушення в кіберпросторі» є найбільш вдалим та доволі об'ємно розкриває сутність явища подібного виду злочинності. Проаналізувавши доктринальні джерела вітчизняних та зарубіжних учених, ми можемо стверджувати, що сьогодні в юридичній науці простежується дихотомія доктринальних та 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 05 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 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. Мамлєєвим 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 [76].

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, змінювальної у віртуальному просторі мережі Інтернет [283,
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 [126, с. 18].

Будучи обізнаними про значні прогалини в законодавстві, що 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 і телекомунікаційними технологіями, – банальна крадіжка, замасковані вандалізм, плагіат, «піратство» щодо інтелектуальної власності, ухилення від виплати авторської винагороди [308, с. 24].

Пізнаючи кіберпростір із позицій криміналістики, виділимо найважливішу методологічну специфіку цієї науки: вона досліджує будь-які предмети матеріального та ідеального макро- й мікросвіту. Іншими словами, склад виконуваних завдань під час дослідження кіберпростору та 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 загальнонаукових й спеціальних криміналістичних знань [473].

Узагальнення різних аспектів здійснення релігійної та розслідування віртуальної злочинності, досліджуваних багатьма авторами, дозволяє

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 «кримінального правопорушення в кіберпросторі» надано в Законі України «Про основні засади забезпечення кібербезпеки в Україні» як «кіберзлочин». Одночасно в 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, в якому фактично відсутня регламентація та нормативна база відповідальності за кримінальні правопорушення в кіберпросторі. Окреслено, що поняття «кримінальне правопорушення в кіберпросторі» не є тотожним до понять «комп'ютерне кримінальне правопорушення» та «кримінальне правопорушення у сфері комп'ютерної інформації», а вони є його підтипом.

До основних характеристик кримінальних правопорушень у кіберпросторі належить: 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 заподіює шкоду різним суспільним відносинам шляхом використання інформаційно-телекомунікаційних технологій, інформаційно-телекомунікаційних систем і мереж та створюваного ними кіберпростору.

Висновки до розділу 1

1. Ретроспективно узагальнено та систематизовано наукові дослідження, присвячені кримінально-правовій охороні кіберпростору. На підставі аналізу наукових праць установлено, що питання кримінальних правопорушень в кіберпросторі є досить новим суспільно небезпечним явищем, яке стрімко розвивається одночасно з розвитком та цифровізацією суспільства. Наголошено, що наявний масив наукових праць кримінально-правового спрямування не встигає за динамічним розвитком кримінального законодавства, тому питання кримінально-правової охорони кіберпростору в Україні потребує системного, детального, комплексного та об'єктивного дослідження з метою забезпечення ефективного встановлення кримінальної відповідальності за суспільно небезпечні діяння у кіберпросторі.

2. Наголошено, що беззаперечним елементом успіху наукового дослідження є використання правильної методології, яку б у повній мірі забезпечувала системність та комплексність наукового дослідження та одночасно дозволила б розробити висновки та рекомендації, які б відображали вагоме та змістовне значення як для наукової, так і для практичної діяльності. Підбір правильної методології має важливе практичне значення для дисертаційного дослідження, оскільки будь-яке дослідження у

сфері права передбачає розроблення нових та вдосконалення існуючих правових норм у певній сфері. Автором було використано різні принципи, підходи та методи (метод аналізу, емпіричний метод, метод контент-аналізу, метод кейс-студії, порівняльно-правовий метод, метод системного аналізу), які застосовувалися у взаємозв'язку й взаємозалежності, що також забезпечило повноту та об'єктивність цього дослідження.

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

4. Здійснено співвідношення понять «кіберпростір»,

«інформаційний простір», «віртуальний простір» та «інтернет-простір» та визначено, що «кіберпростір» є вужчим за змістом від понять «інформаційний» та «віртуальний» простір, однак ширший за поняття «інтернет-простір». Надано авторське визначення дефініції поняття «віртуальний простір», під яким варто розуміти створене комп'ютерними технологіями глобальне комунікативне середовище, в основі якого лежить створення, збереження, упорядкування та обмін інформацією за допомогою електронних мереж.

5. Визначено, що традиційно виділяють три підходи до формування сутності поняття «кіберпростір», зокрема легальний, доктринальний та філософський. Водночас запропоновано в рамках доктринального аспекту розглядати в інформаційному, віртуальному та соціальному ракурсі.

6. Критично проаналізувавши позиції науковців щодо сутності поняття «кіберпростір», виділено його основні характеристики та принципи. Зокрема, серед основних характеристик було виділено віртуальність, мережеву приналежність, середовище взаємодії, динамічність, комунікативність та поєднання територіалізації та територіалізації. Серед принципів, що забезпечують стабільність функціонування кіберпростору, нами були виділені: дисципліна, відповідальність, дотримання прав та свобод людини і громадянина та своєчасного втручання.

7. Розмежовано поняття «кримінальне правопорушення у кіберпросторі», «кримінальне правопорушення у сфері комп'ютерної інформації» та «комп'ютерне кримінальне правопорушення». Так, критично проаналізувавши та узагальнивши позиції вчених, визначено, що поняття «кримінальне правопорушення у кіберпросторі» ширше за поняття «кримінальне правопорушення у сфері комп'ютерної інформації» та «комп'ютерне кримінальне правопорушення», де останні виступають його підтипом, незважаючи на те, що їх об'єднує використання комп'ютерної техніки для вчинення суспільно небезпечних, караних діянь.

8. Визначено та удосконалено основні характеристики

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

9. Визначено, що під кримінальним правопорушенням в кіберпросторі варто розуміти суспільно небезпечне, протиправне, винне, каране діяння, що заподіює шкоду різним суспільним відносинам шляхом використання інформаційно-телекомунікаційних технологій, інформаційно-телекомунікаційних систем і мереж та створюваного ними кіберпростору.

10. Акцентовано увагу на доцільності узгодження термінології Закону України «Про основні засади забезпечення кібербезпеки України» з положеннями та нормами чинного Кримінального кодексу України, зокрема, щодо впровадження та використання терміну «кримінальне правопорушення у кіберпросторі» замість терміну «кіберзлочин».

РОЗДІЛ 2
КРИМІНАЛЬНО-ПРАВОВА ХАРАКТЕРИСТИКА КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ В КІБЕРПРОСТОРІ

2.1. Теоретико-прикладні аспекти типологізації кримінальних правопорушень в 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 установлення істини під час вивчення правових явищ, правових рішень чи виконання інших наукових завдань. Проблема типологізації є складною та багатошаровою, тому її можна розглядати з різних аспектів (економічного, філософського, правового). 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 призводить до дефіциту інформації, який уповільнює суспільний прогрес. Розроблення оптимальної типологізації стає одним із найважливіших завдань сучасної науки кримінального права [6, 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 дозволяє 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 типологізації 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 треба 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 напрямі [307, с. 246].

Кримінальна правова типологізація кримінальних правопорушень є своєрідним шляхом до пізнання об'єкта кримінального правопорушення, невід'ємним засобом до визначення його сутності, дозволяє 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 та вибір застосування слідчим методик розслідування окремих видів кримінальних правопорушень у кіберпросторі.

Дуже неоднозначними є підходи до сутності й 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) [24, с. 244].

Проте ці судження фактично об'єднані двома ідеями, що склалися: 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 слід потрібно застосовувати принципи діалектичної логіки й правило поділу поняття. Очевидно, що для здійснення процесу кримінально-правової типологізації необхідно визначити її об'єктів. Автор зазначає, що об'єкт кримінально-правової типологізації – думка, що відображає суттєві ознаки самого об'єкта чи явища, що є предметом зазначеної типологізації [133].

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 взаємопов'язані підгрупи для цілей слідчої та криміналістичної практик [487, с. 61].

Дещо ширше об'єкт кримінально-правової типологізації визначає В. Антипов. Зокрема, як певну сукупність кримінальних правопорушень, що характеризується відповідною сукупністю кримінально-правових і кримінально-процесуальних, криміналістичних ознак, поділених на взаємопов'язані частини [11, 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 [75, с. 86].

Відповідно до позиції О. Баланюка, кримінальне правопорушення як об'єкт типологізаційного дослідження в кримінології не обмежується лише його кримінально-правовим значенням. Предметом судового дослідження є саме кримінальне правопорушення як конкретний випадок, що має ознаки кримінального правопорушення, характеризується особливою структурою та специфічними закономірностями механізму його здійснення [14, с. 123].

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

Виконання низки завдань у процесі кваліфікації 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, більш точно 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.

Тому 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 [279, 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, що передбачені Розділом XVI Кримінального кодексу України України [125, 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 [211, с. 455].

Н. Міщук також переконаний, що кримінальні правопорушення в кіберпросторі потрібно типологізувати відповідно до об'єкта посягання. Він виділяє наступні 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 [141, с. 176].

В. Голіна у своїх кримінологічних наукових працях визначає, що кримінальні правопорушення в кіберпросторі можуть бути агресивними та 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 [57, 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 та розповсюдження шкідливих програм; 6) кримінальні правопорушення проти суспільної моральності; 7) кримінальні правопорушення проти безпеки держави [67].

А. Русецький вважає, що найпоширенішими видами кримінальних правопорушень у світі є такі: 1) кардинг; 2) вішинг; 3) фішинг;
4) онлайн-шахрайство; 5) кард-шарінг; 6) кіберпіратство; 7) мальваре;
8) соціальна інженерія; 9) рефайлінг [465, 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, що посягають на моральність громадськості; 6) суспільно небезпечні дії, що посягають на громадську безпеку [324, с. 148].

Shailendra Singh пропонує типологізацію кримінальних правопорушень у кіберпросторі залежно від характеру використання електронно-обчислювальної техніки: 1) електронно-обчислювальна техніка використовується, як засіб вчинення кримінального правопорушення;
2) електронно-обчислювальна техніка є предметом кримінального правопорушення [477, 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 [313].

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 – шахрайства 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 (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 [436].

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 [121].

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 викликана насамперед суспільною небезпечністю такого діяння й швидкою динамікою його росту. Відповідно до Кримінального кодексу 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 передаються 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) ввезення, виготовлення або розповсюдження творів, що пропагують культ насильства і 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 та 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, 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); 27) 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); 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) [121].

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 відсутній розділ, 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, що може нанести шкоду 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 р. 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 інші її напрями [200].

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 визначений 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, здійснювана в кіберпросторі; 2) здійснення державою-агресором кібератак і кібердиверсій 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 [207].

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

Необхідно наголосити, що кримінальними правопорушеннями в кіберпросторі зазначеної групи будуть лише кримінальні правопорушення, визначені з використанням кіберпростору. Як ми вже зазначали, до них належать: 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) [30].

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 основним безпосереднім об'єктом кожного окремого злочину проти основ національної безпеки, вчиненого в кіберпросторі, – національна безпека в тій чи іншій її сфері [454, 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 суверенітетові [139, с. 86].

Відповідно до Закону України «Про державну таємницю» до державної таємниці в порядку, встановленим Законом України «Про державну таємницю», належить інформація у сферах оборони, економіки науки й техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, що підлягають 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 установлено, що особа завербована в 2019 році

країною-агресором й виконувала завдання з передавання через різні месенджери про діяльність Збройних сил України, переміщення техніки та передавала іншу інформацію на шкоду територіальній цілісності й суверенітетові 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 обрано запобіжний захід у вигляді тримання під вартою [246].

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. Наведемо приклад зазначеного кримінально протиправного діяння. Працівниця АК «Укрaлізниця» на посаді касира, усвідомлюючи обставини та достовірно знаючи про заборону поширення інформації про направлення, переміщення зброї, озброєння територією України, громадянка України Особа 1 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, та призначено їй покарання 3 роки позбавлення волі. Однак на підставі статті 75 Кримінального кодексу України було визначено звільнити Особу 1 від відбування призначеного покарання з випробувальним терміном 1 рік [40].

Ще один із прикладів варто навести діяльність громадянина України, який збирав розвіддані про місця дислокації й переміщення підрозділів ЗСУ та Тероборони, функціонування резервних аеродромів і військових полігонів на півдні Одеської області. Зокрема, агент спецслужб Російської Федерації через різноманітні месенджери на зразок Telegram Signal WhatsApp та 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 ч. 2 ст. 111 Кримінального кодексу України (державна зрада, вчинена в умовах воєнного стану) та обрано запобіжний захід у вигляді тримання під вартою [238].

Як можна помітити з наведених судових 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 у тому випадку, якщо 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 у формі шпигунства. В диспозиції статті 114-2 Особливої частини Кримінального кодексу України розуміється передача та

оприлюднення зазначеної інформації у відкритих джерелах, наприклад у телеграм-каналі [247].

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, зокрема 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 в разі відсутності ознак державної зради та шпигунства.

З об'єктивної сторони кримінальні правопорушення проти основ національної безпеки України, вчинені в кіберпросторі, характеризуються переліком протиправних дій: 1) державна зрада (стаття 111 Кримінального кодексу України) шпигунством (кібершпигунством), тобто передачею або зібранням з 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) передачею або зібранням з метою передачі 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 громадянином України до підтримки рішень або дій держави-агресора, збройних формувань, здійсненням інформаційної діяльності у 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 є усіченим, тобто кримінальне правопорушення є закінченим з 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, варто віднести до обов'язкового елементу ознаки об'єктивної сторони 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 в рамках кіберпростору, через які здійснюють публічні заклики, виправдовування громадянином України збройної агресії проти України.

На нашу думку, саме засіб вчинення зазначеного виду кримінальних правопорушень в 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 дозволяє правопорушникам залишатися непокараними. Варто зауважити, що кримінальні правопорушення зазначеної групи, що вчинюються в кіберпросторі, є дуже латентними, і тому зіставити реальну картину відкритих кримінальних проваджень та кількість скоєних кримінальних

правопорушень фактично неможливо.

Велику проблему 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, – 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 був у Луганській області [270].

Варто наголосити, що випадки вербування неповнолітніх до вчинення дії протиправного характеру, зокрема у сфері національної безпеки, об'єктивна сторона яких, зазвичай, окреслюється переданням відомостей про позиції Збройних Сил України та ін., має дедалі більш масовий характер, а латентність і складна процедура розслідування таких кримінальних правопорушень у кіберпросторі не дозволяє своєчасно викрити правопорушників й запобігти переданню ними 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 та використання у військових діях осіб, які не досягли 18-річного віку [165].

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 наше переконання, ураховуючи суспільну небезпечність кримінальних правопорушень проти основ національної безпеки України, вчинених у кіберпросторі, 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, вчинювані 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 небезпечність цього протиправного діяння. Усе це зумовлює вдосконалення системи норм, яка відображає кримінальні правопорушення проти власності, вчинювані в кіберпросторі, оскільки вона повністю не відображає всього рівня загроз, наразі актуальних в кіберпросторі.

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 використання електронно-обчислювальних машин, як знарядь 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.

Зокрема, «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

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 ідентично 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 такому сервісі можна завести віртуальний криптовалютний гаманець і купити та зберігати криптовалюту. Зловмисники у своїх повідомленнях або в повідомленнях, надсилаючи посилання нібито цього сайту, змінюють декілька або взагалі одну букву на інші знаки так, щоб це було не помітно.

Наприклад, справжнє посилання цієї системи таке: www.myetherwallet.com, а посилання зловмисника буде виглядати приблизно так: www.myetherwalIet.com.

Необхідно наголосити, що за допомогою фішингу вплив програмних засобів на комп'ютер жертви не відбувається. 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.

Наступним кримінальним правопорушенням цієї групи є вішинг. За своєю сутністю вішинг виступає підвидом фішингу і становить вид телефонного або смс-шахрайства, яке полягає у випитуванні конфіденційної інформації в особи з метою її використання у своїх протиправних намірах. Сьогодні через телефонні дзвінки шахраї дізнаються дані з банківських карт і рахунків, примушуючи методами соціальної інженерії до переказування грошових коштів зловмисникам [103, с. 114].

Найбільш вразливою 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 із наведених країн здійснюють свою діяльність щодо громадян України. Варто зауважити, що в період пандемії та власне збройної агресії Російської Федерації шахраї безжально користуються скрутним становищем українців під час війни та 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 проявом є представлення зловмисника працівником правоохоронного органу й подальше вимагання грошових коштів за звільнення нібито затриманого члена сім'ї. Такий прояв вішингу заполонив 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 шахраю грошові кошти. Сьогодні зазначений вид телефонного шахрайства поступово втрачає актуальність через широке висвітлення цього виду шахрайства в засобах масової інформації й підвищення рівня культури кібербезпеки в громадян зокрема.

Іншим проявом вішингу є випадки, коли 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 питання. У цьому разі перевірити чи дійсно шахрай працює в банку, швидко неможливо, адже на сайтах банків немає інформації щодо їх співробітників та їх особистих даних [50, 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 увести 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 одержують інформацію про дані банківської картки, яку потім можуть використовувати в інших видах кримінальних правопорушень у кіберпросторі [161].

Предметом зазначеного виду кримінальних правопорушень у сфері власності, вчинених у кіберпросторі, є конфіденційна інформація. Загалом можна виділити декілька видів інформації, яка використовується шахраєм у своїй протиправній діяльності для досягнення злочинного результату, відповідно до рівня її небезпеки для жертви. Таку інформацію можна класифікувати на: 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 особи, чи є особа утримувачем картки того чи іншого банку, працівником тієї чи іншої юридичної особи тощо); 2) допоміжну інформацію, що дає доступ до інформації з високим рівнем тяжкості одержання (номери карток, кодові слова та ін.);
3) конфіденційну інформацію, що надає прямий доступ до того, що цікавить скаммера. Це можуть бути пінкоди, паролі й подібна інформація.

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

Спосіб скоєння зазначеного типу кримінальних правопорушень проти власності, вчинених у кіберпросторі, буде визначатися, як сукупність

прийомів і методів, застосовуваних під час вчинення кримінального правопорушення. Наголосимо, що майже всі кримінальні правопорушення в кіберпросторі мають дистанційний спосіб вчинення, що не зменшує, а, навпаки, збільшує їх суспільну небезпечність. Дистанційність як спосіб вчинення кримінальних правопорушень зазначеної групи дозволяє зловмисникам не залишати фізичних слідів, властивих класичним злочинам цієї групи, як результат – ускладняється процес виявлення правопорушника та власне і процес доказування. Дистанційність є обов'язковою ознакою об'єктивної сторони кожного кримінального правопорушення в кіберпросторі із зазначеного виду.

Безумовно, залежно від виду кримінального правопорушення проти власності, вчиненого у кіберпросторі, спосіб скоєння 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 до вчинення дії в інтересах зловмисника [138, 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 [150].

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 ч. 1 ст. 22 КК 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, вчинених в кіберпросторі, він становить 14 років» [293, 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: «віртуальність – як існування речей, подій, процесів тощо; глобальність – як існування єдиних, універсальних для всієї системи відносин, усіх локальних співтовариств (формальних і неформальних) та інститутів взаємодії; фрагментарність – властивість, що характеризується уривчастістю й неповнотою» [44, с. 23].

Суб'єктивна сторона цього виду кримінальних правопорушень проти власності, вчинених у кіберпросторі, характеризується прямим умислом і корисливим мотивом.

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. Так, 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 [152]; 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, одержані 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, в тому числі і з віртуальними активами та іншим майном, одержаними внаслідок предикатного кримінально-протиправного діяння; 2) набуття, володіння або використання злочинних грошових коштів чи віртуальних активів; 3) дії, спрямовані на приховування чи маскування (незаконне походження, володіння, джерела походження, переміщення, місцезнаходження злочинного майна, грошових коштів і віртуальних активів).

Засобами вчинення кримінальних правопорушень у сфері господарської діяльності, вчинених в 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 та прекурсорів, сильнодійних та отруйних речовин та одурманюючих засобів, радіоактивно

забрудненої продукції, мікробіологічних та інших біологічних агентів і токсинів як складової частини здоров'я населення [234, 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 потребує 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, сильнодіючих і психотропних речовин, їх аналогів і прекурсорів – це згруповані в списки наркотичні засоби, психотропні речовини і 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 уповноваженого органу виконавчої влади в галузі охорони здоров'я. Його публікують в офіційних друкованих виданнях [5, 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 та місце вчинення кримінального правопорушення. Так, засобом вчинення цієї групи кримінальних правопорушень у кіберпросторі виступають інформаційно-телекомунікаційні мережі та 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 цього ресурсу може перебувати в будь-якій точці світу та інформувати українського покупця, де взяти наркотичні засоби, сам ніколи в житті безпосередньо не стикаючись із наркотичними засобами [291].

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 та 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 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 [205].

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 цьому разі виражається в тому, що безпосереднього 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 реальному світі, а їх комунікація відбувається за допомогою «нікнеймів» безпосередньо в кіберпросторі. Злочинні організації такого типу переважно створюють для вчинення конкретного одного кримінального правопорушення і 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 програмою е-підтримка 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 та 2 статті 255, частинами 3 та 4 статті 190

Кримінального кодексу України [178].

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 передбачала, що її дії створюють загрозу громадській безпеці, і бажала настання таких наслідків.

У цьому розділі ми не будемо детально аналізувати склад кримінального правопорушення, передбаченого статтею 258 «Терористичний акт», а зупинимося лише на визначенні поняття «тероризму в кіберпросторі» та у якій формі він проявляється. Тероризм у кіберпросторі, або «кібертероризм» – це певні дії, що проявляються в дезорганізації інформаційних систем, небезпечні для життя людей, що призводять до майнової шкоди чи інших тяжких суспільно небезпечних наслідків, спрямовані на залякування населення та 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, – це 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 та нормальної роботи електронно-обчислювальних машин та електронних комунікаційних мереж. Основним безпосереднім об'єктом цих кримінальних правопорушень є окремі інформаційні процеси, зокрема: 1) цілісність, доступність, конфіденційність інформації, її оброблення й передача (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 вчиняється 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 віку 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, зазначена типологізація сьогодні є еталоном нормативно правового акта, 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 містить у собі 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 охоплює кримінальні правопорушення в кіберпросторі, пов'язані з комп'ютером. Зокрема, до цієї групи належать; 1) підробка, яка 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 кримінальні правопорушення в кіберпросторі – порушення авторських та суміжних прав. Водночас установлення кримінальної відповідальності за такі кримінальні правопорушення є компетенцію законодавств держав [19].

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 [71].

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 та фандрейзингу; г) 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; д) 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 – основа 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 машин, 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 отримання конфіденційної інформації; 3) кримінальні правопорушення, у яких електронно-обчислювальні машини, інформаційно-комунікаційні мережі є засобом забезпечення злочинної діяльності: незаконний збір та 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 заподіюють шкоду лише одному об’єкту, наприклад відносинам у сфері власності. Двооб’єктні поряд з основним об’єктом, який характеризується відносинами, наприклад, у сфері власності, заподіює шкоду і відносинам у сфері комп’ютерної інформації [285].

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 Черкас 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 акаунта 1хбет» Особи 2 на власний рахунок, а під виглядом ставок переконала Особу 2, що гроші були програні на букмекерській платформі [41].

Щодо двооб’єктного кримінального правопорушення проти власності, вчиненого у 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 картки й CVV код розрахункової картки клієнта зазначеного банку. Маючи єдиний умисел, вона таємно викрала грошові кошти з наведеного 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 з одного боку було заподіяно шкоду відносинам 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. Ці кримінальні правопорушення 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 в кіберпросторі; г) порушення таємниці листування, переписки, телефонних розмов, поштових та інших повідомлень в 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 які містяться в інформаційно-телекомунікаційних системах та електронних комунікаційних мережах з метою неправомірного доступу до зазначених мереж і систем; д) 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, яка оброблюється 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, що оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах чи комп'ютерних мережах; 4) неправомірне розповсюдження інформації, оброблюваної в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах чи комп'ютерних мережах;

5) викрадення інформації, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах чи комп'ютерних мережах.

Десятою підставою типологізації кримінальних правопорушень у кіберпросторі є мета їх вчинення. На нашу думку, варто виділити кримінальні правопорушення в кіберпросторі, які вчинюються з метою:

1) отримання прибутку; 2) нанести шкоду національним інтересам та обороноздатності держави; 3) порушення громадської безпеки;

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, є такими: 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 об'єктивної сторони кримінального правопорушення.

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 Інтерент 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 та 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 [362, с. 29].

Можемо помітити: кримінальні правопорушення в кіберпросторі є надзвичайно соціально небезпечним, протиправним явищем, що становить загрозу не лише національним, а й міжнародним інтересам. Сьогодні боротьба з феноменом кримінальних правопорушень у кіберпросторі є однією з головних завдань правоохоронних органів як національного, так і міжнародного рівня. На нашу думку, для комплексної боротьби, по-перше, на національному рівні необхідно насамперед узгодити та законодавчо закріпити основні кримінальні правопорушення в кіберпросторі в рамках діючих нормативно-правових актів. Удосконалення чинного законодавства щодо визначення основних видів кримінальних правопорушень у кіберпросторі, завершення процесу імплементації норм міжнародно-правових актів в законодавство України, дасть змогу біль точно 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 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 в 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 [107; 121].

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 виступає знаряддям, засобом чи метою їх вчинення [105, с. 155].

На нашу думку, це дуже узагальнене розуміння категорії кримінальних правопорушень у кіберпросторі, що не розкриває повністю його сутнісних особливостей, адже за допомогою цифрових технологій можна вчиняти переважну більшість класичних кримінальних правопорушень, безпосереднім об'єктом яких будуть різні суспільні відносини, непов'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 [239, 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, аби спричинити збитки суспільним, майновим або інтересам держави, підприємствам, відомствам, організаціям, кооперативам та громадянам, а також правам окремої особи [66, с. 226].

Кримінальні правопорушення у сфері комп'ютерної інформації – це всі суспільно небезпечні діяння, родовим об'єктом яких є комп'ютерна інформація. Отже можна наголосити, 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 машина» був уведений ще наказом Міністерства праці та соціальної політики України від 10 лютого 1999 року, і 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) [194].

Але відповідно до наказу Міністерства соціальної політики України від 14 лютого 2018 року він був замінений на поняття екранний пристрій – електронний засіб для відтворення будь-якої графічної або алфавітно-цифрової інформації (на основі електронно-променевої трубки, рідкокристалічних, плазмових, проєкційних, органічних світлодіодних моніторів та інших новітніх розробок у сфері інформаційних технологій) [192].

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, вбачається, що 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, і флеш-носії, жорсткі та компакт-диски, які, на наш погляд, не підпадають під категорію електронно-обчислювальних машин. Тому ми переконані, що варто викреслити 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 вважаємо за доцільне закріпити в статті 1 Закону України «Про захист інформації в

інформаційно-комунікаційних системах» термін «цифровий пристрій».

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. В Законі України «Про захист інформації в інформаційно-комунікаційних системах» від 16 грудня 2020 року надано поняття інформаційної та інформаційно-комунікаційної системи. Інформаційна (автоматизована) система – організаційно-технічна система, в якій реалізується технологія оброблення інформації з використанням технічних і програмних засобів. Інформаційно-комунікаційна система – сукупність інформаційних та електронних комунікаційних систем, які у 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 [195].

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 системах та телекомунікаційних мережах», а надалі при 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. Одночасно з цим пропонуємо ввести термін інформаційно-телекомунікаційні технології, системи та мережі в статтю 1 Закону України «Про основні засади забезпечення кібербезпеки України». 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, яка 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 (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) [121].

Сутність кримінальних правопорушень у кіберпросторі, передбачених XVI розділом Особливої частини Кримінального кодексу України, полягає в

недопущенні суспільно небезпечних, протиправних діянь, які посягають на безпеку цифрової інформації й нормального функціонування інформаційно-телекомунікаційних систем. Водночас самі цифрові пристрої завжди являють собою засіб вчинення кримінального правопорушення.

Суспільна небезпечність 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 шкоду матеріального характеру, 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 і 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 у мережі Інтернет, а також програми (передавання) організацій мовлення, що ретранслюються з використанням мережі Інтернет [180].

На нашу думку, зазначене визначення поняття «цифрової інформації» притаманне саме для сфери захисту інтелектуальної власності. Під цифровою інформацією ми пропонуємо розуміти сукупність даних та програмних компонентів, які обробляються, передаються, зберігаються в інформаційно-телекомунікаційних системах. Тому вважаємо за доцільне в статтю 1 Закону України «Про основні засади забезпечення кібербезпеки України» ввести термін та його визначення «цифрова інформація»

Варто відмітити, що в доктринальних джерелах під час визначення

предмета кримінальних правопорушень у кіберпросторі, передбачених XVI розділом Особливої частини Кримінального кодексу України, часто зустрічається поняття комп'ютерної інформації. Комп'ютерна інформація – це текстова, цифрова, графічна чи інша інформація (дані, відомості) про осіб, предмети, події, явища, що існує в електронному вигляді і знаходиться в електронно-обчислювальній машині, автономній системі чи в 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 із використовуванням сучасних електронно-інноваційних технологій, та ін. [147].

Незважаючи на відсутність законодавчого визначення поняття «комп'ютерна інформація», вважаємо, що за своєю сутнісною характеристикою та з технічної точки зору поняття «цифрова інформація» є ширшим за «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 XVI розділом 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 та 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) причинно-наслідковий зв'язок.

Кримінальне правопорушення несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж за частиною першою та другою є кримінальним правопорушенням із формальним складом, а за частиною третьою – кримінальне правопорушення з матеріальним складом.

В 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 третій [153].

Відповідно до частини першої статті 361 Особливої частини Кримінального кодексу України «Несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж»

можна дійти висновку, 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, які зазначені в частині третій цієї статті. Несанкціоноване втручання фактично свідчить про порушення установленого власником режиму доступу до системи, його розмежування або відсутність. Фактично відповідно до частин першої та другої статті 361 склад кримінального правопорушення буде формальним, тобто незалежно від настання суспільно небезпечних наслідків. Власне сам факт самого проникнення в інформаційно-телекомунікаційну систему або мережу обумовлює кримінальну відповідальність за вчинене діяння. На практиці маємо зовсім протилежне розуміння значення словосполучення «несанкціоноване втручання». Зокрема, виникає проблема при 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 небезпечність 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 [219].

У зазначеному прикладі ми бачимо суспільно небезпечні наслідки у формі витоку й блокування інформації, передбачені як кваліфікуючі 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 підкреслити, що при 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 несанкціонованого втручання, під яким пропонуємо розуміти отримання можливості для ознайомлення та (або) використання цифрової інформації, яка 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.

На наше переконання, враховуючи зміст запропонованого поняття «несанкціоноване втручання», основними наслідками є: 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 обробки цифрової інформації.

На нашу думку, варто розглянути окремо кожен з визначених суспільно небезпечних наслідків. Зокрема, під витоком інформації в Законі України «Про захист інформації в інформаційно-комунікаційних системах» визначено результат дій, внаслідок яких інформація в системі стає відомою чи доступною фізичним та/або юридичним особам, що не мають права доступу до неї [196].

Як приклад можна навести дії особи, яка за допомогою шкідливого

програмного забезпечення втрутилася в цифровий пристрій жертви, яким був комп'ютер, і 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. Варто звернути увагу на кримінальне провадження № 522/14602/13-к, вирок Приморського райсуду м. Одеса від 27 червня 2013, яким установлено, що Особа 1 із метою незаконного одержання та подальшого використання 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 карт. У цьому разі виток цифрової інформації ототожнено із зчитуванням інформації. Проте, на нашу думку, зчитування цифрової інформації є саме способом вчинення кримінального правопорушення, адже це активні дії, а виток цифрової інформації – як наслідок [117].

Блокування цифрової інформації – це дії, унаслідок яких унеможливлюється доступ до інформації в системі [215].

Наразі наслідок несанкціонованого втручання у формі блокування цифрової інформації є одним з найбільш суспільно небезпечних серед усіх інших. Шкідливе програмне забезпечення, метою якого є блокування цифрової інформації, яка обробляється в інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж, зараз як є у відкритому доступі, так і продається на різноманітних даркнет-форумах. Можливості масового розповсюдження такого програмного забезпечення лише додають суспільної небезпечності цьому діянню. Сьогодні фактично кожен 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. 27 червня 2017 року сталася масштабна кібератака на корпоративні та державні інформаційні (автоматизовані) системи, внаслідок якої було заблоковано більшу частину комп'ютерів державного й приватного сектору. Вірус Petya шифрує інформацію на комп'ютері, після чого виводить на екран повідомлення-вимогу перевести 300 доларів у біткоїнах за розблокування. Найбільш імовірно, що дія вірусу поширюється лише на комп'ютери із системою Windows. Зараження комп'ютерів відбувається через фішингові листи (фішинг – вид інтернет-шахрайства, коли під виглядом листів від імені популярних брендів злочинці одержують доступ до конфіденційних даних користувачів). Фахівці стверджують, що вірус використовував сфальшований електронний підпис Microsoft [94].

Знищення цифрової інформації є дією, унаслідок якої інформація в системі зникає. Тобто це її пряме вилучення, за якого вона може видалятися автоматизовано, – або 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, яка обробляється на сервері банківської установи. 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 остаточним замахом на кримінальне правопорушення, передбачене частиною третьою статті 361 Особливої частини Кримінального кодексу України та вчинене в сукупності з кримінальним правопорушенням, передбаченим частиною першою статті 361-1 Особливої частини Кримінального кодексу України [267].

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, внаслідок якого унеможливлюється зчитування з нього інформації. Варто акцентувати увагу, що в разі умислу особи лише на заподіяння 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 від несанкціонованого копіювання несанкціоноване перехоплення за способом вчинення цифрової інформації неможливе без спеціальних технічних засобів, використовуваних для негласного одержання інформації, що перебувають в обмеженому цивільному обігу [478].

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 [118].

Варто зауважити, що серед науковців точиться дискусія стосовно класифікації поняття «перехоплення цифрової інформації» до аналогій з «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 закінченим із моменту початку активних дій зі створення додаткової лінії зв'язку в інформаційно-телекомунікаційних системах.

Варто 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 [152].

М. Карчевський під цим суспільно небезпечним наслідком розуміє одержання в результаті операцій з комп'ютерною інформацією, здійснюваних за допомогою технічних чи програмних засобів, результатів, що не відповідають характеристикам технічних засобів або алгоритму комп'ютерної програми [93].

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 2012-2014 роки. Зокрема, Особа 1 за матеріальну вигоду встановила Особі 2 супутникову антену, призначену для прийому 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 [13].

Ми погоджуємося з М. Дмитрук, яка відзначає, що порушення установленого порядку маршрутизації цифрової інформації є одним із наслідків спотворення процесу оброблення інформації. 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 [69].

Власне під порушенням установленого порядку маршрутизації цифрової інформації ми розуміємо протиправну зміну адресата цифрової інформації, яка обробляється 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, – 16 років.

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

Кваліфікуючими ознаками аналізованого кримінального правопорушення є: 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 третьою або четвертою 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, 363-1 вважається шкода, що в триста й більше разів перевищує неоподатковуваний мінімум доходів громадян. Станом на 2023 рік значна шкода в грошовому еквіваленті 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 шостої статті 361 Особливої частини Кримінального кодексу України дії, передбачені частинами першою – четвертою 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 та не соціально обумовленою диспозицію частини п’ятої статті 361 Особливої частини Кримінального кодексу України, що містить у собі кваліфікаційну ознаку у формі вчинення дій, передбачених частиною третьою або четвертою цієї статті в умовах воєнного або надзвичайного стану, оскільки фактично будь-яке несанкціоноване втручання в інформаційно-телекомунікаційні технології, системи та мережі, має один з альтернативних наслідків у формі витоку, втрати, підробки, блокування інформації, спотворення процесу її оброблення інформації або до порушення установленого порядку її маршрутизації, в умовах воєнного або надзвичайного стану буде кваліфікуватися за частиною п’ятою статті 361 Особливої частини Кримінального кодексу України, незалежно від заподіяної шкоди.

Пропонуємо викласти 361 статтю Особливої частини Кримінального кодексу України у наступній редакції:

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

1. Несанкціоноване втручання в роботу інформаційно-телекомунікаційних технологій, систем та мереж, тобто отримання 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) поза дозволом власника інформаційно-телекомунікаційної технології, системи або мережі, що не призвело до наслідків у вигляді витоку, копіювання, модифікації, спотворення процесу обробки, перехоплення, блокування та (або) знищення цифрової інформації, -

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

3. Дії, передбачені частинами першою або другою цієї статті, якщо вони призвели до витоку, перехоплення, копіювання, спотворення процесу обробки та (або) модифікації цифрової інформації, -

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

5. Дії, передбачені частинами першою-четвертою цієї статті, якщо вони вчинені організованою групою або злочинною організацією, або заподіяли значну шкоду чи створили небезпеку тяжких технологічних аварій або екологічних катастроф, загибелі або масового захворювання населення чи інших тяжких наслідків, -

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

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

Запропоновані зміни до статті 361 Особливої частини Кримінального кодексу України гуртуються 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, що вчиняє кримінальне правопорушення у формі незаконного доступу до цифрового пристрою потерпілої особи, якщо при цьому воно не спричинило наслідків у формі витоку, копіювання, перехоплення, модифікації, спотворення процесу обробки, блокування та знищення цифрової інформації.

Як приклад кваліфікації суспільно небезпечного діяння за частиною

першою аналізованої статті хочемо навести: Особа 1, працюючи у фірмі з надання ІТ-послуг, маючи пароль від персонального комп'ютера Особи 2, шляхом введення паролю здійснив авторизацію під обліковим записом Особи 2. Не маючи на меті копіювання інформації, Особа 1 здійснила огляд цифрових документів, які містили звіти про роботу Особи 2, з наступним використанням зазначеної інформації у своїй роботі.

Зазначений приклад чітко відображає, як кваліфікувати дії особи, що вчинила кримінальне правопорушення, передбачене запропонованою нами частиною першою статті 361 Особливої частини Кримінального кодексу України. Однак, на нашу думку, вчиняючи діяння, яке передбачене як запропонованою нами частиною першою 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 обробки, блокування та знищення цифрової інформації. Тому, на наше переконання, фактично у всіх випадках суд повинен додатково кваліфікувати дії особи, як замах на кримінальне правопорушення, передбачене частинами третьою-четверною аналізованої статті (зі змінами).

На нашу думку, використання такої конструкції більш прийнятне для чинного кримінального законодавства України, оскільки в ній ураховано суспільну небезпечність того чи іншого наслідку, заподіяного несанкціонованим втручанням в 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 першою цієї статті як додатковою, а лише у випадках 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 першою статті 361 в обов'язковому порядку. Наприклад, у разі знищеня цифрової інформації особа, яка вчинила кримінальне правопорушення, може не спричинити наслідків у формі ознайомлення (витоку) цифрової інформації, а тому її дії кваліфікуватимуть за частиною третьою 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 [55].

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 та транснаціональним, а ризику шкідливого впливу піддаються не тільки комп'ютери, а й інші цифрові пристрої та інформаційно-телекомунікаційні системи та мережі. Протиправність і суспільна небезпечність використання шкідливого програмного забезпечення та технічних засобів полягають здебільшого у тому, що користувачі навіть не здогадуються, що їх цифрові пристрої були заражені такими програмами.

Німецькою 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 у всьому світі. Так, більше 90 % опитуваних переконані в тому, що шкідливе програмне забезпечення заподіює помітну шкоду їх цифровим пристроям, зокрема комп'ютеру. Приблизно 45 % опитуваних вважають, що через зараження комп'ютера шкідливим програмним забезпеченням функціональність та роботоздатність комп'ютера одразу погіршується. Майже 55 % переконані, що в такому разі хоча б одна з функцій, які 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 більш детально 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 у 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, що не можуть бути використані для іншої роботи; 2) традиційні технічні засоби, які після модифікації застосовують для вчинення кримінальних правопорушень; 3) традиційні технічні засоби, що можуть використовуватися для вчинення кримінальних правопорушень.

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

Автомобільний кодграббер – це пристрій для зчитування, аналізу й генерування кодових послідовностей радіочастотних сигналів та імпульсів, основне призначення якого – несанкціоноване вимкнення й управління радіоелектронними пристроями [297].

Банкоматний скімер являє собою мініатюрний модуль, що зазвичай кріплять на банкомат. Зловмисники розміщують його всередині картоприймача, що дає змогу зробити модуль максимально непомітним і спрощує процедури зчитування й копіювання необхідних даних [300].

До другої групи можна класифікувати такий технічний 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, при якому прочитуються радіосигнали або записуються дані, що зберігаються в так званих транспондерах (RFID-мітках). Ці мітки містять інтегровані чипи та антени для прийому і передачі сигналів. Коли мітка знаходиться в радіусі дії зчитувача, антена генерує електричний струм, який активує чип. Залежно від типу зчитувача його діапазон може варіюватися від кількох сантиметрів до 30 метрів. Для передачі даних застосовується технологія NFC (зв'язок ближнього поля), що працює на відстані до 10 сантиметрів на частоті 13,56 МГц. Обмежена дальність NFC служить першим бар'єром захисту: неможливо зчитати інформацію, якщо карта знаходиться безпосередньо біля терміналу.

Проте шахраї вже створили зчитувачі, які можуть працювати на більші відстані. Іспанські хакери Рікардо Родрігес і Хосе Вілла розробили троянський концепт, що перетворює смартфон у ретранслятор NFC-сигналу, коли телефон і карта знаходяться поруч. Це дозволяє вкрасти інформацію про банківську картку, а не саму транзакцію, оскільки остання захищена шифруванням одноразовим кодом [91].

Зауважимо, що використання NFC-технології у сучасних банківських системах створює нові можливості для шахраїв, особливо коли мова йде про створення засобів обходу стандартних заходів безпеки. Обмежена дальність передачі NFC створена як захисний механізм, але технічна креативність зловмисників знаходить шляхи для її обходу. Новації, такі як різного типу шкідливе програмне забезпечення, що перетворює смартфони в ретранслятори сигналів, вимагають від фахівців у галузі кібербезпеки постійного оновлення знань та методів захисту. Водночас це також підкреслює необхідність для користувачів бути обізнаними щодо потенційних ризиків і методів захисту своїх фінансових даних в епоху цифрових технологій.

До останнього виду належать традиційні технічні засоби, що не мають ознак шкідливого технічного засобу, водночас виступають 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, яка 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 шкідливого програмного забезпечення. За функцією розмноження (саморозповсюдження) виділяємо таке шкідливе програмне: 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, щоби вбудувати 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 [488].

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, відображення

небажаної реклами, створення ботнетів та DDOS-атак.

Комп’ютерні хробаки – це мережеві віруси, здатні до розповсюдження по комп’ютерній мережі шляхом своєї реплікації [489, с. 226].

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 [511].

Незважаючи на шкідливість цього типу шкідливої програми, її здебільшого використовують для введення корисних навантажень, що можуть бути іншими шкідливими програмами, зокрема такими, як троянські віруси або бекдори [482].

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 [409].

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) кейлогер (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 [83].

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 з 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 [129].

Руткіт 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 [427].

Залякувальне програмне забезпечення (scareware) являє собою шкідливий програмний код, здебільшого графічний, що спонукає користувача до купівлі чого-небудь. Таке програмне забезпечення у разі потрапляння на комп'ютер жертви спливанням різних вікон може повідомляти користувача про те, що його цифровий пристрій, наприклад, заражений вірусною програмою, з подальшим схиляннням користувача 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 вчинила кримінальне правопорушення. Такі шкідливі програми збирають хеші

паролів і кейлогери. Викрадач інформації (stealer) використовує 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 небезпечності 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 й переважно їх виявляє антивірусне програмне забезпечення;

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, внаслідок 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

кейлогер (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 у паролях для інтернет-банкінгу. Вони також можуть використовувати шпигунське програмне забезпечення для потреб викрадення іншої особистої інформації, наприклад документів, збережених на вебсайті комп'ютера [355, 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 вчинила кримінальне правопорушення в кіберпросторі, змушує жертву платити гроші за відновлення доступу до них [82].

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. Отже під час переказування грошей особа, вводячи реквізити потенційного отримувача, зіштовхується з наслідками кліперу, що полягають у заміні введених реквізитів на переказ на реквізити особи, яка вчинила кримінальне правопорушення. В результаті грошові кошти перераховуються зловмисникові. Кліпер є новим типом шкідливого програмного забезпечення. Його використовують переважно у сфері віртуальних активів, у які здійснення чарджбеку є неможливим.

Ще одним типом шкідливого програмного забезпечення, пов'язаним з

віртуальними активами, є майнер. Варто зауважити, що за своїми характеристиками він не є шкідливим програмним забезпеченням, а переходить у цей тип лише тоді, коли він несанкціоновано був інстальований на цифровий пристрій жертви без її відома. Основне завдання майнера 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 виходу його з ладу внаслідок перевантаження.

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

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

На наше переконання, 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 та технічних засобів;

3) збут шкідливих програм та технічних засобів.

Під створенням шкідливих програмних чи технічних засобів розуміють розробку абсолютно нового шкідливого програмного чи технічного засобу, а також модифікацію вже існуючого засобу чи програми, наслідком якої є зміна його властивостей [253].

А. Боровик та І. Коптун під створенням шкідливого програмного

забезпечення й технічних засобів розуміють творчу діяльність, унаслідок якої одержують якісно нову програму або технічний засіб, явно наділений функціями, виконання яких може заподіювати шкоду конфіденційності, цілісності та доступності інформації, обробляється в інформаційно-телекомунікаційних системах [25, 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 [294].

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 [293].

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

Під розповсюдженням шкідливого програмного забезпечення, на наше переконання, 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 розміщенні 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, їх поширення через

телекомунікаційні мережі [25, с. 248].

Збут шкідливого програмного забезпечення чи технічних засобів визначають як оплатне чи безоплатне (наприклад, подарунок) передавання зазначених засобів певній особі [151].

На перший погляд може здаватися, що змістовність 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 та 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 та технічних засобів від збуту полягає в тому, що в першому випадку особа своїми діями бажає надати доступ до шкідливого програмного забезпечення якомога більшій кількості користувачів кіберпростору, водночас мета отримання прибутку від таких дій є необов’язковою ознакою. Навпаки, у разі збуту шкідливого програмного забезпечення й технічних засобів першочергова мета особи полягає в отриманні прибутку від кримінально-протиправної діяльності. Крім того, на нашу думку, ще однією ознакою відмінності буде саме якість шкідливого програмного забезпечення чи технічного засобу. У разі розповсюдження шкідливого програмного забезпечення та технічних засобів унаслідок того, що така діяльність носить масовий характер, якість шкідливого програмного забезпечення та технічних засобів здебільшого є низькою, а сама особа, яка вчинила кримінальне правопорушення, переслідує цілі якомога більшого ураження цифрових пристроїв своїх жертв.

Суб’єктом цього кримінального правопорушення є фізична осудна

особа, яка досягла віку 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 першою 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;

Несанкціоновані збут або розповсюдження цифрової інформації з обмеженим доступом, що зберігається в інформаційно-телекомунікаційних технологіях, 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: 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 [25, с. 250].

Правова регламентація інформації з обмеженим доступом міститься в Законі України «Про доступ до публічної інформації» від 19.02.2022 року та Законі України «Про інформацію» від 20.11.2022 року [198; 190].

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 другої статті 6 цього Закону, розголошення якої може завдати шкоди особі, суспільству і державі. Таємною визнається інформація, яка містить державну, професійну, банківську, розвідувальну таємницю, таємницю досудового розслідування та іншу передбачену законом таємницю [190].

Частина друга статті 6 зазначеного Закону визначає вимоги, при яких здійснюється обмеження доступу до інформації: 1) виключно в інтересах національної безпеки, територіальної цілісності або громадського порядку з метою запобігання заворушенням чи кримінальним правопорушенням, для

охорони здоров’я населення, для захисту репутації або прав інших людей, для запобігання розголошенню інформації, одержаної конфіденційно, або для підтримання авторитету і неупередженості правосуддя; 2) розголошення інформації може завдати істотної шкоди цим інтересам; шкода від оприлюднення такої інформації переважає суспільний інтерес в її отриманні [190].

Звернімо увагу, що Закон України «Про доступ до публічної інформації» під час визначення підтипів таємної інформації відсилає до інших нормативно-правових актів. Так, в статті 1 Закону України «Про державну таємницю» надається 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 у порядку, установленому Законом України «Про державну таємницю», державною таємницею і підлягають охороні державою (ст. 1 Закону України «Про державну таємницю»). Визначення адвокатської таємниці надається в статті 22 Закону України «Про адвокатуру». Нею є будь-яка інформація, що стала відома адвокату, помічнику адвоката, стажисту адвоката, особі, яка перебуває у 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 і відомості, одержані адвокатом під час здійснення адвокатської діяльності [181].

Нотаріальна таємниця – це сукупність відомостей, отриманих під час вчинення нотаріальної дії або звернення до нотаріуса заінтересованої особи, в тому числі про особу, її майно, особисті майнові та немайнові права і обов’язки тощо [201].

Банківська таємниця – це інформація щодо діяльності та фінансового

стану клієнта, яка стала відомою банку в процесі обслуговування клієнта та взаємовідносин із ним чи третім особам при наданні послуг банку і розголошення якої може завдати матеріальної чи моральної шкоди клієнту, зокрема: 1) відомості про банківські рахунки клієнтів, у тому числі 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 та здійснення охорони банку та осіб, які перебувають у приміщеннях банку; 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 по окремому банку, за винятком тієї, що підлягає опублікуванню; 8) коди, що використовуються банками для захисту інформації; 9) інформація про фізичну особу, яка має намір укласти договір про споживчий кредит, отримана під час оцінки її кредитоспроможності; 10) інформація про організацію та здійснення 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 та систем розрахунків, а також нагляду у сфері запобігання та протидії легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового знищення; 12) інформація про банки чи клієнтів банків, отримана 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, про віднесення банку до категорії неплатоспроможних, про відкликання банківської ліцензії та ліквідацію банку [182].

За конструкцією об’єктивної сторони кримінальне правопорушення, передбачене статтею 361-2 Особливої частини Кримінального кодексу України, є формальним, тобто є закінченим з 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 оплатне або безоплатне відчуження [173, с. 257].

Суб’єкт кримінального правопорушення є загальним – 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 першою 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, 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, передбачене статтею 362 Особливої частини Кримінального кодексу України.

Хочемо наголосити, що вважаємо за необхідне замінити термін «електронно-обчислювальна машина» на «цифровий пристрій», а автоматизовані системи та комп'ютерні мережі визначати в сукупності як інформаційно-телекомунікаційні мережі, враховуючи, що така інформація може зберігатися не лише у 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, яка обробляється в телекомунікаційних пристроях інформаційно-телекомунікаційних мереж. Закон України від 16. 12. 2020 «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, які здійснюються в системі за допомогою технічних і програмних засобів. Варто зауважити, що виходячи з диспозиції частин 1 та 2 статті 362 Особливої частини Кримінального кодексу України, кримінально-протиправними діяннями вважаються лише несанкціонована зміна, знищення, блокування, копіювання та перехоплення цифрової інформації особою, яка має право доступу до неї. Під час аналізу об'єктивної сторони цього кримінального правопорушення вважаємо, що окремо варто 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 та 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, спотворення 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 втрачається її 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) причиновий зв'язок.

Ми не будемо детально зупинятися на об'єктивній стороні цього кримінального правопорушення, оскільки всі її форми й наслідки, що можуть бути ними спричинені, наведені у 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 певних аспектах перехоплення.

Насамперед нагадаємо, що перехопленням цифрової інформації варто вважати процес неправомірного одержання інформації в кіберпросторі. Водночас копіювання та виток, 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 диспозиції статті 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 у 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 у такій редакції:

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

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 стосовно цієї інформації встановлюються володільцем інформації. Порядок доступу до державних інформаційних ресурсів або інформації з обмеженим доступом, вимога щодо захисту якої встановлена законом, а також перелік користувачів та їх повноваження щодо цього типу інформації встановлюється законодавством [197].

Законом України «Про захист інформації в інформаційно-комунікаційних системах» також установлено, що власник системи забезпечує захист інформації в системі в порядку й на умовах, визначених у договорі, укладеним 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 із порушенням порядку доступу до такої інформації, установленого відповідно до законодавства.

Кваліфікуючими ознаками статті 362 Особливої частини Кримінального кодексу України є такі: 1) несанкціоноване перехоплення або копіювання інформації, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, якщо це призвело до її витоку, вчинені особою, яка має право доступу до такої інформації; 2) дії, передбачені частиною першою або другою 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, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, якщо це призвело до її витоку, вчинені особою, яка має право доступу до такої інформації, ми розглянули в аналізі об'єктивної сторони цього кримінального правопорушення. Тому зупинимося лише на нагальності заміни та 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, яка 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, яка 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 роз'яснення, які 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. Аби визначити, 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, що 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 варто розуміти недотримання вимог, що ставляться 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 встановленні на сервер, де розташований вебсайт шкідливого коду, який 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 невілювання додаткового процесу фільтрації шкідливого програмного забезпечення в системі [118].

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

інформаційно-телекомунікаційній системі. Прикладом такого діяння може бути робота з інформацією, що має таємний доступ, за відсутності належним чином сертифікованої системи захисту. Вироком Шевченківського районного суду міста Київ 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 порушенням правил захисту цифрової інформації, вони не є ідентичними за змістом. Під порушеннями правил захисту цифрової інформації варто 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 було модифікована, скопійована, знищена або заблокована. Таку інформацію з паролями від вебресурсів і вебсерверів вона зберігала на багатьох носіях, зокрема у 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 з паролями від вебресурсів та вебсерверів підприємства. Використавши зазначені паролі доступу, Особа 2 скопіювала всю інформацію про клієнтів підприємства.

Варто відмітити, що наразі відповідальність за забезпечення захисту

інформації покладається на власника системи. Крім того, сьогодні немає уніфікованих норм і правил, які регулюють експлуатацію інформаційно-телекомунікаційних технологій, а також порядок та правила 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 зафіксувати: «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, підписавши їх. 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 повинно бути необережним. Якщо настання наслідків охоплюється прямим умислом особи, яка вчинила кримінальне

правопорушення, склад кримінального правопорушення, яке передбачене 363 статтею Особливої частини Кримінального кодексу України, відсутній.

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 порушення правил захисту цифрової інформації спричинили наслідки у вигляді блокування, копіювання, зниження, модифікації або розповсюдження та збуту такої інформації, дії особи, яка вчинила кримінальне правопорушення, варто 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 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» [25, 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 за умов, що 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, яка в них оброблюється, -

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

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, які здійснюються 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.

Оскільки склад кримінального правопорушення є матеріальним, об'єктивна сторона виражена у формі: 1) діяння, що полягає в масовому поширенні повідомлень електрозв'язку, яке здійснено 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 та 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 [118].

А. Боровик вважає, що розповсюдження варто вважати масовим тоді, коли одне або декілька повідомлень одержують більше ніж один адресат [25, с. 230].

А. Бойко переконаний, що розповсюдження повідомлень електрозв'язку потрібно вважати 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 опинились у розпорядженні відправника та внесені ним до певного списку, згідно з яким провадиться розсилання [146].

Масове розповсюдження повідомлень електрозв'язку визначається як «спам». Відповідно до Закону України від 16. 12. 2020 «Про електронні комунікації», спам визначається, як електронні, текстові та/або мультимедійні повідомлення, що без попередньої згоди (замовлення) користувачів неодноразово (більше п'яти повідомлень одному абоненту) 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.

Варто зазначити, що в цьому разі така ознака, як «масовість», є оцінковою, щодо розповсюдження повідомлень електрозв'язку вона буде

обов’язковою характеристикою, а стосовно адресатів має необов’язковий характер.

Така характеристика, як відсутність попередньої згоди адресатів, 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 [116].

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

Найпопулярнішим типом цього кримінального правопорушення виступають 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 не може їх обробити. Як наслідок – виникають збої в її роботі або вона взагалі перестає повноцінно функціонувати [304].

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 винною у формі прямого умислу

стосовно вчиненого суспільно небезпечного діяння та умисними або необережними ставленнями до наслідків.

Кваліфікуючими 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.

Варто зазначити, що значна шкода визначається для кожного правопорушення окремо й здебільшого міститься в примітці до статті. Так, наприклад, у примітці до статті 185 Особливої частини Кримінального кодексу України зазначається, що у статтях 185, 186, 189 та 190 Особливої частини Кримінального кодексу України значна шкода визнається із 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 і 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, все 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 та прогнозованого часу його непрацездатності. У другому випадку фахівець з DDoS-атак знаходить
вебресурси, як правило електронної комерції, визначає за допомогою фільтрів приблизний денний прибуток такого вебресурсу і починає здійснювати DDoS-атаки на цей вебресурс. Наступний крок – звернення до володільця атакованого вебресурсу з виплатою певної грошової суми, переважно у віртуальних активах, з метою наступного припинення протиправних діянь. Варто зауважити, що DDoS-атаки здійснюються або за допомогою 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 [286].

На хакерських форумах ботнет із 400 000 користувачами оцінюється від 10 000 доларів. На відміну від ботнету стресер є сервісом з перевірки мережі або серверу на стійкість. Ще одна відмінна риса стресеру від ботнету є його доступність, тобто будь-яка особа може купити підписку на той чи інший стресер, замовити бажані характеристики і в подальшому здійснювати кримінально-протиправні дії. Найпопулярнішими сервісами-стресерами є Str3ssed Booter, Free ip stress, free stresser.

Варто зауважити, 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 установлення особи, яка вчинила кримінальне правопорушення в кіберпросторі [286].

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 та 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, 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» [156].

Загалом пропонуємо викласти диспозицію статті 363-1 Особливої частини Кримінального кодексу України в такій редакції:

«Перешкоджання роботі інформаційно-телекомунікаційних технологій, систем та 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 заподіяли значну шкоду, -

3. Дії, передбачені частиною першою або другою цієї статті, якщо вони спричинили тяжкі наслідки або вчинені з корисливих мотивів, -

4. Дії, передбачені частиною першою або другою 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, яка оброблюється 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 XVI розділом 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: 1) віруси; 2) комп'ютерні хробаки; 3) бекдор (backdoor); 4) викрадач інформації (stealer);
5) руткіт (rootkit); 6) залякувальне програмне забезпечення (scareware);
7) кейлогер (keylogger); 8) вірус-вимагач (ransomware); 9) кліпери (clippers); 10) майнери (miners).

2.3. Кримінально-правова характеристика кіберутворювальних кримінальних правопорушень в 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, які передбачені різними розділами Особливої частини Кримінального кодексу України;
2) засобом вчинення кримінального правопорушення завжди будуть елементи інформаційно-телекомунікаційних технологій, систем та мереж; 3) в окремих кримінальних правопорушеннях цього типу кіберпростір є місцем вчинення суспільно небезпечного діяння; 4) закріплені в законі України, шляхом введення в окремі статті Особливої частини Кримінального кодексу України, або визначені в рамках кваліфікуючих ознак, що передбачають кримінальну відповідальність за конкретні суспільно небезпечні діяння.

Пропонуємо зосередити увагу на кожній із наведених особливостей. Кіберутворювальні кримінальні правопорушення, на відміну від кіберзалежних, представлені в різних розділах Особливої частини Кримінального кодексу України, і 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 його як засобу вчинення, установивши кваліфікаційні ознаки. Такі 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) ввезення, 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) [121].

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) [121].

Водночас спостерігаємо і кримінальні правопорушення, у яких кіберпростір є елементом підвищеної суспільної небезпеки, однак 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 нашу кримінально-правову характеристику кіберутворювальних кримінальних правопорушень ми будемо здійснювати, враховуючи 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 [263].

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 - шахрайств; 4) 2 949 кримінальних правопорушень у сфері комп’ютерних систем [262].

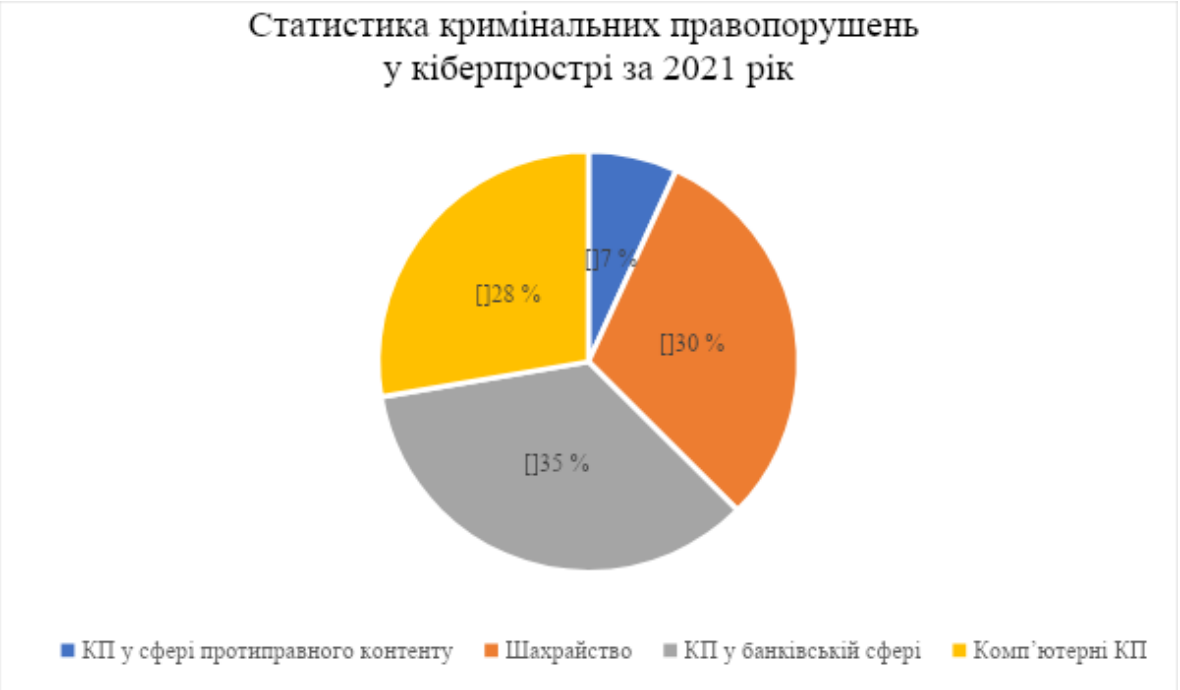


Рисунок 5 – Статистика кримінальних правопорушень у кіберпрострі за 2021 рік

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 2320 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 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 [102].

Згідно з даними Агентства Європейського Союзу з питань мережевої та інформаційної безпеки частка шахрайства у кіберпросторі серед усіх вчинених кримінальних правопорушень в кіберпросторі 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 [4].

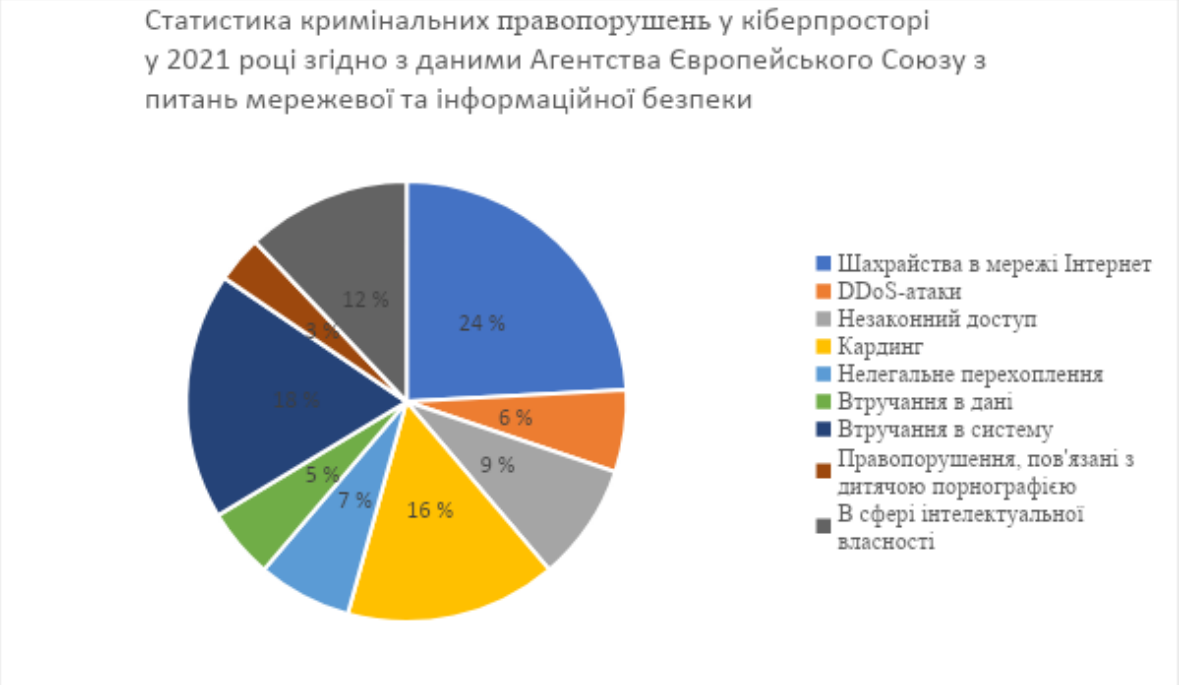


Рисунок 6 – Статистика кримінальних правопорушень у кіберпросторі у 2021 році згідно з даними Агентства Європейського Союзу

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 законодавець у Кримінальному кодексі України від 5 квітня 2001 року передбачив частиною 3 статті 190 Особливої частини Кримінального кодексу України кваліфікуючу 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 змістовних змін. Пропонуємо розглянути шахрайство у 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 у дистанційній формі, тобто саме з використанням інформаційно-телекомунікаційних технологій (пристроїв, систем або мереж) [287, с. 162].

Сам факт обману чи зловживання довірою в кіберпросторі можливий шляхом спілкування з жертвою через різні чати, форуми, відео- та 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 простими у реалізації способи 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 [504].

На думку М. Маккінона, різноманітність видів шахрайства в кіберпросторі зумовлена насамперед анонімністю як самого кіберпростору, так і його користувачів. Кіберпростір дає змогу особі, яка вчинила 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 [407].

Зазначимо, що сьогодні найпоширенішими сферами діяльності суспільства в кіберпросторі є: 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.

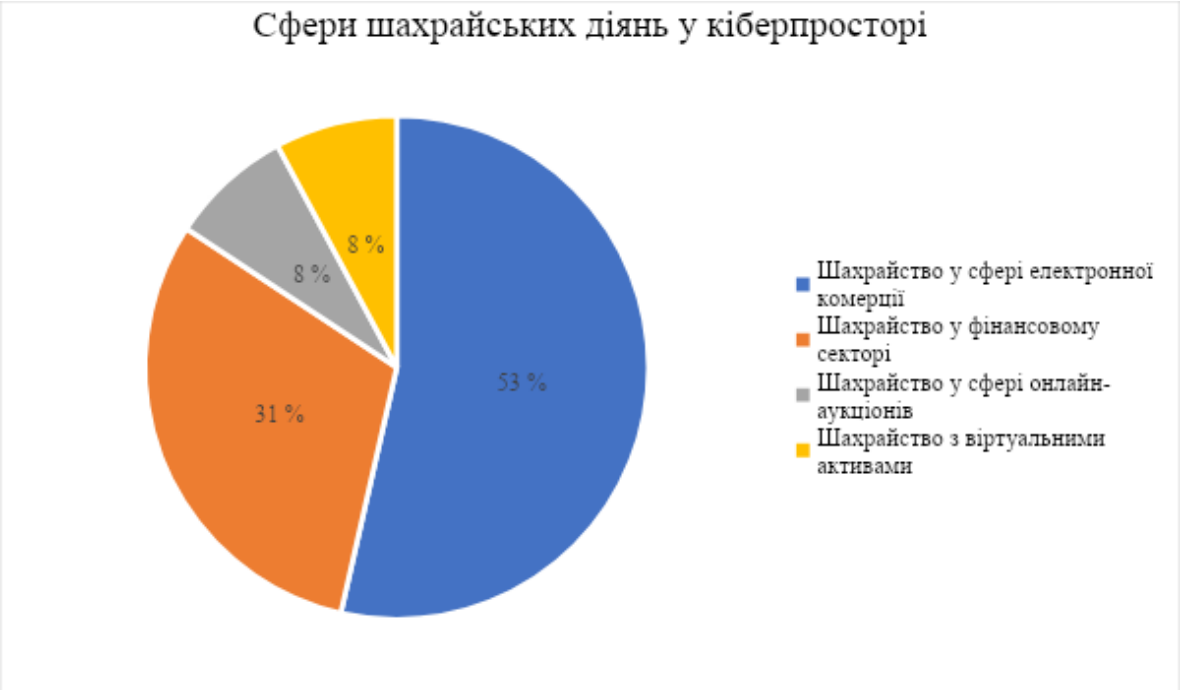


Рисунок 7 – Сфери шахрайських діянь у кіберпросторі

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 напряму діяльності шахраїв. Хочемо зазначити, що шахрайські схеми в кіберпросторі не є вичерпними, а динамічно змінюються й пристосовуються до потреб суспільства. Вибір суспільно небезпечних діянь, вчинеих у формі обману або зловживання довірою, ми робили на основі їх суспільної небезпечності, статистики вчинення й поширеності. Пропонуємо проаналізувати саме види шахрайських дій у кожному секторі [191].

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 [370].

Під час реалізації зазначеної шахрайської схеми особа може діяти як продавець товару чи послуги, так і його покупець. Перший варіант передбачає створення фейкових оголошень з продажу товарів чи послуг на різних онлайн маркетплейсах типу Olx, Prom, Rozetka, Shafa, Skidka та ін. Фейковість оголошення в цьому 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 сплати 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 [272; 370].

У початковий період збройної агресії Російської Федерації шахраї пропонують послуги з перетину державного кордону або довідку про відстрочку від мобілізаційного призову. 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 стосовно нових інцидентів, пов'язаних із цією шахрайською схемою [65].

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 післяоплату 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. Як результат – продавець не несе втрат за доставку товару, а кошти покупця захищені до отримання, огляду й прийняття товару [299].

Варто наголосити, що незважаючи на те, що такий сервіс функціонує

вже декілька років, лише 10 % від користувачів платформи користуються ними, а шахраї своєю чергою активно це використовують. Так, дуже часто продавці товарів створюють фейкові, фішингові вебсайти, що ззовні 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 гроші безпосередньо на мерчант-систему шахрая [306].

Хочемо звернути увагу, що саме шахрайство із сервісами доставки вчиняється в співучасті, організованими групами, є цілі центри, які займаються такою протиправною діяльністю. Водночас сам шахрай може не створювати фейковий вебресурс та мерчант-систему, а одержати доступ до такого сервісу за певний відсоток від кожної шахрайської угоди, в подальшому отримавши завдяки цьому «чисті» гроші від власника сервісу.

Поширення інтернет-торгівлі через соціальні мережі зумовило збільшення шахрайства цієї категорії. Однак якщо в першому розглянутому варіанті реалізації були хоч якісь 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 ніби-то для покриття витрат у разі відмови від нього після отримання. За цією схемою шахраї діють і досягають свого злочинного результату завдяки масовості пропозицій на ринку й відповідної заниженої ціни за аналогічний товар на маркетплейсі [212].

Відповідно до другого варіанта шахрай діє як покупець певного товару. Як приклад, хочемо навести такий різновид шахрайства, як рефандинг. Рефандинг – це кредитова фінансова операція, здійснювана після списання грошей 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 у шахрая. Зауважимо, що кожна запропонована компанія має свій алгоритм повернення грошей за сплачений товар із певних причин, зокрема отримання товару неналежної якості, неотримання товару або отримання іншого товару. Варто наголосити, що реалізація кожного варіанта рефандингу просто 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 повернення грошей. Зазначимо, що товар також залишається в шахрая й після незначного ремонту підлягає продажу.

К. Голдман у своїй праці «Протидія фінансовим кіберзлочинам» серед найпопулярніших способів рефандингу, пов'язаного з отриманням товару неналежної якості, виділив: 1) вміст коробки з посилкою був наповнений паразитами чи комахами, які її зіпсували; 2) вміст коробки з посилкою був наповнений порошком, візуально подібним до наркотичної речовини, як наслідок – коробка із вмістом була викинута [384].

Такий спосіб рефандингу, 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 рідко 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» повернення грошей на свою картку [334].

Наступним видом шахрайства з використанням інформаційно-телекомунікаційних технологій виступає шахрайство на інтернет-аукціонах. Шахраї пропонують взяти участь в аукціоні, де лотом виступає 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 з вказаного карткового рахунку гроші на гарантійний рахунок сервісу, які після схвалення жертвою надсилаються шахраю [29, 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, далі жертви втрачають гроші й не отримують товарний лот [287, с. 162].

Наступним сектором шахрайських дій, які 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 через їх перенесення в рамки кіберпростору вони набувають більшої суспільної небезпечності [265]. Шахрайство, за якого телефон або інший подібний телекомунікаційний гаджет виступає 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, коли особа, яка вчиняє кримінальне правопорушення, ретельно все планує для вчинення одного або декількох суспільно небезпечних діянь, телефонне шахрайство в кіберпросторі здебільшого спрямоване на масовість, де реалізація діяння

заміняється кількістю можливих жертв. Такі ознаки, як дистанційність та відсутність фізичного контакту шахрая з жертвою, лише підвищують рівень суспільної небезпечності. 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 безпосередньо залежить від навичок соціальної інженерії особи, яка вчинила кримінальне правопорушення.

Напевно найпопулярнішою схемою серед телефонних шахраїв є «телефонний скамінг». Телефонний скамінг – це діяльність із переконання жертви щодо переказу грошей 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, зокрема 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 [36].

Ще одним різновидом «телефонного скамінгу», який шахраї активно використовують у своїй діяльності, є дзвінки від співробітників банку, що одержала назву «банківський працівник». Сутність цієї схеми полягає в тому, що шахрай, представляючись співробітником банку або його служби безпеки,

намагається дізнатися дані банківської карти, пароль від інтернет-банкінгу та CVV-код, аби потім привласнити кошти жертви. Зокрема, такі шахрайські дії проходять в декілька етапів, водночас із певним проміжком часу між кожним, і здійснюються в організованій групі. Наприклад, на першому етапі шахрай, маючи певний «бекграунд» про власника картки, може ставити певні уточнюючі питання, інформація про які вже є у 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, і під приводом можливої небезпеки щодо її рахунку переконує її зняти гроші з основного рахунку та перевести на резервний рахунок банку. Як результат – жертва втрачає свої кошти [155].

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 за двома форматами: 1) масовим; 2) цільовим [371].

Відповідно до масового способу шахраї через спам-розсилки (соціальні мережі, імейл) надсилають користувачам повідомлення жалісливого змісту, у яких описуються неіснуючі життєві проблеми, сподіваючись на емпатію жертви. Здебільшого в цьому разі кількість жертв порівняно з кількістю розісланих спам-листів незначна, але саме за рахунок 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 сьогодні схему «постраждалі під час війни», коли шахраї переконують жертву, що вони втратили свій дім і потребують коштів на життя, прикріпляючи фейкові фоти й відео. Дуже часто маємо ситуації, коли шахраї, прикидаючись військовослужбовцями, просять гроші на пальне,

військовий одяг або дрони [88].

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 у тому, що жертва отримує 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 ніби-то суспільно небезпечні дії буде повідомлено правоохоронні органи, засоби масової інформації, знайомих або родичів, якщо особа не переведе визначену шахраями певну суму грошей. 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 кошти шахраям.

Останнім підвидом шахрайства цього сектору є скамеринг-обдзвонювання жертви всевдопредставниками 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, який його вилікує [287, 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 міні-кредитування лише за наявності паспортних даних. Кошти в такому разі зараховуються на карткові рахунки клієнта. Наразі такі послуги є дуже популярними, їх використовують, коли для оплати певного товару не вистачає власних коштів, а купувати товар у кредит особа не хоче. Шахрай може взяти кредити на чуже ім'я, надаючи фінансовій кредитній установі чужі паспортні дані [288].

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 небезпечність аналізованого способу вчинення шахрайства в кіберпросторі.

Особливість зазначеного способу вчинення шахрайства в кіберпросторі полягає в тому, на яку банківську картку шахрай отримує кредитні кошти. У більшості випадків шахраї створюють мережу «дроповських банківських карт». Дроп, або «грошовий мул» – це та людина, яка погоджується, щоб її банківська картка стала «транзитною» для вкрадених шахраями грошей. Дроп переводить незаконно отримані гроші між різними рахунками. Такий ланцюжок переказів потрібен для того, щоб заплутати сліди кіберзлочинців та ускладнити роботу слідства [158].

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

напрямі. 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, опинившись ошуканою. Як і в першому аналізованому способі вчинення шахрайства у кіберпросторі у сфері кредитування, шахраї використовують чужі банківські картки для прийому безготівкової національної валюти [208].

Шахрайство у сфері обміну віртуальної валюти, на відміну від 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 обманювали громадян, охочих провести операції з обміну віртуальних активів. Шахраї створили власну CMS-систему з обміну віртуальних активів, куди за допомогою реклами в соціальних мережах перенаправляли жертв. Як результат – втрата безготівкової національної валюти жертвами цього суспільно небезпечного діяння [98].

Не менш актуальна й суспільно небезпечна шахрайська схема, яка переважно реалізується в співучасті, – «шахрайство у сфері надання інвестиційних послуг». Зазначений вид шахрайства є найбільш високоприбутковим 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 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 створюється власна інвестиційна платформа 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 у декількох містах або навіть країнах, та набирається персонал.

Третій етап полягає в реалізації злочинного умислу шляхом обдзвонювання потенційних жертв із метою пропонування інвестицій в 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, він пропонує подвоїти свій внесок для більшого прибутку.

На четвертому етапі, коли вкладник вже 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 коштів [100].

Незважаючи на віднесення проаналізованих способів вчинення шахрайств 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 зазначеної статті чітко вказано, що таке шахрайство вчинене шляхом незаконних операцій із використанням

електронно-обчислювальної техніки. При цьому законодавець не надає визначення, що саме розуміється під незаконними операціями. Крім того, визначення електронно-обчислювальної техніки як засобу кримінального правопорушення суттєво 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 грошима 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 вирокові суду визначено, що кваліфікуючу шахрайство обставину утворюють лише операції, здійснення яких без використання електронно-обчислювальної техніки є неможливим [222].

Органи досудового розслідування кваліфікували дії обвинуваченого по вказаних епізодах за частиною 3 статті 190 Особливої частини Кримінального кодексу України, як шахрайство вчинене шляхом незаконних операцій з використанням електронно-обчислювальної техніки, що, на переконання суду, є неправильним.

Хочемо звернути увагу на те, що Департамент кіберполіції Національної поліції України аналогічні суспільно небезпечні діяння з ознаками шахрайства в разі оголошеня підозри розглядає саме як вчинені з використанням електронно-обчислювальної техніки, незважаючи на те, вчинене зазначене діяння з використанням телефона або комп'ютера [99; 101; 144; 209].

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 з продажу неіснуючих товарів або надання послуг не можна вважати незаконними, адже фактичного втручання в систему в цьому разі 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 наше переконання, не є соціально обумовленою норма частини 3 цієї статті через невідповідність змісту норми й категорії діянь, вчинюваних у кіберпросторі шляхом обману чи зловживання довірою. Крім того, вважаємо за потрібне 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 необхідно в Постанові пленуму Верховного суду України акцентувати увагу, що кваліфікуюча ознака «шляхом операцій з

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 з використанням інформаційно-телекомунікаційних технологій, систем і мереж дії особи, за яких кіберпростір використовується лише для пошуку потенційних жертв із подальшим фізичним контактом при реалізації шахрайських дій.

Проаналізувавши склад кримінального правопорушення, передбачений частиною 3 статті 190 Особливої частини Кримінального кодексу України, та визначивши його специфічні риси, постає питання нагальності виключення цієї кваліфікуючої ознаки з чинного кримінального законодавства й можливості запровадження спеціальної норми, що визначала б кримінальну відповідальність за шахрайство у сфері цифрової інформації.

Насамперед хочемо зауважити, які саме діяння можуть підпадати під кваліфікуючу ознаку аналізованої статті. Відповідно до статті 8 «Конвенції про кіберзлочинність», що має назву «Шахрайство, пов’язане з комп’ютером», до таких суспільно небезпечних діянь належить:

1) заволодіння чужим майном або правом на майно шляхом введення, зміни, знищення чи приховування комп’ютерних даних; 2) заволодіння чужим майном або правом на майно, шляхом будь-якого втручання у функціонування комп’ютерної системи [107].

З огляду на практику вирішення судами справ за частиною 3 статті 190 Особливої частини Кримінального кодексу України маємо ситуацію, коли фактично тотожні за своїм змістом діяння кваліфікують по-різному.

Проблемою законодавства в цьому питанні є відсутність тлумачення таких понять, як введення інформації або будь-яке втручання в функціонування комп’ютерної системи [122].

Водночас хочемо наголосити: сам зміст аналізованої кваліфікуючої 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 [268].

Не можемо не звернути увагу на те, що переважна більшість науковців розуміє під незаконними операціями з використанням електронно-обчислювальної техніки такі суспільно небезпечні дії, як «фішинг» [275].

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 [62].

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 за допомогою «фішингу» одержала персональні дані онлайн-банкінгу або дані картки з подальшим заволодінням грошовими коштами? Чи підлягає вона кримінальній відповідальності за частиною 3 статті 190 Особливої частини Кримінального кодексу України? На нашу думку, зазначене суспільно небезпечне діяння не може кваліфікуватися за

частиною 3 статті 190 Особливої частини Кримінального кодексу України з огляду на відсутність обману або зловживання довірою [179].

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 виключно 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 [249].

Залишається невирішеним питання кваліфікації низки ряду суспільно небезпечних діянь, вчинених таємним способом і спрямованих на викрадення чужого майна або права на таке майно. Ми вважаємо, що недоцільно вводити до статті 185 Особливої частини Кримінального кодексу України кваліфікуючу ознаку, спрямовану на викрадення чужого нематеріального майна, оскільки це призведе до деформації змісту цієї статті й проблем кваліфікації такого кримінального правопорушення.

Водночас, на наше переконання, 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 дематерелізувавши 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 вчинила кримінальне правопорушення, уникає безпосереднього контакту з потерпілою особою – власником безготівкових, електронних грошей або віртуальних активів [249].

Залежно від фінансового інструмента ми виділили такі способи таємного викрадення безготівкових, електронних грошей або віртуальних активів: 1) шляхом оплати покупок із використанням персональних даних власника картки, або електронного гаманця в інформаційно-телекомунікаційних мережах; 2) шляхом одержання доступу до системи дистанційного банківського обслуговування; 3) шляхом зняття 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 увведення персональних даних володільця картки або електронного гаманця у вигляді цифрової інформації; 2) шляхом іншого втручання в роботу інформаційно-телекомунікаційних технологій.

У першому випадку ми вбачаємо ситуацію, за якої особа, одержавши будь-яким способом персональні дані власника картки шляхом уведення даних цієї картки на будь-якому маркетплейсі, купує товари чи послуги за рахунок коштів володільця карти. 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 оцінки фінансових транзакцій в Інтернеті на предмет підозрілості з точки зору шахрайства, 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 більш складнішим для подолання [12].

До таких фільтрів належить регіон, із якого вчиняється купівля, девайс, IP-адреса, відбиток браузера та багато іншого. Для прикладу, змоделюємо ситуацію, за якої Особа 1 територіально перебуває в Латвії, купивши персональні дані банківської платіжної картки Особи 2, яка є громадянином України. Особа 1 захотіла здійснити покупку через популярний маркетплейс Amazon подарункового сертифікату з певним грошовим номіналом, використавши дані банківської картки Особи 2. Водночас використовуючи IP-адресу Литви, антифрод-система, розуміючи, що дані банківської картки належать до Української банківської системи, а транзакція здійснюється з Литовської IP-адреси, сервіс 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 той факт, що особа може здійснювати операції з незаконної купівлі даними чужої банківської картки у безлічі маркетплейсів, незважаючи на факти блокування транзакції антифрод-системою, лише підвищує суспільну небезпечність.

Фактично за допомогою уведення 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, застосовує не персональні дані власника банківської картки або електронного гаманця, а використовує лог-файли для своєї протиправної діяльності. Лог-файли – це файли, що містять системну інформацію роботи сервера або комп'ютера, до яких заносяться певні дії користувача або програми [298].

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 небезпечність, 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 шляхом 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, яка обробляється 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 -

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

2. Крадіжка у сфері обігу безготівкових або електронних грошей і

віртуальних активів внаслідок іншого втручання в роботу інформаційно-телекомунікаційні технології, системи і мережі, -

3. Діяння, передбачене частинами першою – другою цієї статті, вчинене повторно, або за попередньою змовою групою осіб, або таке, що завдало значної шкоди потерпілому, -

4. Діяння, передбачене частинами першою – другою цієї статті, якщо воно вчинене шляхом модифікації цифрової інформації, -

5. Діяння, передбачене частинами першою – другою, вчинене у великих розмірах або організованою групою.

Водночас у примітках до цієї статті визначити, що є введенням цифрової інформації та іншим втручанням у роботу інформаційно-телекомунікаційної технології, системи та мережі.

Під уведенням цифрової інформації під час вчинення крадіжки безготівкових або електронних грошей і віртуальних активів варто вважати втручання у функціонування засобів оброблення, зберігання або передавання цифрової інформації, внаслідок якого відбувається додавання нової цифрової інформації в інформаційно-телекомунікаційну технологію, систему або мережу.

Під іншими втручанням 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 і 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, яке ми хочемо проаналізувати, є вимагання, яке 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 [140, с. 261].

Зазначимо, що вимагання в кіберпросторі принципово відрізняється від традиційного вимагання, відсутністю фізичного контакту між особою, яка вчинила кримінальне правопорушення, та потерпілою особою. На нашу думку, така характерна ознака вимагання у кіберпросторі не зменшує суспільну небезпечність діяння, а навпаки, підвищує її. Крім того, вимагання у кіберпросторі є гіперлатентним кримінальним правопорушенням.

Характер погроз вимагання у кіберпросторі може бути виражений через месенджери, соціальні мережі, відеочати, електронну адресу або особисті повідомлення [145].

Найбільш поширеним способом вимагання в кіберпросторі сьогодні є погроза розголошення відомостей, що потерпілий або його близькі родичі хотіли зберегти в таємниці. Розглянемо два різних способи скоєння цього кримінального правопорушення, де за першим варіантом не потрібна

додаткова кваліфікація за відповідною статтею Розділу XVI Особливої частини Кримінального кодексу України, а за другим – потрібна. Відповідно до першого варіанту хочемо навести приклад, у якому 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 може супроводжуватися різними електронними платіжними системами, що значно ускладнює ідентифікацію особи, яка вчинила кримінальне правопорушення [263].

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, внаслідок чого особи, які вчинили кримінальне правопорушення, вимагали гроші за нерозповсюдження інформації інтимного характеру потерпілих [87].

Іншим способом вимагання, що полягає в погрозі обмеження прав, свобод або законних інтересів, є DDoS-атака. Ми детально розбирали 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 можливе 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 такі дії не можна розцінювати як пошкодження або знищення майна. На наше переконання, варто виділити такий спосіб як окрему кваліфікуючу ознаку, зокрема: «*погроза блокування, видалення, знищення, модифікації або погроза іншого несанкціонованого втручання в роботу інформаційно-телекомунікаційних технологій, систем і мереж, що може завдати шкоду правам та інтересам потерпілої особи».*

На нашу думку, подібне нововведення в кримінальне законодавство надасть можливість повністю оцінити суспільну небезпечність 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. В даному випадку 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 та, що перевищує 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: якщо Особа 1 шляхом несанкціонованого втручання в роботу цифрового пристрою завантажила на нього шкідливе програмне забезпечення, що призвело до пошкодження або знищення цифрового пристрою, вартість якого оцінено в 35 тисяч гривень, буде нести лише цивільну відповідальність. Проте, на нашу думку, сам характер дій у кіберпросторі у цьому 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 через 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 таке, що 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 V розділом 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 і суміжних прав (стаття 176 Особливої частини Кримінального кодексу України).

Відповідно до додаткового протоколу Конвенції «Про кіберзлочинність», який 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 кваліфікуючої ознаки до цієї статті, вчинення таких дій у рамках кіберпростору. На нашу думку, немає нагальності внесення зміни до зазначеної статті у вигляді кваліфікуючої ознаки, оскільки фактично наразі саме кіберпростір є певним майданчиком для вчинення таких суспільно небезпечних дій [61, с. 104].

Сьогодні спостерігаємо діяльність багатотисячних груп у соціальних мережах, окремі форуми, веб-сайти, які спеціалізуються на діях ксенофобного та расистського характеру [214, с. 119].

Вчинення зазначених дій із використанням кіберпростору, а саме: соціальних мереж та Інтернету, значно підвищує суспільну небезпечність такого діяння, ускладнючи 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 [108, с. 47].

У зазначеній статті безпосередньо в диспозиції вказано на засіб вчинення кримінального правопорушення. Крім того, відповідно до частини 2 аналізованої статті вбачається кваліфікуюча ознака «вчинення таких дій з використанням спеціальних засобів, призначених для негласного зняття інформації». Проаналізувавши судову практику за останні 10 років, нами було установлено, що в період із 01.01.2013 р. і по сьогодні не було жодного судового рішення у формі вироку за статтею 363 [78].

Незважаючи на задовільну статистику, суспільну небезпечність 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 за потрібне закріпити кваліфікуючу ознаку, а саме: *«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 і 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 буде 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- та 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 первісного 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, яку отримав 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 за доцільне унесення кваліфікуючої ознаки до статті 176 Особливої частини Кримінального кодексу України.

Наступні кріберутворюючі 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, які 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: як електронний або паперовий документ, що використовується суб’єктами переказу, їх клієнтами, кліринговими, еквайринговими установами або іншими установами – учасниками платіжної системи для передавання доручень на переказ коштів [204].

Зауважимо, що наразі цей Закон втратив чинність і дефініція поняття «документи на переказ» у чинному законодавстві не визначена. Відповідно до Закону України від 30.06.2021 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 попередньо оплачених платіжних карток багатоцільового використання), що 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 за потрібне розглянути суспільно небезпечні дії, що характеризують аналізоване кримінальне правопорушення, а саме: 1) підробку платіжних карток, документів на переказ та 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 бути більшим за 19. У нього закладено назву платіжної системи, що використовується карткою, тип картки та належність до певного банку. Наприклад, якщо номер банківської платіжної картки: а) 4 – Visa; б) 5 – MasterCard; в) 3 – American Express; г) Maestro; 2) ім'я та прізвище власника картки (як правило для пострадянських країн такий обов'язковий пункт не застосовується); 3) термін дії картки; 4) логотип платіжної системи й назва банку, який видав платіжну картку; 5) мікросхема для здіснення NFC-платежів.

Так само на зворотньому боці картки повинні бути: 1) магнітна стрічка; 2) голограма; 3) захисний CVV-код; 4) місце для підпису власника картки; 5)

місце для фотографії володільця картки (для пострадянських країн не є обов'язковим).

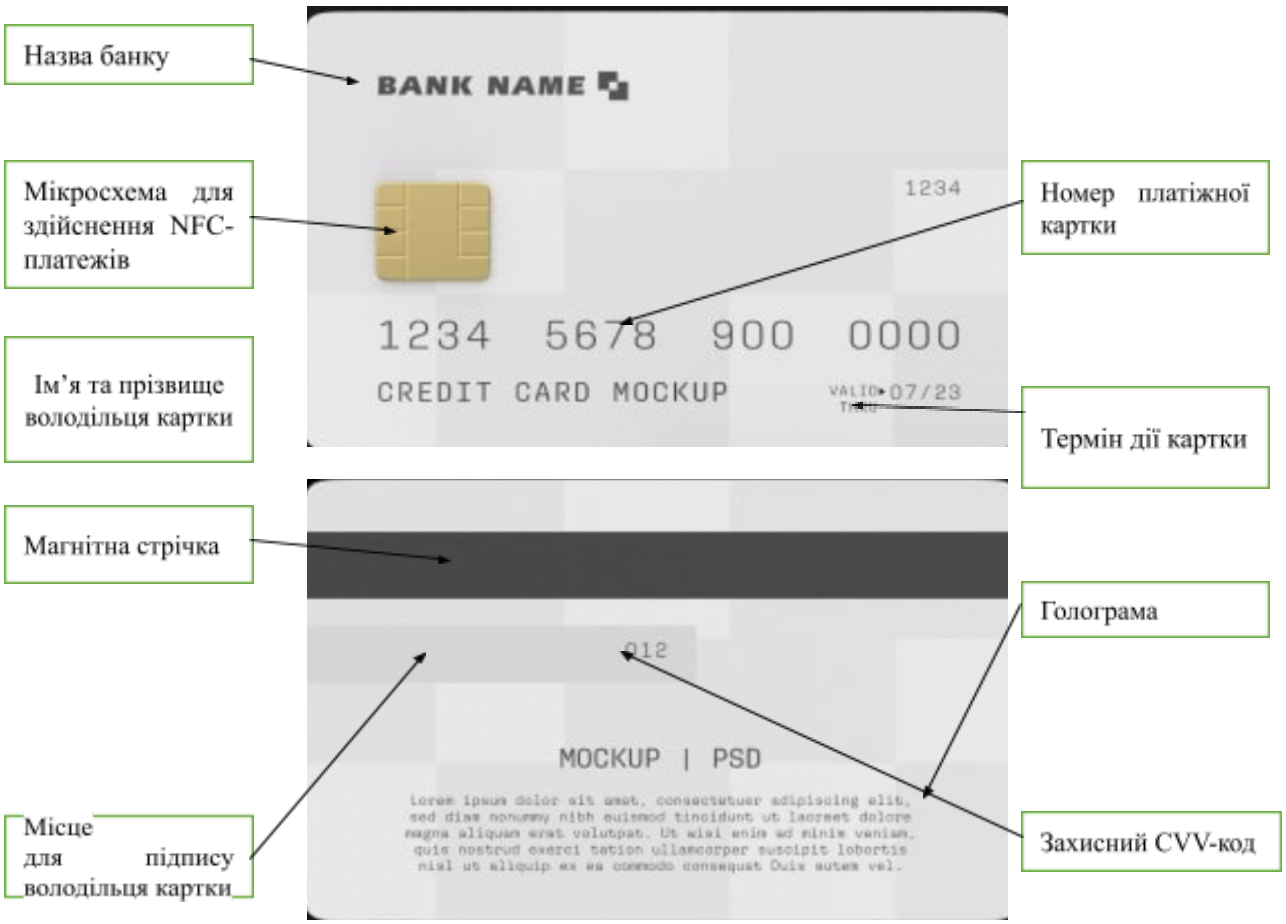


Рисунок 9 – Огляд платіжної картки

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. Отже особа, яка незаконно виготовила підробну платіжну картку, нестиме додаткову відповідальність за статтею 361-1 Особливої частини Кримінального кодексу України [243].

Загалом процес підробки банківської платіжної картки має три основні етапи. На першому етапі особа одержує повну інформацію про банківську платіжну карту. Здебільшого це відбувається за допомогою розміщення POS-систем та POS-терміналів. POS-системи переважно розміщують на банкоматах у вигляді скімерів, а POS-термінали – це дублікати звичайних терміналів, які використовують суб'єкти підприємницької діяльності, що мають функцію щодо 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 дії картки; 3) CVV-код; 4) назва банку та платіжної системи. Потім за допомогою тайпера впаюється чиста магнітна стрічка на пластикову карту, тим самим завершаючи етап повного створення пластикової картки.

Останнім етапом є запис інформації, одержаної на першому етапі, на платіжну картку. За допомогою енкодера 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 у 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 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 скімеру, з наступною оплатою товарів через Інтернет, тобто без фізичного застосування магнітної стрічки платіжної картки, також не створює складу кримінального правопорушення аналізованої статті [124].

Під збутом підроблених платіжних карток варто розуміти їх умисне оплатне чи безоплатне відчуження, що полягає в їх продажу, 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 і 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 й іменні чеки в іноземній валюті, які емітовані за кордоном, що пред'являються для сплати на території України [148; 193].

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 кіберутворюючим кримінальним правопорушенням цієї групи виступає легалізація (відмивання) майна, одержаного злочинним шляхом, яке 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 одержання. При цьому зауважимо, що заміна слова «дохід» у Кримінальному кодексі України редакції 2019 року на «майно» виправдано насамперед ширшим тлумаченням останнього, що охоплює і поняття «дохід» [10].

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 (це, наприклад, нерухомість, транспортні засоби, твори мистецтва) [281].

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 та банківські метали [183].

З огляду на це можемо віднести операції з легалізації майна, отриманого 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, отриманого злочинним шляхом.

Усі способи легалізації майна в кіберпросторі можна поділити на такі групи: 1) легалізація майна, отриманого злочинним шляхом за допомогою вже існуючої інтернет-інфраструктури (маркетплейсів, сайтів оголошень, соціальних мереж, інтернет-аукціонів, краудфандінгу); 2) легалізація майна, отриманого злочинним шляхом, у результаті створення нової вебінфраструктури (інтернет-магазин); 3) легалізація майна, отриманого злочинним шляхом, завдяки використанню обмінників і цифрових (електронних) валют; 4) легалізація майна, отриманого злочинним шляхом за допомогою віртуальних активів.

Напевно одним із найпростіших і водночас найпопулярніших способів легалізації майна, отриманого злочинним шляхом, є продаж неіснуючих товарів на маркетплейсах (prom, olx). Реалізація такої схеми виглядає так. Особа, яка вчиняє кримінальне правопорушення, створює декілька акаунтів

на макретплейсах, 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 меркетплейсі «свої фіктивні» товари. Дохід особа отримує на дійсний банківський рахунок, а в якості доказів 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 для створення пропозиції 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 [391].

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 [422].

Варто зауважити, що особливістю реалізації проаналізованих схем легалізації майна, отриманого злочинним шляхом, є те, що їх може реалізовувати лише одна особа, враховуючи класифікаційний момент щодо вже існуючої вебінфраструктури.

Легалізація майна, одержаного злочинним шляхом, шляхом 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 та товарів, а фінансові операції через підключені до вебмагазину мерчан-системи протікають винятково з «брудними» грошовими коштами за різноманітними схемами.

Ми не будемо зупинятися на схемах легалізації майна, отриманого 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 елементу кіберпростору. У нашому дисертаційному дослідженні ми зосередили увагу на тих кримінальних правопорушеннях, у яких елементи кіберпростору, зокрема інформаційно-телекомунікаційні технології, системи та мережі, значно підвищують суспільну небезпечність 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 кваліфікуючих ознак, які підкреслювали підвищену суспільну небезпечність 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 кваліфікуючу ознаку «погроза блокування, видалення, знищення, модифікації або іншого несанкціонованого втручання в роботу інформаційно-телекомунікаційних технологій, систем і мереж, що може завдати шкоду правам та інтересам потерпілої особи».

Висновки до розділу 2

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

2. Визначено, що за спрямованістю кримінальні правопорушення у кіберпросторі можуть бути: 1) несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж; 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; 5)

порушення авторських і суміжних прав та незаконне використання чужого товарного знаку, якщо такі дії вчиняються в кіберпросторі; 6) кібертероризм та фінансування тероризму, здійснене за допомогою віртуальних активів; 7) кардинг (розкрадання безготівкових грошових коштів, електронних грошових коштів та віртуальної валюти);

8) незаконне виготовлення, зберігання, розповсюдження, рекламування або публічна демонстрація інформації, забороненої до вільного доступу.

3. Встановлено, що основними цілями використання інформаційно-телекомунікаційних технологій, систем та мереж при вчиненні кримінальних правопорушень у кіберпросторі виступають: 1) знищення, блокування, зміни інформації, що міститься в електронно-обчислювальних машинах, а також порушення порядку роботи електронно-обчислювальних машин, інформаційних та електронних комунікаційних мереж; 2) використанням електронно-обчислювальних машин, інформаційно-комунікаційних мереж, мереж електрозв'язку досягається інша ціль, зокрема здійснення шахрайства у кіберпросторі, незаконне отримання конфіденційної інформації; 3) забезпечення злочинної діяльності: незаконний збір та систематизація інформації, ведення «чорної» бухгалтерії, ведення баз даних щодо поширення предметів, що знаходяться в обмеженому обігу, – наркотиків, зброї, листування електронною поштою.

4. Наголошено, що кримінальні правопорушення в кіберпросторі є надзвичайно соціально небезпечним, протиправним явищем, яке становить загрозу не тільки національним, але й міжнародним інтересам, а боротьба з їх феноменом є одним з головних завдань правоохоронних органів як національного, так і міжнародного рівня.

5. Акцентовано увагу на тому, що кримінальні правопорушення, які вчиняються в кіберпросторі, в сфері обігу цифрової інформації та функціонування інформаційно-телекомунікаційних технологій, не є ідентичними за своєю сутністю з кримінальними правопорушеннями в сфері використання інформаційно-телекомунікаційних технологій. Відповідно

визначено, що перші варто називати кіберзалежні, а інші кіберутворювальні кримінальні правопорушення. Зокрема, кіберзалежні кримінальні правопорушення прийнято вважати кіберзалежними, тобто основним предметом цього типу кримінальних правопорушень у кіберпросторі виступає цифрова інформація в сфері цифрових технологій, інформаційно-телекомунікаційних систем та мереж. Кіберутворювальні кримінальні правопорушення є класичними кримінальними правопорушеннями, які внаслідок використання інформаційно-телекомунікаційних технологій перейшли у кіберпростір.

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

7. Обґрунтовано, що суттєвим недоліком чинного кримінального законодавства є невідповідність термінології сучасному стану науки та техніки, зокрема запропоновано замінити термін «електронно-обчислювальні машини» на термін «цифровий пристрій», який об’єднує набагато більшу кількість інформаційно-телекомунікаційних технологій. Одночасно з цим вважаємо за доцільне розглядати інформаційні (автоматизовані), електронні комунікаційні, інформаційно-комунікаційні системи, електронні комунікаційні мережі у сукупності як інформаційно-телекомунікаційні технології, системи та мережі.

8. Зазначено на необхідності законодавчого закріплення поняття несанкціонованого втручання, під яким пропонуємо розуміти одержання можливості для ознайомлення та (або) використання цифрової інформації шляхом проникнення в інформаційно-телекомунікаційні системи та мережі з використанням спеціальних технічних засобів та (або) спеціального програмного забезпечення особою, яка не має права доступу до такої

інформації та (або) роботи з нею.

9. На основі аналізу визначено, що наслідки у вигляді несанкціонованого копіювання та перехоплення цифрової інформації за своїм змістом не є ідентичними. Так, при несанкціонованому копіюванні цифрової інформації спостерігаються обов'язкові наслідки у виді дублювання інформації, як форми завершеного кримінального правопорушення, тоді як при перехопленні інформації наслідки у формі дублікату інформації можуть і не настати, а саме кримінальне правопорушення буде закінченим з моменту початку активних дії в інформаційно-телекомунікаційних системах щодо створення додаткової лінії зв'язку.

10. Запропоновано авторську типологізацію шкідливих технічних засобів, зокрема за процесом створення: 1) шкідливі технічні засоби, які створені спеціально для вчинення певної категорії кримінальних правопорушень і не можуть бути застосовані для іншої роботи;
2) традиційні технічні засоби, які внаслідок модифікації застосовуються для вчинення кримінальних правопорушень; 3) традиційні технічні засоби, які можуть використовуватися для вчинення кримінальних правопорушень.

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

12. Визначено та охарактеризовано основні сектори, в яких

вчиняється шахрайство шляхом використання інформаційно-телекомунікаційних технологій, систем та мереж, зокрема: 1) шахрайство в сфері електронної комерції; 2) шахрайство на інтернет-аукціонах;

3) традиційне шахрайство з використанням інформаційно-телекомунікаційних технологій; 4) шахрайство в сфері надання фінансових послуг.

13. Обґрунтована соціальна необумовленість норми частини 3 статті 190 Особливої частини Кримінального кодексу України з причини невідповідності змісту норми та тієї категорії діянь, які вчиняються у кіберпросторі шляхом обману чи зловживання довірою. Одночасно з цим пропонується доповнити частину 2 статті 190 Особливої частини Кримінального кодексу України, яка б встановлювала кваліфікуючу ознаку використання інформаційно-телекомунікаційних технологій, систем та мереж при вчиненні зазначеного кримінального правопорушення.

14. Установлено, що переважна більшість науковців під шахрайством з використанням інформаційно-телекомунікаційних технологій розуміє «фішинг», 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. Доведено, що суспільно небезпечні діяння у формі «фішингу» необхідно кваліфікувати за частиною 3 статті 361 Особливої частини Кримінального кодексу України з причини специфічного предмета такого кримінального правопорушення, зокрема цифрової інформації. У випадку «фішингу» обман виступає лише як спосіб отримання персональних даних у вигляді цифрової інформації.

15. З’ясовано, що в залежності від фінансового інструменту варто виділяти наступні способи таємного викрадення безготівкових, електронних

грошей або віртуальних активів: 1) шляхом оплати покупок з використанням персональних даних володільця карти або електронного гаманця в інформаційно-телекомунікаційних мережах; 2) шляхом отримання доступу до системи дистанційного банківського обслуговування; 3) шляхом зняття грошових коштів у банкоматі.

16. Визначено основні способи легалізації майна, отриманого злочинним шляхом: 1) легалізація майна, отриманого злочинним шляхом за допомогою вже існуючої інтернет-інфраструктури (маркетплейси, сайти оголошень, соціальні мережі, інтернет-аукціони, краудфандінг); 2) легалізація майна, отриманого злочинним шляхом, шляхом створення нової вебінфраструктури (інтернет-магазин); 3) легалізація майна, отриманого злочинним шляхом використання обмінників та цифрової (електронної) валюти; 4) легалізація майна, отриманого злочинним шляхом за допомогою віртуальних активів.

РОЗДІЛ 3
ОСОБЛИВОСТІ КВАЛІФІКАЦІЇ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ В КІБЕРПРОСТОРІ

3.1. Особливості кримінально-правової кваліфікації кримінальних правопорушень у кіберпросторі, предметом та 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 виняткова в цифровому середовищі, зокрема віртуальні активи [376, с. 143].

Глобалізація та цифровізація, трансформація політичних та соціально-економічних систем є останніми тенденціями в сфері економічної злочинності; вони сприяють поглибленню проблем боротьби із злочинами у сфері економічної діяльності. Відстеження та доведення економічних злочинів стає все більшим викликом для правоохоронних органів. Розвиток кіберзлочинності в економічній сфері, який сприяється впливом технологічних компаній на діяльність державних та недержавних структур у

формі управління великими даними, поглиблює проблему боротьби з економічними злочинами [503].

Постійний розвиток фінансового сектору загалом і ринку валют зокрема призводить 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 правового статусу.

Хочемо наголосити, що Україна здебільшого виступає лідером антирейтингів, наприклад у розрізі захисту прав інтелектуальної власності або рівня корупції, і незважаючи на збройну агресію Російської Федерації та реформи, які передбачені європейською спільнотою, все ще залишається одним із лідерів за цими показниками. Незважаючи на це, 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 [89].

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 [394; 111].

Зауважимо, що часто розвиток суспільних відносин є стрімким, тому

державні інституції просто не встигають забезпечити врегулювання, а отже, і охорону тих чи інших суспільних явищ чи інституцій. На нашу думку, це зумовлено насамперед тим, що держава повільна і 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, порівняно прийнятні ставки за податками.

Поява віртуальних активів, крім позитивного ефекту, стала каталізатором появи нових злочинних схем, зокрема, шахрайства, вимагання та вчинення 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:

1. Анонімність. Застосування методів криптографії та децентралізованих реєстрів надто сильно 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 трансакцій. До таких віртуальних активів Європарламент класифікує Monero, DASH і Zcash [479].

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 трансакції 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 [360].

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 правилами країн – учасників трансакцій можуть бути вагомими, що значно ускладнює роботу правоохоронних органів [387].

6. Децентралізованість. Дає користувачам змогу обмінюватися фінансовими цінностями безпосередньо 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 воєнних конфліктів тощо [162, 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 кожен 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, цей законопроєкт передбачає, що криптовалюта – це окремий специфічний і новий об'єкт цивільних правовідносин. Згідно з цим законопроєктом узаконення криптовалюти повинно відбуватися двома етапами. Упродовж першого етапу є необхідним затвердження правового статусу криптовалют 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 [202].

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 [185].

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 року. Згодом Верховною Радою України 8 вересня 2021 року цей законопроєкт було ухвалено. Водночас Президент України вважає, що цей Закон не може бути підписаний з огляду на те, що: 1) положення Закону «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 та прозорих умов для учасників ринку віртуальних активів та інвесторів, що не сприятиме належному забезпеченню їх прав [186].

Важливо акцентувати, 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, за 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 [225; 226].

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 є абсолютно недопустимим у праві, що повинно мати загальний характер, а особливо в кримінальному праві, а 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.

Тож 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 «віртуальних активів» 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 валютних цінностей; 3) розгляд віртуальних активів як особливого майна, здатного до участі в цивільному обороті, й такого, що має певну цінність [421].

Зокрема, Д. Ангел під віртуальними активами розуміє одну з форм вираження цифрової валюти, емісія та облік якої базуються на асиметричному шифруванні й використанні різних методів криптографічного

захисту [398, 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 [379, с. 260].

Так само А. Берестен не розглядає віртуальні активи, як новий вид платіжного інструменту. На його переконання, вони виступають одним з видів електронних грошей, однак 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 [328].

Подібної точки зору додержуються 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 [37, с. 13].

З-поміж усіх доктринальних визначень поняття віртуальні активи, напевно, найбільш розгорнуто надав А. Карстенс. На відміну від інших науковців, він акцентував увагу на двох ключових моментах обігу віртуальних активів, зокрема – довірі й конвенції. Поширення віртуальних активів лише підкреслює важливу роль 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 [336].

Більш сучасне визначення поняття «віртуальний актив» надає Ю. Полякова: це новий фінансовий інструмент конвертованої

цифрової валюти, що базується на математичних принципах, які автоматично генеруються й контролюються програмним забезпеченням [455, 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 [508, с. 116].

Проте на наше переконання, 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 [28].

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, тобто 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 [60, 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 в 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 при цьому не надав їй статусу цінних паперів [472].

Незважаючи на це, вже у 2014 році Податкова служба Австралії зазначила можливість введення оподаткування криптовалютних операцій. На сьогодні операції з криптовалютою, кріптовалютні 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 [320]. Крім того, в Австралії існує легальна можливість виплачувати заробітну плату в криптовалюті, але лише за наявності договору між працівником і роботодавцем [320].

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

[501].

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 внаслідок 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 [335].

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 забороняються [199].

У 2014 році НБУ Листом №29-208/72889 (Лист НБУ) визначив, що біткоїн як один із видів віртуальних активів є грошовим сурогатом, який не має забезпечення реальної вартості [130].

Тому 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 біткоїнів 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 [131].

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 набув чинності [157].

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 [296].

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, у тому числі гроші та цінні папери, інше майно, майнові права, результати робіт, послуги, результати інтелектуальної, творчої діяльності, інформація, а також інші матеріальні і 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 і що існує лише в інформаційному середовищі. Відповідно до другого варіанта, віртуальний актив виступає як грошова одиниця, яка хоч наразі де-юре такою не є, однак 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 напрямі пішла ще далі. У 2014 році швейцарським парламентом було ухвалено рішення, згідно з яким біткоїн варто розглядати як іноземну валюту [500].

Проаналізувавши ситуацію, можна зробити висновок: віртуальні активи однозначно є засобом платежу. Проте лише це не робить її справжніми грошима. Основні причини, через які не можна визнати віртуальні активи грошима, – це те, що вона емітується децентралізовано, і не існує суб'єкта, що забезпечує її платоспроможність [317].

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 [187].

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 одержує 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 [90].

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 виражене в грошових коштах, за які були придбані віртуальні активи. Тобто в разі неправомірного списання з рахунку власника віртуального активу без його відома їх певної кількості маємо не просто неправомірний доступ до цифрової інформації, що зберігається в інформаційно-телекомунікаційній технології або системи, а крадіжку у кіберпросторі. Власник гаманця віртуальних активів більше не зможе їх використовувати, оскільки просто не матиме до них доступу, особа, яка вчинила крадіжку, навпаки, зможе вільно здійснювати операції з вкраденими 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 вчинила кримінальне правопорушення, спрямовані саме на заволодіння чужим нематеріальним майном – віртуальним активом, який має свій грошовий еквівалент, а не просто є 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 дискуси щодо питання установлення 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 на інформаційно-телекомунікаційних технологіях, системах і мережах.

Водночас визначення шкоди в цьому разі буде лише суб'єктивним переконанням суду незалежно від оціночної вартості віртуальних активів. Змоделюємо ситуацію, за якої Особа 1 шляхом вивчення крадіжки обернула на свою користь 0,2 Bitcoin. На 10 березня 2023 року ціна такого віртуального активу сягла 20 000 доларів, тобто вартість викраденого віртуального активу становила 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 гаманець Особи 1.

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 все-таки 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. Розглянемо ситуацію, коли суд відповідно до частини 3 статті 185 Особливої частини Кримінального кодексу України назначає 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 виступають відносини власності, які фактично стають додатковим об'єктом.

У свою чергу основним об’єктом будуть виступати 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 виступати 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 із 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, представлена в цифровій формі.

Також виникають суперечки з авторськими й суміжними правами. Наприклад, якщо винний без відома власника завантажить програмне забезпечення, 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 і 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 так відносини у сфері нормального обороту цифрової інформації або авторські права, як відносини власності, оскільки 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 правоохоронні органи. Це пов’язано передусім із тим, що переважна більшість володільців віртуальних активів не знають про його реальний правовий статус, думаючи, що вони володіють чимось забороненим на зразок об’єктів, обмежених у цивільному обігу [3].

Ще одне кримінальне правопорушення, предметом якого часто є віртуальні активи, – шахрайство, яке 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 і 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: 1) цільовий фішинг, пов’язаний із перенаправленням цільових користувачів на фіктивні сайти, 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, а 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 всіляких 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 [301].

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, водночас переважно він використовує назву віртуального активу, який ще не вийшов у публічний доступ і має великі перспективи зросту та проводить стадію пошуку й залучення коштів від інвесторів. Найкращими платформами для створення свого віртуального активу є Binance Smart Chain та Uniswap [330; 507].

Третій етап полягає в усебічному рекламуванні в телеграм-каналі свого віртуального активу і створення більш довірливого ставлення до нього. Так шахрай може за допомогою різних програм робити вирізки з вебсайтів новин, ніби-то про колаборацію між начебто 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 [449; 331].

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 залучають до шахрайського капіталу саме віртуальні активи, а не фіатні гроші [289].

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 та транзакцій є можливість конвертації віртуальних активів в 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 [498].

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 і кількість факторів легалізації, скоєних з 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 [444].

До способів легалізації злочинних доходів за допомогою віртуальних активів належать: 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 кількістю 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 дозволяє 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 невілює інтерес із боку органів фінансового контролю та фінансового моніторингу зокрема; 2) швидкість проведення транзакцій. Обмін віртуальних активів на національну або зарубіжну валюту здійснюється менше ніж за годину; 3) велика кількість платіжних систем як в національній, так і в зарубіжній валюті [367].

P2P-обмін можна умовно поділити на здійснюваний в інтернет-середовищі та офлайн-середовищі. Транзакції P2P (від людини до людини) набули популярності 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, сьогодні в світі установлено більше тисячі таких пристроїв, а якщо взяти до уваги латентність даних, можна говорити і про цифри, більші в 30 разів. За комісію розміром 6 % сервіс забезпечує безперебійність перекладу й анонімність клієнта [332].

Останнім часом злочинці почали активно використовувати сайти азартних ігор для легалізації злочинних доходів, через що приблизно третина всіх «брудних» віртуальних активів легалізується саме таким способом. Зауважимо, що значною мірою це стає можливим завдяки ігровій валюті популярних віртуальних ігор, яка використовується як засіб зберігання

вартості цих активів. Придбану ігрову валюту злочинці зазвичай продають за криптовалюту, а вже потім обмінюють її на традиційну грошову валюту за допомогою спеціалізованих конвертаційних сервісів.

Сьогодні застосування азартних ігрових платформ для відмивання грошей стає все популярнішим, оскільки такі платформи пропонують особам, які вчиняють кримінальні правопорушення, відносно анонімний і доступний спосіб перетворення злочинних доходів у легальні активи. Все це створює серйозні виклики для регуляторів і правоохоронних органів, які прагнуть відстежувати та переривати такі фінансові потоки. Разом з тим проблема ускладнюється використанням криптовалют і спеціалізованих сервісів обміну, які можуть забезпечити додатковий рівень анонімності. Розвиток технологій і зростання популярності віртуальних ігор лише посилює необхідність розробки ефективних засобів виявлення та контролю за подібними схемами відмивання грошей.

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 виступає 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 в віртуальній валюті, підключення сервісів одночасної конвертації віртуальних валют AdvCash.

Отже особа, яка безпосередньо здійснює відмивання злочинних коштів, здійснює купівлю певного товару чи послуги 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 зростає і кількість суспільно небезпечних діянь, спрямованих на використання віртуальних активів як предмета або засобу вчинення кримінального правопорушення. Завдяки специфічним особливостям віртуального активу виникає багато запитань щодо кримінальної кваліфікації суспільно небезпечних діянь, спрямованих на їх протиправне заволодіння, зокрема шахрайства й крадіжок. Визначення віртуального активу як цифрової інформації у формі комп'ютерних даних обумовлює виключення його з кола предмета таких протиправних діянь, як крадіжка або шахрайство. Проте сама сфера суспільних відносин, яким заподіюється шкода, незважаючи на традиційність матеріальності предмета, виступають відносини власності. Класифікація цифрових інформаційних продуктів до предмета крадіжки й шахрайства є адекватною та вчасною реакцією на інформаційно-телекомунікаційний розвиток суспільства. Водночас цифровий інформаційний продукт пропонуємо визначити, як сукупність унікальних інформаційно-телекомунікаційних даних, об'єднаних у матеріальний чи віртуальний носій, що мають усі ознаки товару, власну вартість і належать на праві власності іншій особі.

Легалізацію злочинних доходів варто охарактеризувати як багатоетапний процес, основна мета якого – за допомогою низки фінансових операцій надати правомірності володіння незаконно отриманим доходом. Для досягнення цієї мети використовують різні засоби й способи, покликані спотворювати справжню інформацію про джерело отримання грошових

коштів.

Одним із порівняно нових способів вчинення легалізації злочинних доходів, що набуває все більшої популярності, є вчинення цього діяння за допомогою віртуальних активів. До способів легалізації злочинних доходів за допомогою віртуальних активів належать: 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 в 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 серед проблем, що характеризують сучасний стан розвитку кримінальної юстиції в Україні. Для того щоб визначити, що варто розуміти під загальними засадами призначення покарання, потрібно дійти висновку, що таке призначення покарання загалом [137, с. 116].

Призначення покарання – це діяльність суду з вибору виду й розміру покарання за вчинене особою кримінальне правопорушення. Саме від призначення покарання буде залежати 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 недостатньо розкриває сутність та особливості призначення покарання [237, с. 10].

А. Музика дотримується 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 [142, 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 [166, 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 й 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) враховуючи ступінь тяжкості вчиненого кримінального правопорушення, особу винного та обставини, що пом'якшують чи обтяжують покарання.

Призначення покарання судом є ключовим етапом у застосуванні норм кримінального права, який перш за все полягає у визначенні і закріпленні у вироку конкретної міри покарання за здійснене кримінальне правопорушення. Важливо зазначити, що процес призначення покарання завжди базується на чітких законодавчих засадах, встановлених

Кримінальним кодексом України, які визначають обов'язковий порядок дій для суду при виборі покарання.

Варто наголосити, що система призначення покарань в Україні структурована таким чином, що судовий вирок має бути обґрунтованим і справедливим, відповідаючи стандартам, які визначені у Конституції України та Кримінальному кодексі України. Цей процес не просто механічний вибір міри покарання, а обдумане рішення, що враховує багато факторів, включно з тяжкістю злочину, особливостями особи, що скоїла правопорушення, та метою кримінального покарання, яка полягає не тільки у покаранні, а й у попередженні нових кримінальних правопорушень.

Згідно з поглядами А. Васильєва та О. Пироженка, ступінь суспільної небезпеки кримінального правопорушення є основним фактором, який впливає на визначення суворості кримінальної відповідальності. Це відповідає принципу справедливості, що передбачає пропорційність покарання тяжкості злочину. Таким чином, чим серйознішим є правопорушення, тим суворішим повинно бути покарання для забезпечення належного правового порядку і профілактики злочинності. Водночас, на думку Т. Денисової, ефективність покарання залежить передусім від того, наскільки правильно і справедливо призначено покарання і наскільки воно відповідає тяжкості вчиненого злочину. Це означає, що суди повинні ретельно аналізувати всі обставини справи, враховувати ступінь вини та суспільної небезпеки діяння, щоб призначене покарання було не тільки справедливим, але й ефективним у контексті попередження нових правопорушень [15, с. 176; 33, с. 80; 64, с. 260].

Не можемо не погодитися, що принципи визначення покарання, які наведені Васильєвим, Пироженком та Денисовою, відіграють критичну роль у правосудді. Вони наголошують на важливості врахування тяжкості злочину та потенційної шкоди суспільству як детермінантів для визначення масштабу покарання. Справедливе та адекватне покарання не тільки забезпечує моральне задоволення в суспільстві, але й сприяє реабілітації особи, що

вчинила кримінальне правопорушення, запобігаючи його повторенню.

Аналізуючи будь-яку норму Особливої частини Кримінального кодексу України та її взаємозв'язок з нормами Загальної частини, варто зосередитись на санкціях цих статей. Санкція, як одна з основних засад призначення покарання, є визначальним фактором у виборі виду та розміру покарання, що може встановлювати суд. Однак розуміння та застосування санкцій є складним завданням через те, що багато статей Особливої частини включають альтернативні дії з альтернативними покараннями, і не містять чітких критеріїв для вибору конкретного виду покарання залежно від дії.

У теорії кримінального права є декілька видів санкцій, зокрема відносно визначені, абсолютно визначені, альтернативні, відсилочні й неконкретизовані. Зауважимо, що в Кримінальному кодексі України використовуються лише відносно визначені та альтернативні санкції [15, с. 235].

Санкції, що передбачені у статтях Особливої частини Кримінального кодексу, відіграють критичну роль у процесі судового рішення, що не лише обмежує суд у виборі покарання, але й вимагає від нього зважувати на складність кожного конкретного випадку, оцінюючи альтернативні дії та відповідні їм покарання. Відсутність чітких критеріїв для вибору між альтернативними видами покарань, на нашу думку, ускладнить роботу суду, але також забезпечує необхідний простір для судової дискреції, що є важливим для адаптації правосуддя до конкретних обставин кожного випадку.

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 видів покарання, з яких суд обирає лише одне [27].

Пропонуємо в розрізі таблиці розглянути види санкцій за вчинення кіберзалежних кримінальних правопорушень.

Таблиця 3 – Види покарання та санкцій за кіберзалежні кримінальні правопорушення

Санкція частини статті	**Вид покарання**
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 обмеження волі на строк до трьох років.
Частина 2 статті 361 Особливої частини Кримінального кодексу України	Штраф від трьох тисяч до семи тисяч неоподатковуваних мінімумів доходів громадян або обмеження волі на строк від двох до п’яти років, або позбавлення волі на той самий строк.
Частина 3 статті 361 Особливої частини Кримінального кодексу України	Штраф від семи тисяч до десяти тисяч неоподатковуваних мінімумів доходів громадян або позбавлення волі на строк від трьох до восьми років з 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 з 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 з 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	

Санкція частини статті	**Вид покарання**
Частина 1 статті 361-1 Особливої частини Кримінального кодексу України	Штраф від двох тисяч до чотирьох тисяч неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років, або позбавлення 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 тисяч до чотирьох тисяч неоподатковуваних мінімумів доходів громадян або позбавлення волі на строк до двох років.
Частина 2 статті 361-2 Особливої частини Кримінального кодексу України	Позбавлення волі на строк від двох до п’яти років.
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 виправні роботи на строк до двох років.
Частина 2 статті	Позбавлення волі на строк до трьох років з

Санкція частини статті	Вид покарання
362 Особливої частини Кримінального кодексу України	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 з 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	
Стаття 363 Особливої частини Кримінального кодексу України	Штраф від двох тисяч до чотирьох тисяч неоподатковуваних мінімумів доходів громадян або обмеження волі на строк до трьох років з 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 тисяч до чотирьох тисяч неоподатковуваних мінімумів доходів громадян або обмеження 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 позбавлення волі на той самий строк з позбавленням права обіймати певні посади або займатися певною діяльністю на строк до трьох

Санкція частини статті	Вид покарання
	років.

Проаналізувавши систему покарань за вчинення кримінальних правопорушень, які передбачені XVI розділом Особливої частини Кримінального кодексу України, можемо констатувати факт, що основними видами покарання є штраф, обмеження волі 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 XVI розділом Особливої частини Кримінального кодексу України. На рисунку 10 зображено, які кримінальні правопорушення вчинялися найчастіше. На рисунку 11 висвітлено які види покарання були застосовані до осіб, що вчинили кримінальне правопорушення.

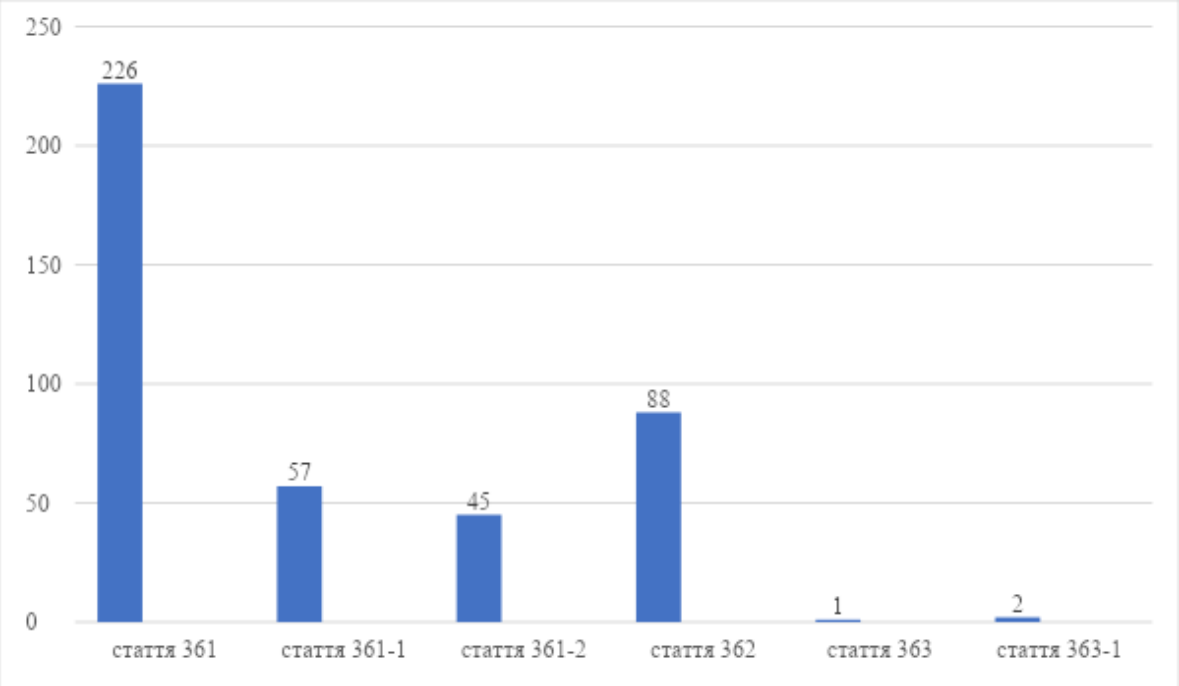


Рисунок 10 – Динаміка вчинення кримінальних правопорушень, передбачених VXI розділом Особливої частини Кримінального кодексу України за період із 01.01.2015 р. по 01.01.2023 р.

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 розглядуваних справ було призначено покарання у вигляді штрафу й у 61 % у вигляді позбавлення волі. Водночас у 98 % осіб, які вчинили кримінальне правопорушення за відповідними статтями Особливої частини Кримінального кодексу України, і яким було призначене 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 висвітлено, які покарання було призначено судом у розрізі статей Розділу XVI Особливої частини Кримінального кодексу України.

Рисунок 11 – Вид призначеного покарання за кримінальні правопорушення, передбачені XVI розділом Особливої частини Кримінального кодексу України

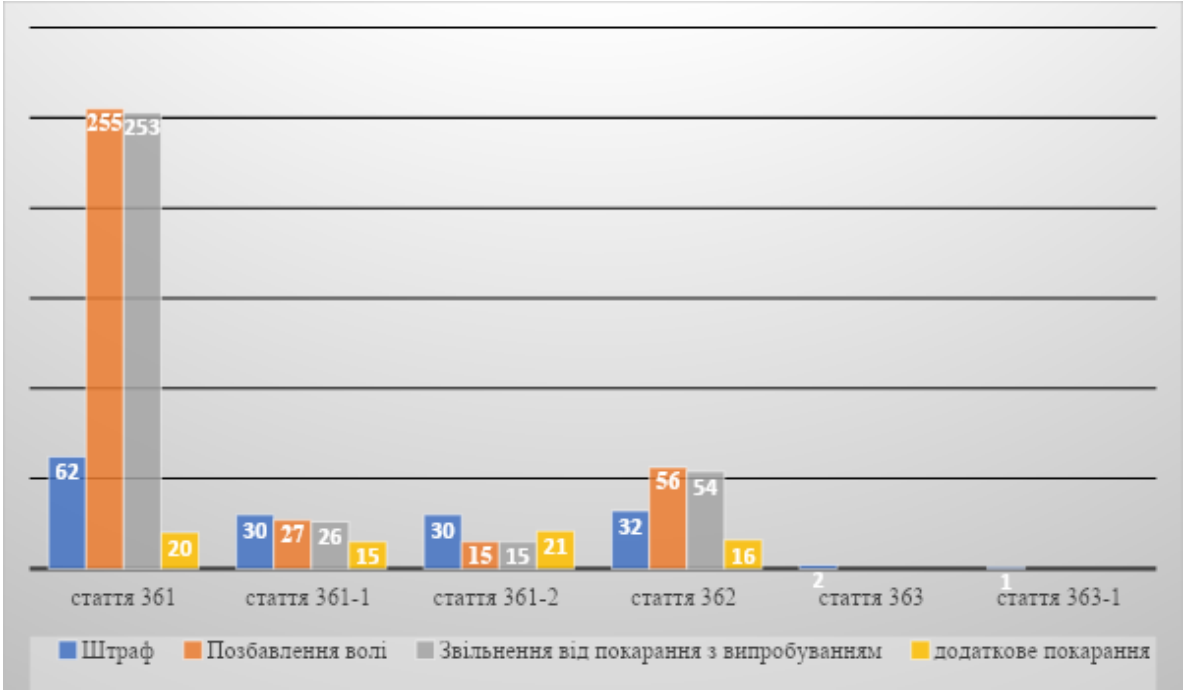


Рисунок 12 – Вид призначеного покарання за кримінальні правопорушення, передбачені VXI розділом Особливої частини Кримінального кодексу України

Перше покарання, яке 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 з-поміж інших кримінальних правопорушень, передбачених XVI розділом Особливої частини Кримінального кодексу України. На нашу думку, це зумовлено насамперед унікальністю цього виду покарання, та його застосування, як основного та додаткового виду покарання.

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 розмірі, установлених в Особливій частині Кримінального кодексу України, з урахуванням положень частини другої статті статті 53 Загальної

частини Кримінального кодексу України.

Стосовно 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, відповідно до якого за рішенням суду із засудженого стягується певна визначена грошова сума в дохід держави [305, с. 411].

Важливим аспектом у визначенні штрафу, запропонованому В. Попрасом, є акцент на його примусовий характер. Штраф застосовується від імені держави за вироком суду, що підкреслює його офіційну природу та роль у системі кримінальної юстиції. Це відповідає загальним принципам покарання, яке призначається судом як реакція на вчинене кримінальне правопорушення [177, с. 144].

Влучне, на наше переконання, 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 [248, с. 170].

А. Попович виділяє такі ознаки штрафу: 1) це захід державного примусу; 2) застосовується винятково державними органами, а саме судом; 2) полягає в обов’язковому грошовому стягненні з особи засудженого;
4) застосовується лише до особи, яка була визнана винною у вчиненні кримінального правопорушення; 5) полягає в обов’язковому обмеженні права власності особи на певну суму грошових коштів [176, с. 142].

Зауважимо, що розмір штрафу визначається судом, залежить від тяжкості вчиненого кримінального правопорушення та з урахуванням 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 небезпечними наслідками. 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 отриманий унаслідок вчинення кримінального правопорушення доходу. Водночас немає різниці, який граничний розмір штрафу, передбачений 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» мінімальна й гранична межа покарання у вигляді штрафу за вчинення кримінального правопорушення, передбаченого частиною першою статті 361 Особливої частини Кримінального кодексу України, була визначена в межах від однієї тисячі до трьох тисяч неоподатковуваних мінімумів доходів громадян та альтернативне покарання у вигляді обмеження волі строком на три роки [189].

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 XVI розділом Особливої частини Кримінального кодексу України.

Друге місце серед застосовуваних покарань за кримінальні правопорушення, передбачені XVI розділом 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 [123, с. 111].

Проблема призначення покарання у вигляді позбавлення волі за кримінальні правопорушення, передбачені XVI розділом Особливої частини Кримінального кодексу України, полягає в їх специфічних особливостях і складності визначення шкоди, завданої такими суспільно небезпечними діянями. Згідно із статистикою з 1 січня 2015 року по 1 січня 2023 року покарання у вигляді позбавлення волі було призначене у
255 випадках, тобто фактично 61 відсоток 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 установлено 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 установлено звільнити Особу 1 від відбування покарання з випробуванням та призначити їй іспитовий строк тривалістю 1 рік [231].

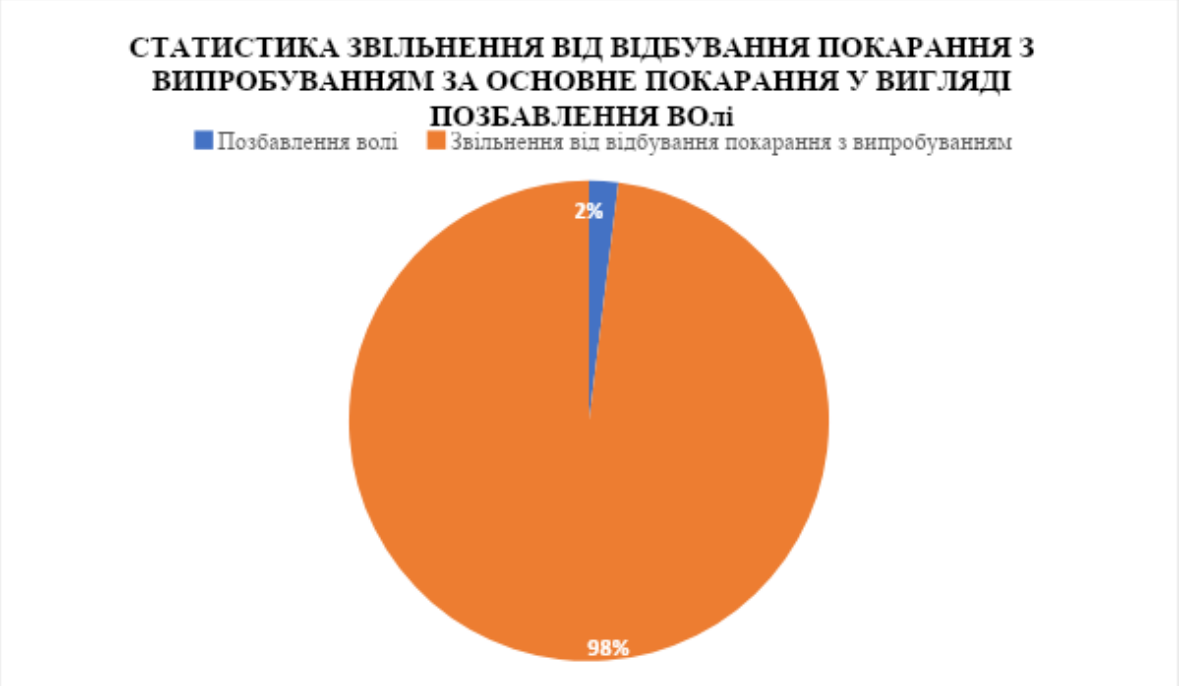


Рисунок 15 – Статистика звільнення від відбування покарання з випробуванням за основне покарання у вигляді позбавлення волі.

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, які передбачені XVI розділом Особливої частини Кримінального кодексу України, варто брати до уваги, що такі суспільно небезпечні діяння завжди вчиняються з використанням інформаційно-телекомунікаційних технологій, представлених у формі цифрових пристроїв. Зважаючи на це, 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 частини 1 та 2 статті 361 Особливої частини Кримінального кодексу України було виключено норму, що визначала конфіскацію майна як додаткове покарання [188].

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, частина 2 статті 59 Загальної частини Кримінального кодексу України встановлює, що 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 і може бути призначена лише у випадках, спеціально передбачених в Особливій частині Кримінального кодексу України [121].

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 або винагороди за його вчинення; 3) були предметом кримінального правопорушення, крім тих, що повертаються власникові, а якщо його не установлено, то 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 [121].

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 XVI розділом 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 [229]	комунікаційних систем, електронних комунікаційних мереж) та частини 1, 2 статі 361-1 (Створення з метою протиправного використання,	Системний блок персонального комп`ютера в корпусі Logic Power; роутер марки tp-linc,	Конфіскація в дохід держави

Номер судової справи	Вчинене кримінальне правопорушення	Речові докази по справі	Рішення щодо долі доказів
	розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут)	мобільний телефон марки Iphone IMEI НОМЕР_3 з сім-карткою оператора зв`язку Київстар № Н	
	Особливої частини Кримінального кодексу України.	НОМЕР_4 ; ноутбук марки Asus серійний номер J7NOCVOT765F з зарядним пристроєм; ноутбук марки Samung серійний номер J9M791ND200008R з зарядним пристроєм; три носії інформації Maxell, San Disk, TAB	
Справа № 161/18959/20 [227]	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 [223]	Стаття 361-1 (Створення з метою протиправного використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут)	Ноутбук MSI s/n K1607N0061779	Повернути особі, заздалегідь знищивши шкідливі програми на жорсткому диску шляхом його форматування тощо

Номер судової справи	Вчинене кримінальне правопорушення	Речові докази по справі	Рішення щодо долі доказів
	Особливої частини Кримінального кодексу України.		

Зауважимо, що в першому та другому випадках судом було призначено покарання у вигляді позбавлення волі строком на 2 роки, у третьому випадку – покарання у вигляді 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 встановлене 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 XVI розділом Особливої частини Кримінального кодексу України, можливість запровадження судами ухвали про спеціальну конфіскацію знаряддя вчинення за кримінальні правопорушення, що вчиняються повторно, в співучасті або спрямовані на інформаційно-телекомунікаційні технології, системи та мережі держави, є цілком обумовленою [228].

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 XVI розділом Особливої частини Кримінального кодексу України, хочемо розглянути основні проблеми під час їх призначення.

Зауважимо, що ми є прихильниками застосування штрафу як основного виду покарання за більшість кримінальних правопорушень, передбачених XVI розділом Особливої частини Кримінального кодексу України, крім тих, які спричинили тяжкі наслідки, були вчинені повторно, або такі, що 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 перш за все самою специфікою кримінальних правопорушень у кіберпросторі.

Першим фактором, який 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 здійснення віддалено несанкціонованого втручання в інформаційно-телекомунікаційну мережу, особі, яка вчиняє кримінальне правопорушення, передусім необхідно одержати дані для доступу до такої системи. Такий доступ особа, яка вчиняє кримінальне правопорушення, може отримати шляхом використання шкідливого програмного забезпечення і його

фактичної інсталяції на цифровий пристрій жертви з подальшим отриманням всіх цифрових файлів, що зберігаються на такому пристрої [266]. Як результат, маємо ситуацію, коли особа фактично вчинила суспільно небезпечне діяння, передбачене статтею 361-1 Особливої частини Кримінального кодексу України, яке фактично буде визначатися як підготовче з подальшим одержанням несанкціонованого доступу, і як результат – втручання в роботу інформаційно-телекомунікаційної мережі, тобто діяння, яке передбачене 361 статтею 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 внаслідок поглинання менш суворого покарання більш суворим буде призначене покарання у вигляді штрафу від 2000 неоподатковуваних мінімумів доходів громадян. Отже, на нашу думку, посягання на первісний об’єкт втрачає свою змістовність.

На рисунку 16 ми навели статистику, які кримінальні правопорушення, передбачені XVI розділом Особливої частини Кримінального кодексу України, найчастіше вчиняються в сукупності з іншими кримінальними правопорушеннями інших розділів Особливої частини Кримінального кодексу України.

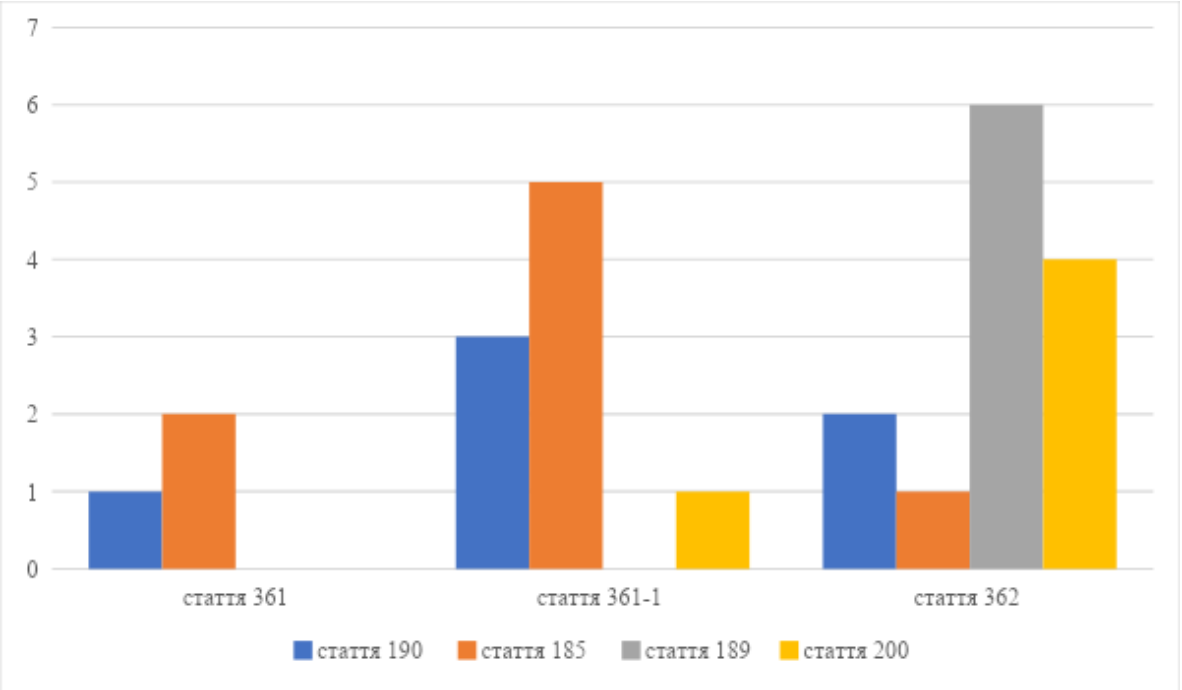


Рисунок 16 – Правопорушення, передбачені XVI розділом Особливої частини Кримінального кодексу України, що найчастіше вчиняються в сукупності з іншими суспільно небезпечними діяннями, передбаченими іншими розділами Особливої частини Кримінального кодексу України

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 поглинання менш суворих покарань більш суворими, остаточне покарання визначалося саме за суспільно небезпечні діяння, передбачені XVI розділом Особливої частини Кримінального кодексу України. Це лише підтверджує нагальність запропонованих нами змін у відповідні статті Особливої частини Кримінального кодексу України [221; 218; 220; 232; 42; 230].

Ще одним фактором є 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 30 % осіб, які вчиняють кримінальні правопорушення, передбачені XVI розділом Особливої частини Кримінального кодексу України, є віком від 15 до 18 років [172].

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 станом на 2020 рік працювало близько 600 тисяч дітей віком від 16 до 18 років, тобто 28 % з-поміж усіх дітей цього віку [68].

Незважаючи на закріплення в Законі України «Про вищу освіту» норми щодо індивідуального плану навчання, переважна більшість закладів вищої освіти не дозволяє його оформлювати як студентам перших та других курсів, так і студентам технікумів та коледжів [184].

Ураховуючи це, можемо стверджувати про відсутність у неповнолітньої особи самостійного доходу. І як результат – застосування штрафу як основного виду покарання за кримінальні правопорушення, передбачені XVI розділом Особливої частини Кримінального кодексу України. У 2020 році згідно зі статистикою Генеральної прокуратури України було обліковано 2 498 кримінальних правопорушень передбачених XVI розділом Особливої частини Кримінального кодексу України,
1 675 особам вручено підозру (з них 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 [79].

Підсумовуючи вищевикладене, хочемо наголосити, що незважаючи на доволі розгалужену систему покарань, які призначаються судом за вчинення кримінальних правопорушень, передбачених XVI розділом Особливої частини Кримінального кодексу України, найбільш поширеними виступають

позбавлення волі на певний строк та штраф. На нашу думку, у зв’язку із застосуванням судами норми статті 75 Загальної частини Кримінального кодексу України, звільнення від покарання з випробуванням, повністю навіюються самі засади призначення покарання. Особливості вчинення кримінальних правопорушень у кіберпросторі, зокрема сукупності різних суспільно небезпечних діянь, які спрямовані на досягнення одного злочинного результату, не дозволяють застосувати штраф, як основне покарання у більшості випадків, де це є нагальним та обумовленим. Визначення ступеня тяжкості вчиненого кримінального правопорушення та призначення справедливого та достатнього покарання за нього, є певним каталізатором впровадження певних єдиних уніфікованих правил, якими б керувалися судді при призначенні 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 визначають 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 і поваги до держави та суду [271].

У сучасному світі інформаційно-телекомунікаційні технології, системи й мережі є необхідною складовою життєдіяльності держави та суспільства. Зростання її ролі призвело до збільшення кількості кримінальних правопорушень у кіберпросторі. Зважуючи 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 [121].

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 це, 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 [97; 174].

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 в 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 одразу 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 характеризуванні таких елементів вчинення кримінального правопорушення, зокрема: 1) електронних слідів (виявлення проміжків часу, упродовж яких було здійснено певні дії, що могли вчинятися лише із залученням кількох осіб); 2) зв'язків (дослідження соціальних мереж, електронної пошти, будь-яких інших повідомлень, що свідчать про взаємозв'язок між кількома підозрюваними особами); 3) стилю дій злочинця. Аналіз стилю дій вчинення кримінального правопорушення в кіберпросторі дає змогу дізнатися, наприклад, скільки осіб були причетні до кримінального правопорушення, зазвичай кожна особа має індивідуальний підхід до написання коду або порядку вчинення окремих дій; 4) фізичних доказів (у результаті аналізу аудіо-, відеозаписів показаня свідків дозволить виявити чи був злочин вчинений 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 на 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: 1) виманювання даних платіжних карток та інших банківських реквізитів із метою їх подальшого використання й викрадення з них коштів; 2) 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 із 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 застосовують 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 оціночних 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 [122, 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, що вчинюються загальнонебезпечним способом, можуть призвести до значної шкоди для громадської й національної безпеки, економіки та інших аспектів життя. Прикладами зазначених кримінальних правопорушень є:

– розповсюдження вірусів, шкідливих програм, що можуть призвести до вимкнення важливих систем, таких як лікарні, 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, що контролює рух повітряних суден, 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 [122, с. 454].

Ця обставина є неабияк актуальною в умовах сьогодення. Україна вже більше року перебуває в умовах воєнного стану. Наразі відбуваються безліч зборів на допомогу Збройним Силам України, Територіальній обороні та іншим підрозділам, задіяними 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 хочуть 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: 1) кібершпигунство, коли 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; 2) кібертероризм, коли злочинець використовує інформаційно-телекомунікаційні технології, системи і мережі для завдання шкоди цивільній, військовій інфраструктурі або іншим системам, що можуть бути важливими для безпеки країни та населення; 3) кібератаки, застосовувані за допомогою інформаційно-телекомунікаційних технологій, систем і мереж задля заподіяння 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 завдати значних проблем для зв'язку військових підрозділів та органів управління; 4) розповсюдження дезінформації або фейків шляхом використання соціальних мереж, медіа- та інтернет-ресурсів для поширення неправдивої інформації, що може підривати національну безпеку, підірвати єдність і спокій нації тощо. В умовах воєнного або надзвичайного стану такі види злочинів можуть бути особливо небезпечними, оскільки злочинці можуть використовувати дезінформацію, щоб спричинити паніку серед населення або змусити владу ухвалити некоректні рішення.

Обставини, які суд залежно від характеру вчиненого кримінального правопорушення вправі не визнати такими, що обтяжують покарання.

1. Вчинення злочину особою повторно та рецидив злочинів. Ця обставина буде застосована, якщо особа, яка вчиняє кримінальне правопорушення, вже скоювала подібні кримінальні правопорушення в кіберпросторі або регулярно вчиняє такі правопорушення. Варто наголосити, що кіберпростору та вчинення суспільно небезпечних діянь у ньому, пролонгує повторність такого вчинення. Наприклад, застосування вірусів або інших шкідливих програм на вебсайтах, вчинення DDoS-атак тощо).

2. Вчинення кримінального правопорушення на ґрунті расової, національної, релігійної ворожнечі чи розбрату або на ґрунті статевої приналежності. Ця обставина застосовується у разі виявлення ознак:

- кібербулінгу, або систематичного приниження, залякування людей через Інтернет, на підставі їх раси, національності, релігії, гендерної приналежності або орієнтації [59];
- нелегального доступу до комп'ютерних систем, що може бути спрямована 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, унеможливлення доступу до цих сайтів або завдання іншої шкоди, наприклад, у вигляді репутаційних наслідків;
- онлайн-шахрайства, де 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, коли злочинці одержують доступ до інформації, зібраною 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 до призупинення функціонування установи або організації, порушення їх законної діяльності;
- розповсюдження шкідливих програм, вірусів для одержання доступу до систем, що належать установі або організації, в якій працює потерпілий, що спричинить порушення конфіденційної інформації та роботи системи;
- атак на вебсайти та інші ресурси, які можуть спричинити відмову їх обслуговування ресурсу 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 і обсяг якого залежать від особливостей конкретної справи, і тому щоразу встановлюється судом з урахуванням усіх її обставин. При віднесенні

наслідків до тяжких слід ураховувати важливість (соціальну цінність) тих суспільних відносин, яким злочином заподіюється шкода, а також ступінь заподіяння цієї шкоди, яка залежить від характеру (змісту) і розміру (обсягу) спричинених наслідків [149].

До тяжких наслідків здебільшого належать загибель людей, заподіяння тяжкої шкоди здоров'ю людини, великий матеріальний збиток, порушення основних конституційних прав і свобод людини, дезорганізація діяльності органів державної влади й місцевого самоврядування, перешкоджання роботі підприємств, установ та організацій тощо. Серед загальновідомих прикладів варто виділити:

- 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 встановлення необхідних оновлень. Потерпілі компанії зазнали великих збитків і протягом тривалого часу відновлювали свої системи [45].
- атаку Equifax. У 2017 році Equifax, одне з найбільших кредитних бюро в США, було атаковане хакерами, що призвело до крадіжки понад 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 [395].
- атаку на Sony Pictures. У 2014 році хакери, яких пов'язують з КНДР, атакували Sony Pictures і зламали їх системи, що призвело до крадіжки більше ніж 100 терабайт конфіденційної інформації, зокрема електронних листів, фільмів та іншої приватної інформації. Ця атака викликала міжнародний скандал і вплинула на відносини між США та КНДР [480].
- атаки на інфраструктуру України. У 2015–2017 роках та 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 та газу на тривалий час, що істотно ускладнило їх повсякденне життя [264; 95; 316].

- 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 погіршували стан пандемії й завдали шкоди лікарням, що вже працювали в напруженому режимі [282; 163].
- 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 та ін., закликаючи до відправки криптовалюти в шахрайський електронний гаманець. Ця атака призвела до викрадення електронних адрес понад 200 млн користувачів Twitter, втрати великої кількості коштів та порушення довіри до соціальної мережі [502; 278].

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 ця обставина є цілком можливою, наприклад, коли 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 наступним вимаганням грошових коштів за її неоприлюднення.

6. Вчинення кримінального правопорушення щодо особи, яка перебуває в матеріальній, службовій чи іншій залежності від винного. Обставина, коли особа, що вчиняє кримінальне правопорушення, експлуатує залежне

становище своєї жертви для вчинення суспільно небезпечного діяння, значно обтяжує покарання. Таке становище дозволяє винному маніпулювати ситуацією, оскільки жертва, знаходячись у залежності від агресора, або втрачає здатність уникнути нападу, або значно обмежена у можливостях чинити ефективний опір. Ця динаміка не тільки збільшує вразливість потерпілого, але й підвищує суспільну небезпеку самого акту, що вимагає від правосуддя застосування більш суворих заходів реагування. Прикладами подібних правопорушень можуть бути:

- шантаж у кіберпросторі, тобто вимагання коштів, послуг або інформації від особи, яка перебуває в службовій залежності від них;
- 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 або мобільного телефона особи, яка перебуває в залежності від них, що порушує недоторканність приватного життя особи;
- «кібернасильство», що полягає в завданні шкоди за допомогою електронних форм спілкування і 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, який був викликаний 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 [121].

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 все більшого застосування інформаційних технологій та 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 та інформаційна інфраструктура держави відіграють надзвичайно важливу роль у забезпеченні кібербезпеки держави. Вони забезпечують захист державних інформаційних ресурсів від зламів та 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 та 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 покращення захисту такої інформації.

Проте зберігання державної таємниці також може стати об’єктом кіберзагроз, тим паче, 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 різноманітні і залежать від того, як саме їх використовують. Ось декілька прикладів таких кримінальних правопорушень:

- 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 зберігається в них;
- 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 за потрібне доповнити частину 1 статті 67 Кримінального кодексу України пунктом 14: «вчинення кримінального правопорушення, об'єктом якого є державний комп'ютер (державної інфраструктури) 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 пріоритетним елементами в забезпеченні кібербезпеки держави та захисті її інформаційних ресурсів. Вони допомагають виявляти та 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 та призвести 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, які визначені в частині 1 статті 67 Загальної частини Кримінального кодексу України, можуть бути застосовані до суспільно небезпечних діянь, які вчиняються в кіберпросторі. Серед основних обставин, що обтяжують кримінальне покарання, ми виділили: 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 на недоумство, має вади розумового розвитку, а також вчинення кримінального правопорушення щодо малолітньої дитини або у присутності дитини. Водночас, на наше переконання, необхідно доповнити систему обставин, що обтяжують кримінальне покарання, з урахуванням інформаційно-телекомунікаційного буму з однієї сторони й збройної агресії Російської Федерації та умов гібридної війни з іншої, 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.

Висновки до розділу 3

1. Визначено та надано характеристику основним ознакам віртуальних активів: 1) децентралізованість; 2) транснаціональність; 3) конфіденційність операцій; 4) цифровізація; 5) майновий характер; 6) анонімність. Акцентовано увагу на співвідношенні понять «віртуальний актив» та «криптовалюта», доведено неідентичність зазначених понять.

2. Надано визначення «віртуальний актив» як цифрову валюту (віртуальну, без фізичної форми), створення і контроль за якою базується на

криптографічних методах, щодо якої встановлена повна децентралізація, що гарантує коректність операцій в системі, в тому числі відсутності можливості впливати на транзакції учасників криптосистеми.

3. Узагальнено та систематизовано зарубіжний досвід правового регулювання віртуальних активів. На основі розглянутого досвіду та визначеної специфіки віртуальних активів наголошено, що віртуальні активи варто розглядати у трьох аспектах: 1) інформацію; 2) валюту; 3) інше нематеріальне благо.

4. Наголошено, що сьогодні віртуальні активи як предмет кримінального правопорушення за законодавством України можуть виступати лише як елемент цифрової інформації. Водночас пропонується розширити предмет крадіжки, включивши до нього цифровий інформаційний продукт, тобто сукупність унікальних інформаційно-телекомунікаційних даних, об'єднаних у матеріальний чи віртуальний носії, які мають ознаки товару, власну вартість і належать на праві власності іншій особі.

5. На основі аналізу статистичних даних було встановлено: в період з 01.01.2015 р. по 01.01.2022 р. винесено лише 420 судових рішень у формі вироків за вчинення кримінальних правопорушень, які передбачені XVI розділом Особливої частини Кримінального кодексу України, а найбільш вчинюваним кримінальним правопорушенням є несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж, яке передбачене 361 статтею Особливої частини Кримінального кодексу України і займає 64 % від загальної кількості судових рішень у формі вироків за суспільно небезпечні діяння, регламентовані XVI розділом Особливої частини Кримінального кодексу України.

6. Акцентовано увагу на тому, що кіберзалежні кримінальні правопорушення характеризуються вчиненням декількох суспільно небезпечних діянь, які передбачені Особливою частиною Кримінального кодексу України для досягнення одного злочинного результату, та власне

призначення покарання за сукупністю кримінальних правопорушень.

7. Визначені та проаналізовані основні обставини, що обтяжують покарання за кримінальні правопорушення у кіберпросторі з врахуванням специфічних особливостей вчинення таких суспільно небезпечних діянь.

8. Наголошено на необхідності введення додаткової обставини, що обтяжує кримінальні правопорушення у кіберпросторі: 1) заподіяння шкоди інформаційно-телекомунікаційній технології, системи або мережі державного значення, яке має ознаки критичної інфраструктури;

2) предметом кримінального правопорушення виступає 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 стосовно регулювання відносин в 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 врахування 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 у кіберпросторі поширюються норми міжнародного права [84, 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 [109].

Основні принципи міжнародного права закріплені відразу в декількох документах, зокрема мова йде про: 1) Статут Організації Об’єднаних Націй

[252]; 2) Підсумковий акт Організації з безпеки і співробітництва в Європі [63]; 3) Декларація про міжнародні принципи відповідно до статуту Організації Об'єднаних Націй [85].

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

Пропонуємо розглянути зазначені принципи в розрізі їх реалізації в кібернетичному просторі [369].

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 ст. 2 Статуту ООН: «Організацію засновано на принципі суверенної рівності всіх її членів» [47; 252].

Характеризуючи принцип суверенної рівності держав в 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 усіма країнами–членами світового товариства, а не кожною країною окремо. З огляду на цю концепцію роль окремої держави щодо регулювання відносин у кіберпросторі фактично невілюється. 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 у цій сфері. На нашу думку, створення єдиної уніфікованої нормативної бази щодо міжнародного регулювання питань, пов'язаних із кібернетичним простором з подальшою імплементацією в законодавства держав–ратифікантів, повинно стати пріоритетним завданням міжнародної спільноти цього десятиліття [250].

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) забезпечення національної безпеки держави від кіберзагроз [385].

Через неможливість застосувати зброю в кіберпросторі в класичному її 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 кібератаки, 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 та інше в розвинених країнах світу керуються та 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 сектори національної оборони нашої держави, урядовий і фінансовий сектор. Крім того, не можемо не звернути увагу на кібератаки з боку Російської Федерації на пострадянські країни, зокрема Литву, Латвію, Молдову, Естонію [43; 77].

Хочемо зауважити, що незважаючи на закріплення в законодавствах більшості держав стратегії кібербезпеки та установлення 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 з боку інших держав або окремих осіб за сприяння конкретних держав.

Тож 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 [315].

Наступним принципом, який ми хочемо охарактеризувати в розрізі кіберпростору, є принцип співробітництва держав. Оскільки переважна більшість питань, пов'язаних із діяльністю в кіберпросторі, є неврегульованою, принцип співробітництва держав набуває основоположного значення. На наше переконання, 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 [374].

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 [261].

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 втручанням. Це може проявлятися в перехопленні конфіденційної інформації шляхом розміщення серверу передавання такої цифрової інформації на території країни, яка 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, закріплених 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 [397].

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 і 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 кіберпросторі 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, який би ми хотіли охарактеризувати, – принцип поважання прав людини та 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 на його честь і репутацію. Кожна людина має право на захист закону від такого втручання або таких посягань [81].

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, тим самим порушуючи цей 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 наголосити, що більшість із них має 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 та 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 [32].

Проаналізувавши загальні й спеціальні міжнародно-правові принципи використання кіберпростору, хочемо проаналізувати основні міжнародні нормативні акти, що визначають правове регулювання кримінальних правопорушень у кіберпросторі.

Історично першим нормативним актом, присвяченим питанням регулювання кримінальних правопорушень у кіберпросторі, була Рекомендація № R 89 (9) Комітету Міністрів країн-членів Ради Європи «Про злочини, пов’язані з комп’ютерами» від 13 вересня 1989 року [345].

Відповідно до цього документа державам-членам Ради Європи під час розроблення національного законодавства щодо установлення 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 [497].

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 [309, 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. Заподіяння шкоди комп'ютерним даним або програми, тобто незаконне видалення, заподіяння шкоди, або погіршення якості даних чи програм комп'ютера [375, 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 [386].

6. Несанкціоноване відтворення комп'ютерної програми, охоронюваної

авторським правом. Під ним розуміється досконале неправомірне поширення, відтворення або передавання в громадське користування комп'ютерною програмою, що охороняється законом [459, с. 17].

7. Комп'ютерна фальсифікація, тобто введення, зміна або видалення даних (програм) комп'ютера або інше втручання у 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 [476].

8. Несанкціоноване відтворення мікросхеми, тобто досконале неправомірне відтворення мікросхеми виробу на напівпровідниках, якщо вона охороняється законом, або неправомірне використання або 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» включає такі склади кримінально-протиправних діянь: 1) неправомірна зміна 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 [388].

Несанкціоноване використання комп'ютерної програми – незаконні та неправомірні дії щодо використання охоронюваної законом комп'ютерної програми охороняється законодавством: неправомірне використання охоронюваної, вчинені з метою отримання незаконного прибутку для зловмисника чи третіх осіб, чи з метою заподіяння правовласнику шкоди

[419].

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 користувачу комп'ютерної системи; 3) будь-якою особою з фактичним заподіянням шкоди комп'ютерній системі загалом [450].

Варто зауважити, що Рада Європи розробила низку інструментів для гармонізації законодавства у сфері кримінальних правопорушень у кіберпросторі, і незважаючи на 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 небезпечності. Зокрема мова йде про такі кримінальні правопорушення, як фальсифікація цифрових даних та 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 та 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 [164].

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 власникові майна шляхом неправомірного введення, видалення, модифікації цифрової інформації або несанкціонованого втручання у функціонування цифрового пристрою або програмного забезпечення [361].

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 [368].

Варто зауважити, що норми Конвенції містили спробу нормативного регулювання трьох основних блоків питань, зокрема: 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, що варто внести до національного законодавства [244, с. 95].

Закріплені в Конвенції склади розділені на чотири групи відповідно до об'єкта зазіхання: 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 [19].

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 відносяться наступні суспільно небезпечні діяння: 1) незаконний доступ, тобто навмисний, без права на це доступ до інформаційно-телекомунікаційних технологій, систем або мереж, з'єднаної з іншим комп'ютером, порушує заходи безпеки і вчинений з метою оволодіти цифровими даними чи з іншим злим наміром; 2) нелегальне перехоплення, під яким розуміється здійснений з використанням цифрових технічних засобів та навмисно, без права на це, 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 установлено злий намір [390].

Діяння у формі втручання в дані являє собою псування цифрових даних різними способами, вчинене умисно, і без права на таке псування.
Г. Родерік визначає, що саме можна вважати псуванням цифрових даних, зокрема, це – зміна, пошкодження, видалення, блокування, погіршення цифрових даних, збережених в інформаційно-телекомунікаційний системі [464, 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 можуть 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 допуск до інформаційно-телекомунікаційної системи або її частини та використовувати її для скоєння правопорушення [447, с. 12].

До кримінальних правопорушень, пов’язаних із комп’ютерами, Конвенція класифікує підробку та шахрайство, пов’язане 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, вчинене умисно 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 із 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, яке здійснюється несанкціоновано та навмисно, з метою подальшого поширення у вигляді комп'ютерної системи; 2) пропозиція чи подання дитячої порнографії через комп'ютерну систему у користування; 3) придбання через комп'ютерну систему дитячої порнографії особистого використання або третіх осіб;

4) володіння дитячою порнографією, як збереженою на комп'ютерних носіях, і розміщеної в комп'ютерній системі [312].

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 [410]

Остання група правопорушень, що однак не закріплена 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 [474].

Зауважимо, що в 2003 році Рада Європи підписала Додатковий протокол до Конвенції «Про кіберзлочинність», відповідно до якого держави-учасниці повинні були у своїх законодавствах криміналізувати 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 ньому або замах. Водночас установлення відповідальності за підбурювання та співучасть є обов'язком держави-підписанта Конвенції, а криміналізація замаху – правом [418].

Зауважимо, що відповідно до 12 статті Конвенції держави-учасниці повинні вжити таких заходів, що давали б змогу нести кримінальну відповідальність юридичні особи за весь спектр протиправних дій, передбачених Конвенцією.

Здійснивши аналіз основних норм 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 та мереж. На нашу думку, це потребує насамперед істотного доповнення та уточнення в рамках національних законодавств держав-учасниць.

Водночас з цим 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, збережених на території Сторони 2 , або одержати їх, якщо ця Сторона 2 має законну та 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 випадку 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 статтями 111, 114, 163 Особливої частини Кримінального кодексу України.

Стаття 4 Конвенції передбачає необхідність кваліфікувати як кримінальне правопорушення, умисне створення серйозних перешкод функціонування комп'ютерної системи шляхом маніпуляцій із цифровими

даними. Зазначені діяння підпадають під склад кримінального правопорушення, який 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'ютерні програми, розроблені та адаптовані для 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».

Що стосується комп'ютерних паролів, кодів доступу чи інших аналогічних даних, за допомогою яких може бути одержаний доступ до комп'ютерної системи, 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 установлення 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 статтями Особливої частини Кримінального кодексу України, зокрема: 1) незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, електронними грошима, обладнанням для їх виготовлення (200 стаття); 2) незаконне виготовлення, підроблення, використання чи збут підроблених документів на отримання наркотичних засобів, психотропних речовин або прекурсорів (стаття 318); 3) підроблення документів, печаток, штампів та бланків, збут чи використання підроблених документів, печаток, штампів (стаття 358); 4) службове підроблення (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, залишаються поза правовим регулюванням.

Правопорушення, пов'язані з дитячою порнографією, визначаються у 9 статті Конвенції, одночасно такі норми знайшли своє закріплення 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 в статті 10 Конвенції, передбачає відповідальність за порушення авторського права та суміжних прав. В Кримінальному кодексі України зміст діянь, передбачених 10 статтею Конвенції, окреслює кримінальну відповідальність за декількома статтями Особливої частини Кримінального кодексу України, зокрема: 1) порушення авторського права і 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 діяння, передбачене статтею 3 Додаткового протоколу до Конвенції

«Про кіберзлочинність», також знайшло своє закріплення в кримінальному законодавстві України, зокрема у 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 небезпечності, як рекомендує Конвенція. В таблиці 5 ми навели співвідношення норм Конвенції «Про кіберзлочинність» і Кримінального кодексу України в розрізі використання елементів інформаційно-телекомунікаційних технологій при вчиненні кримінального правопорушення і його закріплення в якості 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**
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),	Виконано лише в частині установлення відповідальності щодо спеціального суб’єкта такого кримінального правопорушення, але саме діяння у формі перехоплення в його

Конвенція «Про кіберзлочинність»	**Кримінальний кодекс України**	**Реалізація**
	автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї;	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 оброблення цифрової інформації або до порушення
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

Конвенція «Про кіберзлочинність»	**Кримінальний кодекс України**	**Реалізація**
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
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, в цілому вважаємо, що підробка у сфері цифрової інформації на даний момент фактично не криміналізована, більше того предметом будь-якого підроблення згідно з чинним кримінальним законом не може виступати цифрова інформація.
Стаття 8 – шахрайство, пов'язане з комп'ютерами	Частина 3 статті 190 – шахрайство	Незважаючи на наявність в чинному кримінальному законі кваліфікаційної ознаки шахрайства, вчиненого шляхом незаконних операцій з використанням електронно-обчислювальної техніки, суспільно небезпечні діяння в силу особливостей статті 190 Особливої частини Кримінального кодексу України не можуть бути кваліфіковані як діяння, що вчинені обманом або

Конвенція «Про кіберзлочинність»	**Кримінальний кодекс України**	**Реалізація**
		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 кваліфікуючої ознаки, вчинення кримінального правопорушення шляхом використання інформаційно-телекомунікаційни х технологій, систем та мереж.
Стаття 10 – правопорушення, пов'язані з порушенням авторських та суміжних прав	Стаття 177 - порушення авторського права і суміжних прав	Не спостерігається виділення, як кваліфікуючої ознаки, вчинення кримінального правопорушення шляхом використання інформаційно-телекомунікаційни х технологій, систем та мереж.
Стаття 3 – (Додатковий протокол до Конвенції «Про кіберзлочинність»)	Статті 161, 300, 442 - порушення рівноправності громадян залежно від їх расової, національної, регіональної належності, релігійних переконань, інвалідності та за іншими ознаками; ввезення, виготовлення або розповсюдження творів, що пропагують культ насильства і жорстокості, расову, національну чи релігійну нетерпимість та дискримінацію; геноцид.	Не спостерігається виділення, як кваліфікуючої ознаки, вчинення кримінального правопорушення шляхом використання інформаційно-телекомунікаційни х технологій, систем та мереж.

Підбиваючи підсумки викладеного перед цим, 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. Незважаючи на швидку трансформацію кіберпростору й похідного від нього інтернет-простору, адаптації кіберзлочинців до реалій суспільства, єдиним чинним міжнародним актом щодо установлення 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 в кіберпросторі за законодавством зарубіжних держав

Аналізуючи проблематику кримінально-правової відповідальності за кримінальні правопорушення, вчинені у 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 дозволяє по-іншому поглянути на національний кримінальний закон, тим самим виявивши його слабкі та сильні сторони, одночасно запропонувати пропозиції щодо подальшого якісного його реформування [393].

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, аніж 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 по боротьбі з кримінальними правопорушеннями в кіберпросторі значно раніше ніж інші держави [241, 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 кіберугруповань і вчинення перших кримінальних правопорушень у кіберпросторі, як наслідок – ранній сплеск кіберзлочинності та одночасного усвідомлення негайного правового регулювання цього суспільно небезпечного явища [2].

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 в країнах із прецедентним правом акцент здійснюється на визнання 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 [457].

Варто зауважити, що незважаючи на відмінності у правовому регулюванні установлення кримінальної відповідальності між різними країнами, спільним для всіх країн є факт загрози таких суспільно небезпечних діянь з урахуванням їх пріоритету правового регулювання [1]. Сьогодні ми з упевненістю можемо зазначити, що правове регулювання установлення 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, які приймаються країнами у сфері установлення 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 установлення 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» вказує на необхідність приведення національних законодавств країн-учасниць до одноманітності [415].

Для вироблення рекомендацій щодо вдосконалення правового регулювання вчинення кримінальних правопорушень у кіберпросторі в Україні вважаємо за потрібне провести порівняльний аналіз конкретних способів правового регулювання відповідальності за вчинення цих суспільно небезпечних діянь у законодавстві інших країн.

На нашу думку, найбільш розроблене законодавство у сфері правового регулювання установлення кримінальної відповідальності за вчинення кримінальних правопорушень у кіберпросторі мають Сполучені Штати Америки. Зауважимо, що саме США 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 установлення 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 [342].

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 установлення кримінальної відповідальності за вчинення кримінальних правопорушень шляхом використання інформаційно-телекомунікаційних технологій на рівні окремих штатів [383].

Акт «Про комп'ютерне шахрайство» надає 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 [389].

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, розмір завданих збитків, тяжкості діяння та спричинених наслідків [326, с. 461].

Одночасно з цим законодавство Сполучених Штатів Америки закріплює спеціальний понятійний апарат щодо установлення 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 [311,
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», відповідно до якого, крім копіювання та переміщення цифрової інформації, одержання також охоплює процес самого «читання», тобто ознайомлення з цифровою інформацією без подальшого її 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 до більш правильної кваліфікації суспільно небезпечного 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 находження 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 та характер збитків у кожному випадку індивідуально, ураховуючи всі обставини справи [323, 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 прикладі цих штатів питання урегульованості установлення кримінальної відповідальності за вчинення окремих видів 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 передбачене покарання у вигляді позбавлення волі на строк до 6 років [318].

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 комп'ютерне шахрайство карається штрафом до 10 тисяч 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 [339].

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 у попередньому варіанті, законодавство дає змогу одночасного застосування обох видів покарання. Цікавим є досвід запровадження як кваліфікуючої ознаки в разі вчинення зазначеного кримінального правопорушення інтернет-мережі. Так, якщо особа, яка вчиняє комп'ютерне шахрайство, робить це з використанням Інтернет-мережі, встановлюється додаткове покарання у вигляді позбавлення волі строком не менше одного року [424].

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 [396].

Варто зазначити, що окремо законодавство штату Іллінойс виділяє посягання на власність, що здійснюються 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 якого пов'язаний з учиненням винним дій щодо оплати товарів чи послуг у 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 [432].

Не можна не звернути увагу на досвід криміналізації суспільно небезпечних діянь проти власності штату Джорджія. На відміну від інших штатів, у своєму Зводі законів Джорджія використовує категорію не комп'ютерного шахрайства, а крадіжки за допомогою комп'ютера. У розділі, присвяченому комп'ютерним кримінальним правопорушенням, 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, з 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 [338].

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 [490].

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 установлення 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 установлення кримінальної відповідальності за кримінальні правопорушення в кіберпросторі є Акт «Про комп'ютерні зловживання» 1990 року [343].

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 [443].

Неправомірний доступ у рамках Акту «Про комп'ютерні зловживання» поділено на: 1) доступ до цифрової інформації, яка 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 [329, с. 607].

Також кримінальним правопорушенням визнається неправомірна модифікація комп'ютерних даних, тобто зміна змісту цифрового програмного коду, який 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, передбачений відповідною статтею, щодо неправомірного доступу, зміни цифрової інформації тощо;

2) поінформованість особи, яка вчинила кримінальне правопорушення, що внесені нею зміни 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» [470] 1956 року особи

можуть підлягати кримінальній відповідальності за виготовлення та розповсюдження порнографічних зображень дітей віком до 16 років, здійснювані з використанням інформаційно-телекомунікаційних технологій, систем і мереж. Так само Закон «Про тероризм» 2000 року [493] закріплює, що неправомірний доступ до цифрової інформації, що зберігається в інформаційно-телекомунікаційних технологіях, системах і мережах, розцінюється як терористичний акт і тягне за собою підвищену кримінальну відповідальність, якщо одержана таким чином інформація завдала значної шкоди або використовувалася для організації масових заворушень.

На нашу думку, запозичення позитивного досвіду Великої Британії в рамках боротьби та установлення кримінальної відповідальності за кібертероризм є обов'язковим кроком у рамках становлення стратегії кібербезпеки держави й тих кібернетичних загроз, які ми маємо сьогодні з боку Російської Федерації.

Не можна не акцентувати увагу на досвіді Ірландії у 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 [352].

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 [353].

Кримінальний кодекс Канади в статті 403 установлює 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. Водночас 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 [347].

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 [442].

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 установлення 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, яка 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 V розділі Кримінального кодексу Нідерландів. Варто звернути увагу на систему й розмір покарань цієї країни. З упевненістю

можемо говорити, що кримінальне законодавство Нідерландів у частині установлення 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 [453].

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 установлення кримінальної відповідальності за «дії у формі розповсюдження цифрових даних, спрямовані на заподіяння шкоди, шляхом їх подальшого самокопіювання в інформаційно-телекомунікаційної 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 і 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 [365, 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 зауважимо, 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 [372].

Кримінальний кодекс Іспанії регламентує відповідальність за кримінальні правопорушення в кіберпросторі в X розділі. 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 установлення кваліфікаційних ознак, що регламентували б кримінальні правопорушення в кіберпросторі, у вітчизняне законодавство України цілком виправданим, ураховуючи підвищений ступінь суспільної небезпеки [481].

Цікавим є досвід Данії у встановленні кримінальної відповідальності за шахрайські дії, вчинені у кіберпросторі. Статтею 279 «а» комп'ютерне шахрайство визначається як незаконна зміна, доповнення або видалення цифрової інформації або програмного коду, що використовуються для цифрової автоматизованої обробки 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 дії, що мають ознаки як крадіжки, так і шахрайства [496].

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 би присвячувався кримінальній відповідальності за кримінальні правопорушення в кіберпросторі. Основними кримінальними

правопорушеннями в кіберпросторі, передбаченими Кримінальним кодексом Німеччини, є:

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 [378].

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 не є 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 [402].

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 категорійний апарат. Зокрема, в пункті 2 статті 202 а Кримінального кодексу Німеччини дається визначення поняття «дані», під яким розуміються цифрові дані, що збираються та передаються електронним, магнітним або іншим способом, яким не сприймаються у фізичному вимірі [346].

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 [405].

Наступна 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 установлення 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 XIII розділом 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 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 [516].

Зауважимо, що зазначені статті за змістом подібні до закріплених у XVI розділі Особливої частини Кримінального кодексу України.

Кримінальний кодекс Республіки Казахстан містить дві статті, що регламентують відповідальність за скоєння кримінальних правопорушень з 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 установлення кримінальної відповідальності за кримінальні правопорушення в кіберпросторі не виділені в окремий розділ, а розміщуються в главі 7 кодексу «Кримінальні правопорушення у сфері економічної діяльності» [517].

На нашу думку, не можна не звернути увагу на досвід Естонії в питаннях регулювання установлення 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) [366].

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 би визначав 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 та 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 і 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 установлення кримінальної відповідальності

за кримінальні правопорушення у кіберпросторі

Країна	**Позитивний досвід**	**Можливості та шляхи впровадження в кримінальний закон України**
Естонія	Підвищена кримінально-правова охорона об’єктів та 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 вчинені щодо державної інформаційно-телекомунікаційної технології, системи чи мережі»; 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 отримання цифрової інформації	Враховуючи 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

Країна	Позитивний досвід	Можливості та шляхи впровадження в кримінальний закон України
		пропонуємо в примітці до цієї статті визначити поняття «виток цифрової інформації». Водночас вважаємо за потрібне наголосити форми витоку цифрової інформації, зокрема ознайомлення, читання.
Данія	Визначення складу кримінального правопорушення «комп' ютерне шахрайство», як незаконна зміна, доповнення або видалення цифрової інформації або програмного коду, яка використовується для цифрової автоматизован ої обробки даних з метою отримання для себе або третіх осіб незаконної вигоди.	Проблеми кваліфікації, відповідно до частини 3 статті 190 Особливої частини Кримінального кодексу України, викликають потребу до правильного формулювання та тлумачення суспільно небезпечних дій у формі незаконних операцій з використанням електронно-обчислювальної техніки. Формулювання, запропоноване кримінальним законодавством Данії, по-перше, невілює всі питання, пов'язані 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 установлення кримінальної відповідальності за кримінальні правопорушення в кіберпросторі, переважно розміщена в окремих нормативних актах. Водночас така країна, як Сполучені Штати Америки, крім загального регулювання відносин щодо установлення 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, кримінальне законодавство цих країн значно відрізняється 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.

Висновки до розділу 4

1. На основі аналізу Статуту Організації Об'єднаних Націй, Підсумкового акту Організації з безпеки і співробітництва в Європі та Декларації про міжнародні принципи відповідно до статуту Організації Об'єднаних Націй наголошено на основних принципах міжнародного права та надано їх характеристику через призму їх регулювання міжнародних відносин в рамках кіберпростору.

2. Аналізуючи принцип суверенної рівності держав в рамках кіберпростору, наголошено на існуванні двох концепцій державного кібернетичного суверенітету, зокрема: 1) кібернетичний простір є централізованим та фактично регулюється відповідно до комплексного підходу усіма країнами-членами світового товариства, а не кожною країною окремо; 2) кібернетичний простір має певний імунітет від державного суверенітету.

3. Наголошено, 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 та фактично невілює можливості міжнародно-правового захисту держав від вчинення кібератак з боку інших держав, або окремих осіб за сприяння конкретних держав.

4. Акцентовано увагу, що співробітництво держав в рамках регулювання відносин, що виникають в кіберпросторі та прийнятті декількох міжнародних нормативних актів, жоден 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, де б визначалися поняття «кримінальне правопорушення у кіберпросторі», «кіберпростір», «кібертероризм», «кіберзагроза», «кібератака», «кіберзброя». Одночасно з цим в такому акті повинно бути врегульоване питання щодо притягнення до відповідальності за кібератаки, превентивні кібератаки та кібератаки у відповідь.

5. Проаналізовано основні міжнародно-правові акти з питань встановлення кримінальної відповідальності за кримінальні правопорушення у кіберпросторі: 1) Рекомендація NR 89 (9) Комітету Міністрів країн-членів Ради Європи «Про злочини, пов'язані з комп'ютерами»; 2) Конвенція «Про кіберзлочинність». Названо результат імплементації норм Конвенції «Про кіберзлочинність» у законодавство України.

6. Узагальнено та систематизовано зарубіжний досвід правового регулювання відповідальності за вчинення кримінальних правопорушень шляхом використання інформаційно-телекомунікаційних технологій. З’ясовано, що країни, які відносяться до англо-саксонської правової сім’ї, окрім нормативного регулювання, широко застосовують систему судових

прецедентів, при цьому правова регламентація встановлення кримінальної відповідальності за кримінальні правопорушення в кіберпросторі, переважно розміщена в окремих нормативних актах, при цьому така країна, як Сполучені Штати Америки, крім загального регулювання відносин щодо встановлення кримінальної відповідальності за кримінальні правопорушення у кіберпросторі, застосовує регулювання на рівні окремих штатів, яке дуже різниться між собою. Навпаки, країни романо-германської правової сім'ї характеризуються уніфікацією своєї правової регламентації щодо кримінальної відповідальності за кримінальні правопорушення у кіберпросторі. Однак незважаючи на приналежність до одної правової сім'ї, кримінальне законодавство цих країн суттєво різниться між собою. Так, країни Західної та Центральної Європи не виділяють в окремий розділ кримінальні правопорушення у кіберпросторі, а кримінальна відповідальність за них передбачена різними розділами їх Кримінальних кодексів. А ось у країнах Північної Європи кримінальна відповідальність за суспільно небезпечні діяння шляхом використання інформаційно-телекомунікаційних технологій, систем та мереж виділені в окремий розділ.

ВИСНОВКИ

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

2. Проєктування методології дослідження є важливим кроком для забезпечення ефективного, надійного та юридично відповідного розслідування кіберзлочинів. Вона сприяє покращенню кібербезпеки, забезпеченню справедливості та захисту прав потерпілих сторін. Методологія є загальним підходом до дослідження кіберзлочинів та може варіюватись

залежно від конкретного випадку та доступності ресурсів. У контексті цього дослідження були використані наступні наукові методи: метод аналізу, емпіричний метод, метод контент-аналізу, метод кейс-студії, порівняльно-правовий метод, метод системного аналізу.

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

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

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

6. На основі аналізу існуючих доктринальних підходів до типологізації видів кримінальних правопорушень в кіберпросторі запропоновано вдосконалений розширений авторський підхід. По-перше, типологізувати кримінальні правопорушення у кіберпросторі за родовим об’єктом. По-друге, відповідно до кваліфікації суб’єктів вчинення кримінальних правопорушень у кіберпросторі. По-третє, залежно від кількості об’єктів посягання. По-четверте, залежно від спрямованості кримінальних правопорушень у кіберпросторі. По-п’яте, залежно від чисельності суб’єктів вчинення

кримінального правопорушення. По-шосте, залежно від цілі використання електронно-обчислювальних машин інформаційно-телекомунікаційних мереж. По-сьоме, залежно від мети вчинення кримінальних правопорушень у кіберпросторі. По-восьме, залежно від повноти ознак кримінальних правопорушень у кіберпросторі. По-дев'яте, залежно від правового режиму інформації, яка є предметом кримінальних правопорушень у кіберпросторі. По-десяте, залежно від сутності кримінальних правопорушень у кіберпросторі. По-одинадцяте, залежно від кількості суб'єктів вчинення кримінальних правопорушень у кіберпросторі. По-дванадцяте, відповідно до видів кримінальних правопорушень у кіберпросторі, передбачених Конвенцією Ради Європи «Про кіберзлочинність». По-тринадцяте, відповідно до статті 12 Кримінального кодексу України на кримінальні проступки та злочини.

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

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

9. Кіберзалежні кримінальні правопорушення характеризуються вчиненням декількох суспільно небезпечних діянь, які передбачені

Особливою частиною Кримінального кодексу України для досягнення одного злочинного результату, та власне призначення покарання за сукупністю кримінальних правопорушень.

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

11. Основними способами легалізації майна, отриманого злочинним шляхом, є: 1) легалізація майна, отриманого злочинним шляхом за допомогою вже існуючої інтернет-інфраструктури (маркетплейси, сайти оголошень, соціальні мережі, інтернет-аукціони, краудфандінг);

2) легалізація майна, отриманого злочинним шляхом, шляхом створення нової вебінфраструктури (інтернет-магазин); 3) легалізація майна, отриманого злочинним шляхом, використання обмінників та цифрової (електронної) валюти; 4) легалізація майна, отриманого злочинним шляхом за допомогою віртуальних активів.

12. Основними ознаками віртуальних активів є:

1) децентралізованість; 2) транснаціональність; 3) конфіденційність операцій; 4) цифровізація; 5) майновий характер; 6) анонімність. Акцентовано увагу на співвідношенні понять «віртуальний актив» та «криптовалюта», доведено неідентичність зазначених понять.

13. Наголошено на необхідності введення додаткової обставини, що обтяжує кримінальні правопорушення у кіберпросторі: 1) заподіяння шкоди інформаційно-телекомунікаційній технології, системі або мережі державного значення, яке має ознаки критичної інфраструктури;

2) предметом кримінального правопорушення виступає цифрова інформація, яка має ознаки державної таємниці.

14. На основі аналізу Статуту Організації Об’єднаних Націй,

Підсумкового акту Організації з безпеки і співробітництва в Європі та Декларації про міжнародні принципи відповідно до статуту Організації Об'єднаних Націй визначені основні міжнародні принципи міжнародного права та надано їх характеристику через призму їх регулювання міжнародних відносин в рамках кіберпростору.

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

16. Співробітництво держав в рамках регулювання відносин, що виникають у кіберпросторі, та прийнятті декількох міжнародних нормативних актів. Жоден 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, де б визначалися поняття «кримінальне правопорушення у кіберпросторі», «кіберпростір», «кібертероризм», «кіберзагроза», «кібератака», «кіберзброя». Одночасно з цим в такому акті повинно бути врегульоване питання щодо притягнення до відповідальності за кібератаки, превентивні кібератаки та кібератаки у відповідь.

17. Узагальнено та систематизовано зарубіжний досвід правового регулювання відповідальності за вчинення кримінальних правопорушень шляхом використання інформаційно-телекомунікаційних технологій. З'ясовано, що країни, які відносяться до англо-саксонської правової сім'ї, окрім нормативного регулювання широко застосовують систему судових прецедентів, при цьому правова регламентація встановлення кримінальної

відповідальності за кримінальні правопорушення у кіберпросторі переважно розміщена в окремих нормативних актах. При цьому така країна, як Сполучені Штати Америки, крім загального регулювання відносин щодо встановлення кримінальної відповідальності за кримінальні правопорушення у кіберпросторі, застосовує регулювання на рівні окремих штатів, яке дуже різниться між собою. Навпаки, країни романо-германської правової сім'ї характеризуються уніфікацією своєї правової регламентації щодо кримінальної відповідальності за кримінальні правопорушення у кіберпросторі. Та незважаючи на приналежність до одної правової сім'ї, кримінальне законодавство цих країн суттєво різниться між собою. Так, країни Західної та Центральної Європи не виділяють в окремий розділ кримінальні правопорушення у кіберпросторі, а кримінальна відповідальність за них передбачена різними розділами їх Кримінальних кодексів. У свою чергу у країнах Північної Європи кримінальна відповідальність за суспільно небезпечні діяння шляхом використання інформаційно–телекомунікаційних технологій, систем та мереж виділені в окремий розділ.

Запропоновано наступні зміни до Кримінального кодексу України:

1. Викласти статтю 361 у такій редакції:

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

Несанкціоноване втручання в роботу інформаційно-телекомунікаційних технологій, систем та мереж, тобто отримання 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 обробки, перехоплення, блокування та

(або) знищення цифрової інформації, -

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

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

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

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

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

Дії, передбачені частиною третьою-четвертою цієї статті, якщо вони вчинені під час дії воєнного стану, -

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

2. Викласти частину другу статті 362 у такій редакції:

Несанкціоноване копіювання цифрової інформації, яка обробляється в інформаційно-телекомунікаційних технологіях, системах та мережах, якщо це призвело до її витоку, вчинені особою, яка має право доступу до такої інформації.

3. Викласти статтю 363 у такій редакції:

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

1. Порушення правил експлуатації інформаційно-

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

4. Викласти статтю 363-1 у такій редакції:

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

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

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

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

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

5. Виключити з частини третьої статті 190 або шляхом незаконних операцій з використанням електронно-обчислювальної техніки.

6. Доповнити частину другу статті 190:

Шахрайство, вчинене повторно або за попередньою змовою групою осіб, або таке, що завдало значної шкоди потерпілому, або шляхом операцій з використанням інформаційно-телекомунікаційних технологій, систем та мереж.

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

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

1. Крадіжка в сфері обігу безготівкових або електронних грошей та віртуальних активів, вчинена шляхом введення цифрової інформації в

інформаційно-телекомунікаційні технології, системи та мережі.

2. Крадіжка в сфері обігу безготівкових або електронних грошей та віртуальних активів іншого втручання в роботу інформаційно-телекомунікаційні технології, системи та мережі.

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

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

5. Дії, передбачені частинами першою – другою, вчинені у великих розмірах або організованою групою.

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

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. 16 Latest Cybercrime Trends & Predictions for 2024 and Beyond. URL: https://financesonline.com/cybercrime-trends/

2. 16 Latest Cybercrime Trends & Predictions for 2022/2023 and Beyond : веб-сайт. URL: https://financesonline.com/cybercrime-trends/.

3. 20-річному українцю загрожує 8 років в'язниці за крадіжку криптовалюти. *Obozrevatel*: веб-сайт. URL: http://surl.li/ibiuo.

4. 2021 Report on CSIRT-Law Enforcement Cooperation. *European Union agency for cybersecurity.* URL: http://surl.li/iaoas.

5. 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 : методичні рекомендації. Одеса : ОДУВС. 2018. 100 с.

6. Адамова О. С. Поняття правової класифікації. *Часопис цивілістики.* 2015. № 18. С. 19–24.

7. Азаров Д. В. Злочини у сфері комп’ютерної інформації: кримінально-правове дослідження. *Монографія : Київ. Атіка*. 2007. С. 304.

8. Алексєєва О. Р. Інтернет-простір та медіа засоби 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.

9. Амелін О. В. Визначення кіберзлочинів у національному законодавстві. *Науковий часопис Національної академії прокуратури України*. 2016. № 3. С. 1–10.

10. Аналіз статті 209 Кримінального кодексу України доступний для ознайомлення. *Академія фінансового моніторингу* : веб-сайт. URL: http://surl.li/ibgqu.

11. 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.

12. Антифрод. *Wikipedia* : веб-сайт. URL: http://surl.li/iaxka.

13. 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.

14. Баланюк О. В. До питання про значення та класифікацію підготовчої діяльності до вчинення та приховування злочину. Актуальні проблеми держави і права. 2008. № 5. С. 123-126.

15. Бабанли Р. Ш. Призначення покарання в Україні: теоретико-прикладні засади. Чернігів: *Десна Поліграф.* 2019. 488 с. ISBN 978-617-7648-86-3.

16. Бельський Ю. Призначення покарання за несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку. *Підприємництво, господарство і право*. 2016. № 5. С. 72-76.

17. Бельський Ю. Щодо визначення поняття кіберзлочину. *Юридичний вісник.* 2014. № 6. С. 414-418.

18. Бєлєнький В. Відповідальність за кіберзлочини за кримінальним правом США, Великобританії та України : автореф. дис. кан. юрид. наук : 12.00.08. Київ. 2016. 19 с.

19. Біленчук П. Д., Зубань М. А. Комп'ютерні злочини: соціально-правові та кримінолого-криміналістичні аспекти. Українська академія внутрішніх справ. 1994. С. 6. URL: http://elar.naiau.kiev.ua/bitstream/123456789/18828/1/%D0%97%D0%BB%D0%BE%D1%87.%D0%B2%20%D0%B1%D0%B0%D0%BD%D0%BA.%D0%B8%D0%BD%D0%B4%D1%83%D1%81%D1%82%D1%80.pdf

20. Біловус Л. Український інформаційний простір: сьогодення та перспективи. URL: http:// ijimv.knukim.edu.ua/zbirnyk/1_1/bilovus_l_i_ ukrayinskyy_informatsiynyy_prostir.pdf.

21. Богач О. В. Кіберпростір і перспектива соціалізації особистості старшокласників. *Психологічні перспективи. Спеціальний випуск: Проблеми кібераграсії*. Київ: Інститут соціальної та політичної психології НАПН України. 2012. Т. 1. С. 158-167.

22. 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.

23. Більшість кіберзлочинів у Білорусі - це крадіжка грошей з банківськихкарток. *Мінск новини* : вебсайт. URL: https://minsknews.by/bolshinstvo-kiberprestupleniy-v-belarusi-eto-krazha-deneg-s-bankovskih-kart/.

24. Бондаренко О. С. Концепція кримінально-правової протидії корупції : монографія О. С. Бондаренко. Суми : Сумський державний університет. 2021. 472 с.

25. Боровик А. В. Кіберзлочини в Україні (кримінально-правова характеристика) : навч. посіб., за ред. А. В. Боровик, І. М. Копотун ; Луцьк: Волиньполіграф. 2019. 314 с.

26. Бохенко В. М. Кримінологічні ризики обігу криптовалют. *Юридичний науковий електронний журнал.* № 12/2021. С. 327. URL: https://doi.org/10.32782/2524-0374/2021-12/82.

27. Бражник А. А. Абсолютно визначені покарання за злочини проти статевої свободи та статевої недоторканності. URL: https://dspace.nlu.edu.ua/bitstream/123456789/18281/1/Brazhnik_81-84.pdf.

28. Булатова О.В., Сарба М.С. Фінансовий моніторинг як протидія відмиванню коштів та фінансуванню тероризму. Академічні візії. 2023. № 26. С. 1-7. DOI: http://dx.doi.org/10.5281/zenodo.10925445

29. Булатов А. С. Кримінальне маніпулювання під час шахрайства.

Юридична психологія. 2015. № 2. С. 203-213. URL: http://surl.li/iavzf.

30. Буряк М. В. Злочини проти основ національної безпеки України у політичній сфері. URL: http://surl.li/iamuj.

31. Бурячок В. Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник : за заг. ред. д-ра техн. наук, професора В.Б. Толубка. Київ : ДУТ. 2015. 288 с.

32. Василенко А. І. Теоретичні аспекти застосування норм і принципів міжнародного права до регулювання відносин в кіберпросторі. Одеса. 2018. 33 с.

33. 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.

34. Васильковский І. І. Поняття, класифікація та характеристика окремих видів кіберзлочинів. *Прикарпатський юридичний вісник*. Випуск 1(16), том 2. 2017. С. 196-201.

35. Васильковський І. І. Поняття «кіберзлочинність» та «кіберзлочини»: стан та співвідношення. *Міжнародний юридичний вісник: актуальні проблеми сучасності (теорія та практика)*. 2018. № 1. С. 276 – 282.

36. Ваш родич потрапив у ДТП: у поліції розповіли про найпоширеніші шахрайські схеми. *Суспільне* : веб-сайт. URL: http://surl.li/iavzr.

37. Верес І. Електронні гроші та криптовалюта як засоби розрахунків у сфері електронної комерції. Підприємництво і право. 2018. № 11. С. 10–15.

38. Вейц А.М. Криміналістична класифікація кіберзлочинів, вчинених за участю службової особи або такої, яка здійснює професійну діяльність, пов’язану з наданням публічних послуг. *Прикарпатський юридичний вісник.* 2022. № 47. С. 170-175. DOI https://doi.org/10.32782/pyuv.v6.2022.33

39. Вінер Н. Кібернетика, або управління та зв'язок у тварині та машині. URL: https://uberty.org/wp-content/uploads/2015/07/Norbert_Wiener_Cybernetics.pdf

40. Вирок Вінницького міського суду у справі № 127/13877/22. URL: https://reyestr.court.gov.ua/Review/105190434.

41. Вирок Соснівського районного суду м. Черкаси у справі № 712/6176/20. ULR: https://reyestr.court.gov.ua/Review/92814657.

42. Вирок суду у справі № 1-кп/711/173/20. URL: https://reyestr.court.gov.ua/Review/99816224.

43. Війна Росії проти України: хронологія кібератак. URL: https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI(2022)733549_XL.pdf.

44. Вікторія Л. В. Вина як кримінально-правова категорія та її вплив на кваліфікацію злочину. *Молодий вчений*. 2021. № 6 (94). С. 22–25.

45. Вірус WannaCry пошкодив комп’ютери у 99 країнах світу: веб-сайт.URL: https://www.bbc.com/ukrainian/features-39907984.

46. Войтко Б. С. Соціальна інженерія як інструмент для проникнення у інформаційну систему підприємства. Збірник тез доповідей : Секція «Прикладні аспекти використання інформаційних систем і технологій». URL: https://jait.donnu.edu.ua/article/view/9023.

47. Войціховський А. В. Міжнародне право. Навчальний посібник: Харків. 2020. 544 с. URL: http://surl.li/ibqaj.

48. 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.

49. Волонець Д.Ф. Об’єктивна сторона кримінальних правопорушень, передбачених статтями 366-3663 КК України. KELM. 2021. № 6. С. 184-189.

50. 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.

51. 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.

52. Гаркуша Ю. Теоретико-правовий аналіз понять «кіберзлочин» і «кіберзлочинність». *Право і безпека.* 2017. № 1 (64). С. 74-78.

53. 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.

54. Гахов С. О. Застосування методів правового регулювання під час здійснення організаційних заходів щодо кібернетичного захисту інформаційних систем підприємств, установ та організацій. *Сучасний захист інформації.* 2016. № 3. С. 67–71.

55. Генеральна прокуратура України : веб-сайт. URL: http://surl.li/ianqs.

56. Гнатюк С. О. Кібертероризм: історія розвитку, сучасні тенденції та контрзаходи. *Безпека інформації*. 2013. Т. 19. № 2. С. 118–129.

57. Голіна В. В., Головкін Б. М. Кримінологія: Загальна та Особлива частини. Навчальний посібник. Харків. : Право. 2014. 513 с.

58. Голубєв В. О. Боротьба з комп'ютерними злочинами–проблема транснаціонального масштабу. URL: https://ukrreferat.com/chapters_book/pravo/golubev-vo-gavlovskij-vd-tsimbalyuk-vs-2002-problemi-borotbi-zi-zlochinami-u-sferi-vikoristannya-kompyuternih-tehnologij-kniga.html.

59. Градова Ю. В. Кібербулінг як загроза психологічному здоров'ю підлітків. URL: https://univd.edu.ua/general/publishing/konf/26_11_2019/pdf/18.pdf.

60. Грекова І. В. Окремі аспекти криміналістичної характеристики крадіжок автотранспортних засобів. *Південноукраїнський правничий часопис*.

2015. № 4. С. 122–125.

61. Гринчак А. А. Протидія расизму, ксенофобії та екстремізму : навчальний посібник. А. А. Гринчак. Харків. 2018. 248 с.

62. Д. Аколов. Фішинг, хто і як маніпулює вашим вибором. URL: https://kniga.biz.ua/pdf/7451-Fishing.pdf.

63. Декларація про принципи міжнародного права, що стосуються дружніх відношень та співробітництва між державами у відповідності зі Статутом Організації Об'єднаних Націй. *Liga 360*: веб-сайт. URL: http://surl.li/ibpzz.

64. Денисова Т. А. Основні тенденції діяльності держави у сфері застосування кримінальних покарань. *Вісник Львівського університету. Серія: «Юридична»*. 2010. № 50. С. 260–265.

65. Департамент кіберполіції Національної поліції України: вебсайт. URL: https://cyberpolice.gov.ua/news/prodavav-neisnuyuchi-generatory-kiberpolicziya-vykryla-zlovmysnyka-u-shaxrajstvi-3765/.

66. Дердюк Б. М. Поняття та теоретичні основи криміналістичної класифікації комп’ютерних злочинів. *Прикарпатський юридичний вісник.* 2014. № 6. Випуск 3. С. 225–233. URL: http://surl.li/ianij.

67. 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.

68. Діти та робота: особливості працевлаштування неповнолітніх. Безоплатна правова допомога : веб-сайт. URL: http://surl.li/ibjuk.

69. Дмитрук М. М. Типові наслідки «несанкціонованого втручання в роботу ЕОМ, автоматизованих систем, комп’ютерних мереж чи мереж електрозв’язку». URL: http://surl.li/ianqd.

70. Довженко О. Поняття кіберзлочину з криміналістичної позиції. *Трибуна молодого вченого. Юридичний вісник.* 2018. № 3. С 79-83.

71. Додатковий протокол до Конвенції про кіберзлочинність, який

стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи від 28.01.2003 (редакція від 21.07.2006). URL: https://zakon.rada.gov.ua/laws/show/994_687#Text.

72. Дубас О. П. Інформаційно-комунікаційний простір: поняття, сутність, структура. URL: http://dspace.nbuv.gov.ua/bitstream/handle/123456789/26693/22-Dubas.pdf.

73. Дубняк К. А. Інформаційний простір: структура та функціональні параметри. Серія: *Соціальні комунікації*. 2015. № 4 (24). С. 21-24.

74. Дубов Д. В. Кіберпростір як новий вимір геополітичного суперництва : монографія. Д. В. Дубов. Київ : НІСД, 2014. 328 с.

75. Дудоров О. О. Поняття злочину. Класифікація злочинів. Вісник Асоціації кримінального права України. 2013. № 1 (1). С. 84–102.

76. Дуленко В. А., Мамлєєв Р. Р., Пестриков В. А. Використання високих технологій в кримінальному середовищі. *Боротьба зі злочинами в сфері комп'ютерної інформації*: навч. допомога. Київ. 2007.

77. Естонія зазнала масштабної російської кібератаки після демонтажу радянського пам'ятника. *Радіо свобода*: веб-сайт. URL: http://surl.li/ibqbi.

78. Єдиний державний реєстр судових рішень. URL: https://reyestr.court.gov.ua/.

79. Єдиний звіт про осіб, які вчинили кримінальні правопорушення за серпень 2020 року. URL: http://surl.li/ibjwv.

80. За останні роки в Україні зросли кіберзлочини. *Дивись Інфо* : вебсайт. URL: https://dyvys.info/2020/09/25/za-ostanni-roky-v-ukrayini-zrosly-kiberzlochyny/.

81. Загальна декларація прав людини ООН: Міжнародний документ від 10 грудня 1948. URL: http://surl.li/umvi.

82. Загальні рекомендації щодо зменшення наслідків від впливу шкідливого програмного забезпечення URL: https://kingu.edu.ua/wp-content/uploads/2023/03/Кібергігієна.pdf

83. Загальні рекомендації щодо зменшення наслідків від впливу шкідливого програмного забезпечення. Sert-ua: веб-сайт. URL: https://cert.gov.ua/recommendation/2502.

84. Задорожна С. М. Природно-правовий характер принципів міжнародного права. *Науковий вісник Чернівецького університету. Сер. Правознавство. Збірник наук. Праць.* Вип. 660. 2013. С.49–56.

85. Заключний акт НБСЄ в Хельсінкі від 1 серпня 1975 р. URL: http://kimo.univ.kiev.ua/MVZP/75.htm.

86. Закон України "Про основні засади забезпечення кібербезпеки України" від 05.10.2017 № 2163 VIII (редакція від 01.01.2024). URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text.

87. Злиті фото знаменитостей з Eelegram : веб-сайт. URL: http://surl.li/iiper.

88. Каже, що військовий: шахрай намагається видурити гроші в лучан. Інформаційне агентство Конкурент : веб-сайт. URL: http://surl.li/iawbn.

89. Казначева Д. В. Основні види злочинів, що вчиняються із застосуванням криптовалюти. URL: http://surl.li/ibgtc/

90. Калініна А. В. Криптовалюта – цифровий актив злочинності. URL: http://surl.li/ibiui.

91. Карткове шахрайство в Україні: шахраї змінюють способи роботи : вебсайт. URL: http://surl.li/ianrl.

92. Карчевский М. В. Кіберзлочин чи злочин у сфері використання інформаційних технологій? *Кібербезпека в Україні: правові та організаційні питання* : матеріали всеукр. наук.-практ. конф. Одеса : ОДУВС. 2016. с. 10–15.

93. Карчевський М.В. Злочини в 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.

94. Кібератака вірусу Petya: що відомо. URL: http://surl.li/avmrp.

95. Кібератаки, артилерія, пропаганда. агальний огляд вимірів

російської
агресії: веб-сайт. URL: https://cip.gov.ua/ua/news/kiberataki-artileriya-propaganda-zagalnii-oglyad-vimiriv-rosiiskoyi-agresiyi.

96. Кіберзахист, що рятує: як нам посилити опір агресії Росії. *Економічна правда*: веб-сайт URL: https://www.epravda.com.ua/columns/2017/06/1/625543/.

97. Кіберполіція викрила злочинну групу, яка оформлювала кредити на зниклих безвісти і полонених військовослужбовців. Департамент кіберполіції Національної поліції України : веб-сайт. URL: https://cyberpolice.gov.ua/news/kiberpolicziya-vykryla-zlochynnu-grupu-yaka-oformlyuvala-kredyty-na-znyklyx-bezvisty-i-polonenyx-vijskovosluzhbovcziv-8913/.

98. Кіберполіція викрила мережу фейкових веб-обмінників. Інформаційне агентство Інтерфакс-Україна. Інтерфакс : веб-сайт.
URL: https://interfax.com.ua/news/general/512564.html.

99. Кіберполіція викрила організаторів шахрайського call-центру, які ошукали близько 18 тисяч іноземців. Департамент кіберполіції Національної поліції України: веб-сайт. URL: http://surl.li/iaxfm.

100. Кіберполіція викрила учасників транснаціональної шахрайської групи у привласненні грошей сотень тисяч осіб по всьому світу. Департамент кіберполіції Національної поліції України : веб-сайт. URL: http://surl.li/iawev.

101. Кіберполіція провела загальнонаціональну операцію з припинення діяльності ворожих ботоферм. Департамент кіберполіції Національної поліції України : веб-сайт. URL: http://surl.li/iaxgx.

102. Кіберполіція розкрила статистику інтернет-злочинності з початку року. *Finance ua*: веб-сайт. URL: https://news.finance.ua/ua/news/-/483006/kiberpolitsiya-rozkryla-statystyku-internet-zlochynnosti-z-pochatku-roku.

103. 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: Видавець Кушнір Г.

М. 2020. 171 с.

104. 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.

105. Комп'ютерна злочинність: Навчальний посібник : за ред. П. Д. Біленчук, Б. В. Романюк, В. С. Цимбалюк та ін. Київ.: Атіка. 2012. 240 с.

106. Конвенція про захист прав людини і основоположних свобод від 4 листопада 1950 р. *Офіційний вісник України*. 1998. № 13. С. 270–302.

107. Конвенція Ради Європи «Про кіберзлочинність»: від 21.11.2001 (редакція від 07.09.2005). URL: http://zakon.rada.gov.ua/laws/show/994_575.

108. 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.

109. Конспект лекцій з дисципліни міжнародне право. URL: http://surl.li/gwwwa.

110. Конституція України : станом на 1 січня 2023 р. Верховна Рада України. Харків : Право. 2020. 82 с.

111. Конференція Blockcha in UA : веб-сайт. URL: http://surl.li/ibgua.

112. Користін О. Є. Протидія кіберзлочинності в Україні: правові та організаційні засади : навч. посіб. Київ. : «Скіф». Х628.3 П834. 2012. 728. с.

113. 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.

114. Кравцова М. О. Сучасний стан і напрями протидії кіберзлочинності в Україні. *Вісник Кримінологічної асоціації України*. 2018. № 2 (19). С. 155–166.

115. 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.

116. Кримінальна відповідальність за «СПАМ» : веб-сайт. URL: http://surl.li/ianzt.

117. Кримінальне право (Особлива частина) : підручник / за ред. О. О. Дудорова, Є. О. Письменського. Київ. : «ВД «Дакор». 2013. 606 с.

118. Кримінальне право, Особлива частина. Підручник онлайн: веб-сайт. URL: https://pidru4niki.com/1584072059860/pravo/kriminalne_prav_.

119. Кримінальне право, Особлива частина. Підручник. URL: https://dspace.univd.edu.ua/server/api/core/bitstreams/4b73643c-9591-41ba-b399-e15660924037/content

120. Кримінальний кодекс Індії від 06 жовтня 1862 р. URL: https://wipolex.wipo.int/ru/legislation/details/7668.

121. Кримінальний кодекс України від 5 квіт. 2001 р. № 2341-III ; ред. станом на 12 вер. 2020 р. *Відомості Верховної Ради України (ВВР).* 2001. № 25-26. Ст. 131.

122. Кримінальний кодекс України. Науково-практичний коментар : за заг. ред. В. Я. Тація, В. П. Пшонки, В. І. Борисова, В. І. Тютюгіна. Харків: Право. 2013.

123. Кріпак А. А. Покарання у вигляді позбавлення волі у законодавстві України та окремих країн Західної Європи. *Вісник Пенітенціарної асоціації України.* 2018. №1. 105–114. URL: https://visnykpau.com/index.php/journal/article/view/131.

124. 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.

125. Кундеус В. Г. Поняття та види кіберзлочинів. *Держава і злочинність. нові виклики в епоху постмодерну.* 2020. № 4. С. 44-46.

126. Курушин В. Д., Мінаєв В. А. Комп'ютерні злочини та інформаційна безпека. *Новий юрист*. 1998. С. 14–21.

127. 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.

128. Лазаренко Н. Л. Комунікація в інтернет-просторі: психологічний аспект. *Information Technologies and Learning Tools*. 2018. 65(3):249. DOI: 10.33407/itlt.v65i3.2036

129. Лефтеров Л. В. Шкідливе програмне забезпечення як знаряддя кіберзлочинності. URL: http://surl.li/iantv.

130. Лист Національного банку України від 08 грудня 2014 № 29-208/72889. URL:https://zakon.rada.gov.ua/laws/show/v2889500-14#Text.

131. Лист Національного банку України від 22 березня 2018 № 40-0006/16290. URL: https://zakononline.com.ua/documents/show/374117___374182.

132. Литвинова О. М. *Кримінальне право України. Загальна частина.* Підручник. Підручник : за заг. ред. проф. О. М. Литвинова. МВС України. Харків : нац. ун-т внутр. справ. Харків. 2020. 428 с.

133. Люликова М. Protiv pravosudia. URL: https://www.academia.edu/24627410/Protiv_pravosudia_2015_1_.

134. Макарчук Д. Поняття кримінально караного діяння у Конституціях України, Франції та ФРН. *Підприємництво, господарство і право.* 2019. № 5. С. 244-249.

135. Маклюен М. Розуміння медіа: зовнішні розширення людини. 2003. С. 400. URL: http://conference.nbuv.gov.ua/report/view/id/838

136. Манжай О. Використання кіберпростору в оперативно-розшуковій діяльності. *Special investigation activity systems of the world, particularly cybercrime fighting systems.* URL: http://surl.li/hyvnn.

137. 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.

138. Марков В. В. До питання щодо зарубіжного досвіду протидії кіберзлочинності. *Право і безпека*. 2015. № 2 (57). С. 107–113.

139. Матвійчук В. К. Злочини проти основ національної безпеки: поняття та загальна характеристика. *Юридична наука*. 2013. № 9. С. 80–87. URL: http://surl.li/iamvq.

140. 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.

141. Міщук Н. Кіберзлочинність як загроза інформаційному суспільству. *Вісник Львівського університету*. *Серія економічна*. 2014. № 51. С. 173–179.

142. Музика А. Інститут призначення покарання: поняття і загальна характеристика. *Право України.* 2011. № 9. С. 174–183.

143. Мягка М. М. Кіберпростір у вимірі комунікативного впливу. *Науковий вісник Міжнародного гуманітарного університету.*
Сер : Філологія. 2017. № 30 (2). С. 141–142. URL: http://surl.li/hyvqw.

144. На Житомирщині правоохоронці оголосили підозру злочинній групі у шахрайстві за схемою «друг просить у борг». Департамент кіберполіції Національної поліції України : веб-сайт. URL: http://surl.li/iaxhk

145. Найпоширеніші схеми кіберзлочинців та способи захисту від них. Навчально-науковий центр інформаційних технологій : веб-сайт. URL: http://surl.li/iaxow.

146. Науково-практичний коментар до Кримінального кодексу України. Юрист-консульт : Народний портал : веб-сайт. URL: https://legalexpert.in.ua/komkodeks/uk.html.

147. Науково-практичний коментар до КК України. URL: http://pravoznavec.com/ua/books/162/12264/28/.

148. Науково-практичний коментар до Кримінального кодексу України : веб-сайт. URL: http://mego.info/.

149. Науково-практичний коментар Кримінального кодексу України ТОМ 1. URL: http://mego.info/матеріал/стаття-67-обставини-які-обтяжують-покарання

150. Науково-практичний коментар до розділу XVII Особливої частини Кримінального кодексу України. URL: https://ips.ligazakon.net/document/KK004886.

151. Науково-практичний коментар Кримінального кодексу України онлайн том 2: веб-сайт. URL: http://mego.info/.

152. Науково-практичний коментар Кримінального кодексу України/ за заг. ред. О. М. Джужі, А. В. Савченка, В. В. Чернєя. Київ: Юрінком Інтер. 2016. 1064 с.

153. Науково-практичний коментар Кримінального кодексу України/ За заг. ред. Копотуна І. М. Київ: «К Н Т». 2023. 932 с.

154. Науково-практичний коментар Кримінального кодексу України/ за заг. ред. В. Я. Тація, В. П. Пшонки, В. І. Борисова, В. І. Тютюгіна. Харків. : Право, 2013. 1040 с.

155. Національна поліція України : офіційний веб-сайт Національної поліції України у Львівській області. URL: http://surl.li/iawas.

156. Нацполіція відкрила провадження за фактом DDoS-атак на українські сайти. Суспільні новини. Суспільне: веб-сайт. URL: http://surl.li/iaoab.

157. НБУ заборонив купувати криптовалюту за гривні. *Delj.ua*: веб-сайт. URL: http://surl.li/ibhrq/ .

158. 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/.

159. 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.

160. Носач Б. О. Віртуальний економічний простір сучасного суспільства: траєкторія соціальних трансформацій. *Гілея: науковий вісник.* - 2017 Вип. 119. С. 242-246. URL: http://nbuv.gov.ua/UJRN/gileya_2017_119_59.

161. Обережно! З'явилася нова шахрайська схема – виплата допомоги від НБУ. *Дебет-кредит:* веб-сайт. URL: http://surl.li/ianaz.

162. Овчаренко А. С. Правове регулювання віртуальних активів та криптовалют в Україні: сучасний стан і перспективи. *Юридичний науковий електронний журнал*. 2020. № 4. С. 200-201.

163. Огляд подій в сфері кібербезпеки, січень 2023. URL: https://www.rnbo.gov.ua/files/2023/NKCK/Cyber%20digest_january_2023_fin.pdf .

164. Окінавська хартія глобального інформаційного суспільства. URL: https://studies.in.ua/inform-pravo-shporu/2201-oknavska-hartya-globalnogo-nformacynogo-susplstva.html.

165. Окупанти пропонують неповнолітнім за гроші здавати позиції ЗСУ. URL: http://surl.li/iamyw.

166. Омельчук О. Загальні засади призначення покарання: законодавче регулювання та практика застосування. *Університетські наукові записки.* 2013. № 4. С. 360–366.

167. Офіційний вебсайт Інтерполу. URL: https://www.interpol.int/News-and-Events.

168. Офіційний вебсайт Массачусетського Технологічного Університету. URL: https://news.mit.edu/.

169. Панов М. І. Кримінальне правопорушення і його види : лекція. Харків: Право. 2019. С. 51. URL: http://surl.li/ibrzv.

170. Пащенко О. О. Закон про кримінальну відповідальність та кримінально-правові норми: питання соціальної обумовленості. *Вісник Луганського державного університету внутрішніх справ імені Е.О. Дідоренка*. 2017. № 4 (80). С. 104-111. URL: http://surl.li/hywln.

171. 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.

172. Піцик Ю. М. Кіберзлочини проти власності: кримінально-правова та кримінологічна характеристика. дис. к.ю.н: 12.00.08 / Київ. "ПрАТ", 2019. 285 с.

173. 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.

174. Поліцейські Києва викрили групу шахраїв, які під приводом продажу техніки ошукали близько 300 громадян. Департамент кіберполіції Національної поліції України : веб-сайт. URL: https://cyberpolice.gov.ua/news/policzejski-kyyeva-vykryly-grupu-shaxrayiv-yaki-pid-pryvodom-prodazhu-texniky-oshukaly-blyzko--gromadyan-4330/.

175. Поняття і характеристика кіберпростору. URL: http://www.elbib.in.ua/ponyattya-i-harakteristika-kiberprostoru-sotsiologiya-internetu.html.

176. Попович А. Г. Теоретичний аспект поняття штрафу як юридичної категорії. *Новітні кримінально-правові дослідження*: зб. наук. Миколаїв: Іліон. 2017. С. 141–144.

177. Попрас В. О. Штраф як вид покарання за кримінальним правом України: монографія. Харків: Право. 2009. 224 с.

178. Правоохоронці викрили учасників двох злочинних організацій у привласненні 10 млн грн з банківських карток громадян. Мультимедійна платформа іномовлення України : веб-сайт. URL: https://www.ukrinform.ua/rubric-society/3556513-sahrai-vikrali-z-bankivskih-kartok-10-miljoniv-obicauci-socviplati.html.

179. Предмет крадіжки : веб-сайт. URL:

https://crimpravo.com/pitannya-ta-vidpovidi/predmet-kradizhky.html.

180. Про авторське право і суміжні права : Закон України від 23.12.1993 № 3792-XII (редакція від 01.01.2023). URL: https://zakon.rada.gov.ua/laws/show/3792-12#Text.

181. Про адвокатуру та адвокатську діяльність: Закон України від 05 липня 2012 № 5076-VI (редакція від 03.08.2023). URL: https://zakon.rada.gov.ua/laws/show/5076-17#Text.

182. Про банки і банківську діяльність: Закон України від 07 грудня 2000 № 2121-III (редакція від 01.01.2024). URL: https://zakon.rada.gov.ua/laws/show/2121-14#Text.

183. Про валюту і валютні операції: Закон України від 21 червня 2018. № 2473-VIII (редакція від 01.01.2024). URL: https://zakon.rada.gov.ua/laws/show/2473-19#Text.

184. Про вищу освіту: Закон України від 01 липня 2014 № 1556-VII (редакція від 27.12.2023). URL: https://zakon.rada.gov.ua/laws/show/1556-18#Text.

185. Про віртуальні активи : Пропозиції Президента до Закону від 11 червня 2020. URL: http://surl.li/ibhac.

186. Про віртуальні активи : Пропозиції Президента до Закону від 17 лютого 2022 № 2074-IX. URL: http://surl.li/gtzs.

187. Про віртуальні активи: Закон України від 17 лютого 2022 № 2074-IX. URL: https://zakon.rada.gov.ua/laws/show/2074-20#Text.

188. Про внесення змін до Кримінального кодексу України щодо вдосконалення інституту спеціальної конфіскації з метою усунення корупційних ризиків при її застосуванні: Закон України від 10 листопада 2015 № 770-VIII. URL: https://zakon.rada.gov.ua/laws/show/770-19/ed20151126#n29.

189. Про внесення змін до Кримінального кодексу України щодо підвищення ефективності боротьби з кіберзлочинністю в умовах дії воєнного стану: Закон України від 24 березня 2022 № 2149-IX. URL: https://zakon.rada.gov.ua/laws/show/2149-20/ed20220403#n6.

190. Про доступ до публічної інформації: Закон України від 13 січня 2011 № 2939-VI (редакція від 08.10.2023). URL: https://zakon.rada.gov.ua/laws/show/2939-17#Text.

191. Про зареєстровані кримінальні правопорушення та результати їх досудового розслідування. Офіс Генерального прокурора: веб-сайт. URL: https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogo-rozsliduvannya-2.

192. Про затвердження Вимог щодо безпеки та захисту здоров'я працівників під час роботи з екранними пристроями : Наказ Міністерства соціальної політики України № 207 від 14 лютого 2018. URL: https://zakon.rada.gov.ua/laws/show/z0508-18#Text.

193. Про затвердження Положення про порядок здійснення операцій з чеками в іноземній валюті на території України: Постанова Правління Національного банку України від 29 грудня 2000. № 520. URL: https://zakon.rada.gov.ua/laws/show/z0152-01#Text.

194. Про затвердження Правил охорони праці під час експлуатації електронно-обчислювальних машин : Наказ Міністерства праці та соціальної політики України, комітет по нагляду за охороною праці України № 21 від 10 лютого 1999. URL: http://surl.li/ianiu.

195. Про захист інформації в інформаційно-комунікаційних системах : Закон України від 05 липня 1994 № 80/94-ВР. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text.

196. Про захист інформації в інформаційно-комунікаційних системах : Закон України від 05 липня 1994 № 80/94-ВР (редакція від 22.01.2014). URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text.

197. Про захист інформації в інформаційно-комунікаційних системах: Закон України від 05 липня 1994 № 80/94-ВР (редакція від 22.01.2022). URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text.

198. Про інформацію: Закон України від 02 жовтня 1992 № 2657-XII (редакція від 27.07.2023). URL:

https://zakon.rada.gov.ua/laws/show/2657-12#Text.

199. Про Національний банк України: Закон України від 20 травня 1999 № 679-XIV (редакція від 01.01.2024). URL: https://zakon.rada.gov.ua/laws/show/679-14#Text.

200. Про національну безпеку України : Закон України від 21 червня 2018 № 2469-VIII (редакція від 31.03.2023). *Верховна Рада України : офіційний веб-сайт*. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text.

201. Про нотаріат: Закон України від 02 вересня 1993 № 3425-XII (редакція від 30.01.2024). URL: https://zakon.rada.gov.ua/laws/show/3425-12#Text.

202. Про обіг криптовалют : Проєкт Закону від 06 жовтня 2017 № 7183. Верховна Рада України : веб-сайт. URL: http://surl.li/boqu/

203. Про основні засади забезпечення кібербезпеки України : Закон України від 05 жовтня 2017 р. № 2163VIII (редакція від 01.01.2024). *Верховна Рада України* : офіційний вебсайт. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text.

204. Про платіжні системи та переказ коштів в Україні: Закон України від 05 квітня 2001 № 2346-III (редакція від 01.08.2022). URL: http://surl.li/jris.

205. Про практику розгляду судами кримінальних справ про злочини, вчинені стійкими злочинними об'єднаннями. Постанова Пленуму Верховного Суду України № 13 від 23 грудня 2005. URL: http://surl.li/bvuha.

206. Про рішення Ради національної безпеки і оборони України : Указ Президента від 15 лютого 2008 року «Про хід реформування системи кримінальної юстиції та правоохоронних органів». URL: https://zakon.rada.gov.ua/laws/show/311/2008#Text.

207. Про рішення Ради національної безпеки і оборони України : Указ Президента України від 14 травня 2021 року : Про Стратегію кібербезпеки України. URL: http://surl.li/iamtt.

208. Про роботу банківської системи в період запровадження воєнного стану: Постанова Правління Національного банку України від 24 лютого 2022

року № 18. URL: http://surl.li/bumgr.

209. Продавав неіснуючі генератори: кіберполіція викрила зловмисника у шахрайстві. Департамент кіберполіції Національної поліції України: веб-сайт. URL: http://surl.li/iaxhv.

210. Поліщук В. Кіберзлочини та кібербезпека: боротьба з комп'ютерними злочинами і кібератаками. Н*аукові праці Міжрегіональної Академії управління персоналом. Юридичні науки*. 2023. № 66. С. 44-47. https://doi.org/10.32689/2522-4603.2023.3.7

211. 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.

212. Прудка Л. М. Психологічні особливості шахрайства в мережі Інтернет. *Південноукраїнський правничий часопис*. 2018. URL: http://www.sulj.oduvs.od.ua/archive/2018/2/10.pdf.

213. Пушкаренко П. І. Кіберзлочинність як новітній феномен тіньової економіки. URL: https://clck.ru/K5g9r.

214. Расизм і ксенофобія в Україні: реальність та вигадки. *Харківська правозахисна група*/ за ред. Б.Є. Захаров. Харків: Права людини. 2009. 192 с.

215. 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.

216. Рибка С. В. Кіберпростір, управління інфраструктурою, кібербезпека. *Стратегічна панорама.* 2015. № 1. С. 126-134. URL: http://nbuv.gov.ua/UJRN/Stpa_2015_1_17.

217. Ричка Д.О. Комп'ютерна фобія. Матеріали Всеукраїнської наукової інтернет-конференції «Вітчизняна наука на зламі епох: проблеми та перспективи розвитку»: Переяслав-Хмельницький, 2018. Вип.41. С. 87-88.

218. Рішення Арбузинського районного суду у справі № 467/1069/21. URL: https://reyestr.court.gov.ua/Review/102133515.

219. Рішення Деснянського районного суду м. Чернігова у справі № 750/4468/19. URL: https://reyestr.court.gov.ua/Review/82055604.

220. Рішення Кам`янець-Подільського міськрайонного суду у справі № 676/4712/21. URL: https://reyestr.court.gov.ua/Review/101616341.

221. Рішення Кіровського суду у справі № 404/4975/21 URL: https://reyestr.court.gov.ua/Review/103688801.

222. Рішення Ковельського міськрайонного суду у справі № 159/2149/17. URL: https://youcontrol.com.ua/ru/catalog/court-document/67836018/

223. Рішення Ковпаківського районного суду у справі № 592/4316/20. URL: https://reyestr.court.gov.ua/Review/89242851.

224. Рішення колегії 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.

225. 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, № 7-рп/2001.

226. Рішення Конституційного суду України у справі за конституційним поданням Уповноваженого Верховної Ради України з прав людини щодо відповідності Конституції України (конституційності) положення третього речення частини першої статті 13 Закону України "Про психіатричну допомогу" (справа про судовий контроль за госпіталізацією недієздатних осіб до психіатричного закладу) від 1 червня 2016 року. Справа № 1-1/2016.

227. Рішення Луцького міськрайонного суду у справі № 161/18959/20.

URL: https://reyestr.court.gov.ua/Review/93155890.

228. Рішення суду у справі № 676/1984/21. URL: https://reyestr.court.gov.ua/Review/96443215.

229. Рішення Ужгородського міськрайонного суду у справі № 308/11741/20. URL: https://reyestr.court.gov.ua/Review/93903445.

230. Рішення Ужгородського міськрайонного суду у справі № 308/4477/21. URL: https://reyestr.court.gov.ua/Review/99768721.

231. Рішення Франківського районного суду м. Львова № 465/2391/19. URL: https://reyestr.court.gov.ua/Review/85733514.

232. Рішення Хмельницького міськрайонного суду у справі № 686/26099/21. URL: https://reyestr.court.gov.ua/Review/101623083.

233. Русецький В. І. Теоретико-правовий аналіз понять «кіберзлочин» і «кіберзлочинність». *Право і безпека*. 2017. № 1 (64). С. 74–78.

234. Савченко А. В. Корупційні злочини (кримінально-правова характеристика): навч. посіб. Київ: Центр учбової літератури. 2016. 168 с.

235. 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.

236. 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.

237. 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.

238. СБУ затримала агента рф, який збирав дані для обстрілів на півдні Одещини. Служба безпеки України : веб-сайт. URL: http://surl.li/iamxa.

239. Селюк А. В. Розслідування комп’ютерних злочинів. Наук.-метод. посіб : за ред. А. В. Селюк. Київ.: Вид-во НА СБУ. 2010. 24 с.

240. 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.

241. Сідак В. С. Забезпечення інформаційної безпеки в країнах НАТО та ЄС: навч. посіб. Київ : КНТ. 2007. 160 с.

242. 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.

243. Скрипник В. Речі, обмежені в цивільному обороті, як об'єкти цивільних прав. *Підприємство, господарство і право*. 2018. № 1. С. 36–40.

244. Скулиш Є. Д. Міжнародно-правове співробітництво у сфері подолання кіберзлочинності. *Інформація і право*. 2014. № 1(10). С. 93–100.

245. Словник термінів з кібербезпеки : за заг. ред. О. В. Копана, Є. Д. Скулиша. Київ: ВБ «АванпостПрим». 2012. 214 с.

246. Служба безпеки затримала шпигунку ФСБ, яка намагалася проникнути в СБУ і стати «подвійним агентом». Служба безпеки України : веб-сайт. URL: http://surl.li/iamwb.

247. Служба безпеки України затримала адміністратора телеграм-каналу, який зняв та опублікував обстріл Бурштинської ТЕС. Одеса онлайн: веб-сайт. URL: https://odessa.online/sbu-zaderzhala-administratora-telegram-kanala-kotoryj-snyal-i-opublikoval-obstrel-burshtynskoj-tes/.

248. Смирнов А. А. Штраф у кримінальному праві України. *Право і безпека.* 2005. № 4. С. 168–172.

249. Соломко А. Г. Особливості кримінальної відповідальності за крадіжку. URL: https://conf.ztu.edu.ua/wp-content/uploads/2022/11/227.pdf.

250. Спронюк О. Поняття санкції у теорії права. *Історико-правовий часопис.* 2016. № 1(7). С. 234-240.

251. 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.

252. Статут Організації Об'єднаних Націй. URL: https://unic.un.org/aroundworld/unics/common/documents/publications/uncharter/UN%20Charter_Ukrainian.pdf.

253. Створення та використання шкідливих програм. URL: http://surl.li/fepzp.

254. Столяр О. Міжнародно-правові проблеми визначення та класифікації «кіберзлочинів». *In: Jurnalul juridic national: teorie şi practică.* 2017. № 4 (26). С. 185-188.

255. 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 веб-сайт Верховного суду України. URL: https://www.viaduk.net/clients/vsu/vsu.nsf/(documents)/AFB1E90622E4446FC2257B7C00499C02.

256. Судовий вирок у справі № 554/7741/22. ULR: https://reyestr.court.gov.ua/Review/106573069.

257. Тарасюк К. В. Прокурорський нагляд при розслідуванні комп'ютерних злочинів. *Комп'ютерно-інтегровані технології: освіта, наука, виробництво.* 2012. № 10. С. 178–181.

258. Терешкун О., Ілюшкін О. Соціальні мережі у сучасному суспільстві: психологічний аналіз. *Соціальна психологія. Український науковий журнал*. 2011. № 5. С. 86-95.

259. Тлумачний словник онлайн. 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.

260. Тітова В. І. Кіберзлочини, їх поняття та правова природа. International Electronic Scientific Journal "Science Online. URL: https://nauka-online.com/wp-content/uploads/2020/06/Titova.pdf

261. Туранський М. В. Пропагандистська кампанія Росії у підготовці

до анексії Кримського півострова. URL: http://surl.li/ibqcb.

262. У 2020 році до кіберполіції надійшло понад 30 тисяч звернень щодо шахрайств в Інтернеті. Департамент кіберполіції Національної поліції України: веб-сайт. URL: http://surl.li/gocxq.

263. У жінки вимагали гроші, погрожуючи розповсюдити в інтернеті її інтимні фото. *Тижневик Exo* : веб-сайт. URL: https://exo.in.ua/news/41358.

264. У Кремлі підгоряє. Російські хакери посилили атаки на інфраструктуру України. *Фокус*: веб-сайт. URL: https://focus.ua/uk/digital/553817-v-kremle-podgoraet-russkie-hakery-uzhestochili-ataki-na-infrastrukturu-ukrainu.

265. У Києві під виглядом правоохоронців та воєнкомів аферисти вимагали гроші у чоловіків. Юридичний вісник України: веб-сайт. URL: https://yvu.com.ua/u-kyyevi-pid-vyglyadom-pravoohorontsiv-ta-voyenkomiv-aferysty-vymagaly-groshi-u-cholovikiv/

266. Узагальнення судової практики розгляду справ про злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), автоматизованих систем та комп'ютерних мереж і мереж електрозв'язку. URL: https://www.viaduk.net/clients/vsu/vsu.nsf/(documents)/AFB1E90622E4446FC2257B7C00499C02

267. 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.

268. Узагальнення судової практики розгляду справ про адміністративні корупційні правопорушення та деякі злочини, передбачені розділом XVII Кримінального кодексу України. URL: http://surl.li/iaxin.

269. Українське кримінальне право. Підручник онлайн. URL: https://pidru4niki.com/1705100856179/pravo/zlochin_diyannya.

270. Українські діти можуть «здавати» окупантам позицій ЗСУ за грошову винагороду. Судово-юридична газета : веб-сайт. URL: http://surl.li/iamyw.

271. Федорчук І. М. Обставини, які обтяжують покарання за кримінальним правом України: монографія. Львів: ЛьвДУВС. 2017. 240 с. URL: http://surl.li/ibpsw.

272. Фейкові COVID-сертифікат в Україні: як каратимуть шахраїв?: веб-сайт. URL: https://www.dw.com/uk/feikovi-covid-sertyfikaty-v-ukraini-yaka-vidpovidalnist-zahrozhuie-shakhraiam/a-59626047.

273. 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 Сташиса В. В*., 9-10 липня 2015 р. Полтава, Харків. 2015. С. 98–103.

274. Філіпенко Т. А. Стан та наслідки комп'ютерної злочинності. *Цифрова платформа: інформаційні технології в соціокультурній сфері.* 2020. Том 3. № 1. С. 73–81. URL: http://surl.li/ibsbq.

275. Фішинг на платформі оголошень – викрили зловмисника. URL: http://surl.li/iaxiy.

276. Фріс П. Л. *Кримінальне право України. Загальна частина: підручник для студентів вищих навчальних закладів.* Київ: Атіка. 2004. 488с.

277. 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://ippi.org.ua/sites/default/files/12fvmsvv.pdf.

278. Хакери зламали твітер-акаунти Гейтса, Маска, Байдена і закликали перевести біткойни. Радіосвобода: веб-сайт. URL: http://surl.li/ibpzj.

279. Хахановський В. Г. Тлумачення та класифікація кримінальних правопорушень як кіберзлочинів. Інформація і право. 2020. № 2. С. 99–104.

280. Хілдрет С. А. Кібертероризм та кібервійна. Матеріали дослідницької служби Конгресу. Доповідь Дослідницької служби Конгресу. URL: https://nsarchive.gwu.edu/document/21678-document-03-steven-hildreth-congressional

281. Цивільний кодекс України від 06 січня 2003. № 435-IV. URL: https://zakon.rada.gov.ua/laws/show/435-15.

282. Час перевірити рівень кібербезпеки в медицині: веб-сайт. URL: https://datami.ua/kiberbezpeka-v-meditsini/.

283. Чекунов І. Г. Сучасні кіберзагрози. Кримінально-правова та кримінологічна класифікація і кваліфікація кіберзлочинів. *Право і кібербезпека.* 2012. № 2. С. 9–22.

284. Чепелєвий Н. В. Проблеми психологічної герменевтики: монографія за ред. Н. В. Чепелєвий. Київ. : *Вид-во Національного педагогічного університету ім. Н. П. Драгоманова*. 2009. 382 с.

285. Чокас Ю. С. Кіберзлочини проти власності: кримінально-правова та кримінологічна характеристика. URL: http://surl.li/iandg.

286. Чи варто боятися BDoS атаки? Що таке DDoS Booter/IP-стрессер? Інструменти для DDoS-атак.: веб-сайт. URL: https://www.cloudflare.com/learning/ddos/ddos-attack-tools/ddos-booter-ip-stresser/

287. Шапочка С. В. Класифікація шахрайства, що вчиняється з використанням комп'ютерних мереж (кібершахрайства). *Наука і правоохорона.* 2015. № 1. С. 159–165.

288. Шахраї взяли на ваше ім'я онлайн-кредит: що робити? Liga Zakon: веб-сайт. URL: https://jurliga.ligazakon.net/news/208174_shakhra-vzyali-na-vashe-mya-onlayn-kredit-shcho-robiti.

289. Шахрайство під виглядом інвестування у криптовалюту – у Києві

викрито злочинну групу. Офіс Генерального прокурора : веб-сайт. URL: http://surl.li/ibiyt.

290. Швиданенко Г. Диджиталізація – сучасний напрям розвитку інноваційного підприємництва. URL: https://core.ac.uk/download/pdf/197269051.pdf.

291. Шевчук Т. А. Розповсюдження наркотичних засобів, психотропних речовин або їх аналогів через мережу інтернет. URL: http://surl.li/ianbv.

292. Шемчук В. В. Кіберзлочинність як перешкода розвитку інформаційного суспільства в Україні. *Вчені записки ТНУ імені В.І. Вернадського.* Серія: юридичні науки. 2018. Том 29 (68). № 6. С. 121-123. URL: https://doi.org/10.32838/TNU-2707-0581/2018.6/21.

293. Шинкарецька Г. Г., Берман А. М. Цифровізація та проблема забезпечення національної безпеки. *Освіта і право*. 2020. № 5. С. 254–260.

294. Шкідливі програмні та технічні засоби : веб-сайт. URL: https://it-crime.at.ua/index/shkidlivi_programni_ta_tekhnichni_zasobi/0-34.

295. 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.

296. Що в Україні можна купити за криптовалюту. Фінансовий портал Мінфін : веб-сайт. URL: http://surl.li/hmhjk.

297. Що таке кодграббер і чи можна від нього захистити свій автомобіль - про авто : веб-сайт. URL: http://autopark.pp.ua/7934-scho-take-kodgrabber-chi-mozhna-vd-nogo-zahistiti-svy-avtomobl-pro-avto.html.

298. Що таке лог файли. *Hostiq* : веб-сайт. URL: http://surl.li/iaxlf.

299. Що таке послуга OLX Доставка?. Olx: веб-сайт. URL: http://surl.li/ovqo.

300. Що таке скімінг? : веб-сайт. URL: http://surl.li/ianrj.

301. Що таке токен на блокчейні. *Bankchart*: веб-сайт. URL: http://surl.li/ibivi.

302. Що таке фішинг? *Вікіпедія :* вебсайт. URL: https://uk.wikipedia.org /wiki/Фішинг.

303. Що таке шкідливе програмне забезпечення? : веб-сайт. URL: https://www.microsoft.com/de-de/.

304. Що таке DDoS-атака? Офіційний сайт державної служби спеціального зв'язку та захисту інформації України : веб-сайт. URL: https://cip.gov.ua/ua/faqs/sho-take-ddos-ataka.

305. Щур К. В. Призначення штрафу, як додаткового виду покарання. *Кримінально-правові та кримінологічні заходи протидії злочинності:* матеріали Всеукраїнської науково-практичної конференції. Одеса: ОДУВС. 2015.

306. 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.

307. 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.

308. Яцишин М. Ю. Використання сили у кіберпросторі в рамках міжнародного права. *Інформація і право*. 2018. № 4 (27). С. 22–31.

309. Abdul Raheem Fathima Shafana. Predictive Data Mining for Phishing Websites: *A Rule Based Approach. ournal of Information Systems & Information Technology* Vol. 5 N. 2 2020. P. 61-71. URL: http://surl.li/ibqcx.

310. Ahmmed F. Meaning and Nature of Cyber Crime. URL: https://www.academia.edu/41411512/Meaning_and_Nature_of_Cyber_Crime.

311. Aïmeur E., Schonfeld D. The ultimate invasion of privacy: Identity theft. *2011 9th Annual International Conference on Privacy, Security and Trust*.

2011. P. 24–31. URL: https://doi.org/10.1109/PST.2011.5971959.

312. Alin Teodorus Drăgan. Child Pornography and Child Abuse in Cyberspace. *Journal of legal studies*. 2018. Volume 21. № 35. P. 52 - 60. URL: https://www.researchgate.net/publication/326401361_Child_Pornography_and_Child_Abuse_in_Cyberspace.

313. 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.

314. Alyona Klochko, Mykola Kurylo, Oksana Kvasha, Zoia Zahynei and Mykola Logvinenko (2020). Combating crime in the banking sector as a method for ensuring its stability (evidence from Ukraine). *Banks and Bank Systems*, 15(1), 143-157. doi:10.21511/bbs.15(1).2020.14

315. Anahit P. Cyberwar. URL: https://www.academia.edu/35526558/Cyberwar_Anahit_Parzyan_pdf.

316. Analysis of the Cyber Attack on the Ukrainian Power Grid : веб-сайт. URL: https://web.archive.org/web/20180401121206/https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf.

317. Ante L. The Influence of Stablecoin Issuances on Cryptocurrency Markets. URL: http://surl.li/ibitn

318. 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/.

319. Armenia Criminal Code. URL: http://surl.li/hywpq.

320. Australia Income Tax Assessment Act 1997. № 40. 2022 and Act № 75. 2022. URL: https://www.legislation.gov.au/Details/C2022C00307.

321. Austria Criminal Code. URL: http://surl.li/hzcez.

322. B. Warf. Borders in Cyberspace. *Invisible Borders in a Bordered World.* DOI: 10.4324/9780429352515-15.

323. 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.

324. Bajaj S. Cyber fraud: a digital crime. *International Conference Information Systems* 2008. P. 147-153. URL: http://surl.li/iampj.

325. Barlow J. P. A Declaration of the Independence of Cyberspace. URL: https://www.eff.org/cyberspace-independence.

326. Barringer T., Roberts B. S. The Credit Card Fraud Act of 1984 Clarification, orFurther Confusion, of the Law of Credit Card Fraud? *American Business Law Journal*. № 24(3). P. 449–466. https://doi.org/10.1111/j.1744-1714.1986.tb00506.x.

327. Beer Sijpesteijn. Describing Cyberspace. URL:https://www.academia.edu/8234339/Describing_Cyberspace.

328. Berentsen A. The Case for Central Bank Electronic Money and the Non-case for Central Bank Cryptocurrencies. Federal Reserve Bank of St. Louis *:* веб-сайт. URL: http://surl.li/ibhki.

329. Bhattacharyya S., Jha S., Tharakunnel K., Westland, J. C. Data mining for creditcard fraud: A comparative study. *Decision Support Systems*. 2011. № 50(3). P. 602–613. https://doi.org/10.1016/j.dss.2010.08.008.

330. Binance : веб-сайт. URL: http://surl.li/bnjlr.

331. Biswap : веб-сайт. URL: https://biswap.org//

332. Bitcoin ATM Map. Coin ATM Radar : веб-сайт. URL: https://coinatmradar.com/.

333. Blikhar M. M. Administrative and legal provision of information security in the internet space. URL: http://surl.li/ibrxb.

334. Breen C. F. ALarge-Scale Measurement of Cybercrime Against Individuals. URL: http://surl.li/iavyy.

335. Canada Has Been Experimenting With A Digital Fiat Currency Called CAD-COIN. Forbes : веб-сайт. URL: http://surl.li/ibhqa.

336. Carstens A. Money in the Digital Age: What Role Central Banks? 2018. URL: https://www.bis.org/speeches/sp180206.htm.

337. Casillas M. G. Computer crimes in Mexico. Recognition in the

criminal laws of the Mexican entities. *Revista de Tecnología y Sociedad*. URL: http://www.udgvirtual.udg.mx/paakat/index.php/paakat/article/view/759.

338. Chek Point. Cyber security report 2021. URL: http://surl.li/ibrrs.

339. Code of Virginia Title 18.2 - Crimes and Offenses Generally. URL: https://law.lis.virginia.gov/vacode/title18.2/.

340. Cohen F. Computer Viruses: Theory and Experiments. *Computers & Security*. 1987. № 6. С. 22–35. https://doi.org/10.1016/0167-4048(87)90122-2.

341. Computer Fraud and Abuse Act (CFAA) in 1986. URL: https://www.nacdl.org/Landing/ComputerFraudandAbuseAct.

342. Computer Fraud and Abuse Act of 1986. Societal impact of the CFAA: How the Computer Fraud and Abuse Act shapes society as we know It. URL: http://surl.li/iiffx.

343. 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.

344. Computer Security Act of 1987. H.R.145. URL: https://www.congress.gov/bill/100th-congress/house-bill/145.

345. Council of Europe. Committee of Misisters. Recommendation No. r (89) 9 on 13 Stptember 1989. URL: http://surl.li/ibqcq.

346. Criminal Code in the version published on 13 November 1998 (Federal Law Gazette I, p. 3322), as last amended by Article 2 of the Act of 22 November 2021 (Federal Law Gazette I, p. 4906. URL: https://www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html.

347. Criminal Code of Canada (R.S.C., 1985, c. C-46). URL: https://laws-lois.justice.gc.ca/eng/acts/c-46/.

348. Criminal code of Georgia. URL: http://surl.li/hywqc.

349. Criminal Code of the Azerbaijan Republic. URL: http://surl.li/hywqq.

350. Criminal code of the Republic of Tajikistan. URL: https://cis-legislation.com/document.fwx?rgn=2324.

351. Criminal code of Turkmenistan. URL: http://surl.li/hzdpi.

352. Criminal Damage Act, 1991. Number 31 of 1991. URL: https://www.irishstatutebook.ie/eli/1991/act/31/enacted/en/print.

353. Criminal justice (theft and fraud offences) Act. 2001. Number 50 of 2001. URL: https://www.irishstatutebook.ie/eli/2001/act/50/enacted/en/pdf.

354. Crypto And Tax In Australia: Everything You Need To Know. Forbes : веб-сайт. URL: http://surl.li/ibhpf.

355. Cuff P. Distributed channel synthesis.. *Trans. Inf. Theory*. 2013. Vol. 59. № 11. P. 7071–7096.

356. D. Ghelerter. Cybercrime in the Developing World. *Conference: 2022 KSU conference on cybersecurity education, research and practice*. DOI: 10.32727/28.2023.10.

357. 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.

358. Definition of Cyber Crime. LawPage. URL: https://lawpage.in/cyber_laws/crime/definition-of-cyber-crime.

359. DGL.RU. На темной стороне Интернета: Что такое Dark Web и Deep Web? URL: https://clck.ru/K5gLD.

360. Dilanchiev A. Factors Influencing Cryptocurrency Adoption in Georgia. *Journal of Business*. 2022. Volume 11. № 2. DOI: 10.5281/zenodo.7628008.

361. 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.

362. Dr. Mike McGuire., Samantha Dowling. Cybercrime: A review of the evidence Summary of key findings and implications. *Home Office Research Report 75*. University of Surrey. 2013. P. 29–46.

363. Eduardo PerafanEduardo Perafan. Cyberspace: *A New Frontier*. URL: https://www.researchgate.net/publication/368954339_Cyberspace_A_New_Frontier.

364. Encyclopedia Britannica. Phreaking. URL: https://www.britannica.com/topic/phreaking.

365. 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.

366. Estonia Penal Code. URL: http://surl.li/hyxak.

367. Exchange rates. Best exchange: веб-сайт. URL: https://www.bestchange.com/.

368. Federico Neri, Paolo Geraci, Gianluca Sanna, Liviana Lotti. Online Police Station : a state-of-the-art Italian SemanticTechnology against cybercrime, URL: http://surl.li/ibqih.

369. Final stage of the Conference on Security and Cooperation in Europe Helsinki, 30 July–1August 1975. URL: http://surl.li/ibqah.

370. Financial crime and fraud in the age of cybersecurity. URL: http://surl.li/iaobj.

371. Financial Crime Guide: A firm's guide to countering financial crime risks (FCG). URL: https://www.handbook.fca.org.uk/handbook/FCG.pdf.

372. France Criminal Code. URL: https://www.equalrightstrust.org/ertdocumentbank/french_penal_code_33.pdf.

373. Fraud and related activity in connection with computers. *18 U.S. Code ¤ 1030.* URL: http://surl.li/hzdwf.

374. G7 Ise-Shima Leaders' Declaration. URL: https://www.mofa.go.jp/files/000160266.pdf.

375. Gagandeep Kaur Rosha. E- Crime Behaviour of Internet Users. *International Journal on Future Revolution in Computer Science & Communication Engineering.* Volume 3. № 11. P. 23–337. URL: http://surl.li/ibqdg.

376. Gakunu P. Reforming the Financial System in Sub-Saharan Africa: the (long) Way Ahead. Finance & Bien Commun. 2007. № 28. P. 139–146.

377. German hospital hacked, patient taken to another city dies. AP NEWS: вебсайт. URL: https://apnews.com/article/technology-hacking-europe-cf8f8eee1adcec69bcc864f2c4308c94

378. Germany Criminal Code. URL: https://www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html.

379. Gervais A. Is Bitcoin a Decentralized Currency. *Security & Privacy.* 2014. № 12. P. 256–270.

380. Gibson W. Burning. Chrome. Omni. 1982. URL: http://www.williamflew.com/omni46b.html.

381. Gibson W. Neuromancer. N.Y. 1984.

382. Glazkova L. V. Extremist Crimes Committed Using the Sphere of Telecommunications and Computer Information. URL: http://surl.li/ibsbf.

383. Goldman L. Interpreting the Computer Fraud and Abuse Act. URL: https://www.researchgate.net/publication/305850068_Interpreting_the_Computer_Fraud_and_Abuse_Act.

384. Goldman Z. K. Deterring Financially Motivated Cybercrime. Economic espionage. URL: http://surl.li/iavym.

385. Goldsmith J., Wu T. Who Controls the Internet?: Illusions of a Borderless World. *Faculty Books*. 2006. P. 175. URL: http://surl.li/ibqax.

386. 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.

387. Gonak I. Cryptocurrency as an object of investment. URL: http://surl.li/ibgvt.

388. Govil J. Ramifications of cyber crime suggestive. *Preventive measure Electro/Information Technology*. 2007. URL: http://surl.li/ibqgc.

389. 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.

390. Gregory B. W. The Community Cyber SecurityMaturity Model. 2007. URL: https://ieeexplore.ieee.org/abstract/document/4076571.

391. Habib A. ACFCS Special Contributor Report: Crowdfunding-An unorthodox way of Money Laundering? Definitely maybe. URL: http://surl.li/ibgrt.

392. Habr. Делаем deface сайта с помощью XSS: веб-сайт. URL: https://habr.com/ru/post/328276/.

393. Harmen van der Wilt. Chapter 1: Legal responses to transnational and international crimes: towards an integrative approach?. Monograph Chapter. 24 Nov 2017. URL: http://surl.li/ibqln.

394. History of virtual assets of Ukraine or something in the crypt : вебсайт. URL: http://surl.li/ibgtr.

395. How 4 Chinese Hackers Allegedly Took Down Equifax: веб-сайт. URL: https://www.wired.com/story/equifax-hack-china/.

396. 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/.

397. International strategy of cooperation on cyberspace. URL: https://www.chinadaily.com.cn/kindle/2017-03/02/content_28409210.htm.

398. James Angel. 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.

399. 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.

400. 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.

401. Jennifer Martin. Working with Cyberspace in the Life-Space. Relational Child and Youth Care Practice. 2011. Volume 24. № 1-2. URL: http://surl.li/ibryb.

402. Johannes Kaspar. Legal and empirical aspects of cybercrime in Germany. URL: http://surl.li/ibruf.

403. John Suler. Department of Psychology. Rider University. Lawrenceville. URL: http://users.rider.edu/~suler/psycyber/suler.html.

404. Joseph M. K. Computer Crimes: A Concise Module. URL: http://surl.li/ibsca.

405. Julia Hörnle. 5 Jurisdiction of the Criminal Courts in Cybercrime Cases in Germany and England. 2021. P. 115 URL: http://surl.li/ibrul.

406. K. Darbik. Cyberspace in a risk society. 2022. DOI: 10.35467/cal/151 808

407. K. Wan Fei Ma. COVID-19 and Cyber Fraud: Emerging Threats During the Pandemic. DOI: 10.13140/RG.2.2.18540.39042.

408. Kansas Criminal Statute of Limitations Laws. URL: https://www.ksrevisor.org/statutes/ksa_ch21.html.

409. Karresand. Separating Trojan horses, viruses, and worms - a proposed taxonomy of software weapons. Information Assurance Workshop. 2003. IEEE Systems, Man and Cybernetics Society. DOI: 10.1109/SMCSIA.2003.1232411.

410. Katie Farina. Cyber Crime: Identity Theft. URL: https://www.researchgate.net/publication/304188885_Cyber_Crime_Identity_Theft .

411. Katsh E. Law in a Digital World: Computer Networks and Cyberspace. *Villanova Law Review.* 1993. Vol. 38. Iss 2. P. 403 – 486.

412. Kester B., Castillo R., Wong T., Franklin L., Cook A., Alwan O., Leuteneker S. A research proposal - Social influence in virtual spaces: Social proof versus authority power. *Psi Beta Journal of Student Research: Brief Reports*. 2022. № 2(1). P. 60–64. https://doi.org/10.54581/TAQT6508.

413. Key Concepts of the Scientific Method. URL:

https://explorable.com/research-methodology

414. Kharytonenko I. H. The phenomenon of cybercrime in modern criminological theory. *Law Review of Kyiv University of Law*. URL: http://surl.li/ibscl.

415. 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.

416. 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.

417. 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.

418. 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.

419. Kweku K. A., Martin S. O, Hein S. V. Considerations Towards a Cyber CrimeProfiling System. 2008. URL: http://surl.li/ibqgv.

420. Latvia Criminal Code. URL: http://surl.li/hyxax.

421. 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.

422. 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.

423. Liepman M. James. Cyberspace: The Third Domain. *Homeland security digital library.* URL: https://www.hsdl.org/?view&doc=89385&coll=public.

424. Louisiana Laws Revised Statutes Title 14 - Criminal Law. URL: https://law.justia.com/codes/louisiana/2021/revised-statutes/title-14/.

425. Lukin S. Modern aspects of digitalization of public spaces. *Public Administration Aspects.* 2020. № 8(1 SI), P. 9193. https://doi.org/10.15421/152049.

426. 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.

427. M. Sikorski. 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.

428. Mahmoud Ahmed Darwish. Methodology of scientific research and its modern divisions according to withney, marquis, good and scates, and van dalen. URL: http://surl.li/ibsao.

429. Maja Živko. Psychological Aspects of Cyberspace. URL: http://surl.li/ibryu.

430. Margot Franois. Un enfoque geopolítico a los conflictos vinculados con larevolución digital. *Revista Telemática*. 2022. Vol. 21 № 3. P. 14–21.

431. Maria Bicudo. Mathematics Education Actualized in the Cyberspace: A Philosophical Essay. URL: http://surl.li/ibrxw.

432. 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.

433. Maria V. T. Conceptions of self-defense in the criminal law of the russia and the united states. *Humanities & Social Sciences Reviews*. 2019. № 7. P. 652-656.

434. Marietjie Havenga. Problem-based learning in a virtual space:

Affordances of active online learning. URL: http://surl.li/ibrxe.

435. 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.

436. Mohamed A, Geir M. K. Cyber Security and the Internet ofThings: Vulnerabilities, Threats, Intruders and Attacks. *Journal of CyberSecurity*. 2015. № 4. P. 65–88.

437. National Military Strategy for Cyberspace Operations. *Department of Defense.* URL: http://www.dod.gov/ pubs/foi/ojcs/07-F-2105doc1.pdf.

438. National security presidential directive/nspd - 23. White House. https://irp.fas.org/offdocs/nspd/nspd-54.pdf.

439. National security presidential directive/nspd - 54. White House. https://irp.fas.org/offdocs/nspd/nspd-54.pdf.

440. National Security Strategy. White House. URL: https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/national_security_strategy.pdf.

441. Ndirangu Ngunjiri. Technological Developments Influence the Cybercrime in Juja Sub-County. URL: http://surl.li/ibrzz.

442. New Zeland Crimes Act 1961. Public Act 1961. № 43. URL: https://www.legislation.govt.nz/act/public/1961/0043/latest/DLM327382.html.

443. 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.

444. O'Leary R. R. Europol Warns Zcash, Monero and Ether Playing Growing Role in Cybercrime. Coindesk: веб-сайт. URL: http://surl.li/ibjda.

445. Official Documents System of the United Nations. URL: http://surl.li/hyvue.

446. Onyshchenko S. The Mechanism of Information Security of the National Economy in Cyberspace. Proceedings of the 4th International Conference

on Building Innovations. URL: http://surl.li/ibrvi.

447. 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

448. Oxford dictionary of English. Oxford. URL: https://www.oxfordreference.com/display/10.1093/acref/9780199571123.001.0001/acref9780199571123;jsessionid=3230C69E7D1037479D75F4779A2A3CED.

449. Pancakeswap : веб-сайт. URL: https://pancakeswap.finance//

450. Patki A. B. Cyber Crime Information System for CyberethicsAwareness. *Department of Information Technology,Government of India*. 2003. URL: http://surl.li/ibqdg.

451. Patrick W. Franzese. Sovereignty in cyberspace: can it exist? *Air Force Law* Review. Vol. 64. URL: http://surl.li/ibqam.

452. Payments System Board Annual Report 2022. *Reserve bank of Australia*: веб-сайт. URL: http://surl.li/ibhop.

453. Penal Code of the Netherlands in 1881-03-03. URL: https://sherloc.unodc.org/cld/document/nld/1881/penal_code_of_the_netherlands.html.

454. 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.

455. Polyakova Y. A., Vorobyova O., Chertakova E., Olinder. Revisiting the formation of the legal status of cryptocurrency in the Russian legislation. *Amazonia Investiga*. 2019. № 28 (22). 711–718. URL: https://www.amazoniainvestiga.info/index.php/amazonia/article/view/824.

456. Portugal Criminal Code. URL: http://surl.li/hzcuq.

457. Potokin Y. N.. The influence of roman law on the formation and development of the romano-germanic legal family. URL: http://surl.li/ibrpv.

458. Pricewaterhouse Coopers : веб-сайт URL: https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threatintelligence/cyber-ye

ar-in-retrospect.html.

459. Prithivi Raj. Analysis of legal measures to control and prevent cyber crimes. *International Journal of Multidisciplinary Research and Development.* 2021. Volume 8 № 4. P. 16–19. URL: http://surl.li/ibqdu.

460. Protection of Children Act 1978. UK Public General Acts. URL: https://www.legislation.gov.uk/ukpga/1978/37/body.

461. Research Methods in Science. URL: https://sciencing.com/research-methods-in-science-12748094.html

462. Riczu Zs., Melypataki G., Mate D. A. Concepts of work: from Traditionalsocial-labor Ideas to Modern effects of Digital Transformation. *Journal of Digital Technologies and Law*. 2023. № 1(1). P. 175–190. https://doi.org/10.21202/jdtl.2023.7.

463. Rimma Aysina. Cyber socialization of youth in the information and communication space of the modern world: effects and risks. *Social Psychology and Society*. 2019. № 10. P. 42–57. URL: http://surl.li/ibrwq.

464. 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.

465. Rusetskyi A. A., Kutsolabskyi D.A. Theoretical and legal analysis of the concepts of cybercrimes and cybercrime. *Pravo i Bezpeka*. №. 1. P. 74–78.

466. 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.

467. Seagrave S. Lords of the Rim: the invisible empire of the overseas URL: http://surl.li/ibgsi.

468. Sehyeon Sim. *The Development of Digital Technologies and Cyber Security Threats*. URL: http://surl.li/ibrvy.

469. Senat Saliu's Lab. Forms Of Cybercrime And Prevention Of Cybercrime In The Republic Of Northern Macedonia. *Journal of Positive School*

Psychology. 2022. Vol. 6. №. 6. P. 9028–9039. URL: http://surl.li/ibscu.

470. Sexual Offences Act 1956. UK Public General Acts. URL: https://www.legislation.gov.uk/ukpga/Eliz2/4-5/69.

471. Shaaban Hussein. Brunschvik and Bachelard between philosophy and science, a critical study. 1993. P. 122–124.

472. Shalani A. A. Impact of Social Media-Related Cybercrimes and Preventive Precautions. *14th International Research Conference of General Sir John Kotelawala Defence University*. Ratmalana: Sri Lanka. 2021. P. 460-468.

473. Shevchuk V. S. Criminalistic didactics in modern conditions of war and digital technologies. *Proceedings of the 4th InternationalScientific and Practical Conference* Scientific Goals and Purposesin XXI Century. 2023. January 19-20. URL: http://surl.li/ibsax.

474. 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.

475. Siegel J. Meatspace is Cyberspace: The Pynchonian Post-human in Bleeding Edge. *Orbit: Writing around Pynchon*. 2016. № 4(2). P. 1–27. DOI: http://dx.doi.org/10.16995/orbit.187.

476. Silviu Jîrlăianu. Computer Related Forgery, Between Concept And Reality. *International conference knowledge-based organization.* 2015. № 21(2). URL: http://surl.li/ibqfz.

477. 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.

478. Siponen M. 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/.

479. Sitthipon T. A Review of Cryptocurrency in the Digital Economy. DOI: 10.25147/ijcsr.2017.001.1.124

480. Sony Hackers Have Flashed A 'Disturbing' New Warning On Staff Computers: веб-сайт. URL: https://web.archive.org/web/20150708173853/http://www.businessinsider.com/sony-hackers-new-warning-on-computers-2014-12.

481. Spain Criminal Code. URL: http://surl.li/hzdvw.

482. 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.

483. Stein Schjølberg. The History of Cybercrime. Volume 11 Publisher: Cybercrime Research Institute. Cologne GermanyEditor: Professor Marco Gercke. URL: https://www.researchgate.net/publication/313662110_The_History_of_Cybercrime_1976-2016.

484. Stephen M. Rodriguez. Uscybercom: A Centralized Command of Cyberspace. URL: http://surl.li/ibryk.

485. Steven Wei Ho. Is There Smart Money? How Information in the Commodity Futures Market Is Priced into the Cross-Section of Stock Returns with Delay. *Journal of Financial and Quantitative Analysis*. URL: http://surl.li/ibrzg.

486. Stevens B. Cyberspace and the state: towards a strategy for cyber power. Abington: Routledge. URL: http://surl.li/hyvsf.

487. Štitilis D. Kai kurie neteisėtos prieigos prie kompiuterinės informacijos kriminalizavimo aspektai. *Jurisprudencija*. 2003. № 47(39). P. 61.

488. Supply Chain Risk - the Cyber Attack URL: https://www.isg-one.com/industries/consumergoods/articles/supply-chain-risk-the-cyber-attack.

489. 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.

490. 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.

491. 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.

492. Tariq H. M. Interpol's crime contexts x-countries. URL: https://www.researchgate.net/publication/358604502_Interpol's_crime_context_x-countries.

493. Terrorism Act 2000. UK Public General Acts. URL: https://www.legislation.gov.uk/ukpga/2000/11/contents.

494. Thackrah J. R. Dictionary of Terrorism. *Taylor & Francis*. 2004. 318 p.

495. The Comprehensive National Cybersecurity Initiative. URL: https://obamawhitehouse.archives.gov/sites/default/files/cybersecurity.pdf.

496. The Criminal Code of Danish. Order No. 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.

497. 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.

498. The Financial Action Task Force : веб-сайт. URL: https://www.fatf-gafi.org/.

499. The MIT Press Journals. Terror and Play, or What Was Hacktivism? (Peter Krapp) URL: https://clck.ru/K5gJj.

500. Thomas W. Etablir la scurit juridique concernant le bitcoin. URL: http://surl.li/ibhud..

501. 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.

502. Twitter зазнав хакерської атаки. У мережу потрапили дані 200 млн користувачів. Forbes: веб-сайт. URL: http://surl.li/ibpxj.

503. Tykhonova O.V, Kholostenko A.V , Herasymenko L.V, Shevchuk O.O. and Akimov M.O, Comparative Analysis of Combating Economic Crimes In Ukraine and European Union, *International Journal of Management*, 11 (3), 2020, pp. 624–632.

504. U. Grigaitytė. Nusikaltimai virtualioje erdvėje – šiuolaikiniai Iššūkiai ir prevencijos galimybės. *Vilnius University Open Series*. DOI: 10.15388/OS.TMP.2020.13.

505. 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.

506. UK Public General Acts. *Computer Misuse Act.* 1990. URL: https://www.legislation.gov.uk/ukpga/1990/18/contents.

507. Uniswap : веб-сайт.URL: https://uniswap.org/.

508. 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.

509. Wall D. S.. Cybercrime: The transformation of crime in the information age. Oxford: Polity. URL: http://surl.li/iamhw.

510. Wasilewski J. Zarys definicyjny cyberprzestrzeni. *Przegląd Bezpieczeństwa Wewnętrznego.* 2013. № 9. P. 227.

511. Website Security Statistics Report. *WhiteHat Security*. 2019. 30 p. URL: https://info.whitehatsec.com/Website-Stats-Report-2019.html.

512. What Are the Different Types of Scientific Research? URL: https://akjournals.com/page/types-of-scientific-research.

513. 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.

514. Završnik A. Cybercrime definitional challenges and criminological

particularities. *Masaryk University Journal of Law and Technology*. P. 27. URL: https://core.ac.uk/download/pdf/230601102.pdf

515. Zhbankov V. A. Forensic computer-technical expertise in the investigation of customs crimes. URL: http://surl.li/ibsbu.

516. Azərbaycan Respublikasının Cinayət Məcəlləsi. URL: https://frameworks.e-qanun.az/46/f_46947.html

517. Қазақстан Республикасының Қылмыстық кодексі. URL: https://adilet.zan.kz/kaz/docs/K1400000226

Д О Д А Т К И

Додаток А

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Монографії

1. Dumchikov M., Bondarenko O., Peculiarities of criminal legal protection of cyberspace and combating cybercrimes : monograph. Germany : AP Lambert Academic Publishing GmbH & Co. KG, 2023. 73 p. (*Особистий внесок здобувача: проаналізовано нові форми вчинення кримінальних правопорушень у кіберпросторі, зокрема, крадіжку з платіжних карт – «кардинг», повернення оплати за отриманий товар – «рефандинг» та основні форми вчинення суспільно небезпечних діянь у кіберпросторі, предметом яких є віртуальні активи).*

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

Статті у фахових виданнях України категорії В

3. Думчиков М. О. Процеси диджиталізації і криміналістика:

ретроспективний аналіз. *Збірник «Криміналістика і судова експертиза.* 2020. Вип. 65. С. 100–108. DOI: https://doi.org/10.33994/kndise.2020.65.11.

4. Думчиков М. О., Рєпін Д. А. Легалізація доходів, отриманих злочинним шляхом, за допомогою використання віртуальної валюти (криптовалюти): кримінологічний та кримінально-правовий аспект. *Журнал східноєвропейського права*. 2020. № 82. С. 32–37. (*Особистий внесок здобувача: досліджено поняття «віртуальний актив» та надано його авторське визначення, окреслено й проаналізовано основні ознаки віртуальних активів, визначено, що саме підпадає під категорію віртуальних активів*).

5. Думчиков М. О., Пахомов В. В., Бондаренко О. С. Криміналістичні проблемні аспекти боротьби зі злочинами у кіберсфері. *Збірник «Криміналістика і судова експертиза*. 2020. № 1. С. 18–22. (*Особистий внесок здобувача: надано рекомендації щодо вдосконалення нормативно-правової бази з питань забезпечення кібербезпеки, здійснено розмежування понять «комп'ютерний злочин» і «кіберзлочин», здійснено криміналістичну типологізацію кримінальних правопорушень у кіберпросторі*).

6. Dumchykov M. O., Bondarenko O. S. Criminological aspects of combatting money laundering in cyberspace. *Legal Horizons*. 2021. № 14. P. 105–110. (*Особистий внесок здобувача: проведено аналіз криміналістичної характеристики легалізації відмивання злочинних доходів у кіберпросторі, зазначено основні способи легалізації майна, отриманого злочинним шляхом, за допомогою віртуальних активів*).

7. Думчиков М. О., Бондаренко О. С. Кримінологічні аспекти протидії легалізації корупційних доходів у кіберпросторі. *Правові горизонти*. 2021. № 14. С. 105–110. (*Особистий внесок здобувача: названо основні напрями вдосконалення методів забезпечення у сфері протидії й попередження легалізації прибутків, пов'язаних із злочинністю в кіберпросторі, виокремлено та проаналізовано основні способи легалізації*

злочинних доходів за допомогою віртуальних активів).

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

9. Думчиков М. О., Шевцов Я. А. До проблеми визначення поняття та ознак кіберзлочинів. *Журнал східноєвропейського права*. 2022. № 104. С. 12–22. (*Особистий внесок здобувача: визначено специфічні ознаки кримінальних правопорушень у кіберпросторі, детально проаналізовано такі ознаки, як анонімність і територіальна складова*).

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

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

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

13. Думчиков М. О., Каріх І. В. Становлення та генеза кримінальної відповідальності за кримінальні правопорушення у кіберпросторі на теренах України. *Юридичний науковий електронний журнал*. 2022. № 5. С. 476–478. DOI: https://doi.org/10.32782/2524-0374/2022-5/113. (*Особистий внесок здобувача: проаналізовано основні етапи становлення злочинності в кіберпросторі на теренах України*).

14. Думчиков М. О., Малетов Д. В. Загальна характеристика та види розкрадань шляхом використання інформаційних технологій як одного з

найпоширеніших видів кримінальних правопорушень у кіберпросторі. *Юридичний науковий електронний журнал*. 2022. № 7. С. 278–28. DOI: https://doi.org/10.32782/2524-0374/2022-8/60. (*Особистий внесок здобувача: дослідження можливості комп'ютерно-технічної експертизи як важливої допомоги в розкритті та розслідуванні кримінальних правопорушень, пов'язаних із розкраданнями коштів із банківських карт, розкрито сутність «кардингу» як найпопулярнішого кримінального правопорушення, пов'язаного з викраденням безготівкових коштів*).

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

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

17. Думчиков М. О. Поняття та ознаки кіберпростору, які роблять його привабливим для вчинення кримінальних правопорушень в сфері комп'ютерної інформації. *Юридичний науковий електронний журнал*. 2022. № 3. С. 195–197. DOI: https://doi.org/10.32782/2524-0374/2022-3/44.

18. Думчиков М. О., Каріх І. В. Зарубіжний досвід протидії кримінальним правопорушенням проти власності, вчиненим із використанням інформаційно-телекомунікаційних технологій. *Прикарпатський юридичний вісник*. 2023. № 2. С. 55-61. (*Особистий внесок здобувача: окреслено основні підходи до встановлення кримінальної відповідальності за вчинення кримінальних правопорушень у кіберпросторі проти власності за законодавством зарубіжних держав, виокремлено позитивний досвід кримінально-правової охорони кіберпростору зарубіжних держав від зовнішніх та внутрішніх посягань*).

19. Думчиков М. О., Каріх І. В. Неправомірний вплив на

інформаційну інфраструктуру України. *Юридичний науковий електронний журнал*. 2023. № 5. С. 111–116. (*Особистий внесок здобувача: визначено основні фактори та загрози державній інформаційній інфраструктурі, що може бути об'єктом учинення суспільно небезпечного діяння, запропоновано підходи до вдосконалення нормативно-правової системи кримінально-правової охорони державної інфраструктури України*).

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

Статті в зарубіжних періодичних наукових виданнях юридичного спрямування

21. Pakhomov V., Bondarenko O., Dumchikov M. Criminal legal characteristic of social engineering as a way of committing fraud. *Legea si Viata*. 2019. № 4/2. P. 149–153. (*Особистий внесок здобувача: визначено значення соціальної інженерії під час учинення кримінальних правопорушень у кіберпросторі, проаналізовано основні суспільно небезпечні діяння, вчинювані в кіберпросторі за допомогою методів соціальної інженерії*).

22. Думчиков М. О., Пахомов В. В. Кіберзлочинність як новітній феномен та джерело високого рівня суспільної небезпеки. *Visegrad Journal on Human Rights*. 2021. № 2. С. 333–340. (*Особистий внесок здобувача: здійснено аналіз кримінальних правопорушень, регламентованих XVI розділом Особливої частини Кримінального кодексу України, визначено їх специфічні характеристики, запропоновано криміналізувати нові види кримінальних правопорушень у кіберпросторі).*

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

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

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

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

26. Dumchikov M., Kononenko N., Batsenko L., Halenin R., Hlushchenko N. Issues of regulating cryptocurrency and control over its turnover: international experience. 2020, 10–20 July. Vol. 9. Issue 31. DOI: https://doi.org/10.34069/AI/2020.31.07.1. (**WoS**). *(Особистий внесок здобувача: надане авторське розуміння поняття криптовалюта, визначено основні схеми використання криптовалюти в протиправній діяльності, окреслено та охарактеризовано основні ознаки криптовалюти, проаналізовано зарубіжні підходи до регулювання криптовалют у зарубіжних державах*).

27. Dumchikov M., Yunin O., Nestor N., Borko A., Yermenchuk O. Criminological and forensic characteristics of forms of embezzlement committed through the use of information technology. *Amazonia Investiga*. 2021. № 10. P. 131–140. DOI: https://doi.org/10.34069/AI/2021.41.05.13. (**WoS**). (*Особистий внесок здобувача: визначено та проаналізовано кримінальні правопорушення, які можуть вчиняти за допомогою інформаційних технологій, як засіб учинення кримінального правопорушення, порівняно системи кримінально-правової охорони кіберпростору України та зарубіжних держав, зокрема, країн Європейського Союзу та Сполучених Штатів Америки*).

28. Dumchikov Mykhailo, Bondarenko Olga, Utkina Maryna. Cybercrime as a Threat to the National Security of the Baltic States and Ukraine: The Comparative Analysis. *International Journal of Safety and Security Engineering*. 2022. № 4. P. 10. DOI: https://doi.org/10.18280/ijsse.120409. (**Scopus**). (*Особистий внесок здобувача: визначено основні загрози для України та країн Балтії у сфері забезпечення кібербезпеки, запропоновано варіанти протидії наявним кіберзагрозам, на підставі аналізування позитивного досвіду країн Балтії запропоноване вдосконалення системи кримінально-правової охорони кіберпростору*).

29. Dumchikov M., Fomenko O., Pakhomov V., & Kabenok Y. The essence and classification of cybercrime in the field of computer information. *Amazonia Investiga.* 2022. № 11 (51). P. 291–299. DOI: https://doi.org/10.34069/AI/2022.51.03.29. (**WoS**). (*Особистий внесок здобувача: здійснено класифікацію кримінальних правопорушень у кіберпросторі, проаналізовано найбільш суспільно небезпечні кримінальні правопорушення, які вчиняються у світі, на основі позитивного зарубіжного досвіду, запропоновано зміни до низки статей Особливої частини Кримінального кодексу України*).

30. Dumchikov M., Horobets N., Honcharuk V., Dehtiar R. Digital Currency as a Subject of Economic Criminal Offenses. *Law, State and Telecommunications Review*
[S. l]. 2022. Vol. 14, No. 1. P. 20–30. DOI: 10.26512/lstr.v14i1.38676. (**Scopus**). (*Особистий внесок здобувача: окреслено поняття «віртуальний актив», проаналізовано кримінальні правопорушення, де віртуальні активи можуть бути предметом кримінального посягання, виокремлено та проаналізовано способи легалізації майна, отриманого злочинним шляхом, за допомогою цифрової валюти*).

31. Dumchikov M. Reznik O. Bondarenko O. Peculiarities of countering legalization of criminal income with the help of virtual assets: legislative regulation and practical implementation. Journal of Money Laundering Control.

2022. DOI: 10.1108/JMLC-12-2021-0135. **(Scopus та WoS).** (Особистий внесок здобувача: визначено та охарактеризовано основні способи легалізації злочинних доходів за допомогою віртуальних активів, проаналізовано нормативні підходи до вдосконалення системи протидії легалізації майна, отриманого злочинним шляхом, за допомогою віртуальних активів).

Тези наукових доповідей

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

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

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

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

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

С. 338–341.

37. Думчиков М. О. Інтернет-шахрайство у сфері комп'ютерної інформації як об'єкт криміналістичного аналізу. *Актуальні питання судової експертології, криміналістики та кримінального процесу* : тези доповідей. Київ : Ліра-К, 2021. С. 108–111.

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

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

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

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

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

доповідей. Київ, 2022. С. 221-225.

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

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

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

46. Думчиков М. О. Кіберзлочини в сфері комп'ютерної інформації: поняття та види. *Актуальні питання юридичної науки та практики : зб. наук. праць студ. та молодих вчених* : тези доповідей. Хмельницький : Вид-во МАУП, 2022. С. 73-77.

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

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

Додаток Б

АНКЕТА

для громадян України (300 осіб)

з метою з'ясування їх думки з питань кримінально-правової охорони кібернетичного простору в Україні.

Шановний учаснику анкетування!

Пропонуємо Вам взяти участь в анкетуванні щодо кримінально-правової охорони кіберпростору в Україні.

Дякуємо Вам за допомогу в проведенні дослідження!

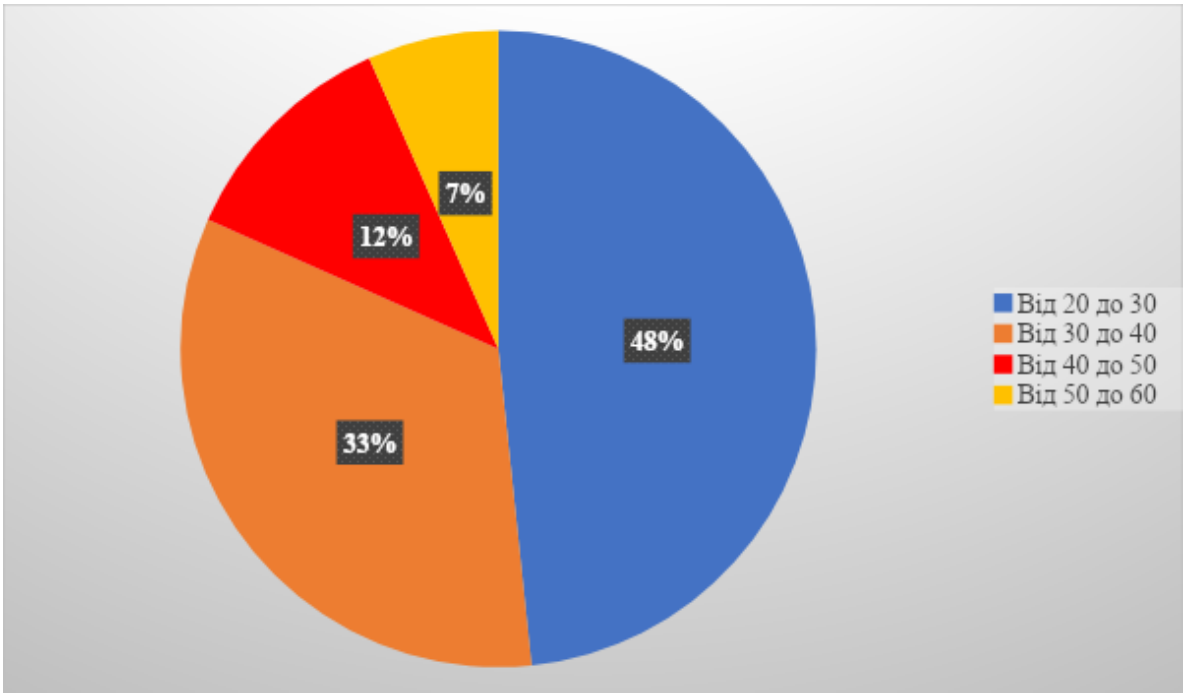
1. Вкажіть ваш вік.

A. Від 20 до 30.

B. Від 30 до 40.

C. Від 40 до 50.

D. Від 50 до 60.

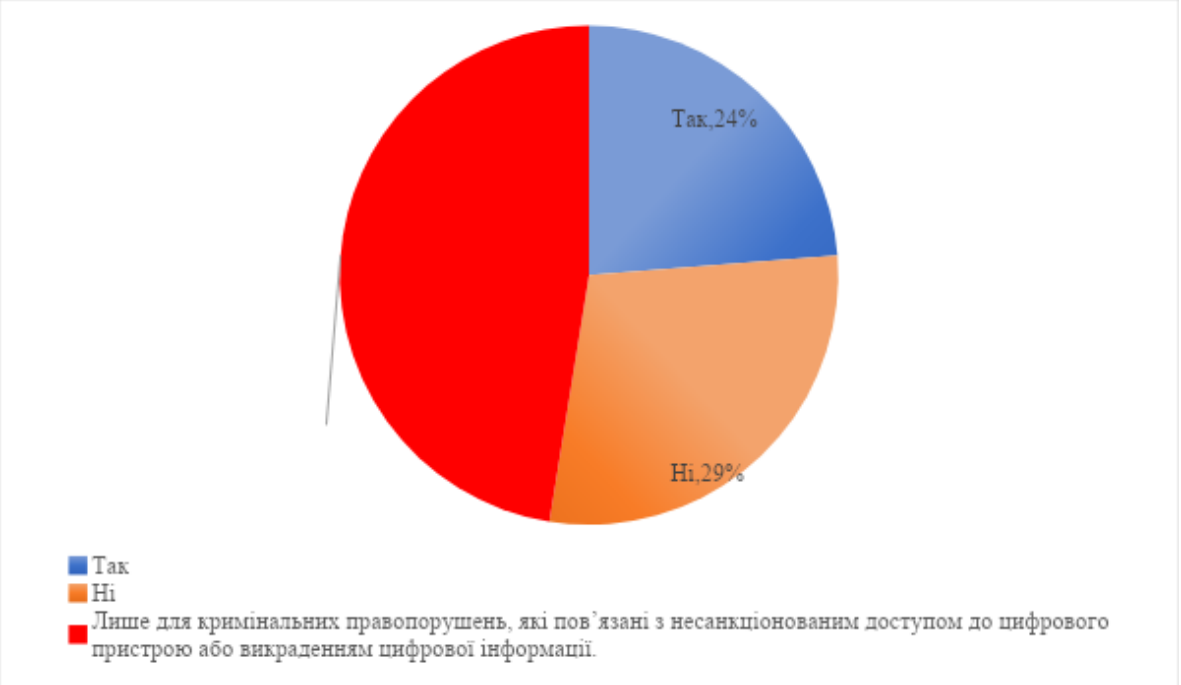


2. На вашу думку, чи може кібернетичний простір виступати місцем вчинення кримінальних правопорушень?

A. Так.

B. Ні.

C. Лише для кримінальних правопорушень, які пов’язані з несанкціонованим доступом до цифрового пристрою або викраденням цифрової інформації.



3. На вашу думку, які основні причини та умови існування злочинності у кібернетичному просторі?

A. Анонімність користувачів кібернетичного простору (12 осіб, 4 % з усіх опитаних).

B. Транскордонний характер такої злочинності (22 особи, 7 % з усіх опитаних).

C. Можливість одержання великих прибутків від заняття такою діяльністю (3 особи, 1 % з усіх опитаних).

D. Відсутність чіткого нормативного регулювання кібернетичного простору (5 осіб, 2 % з усіх опитаних).

E. Бездіяльність правоохоронних органів (8 осіб, 3 % з усіх опитаних).

F. Відсутність спеціальних знань у правоохоронних органів щодо розслідування кримінальних правопорушень у кібернетичному просторі (8

осіб, 3 % з усіх опитаних).

G. Недосконаліть закону про кримінальну відповідальність, який встановлює відповідальність за вчинення кримінальних правопорушень у кібернетичному просторі (7 осіб, 2 % з усіх опитаних).

H. Усі перелічені варіанти (235 осіб, 78 % з усіх опитаних).

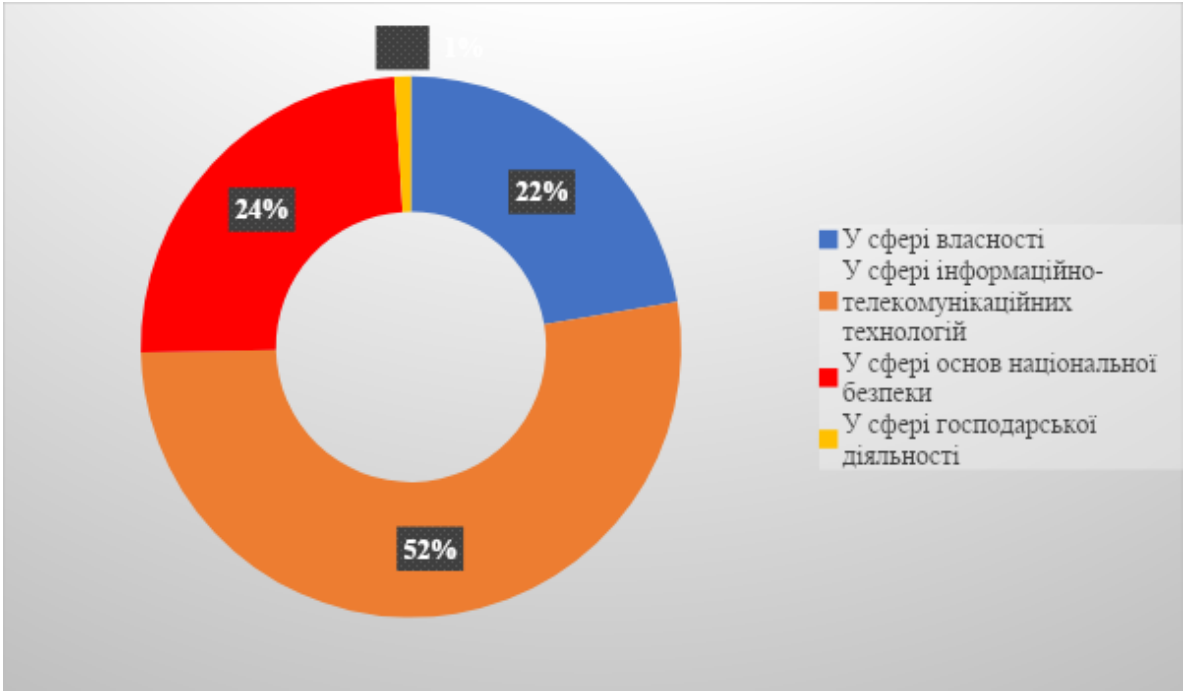
4. В якій сфері, на вашу думку, найчастіше вчиняються кримінальні правопорушення у кібернетичному просторі?

A. У сфері власності (крадіжка, шахрайство).

B. У сфері інформаційно-телекомунікаційних технологій та комп'ютерної інформації (злам, блокування, несанкціоноване втручання).

C. У сфері основ національної безпеки (кібератаки на урядовий сектор).

D. У сфері господарської діяльності (легалізація грошових коштів).

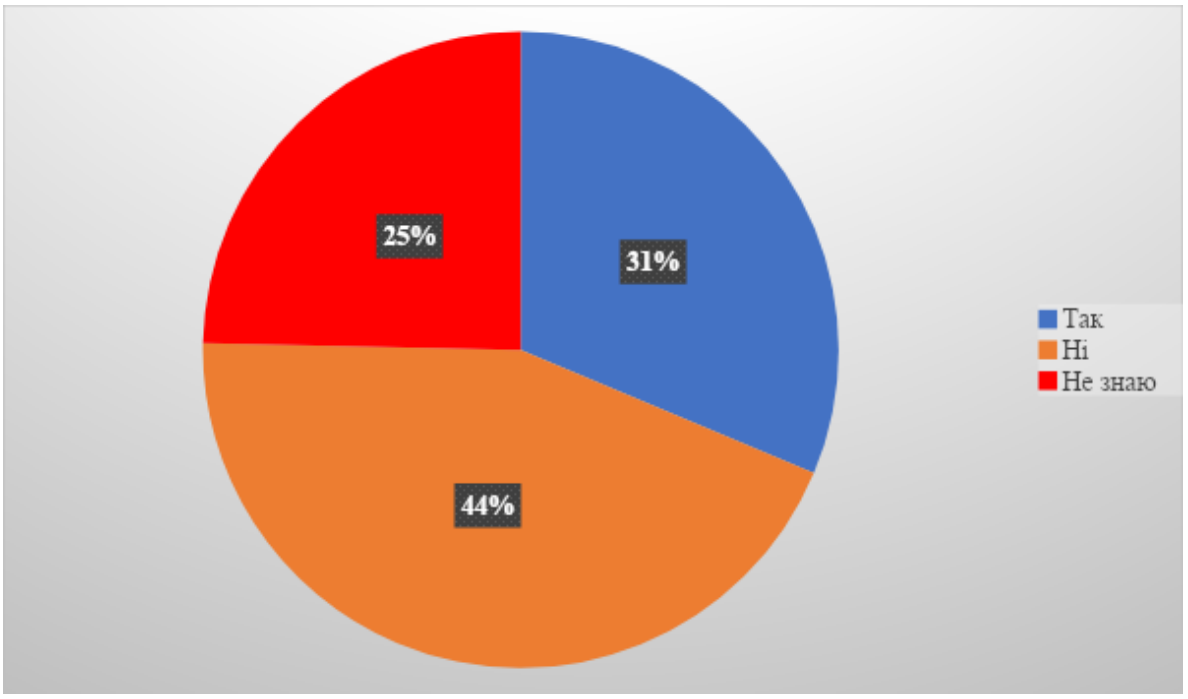


5. Чи були проти вас скоєно кримінальне правопорушення у кібернетичному просторі? Якщо так, то яке саме?

A. Так

B. Ні

C. Не знаю



5.1. Якщо так, то жертвою якого кримінального правопорушення у кібернетичному просторі ви стали?

A. Телефонний скамінг.

B. Шахрайство у соціальних мережах.

C. Викрадення персональних даних.

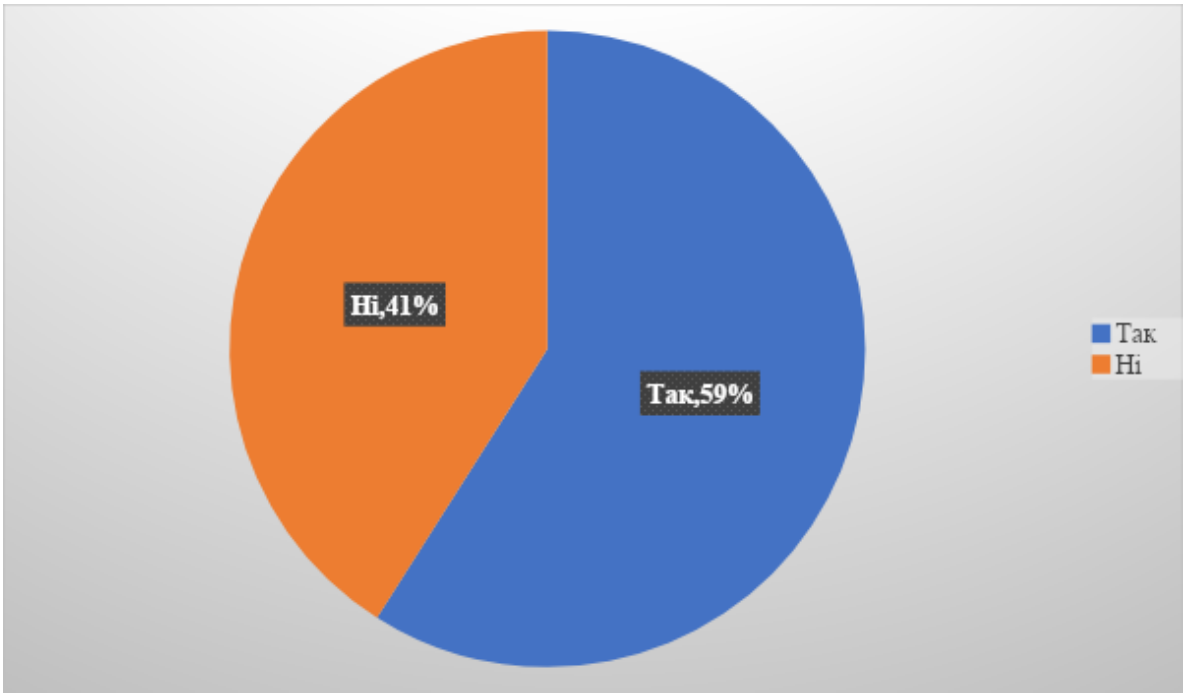
D. Злам цифрового пристрою або інформаційно-телекомунікаційної мережі.

6. На вашу думку, чи можливе вчинення крадіжки (стаття 185

Особливої частини Кримінального кодексу України) в кібернетичному просторі?

A. Так, можливо

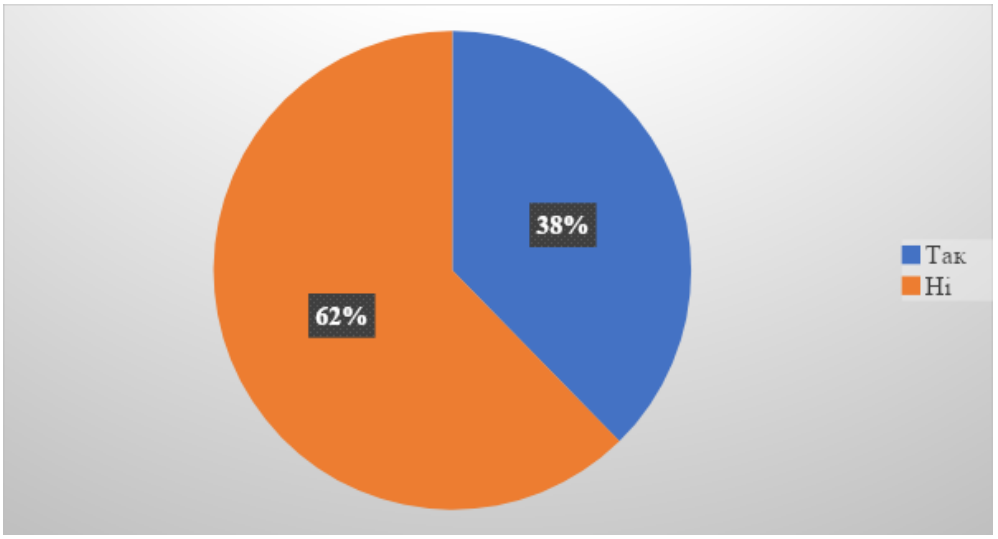
B. Ні, предметом крадіжки можуть виступати лише речі матеріального світу



7. На вашу думку, чи можливе вчинення шахрайства шляхом обману або зловживання довірою у кібернетичному просторі?

A. Так, можливе

B. Ні, не можливе



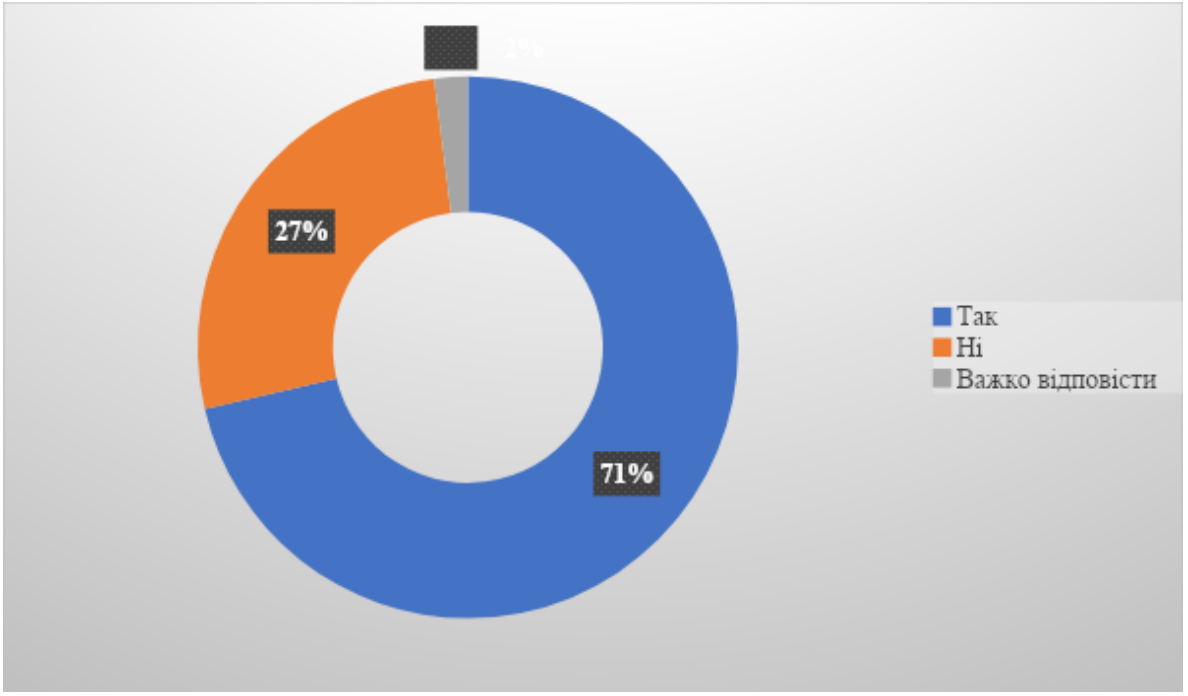
8. На вашу думку, чи може погроза знищення, пошкодження,

блокування або модифікація інформації розглядатися, як спосіб вчинення вимагання (стаття 189 Особливої частини Кримінального кодексу України)

A. Так

B. Ні

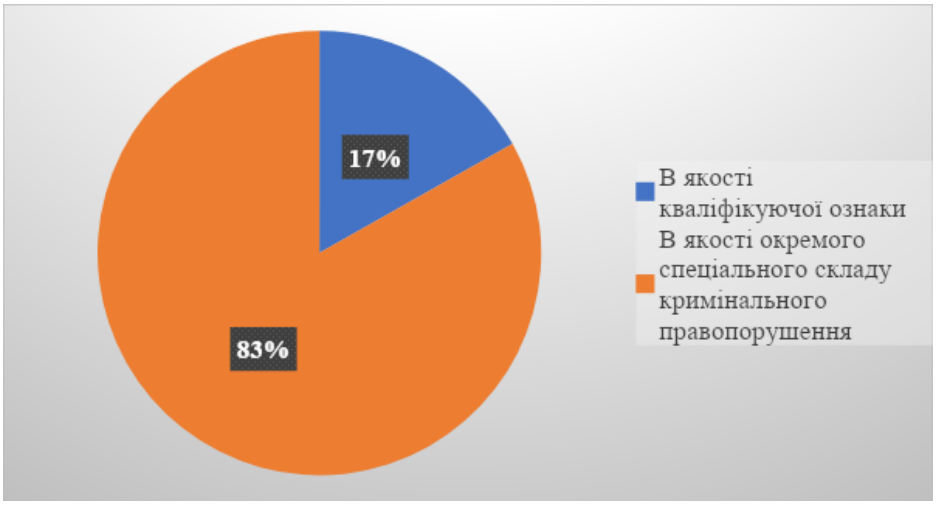
C. Важко відповісти



8.1 Якщо так, то яким чином це повинно бути відображено в чинному Кримінальному кодексі України?

A. В якості кваліфікуючої ознаки (у статті 189).

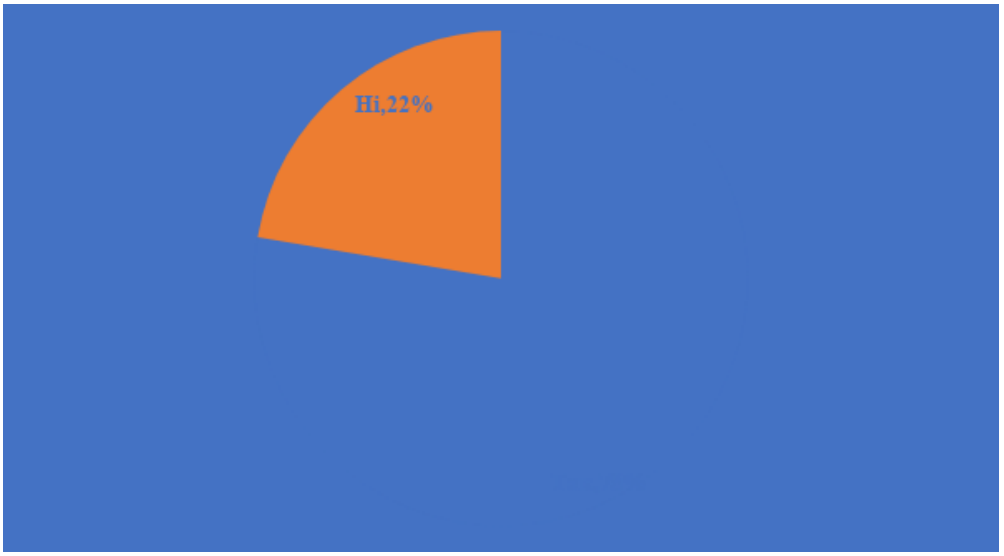
B. В якості окремого спеціального складу кримінального правопорушення.



9. На вашу думку, чи можуть віртуальні активи (криптовалюти) бути предметом крадіжки?

A. Так

B. Ні



9.1 Якщо так, то яким чином це повинно бути відображено в чинному Кримінальному кодексі України?

A. В якості кваліфікуючої ознаки в рамках статті 185 Особливої частини Кримінального кодексу України (крадіжка).

B. В якості кваліфікуючої ознаки в рамках статті 361 Особливої частини Кримінального кодексу України (несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж).

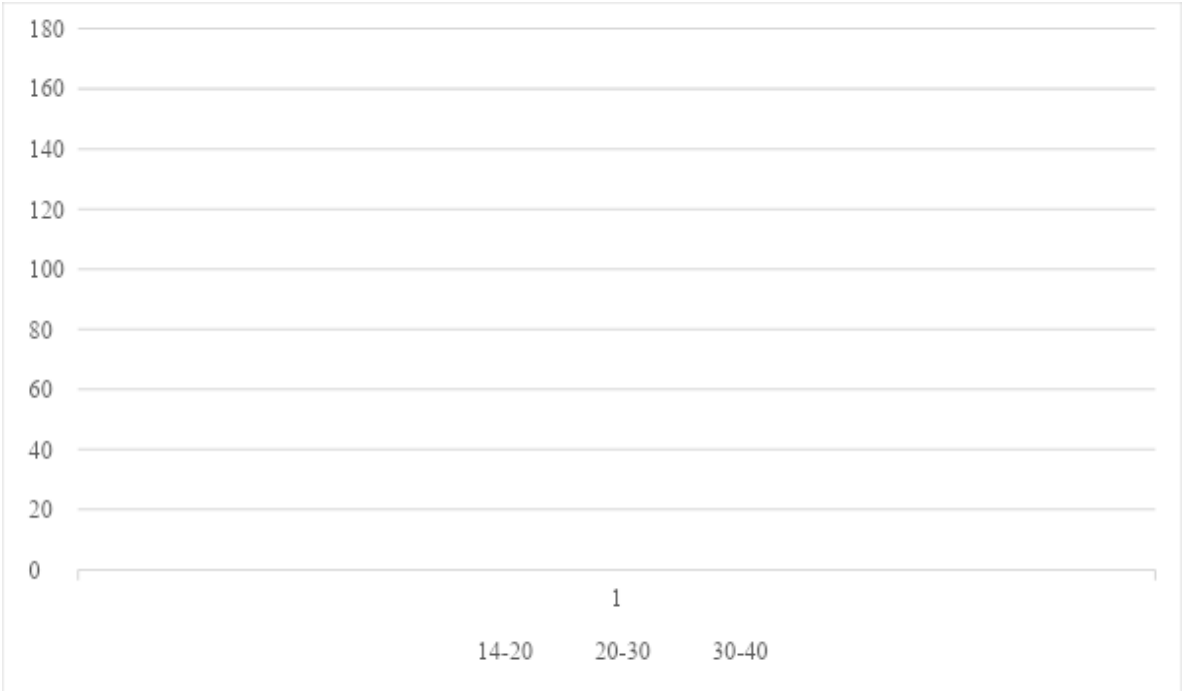
C. В якості спеціального складу кримінального правопорушення.

10. На вашу думку, який середній вік осіб, які вчиняють кримінальні правопорушення у кібернетичному просторі?

A. 14-20.

B. 20-30.

C. 30-40.

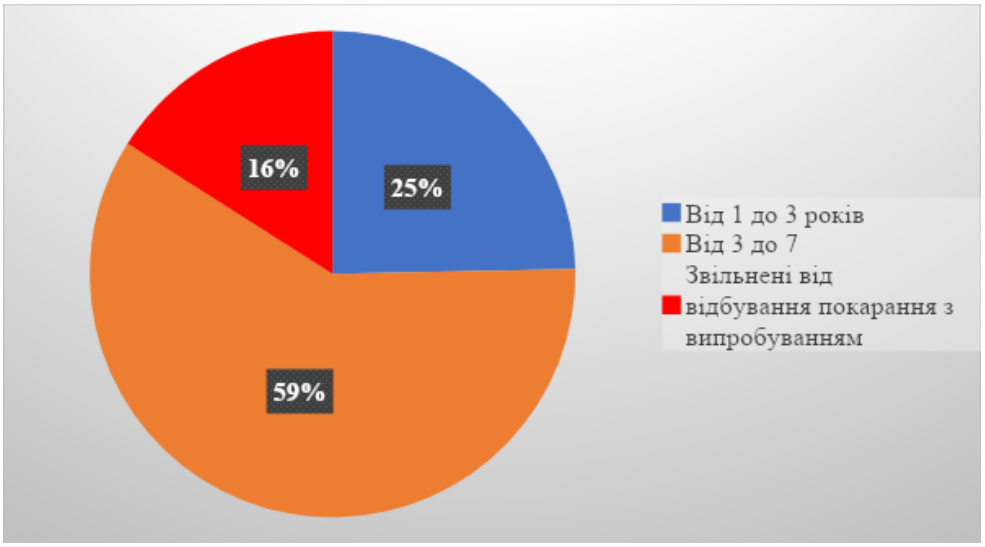


11. На вашу думку, який середній строк призначення судом покарання у вигляді позбавлення волі за вчинення кримінальних правопорушень у кібернетичному просторі?

A. Від 1 до 3 років.

B. Від 3 до 7.

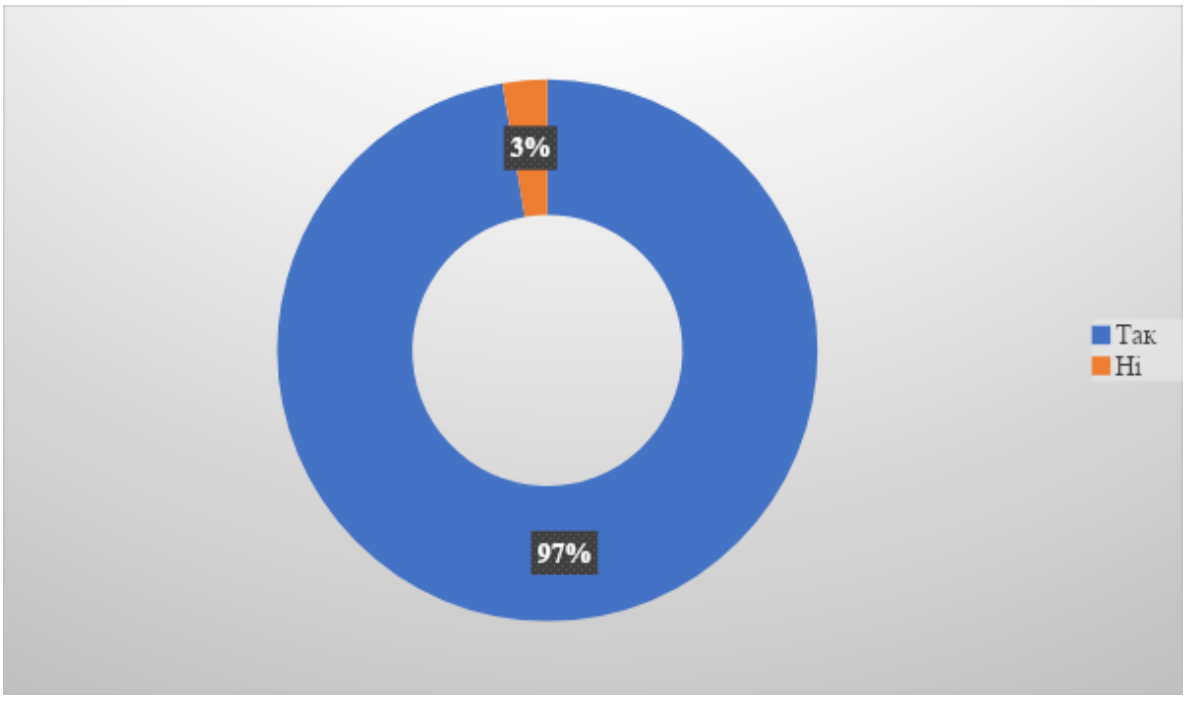
C. Звільнені від відбування покарання з випробуванням.



12. Чи вважаєте ви за доцільне внесення обставиною, що обтяжує вчинення кримінального правопорушення, предметом якого є інформаційна інфраструктура державного критичного значення?

A. Так.

B. Ні.



13. На вашу думку, яке кіберзалежне кримінальне правопорушення вчиняється найчастіше?

A. Несанкціоноване втручання в роботу цифрового пристрою,

вчинене фізично (10 осіб, 3 % з усіх опитаних).

B. Несанкціоноване втручання в роботу цифрового пристрою, вчинене дистанційно (41 особа, 14 % з усіх опитаних).

C. Поширення шкідливого (вірусного) програмного забезпечення (72 особи, 24 % з усіх опитаних).

D. Несанкціоновані дії з інформацією, яка оброблюється в інформаційно-телекомунікаційних технологіях, системах або мережах, або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї (11 осіб, 4 % з усіх опитаних).

E. Порушення правил експлуатації інформаційно-телекомунікаційних технологій, систем і мереж (1 особа, 1 % з усіх опитаних).

F. Масове розповсюдження повідомлень електрозв'язку – спам (120 осіб, 40 % з усіх опитаних).

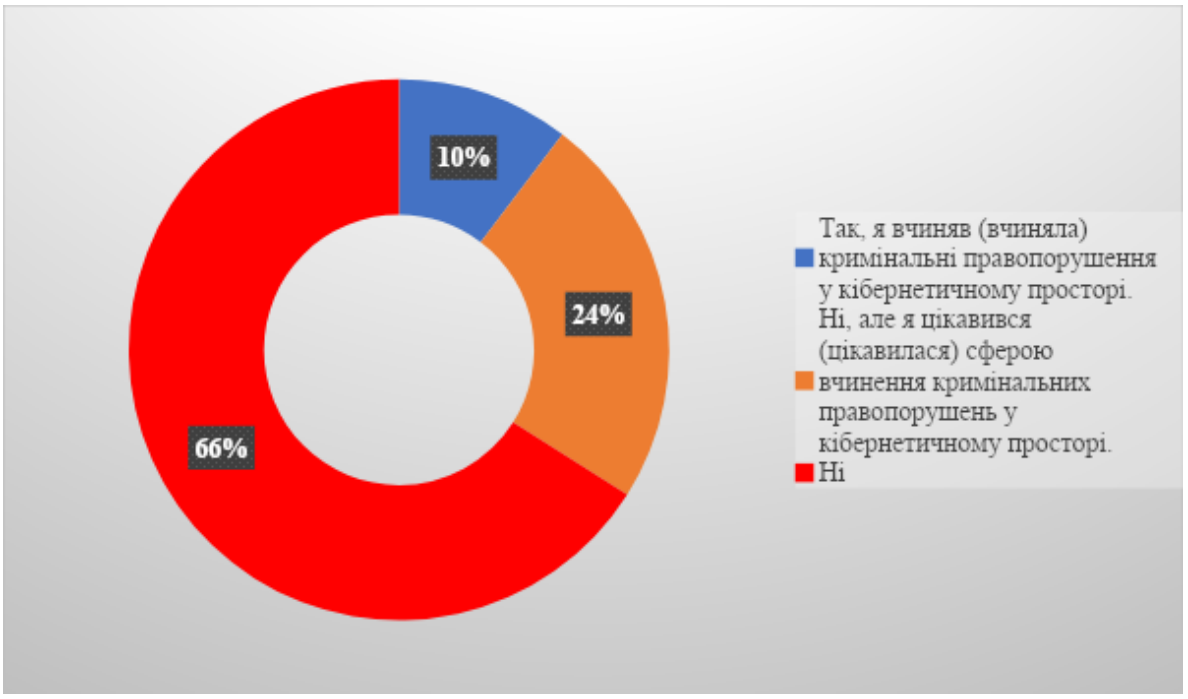
G. Перешкоджання роботі інформаційно-телекомунікаційних систем та мереж – DDos-атаки (45 осіб, 14 % з усіх опитаних).

14. Чи був у вас намір на вчинення кримінального правопорушення у кібернетичному просторі?

A. Так, я вчиняв (вчиняла) кримінальні правопорушення у кібернетичному просторі.

B. Ні.

C. Ні, але я цікавився (цікавилася) сферою вчинення кримінальних правопорушень у кібернетичному просторі.



14.1. Якщо ви вчиняли кримінальні правопорушення у кібернетичному просторі, то яке із перелічених нижче підходить за змістом найбільше вчиненому вами?

A. Шахрайство на передоплаті.

B. DDos-атаки.

C. Фішинг.

D. Телефонне шахрайство.

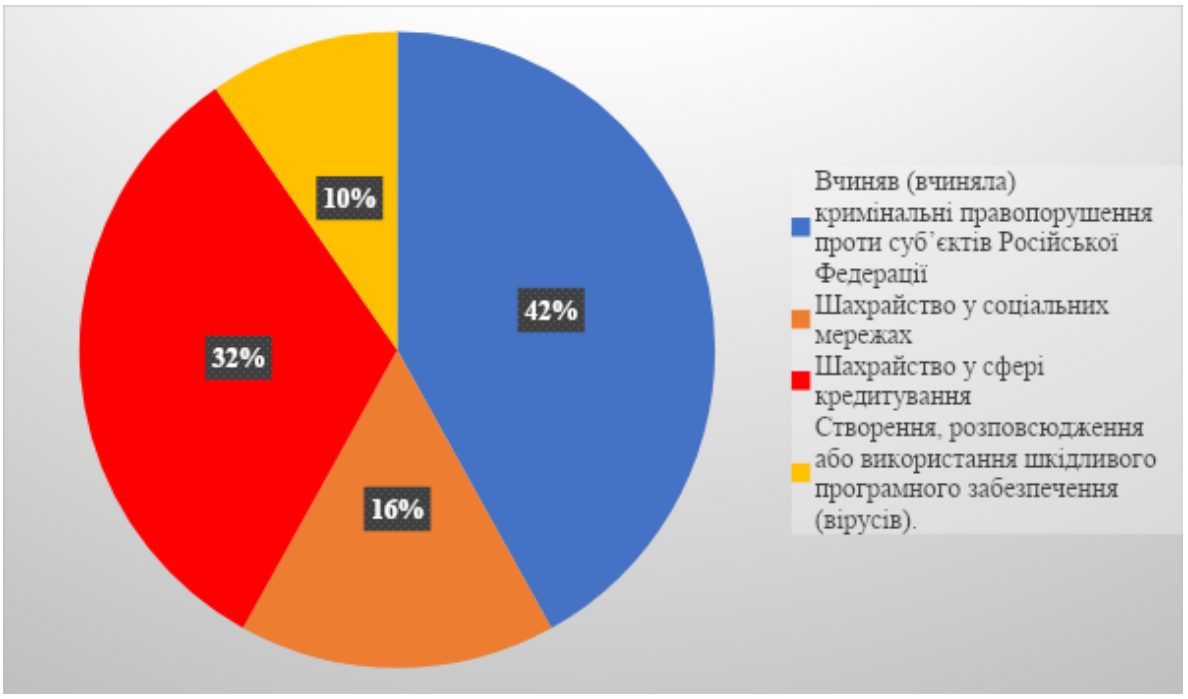
E. Втручання в інформаційно-телекомунікаційні технології системи та мережі, системи або мережі.

F. Шахрайство у сфері кредитування.

G. Шахрайство у соціальних мережах.

H. Створення, розповсюдження або використання шкідливого програмного забезпечення (вірусів).

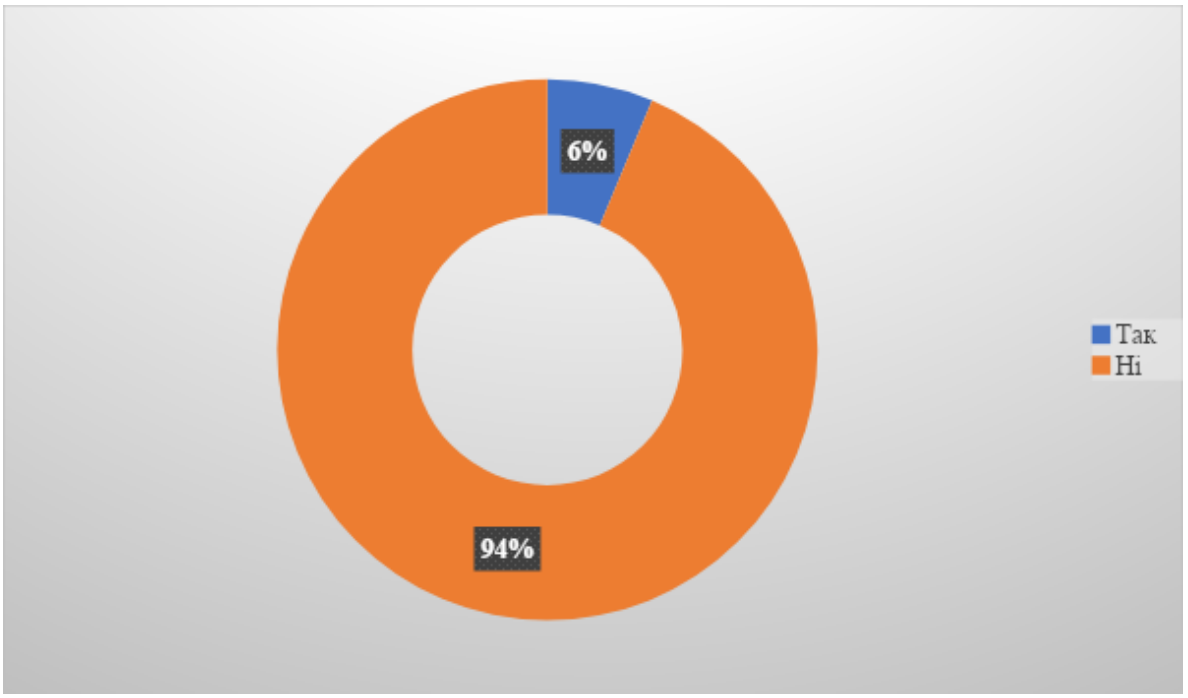
I. Вчиняв (вчиняла) кримінальні правопорушення проти суб’єктів Російської Федерації.



15. Чи допомагаєте ви кібервійськам України блокувати пропагандистські соціальні мережі Російської Федерації?

A. Так.

B. Ні.



Додаток В

Порівняльна таблиця Закону України Про внесення змін до деяких законодавчих актів України щодо підвищення ефективності протидії кримінальним правопорушенням в кіберпросторі

Чинна редакція	Запропонована редакція
Кримінальний кодекс України	
Стаття 361 *Несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж* 1. Несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж - карається штрафом від однієї тисячі до трьох тисяч неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк до трьох років. 2. Ті самі дії, вчинені повторно або за попередньою змовою групою осіб, -	**Стаття 361** *Несанкціоноване втручання в роботу інформаційно-телекомунікаційних технологій, систем та мереж* 1. Несанкціоноване втручання в роботу інформаційно-телекомунікаційних технологій, систем та мереж, тобто отримання можливості для ознайомлення та (або) використання цифрової інформації, які містяться в інформаційно-телекомунікаційній технології, системі або мережі шляхом проникнення особою, яка не має права доступу до інформаційно-телекомунікаційної технології, системи або мережі та (або) поза дозволом власника

караються штрафом від трьох тисяч 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. 3. Дії, передбачені частиною першою або другою цієї статті, якщо вони призвели до витоку, втрати, підробки, блокування інформації, спотворення процесу обробки інформації або до порушення встановленого порядку її маршрутизації, - караються штрафом від семи тисяч до десяти тисяч неоподатковуваних мінімумів доходів громадян або позбавленням волі на строк від трьох до восьми років, з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років або без такого. 4. Дії, передбачені частиною першою або другою цієї статті, якщо вони заподіяли значну шкоду чи створили небезпеку тяжких технологічних аварій або екологічних катастроф, загибелі або масового	інформаційно-телекомунікаційної технології, системи або мережі, що не призвело до наслідків у вигляді витоку, копіювання, модифікації, спотворення процесу обробки, перехоплення, блокування та (або) знищення цифрової інформації - карається штрафом від однієї тисячі до трьох тисяч неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк до трьох років. 2. Ті самі дії, вчинені повторно або за попередньою змовою групою осіб, - караються штрафом від трьох тисяч до п’яти тисяч неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк від двох до п'яти років, або позбавленням волі на той самий строк. 3. Дії, передбачені частинами першою або другою цієї статті, якщо вони призвели до витоку, перехоплення, копіювання, спотворення процесу обробки та (або) модифікації цифрової інформації, - караються штрафом від

захворювання населення чи інших тяжких наслідків, - караються позбавленням волі на строк від восьми до дванадцяти років з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років або без такого. 5. Дії, передбачені частиною третьою або четвертою цієї статті, вчинені під час дії воєнного стану, - караються позбавленням волі на строк від десяти до п'ятнадцяти років з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років. 6. Дії, передбачені частинами першою - четвертою цієї статті, не вважаються несанкціонованим втручанням в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж, якщо вони були вчинені відповідно до порядку пошуку та виявлення потенційних вразливостей таких систем чи мереж.	п'яти тисяч до семи тисяч неоподатковуваних мінімумів доходів громадян або позбавленням волі на строк від трьох до семи років, з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років або без такого. 4. Дії, передбачені частинами першою або другою цієї статті, якщо вони призвели до блокування та (або) знищення цифрової інформації, - караються штрафом від семи тисяч до десяти тисяч неоподатковуваних мінімумів доходів громадян або позбавленням волі на строк від трьох до восьми років, з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років або без такого. 5. Дії, передбачені частинами першою-четвертою цієї статті, якщо вони вчинені організованою групою або злочинною організацією, або заподіяли значну шкоду чи створили небезпеку тяжких технологічних аварій або екологічних катастроф,

	загибелі або масового захворювання населення чи інших тяжких наслідків, - караються позбавленням волі на строк від восьми до дванадцяти років з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років або без такого. 6. Дії, передбачені частинами третьою-четвертою цієї статті, якщо вони вчинені під час дії воєнного стану, - караються позбавленням волі на строк від десяти до п’ятнадцяти років з позбавленням права обіймати певні посади чи займатися певною діяльністю на строк до трьох років.
Назву статті 361-2 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 361-1** Створення з метою	7. Дії, передбачені частинами першою - четвертою цієї статті, не вважаються несанкціонованим втручанням в інформаційно-телекомунікаційні технології, системи та мережі , якщо вони були вчинені відповідно до порядку пошуку та виявлення потенційних вразливостей таких систем чи мереж.

протиправного використання, розповсюдження або збуту, а також розповсюдження або збут шкідливих програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж, -	
Стаття 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 1. Несанкціоновані зміна, знищення або блокування інформації, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах чи комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї, -	**Назву статті 361-2** Несанкціоновані збут або розповсюдження цифрової інформації з обмеженим доступом, що зберігається в інформаційно-телекомунікаційних технологіях (пристроях), системах і мережах. **Частина 1 статті 361-1** Створення з метою протиправного використання, розповсюдження або збуту, а також розповсюдження або збут шкідливих програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу інформаційно-телекомунікаційних технологій, систем і мереж, - **Стаття 362** Несанкціоновані дії з інформацією, яка оброблюється в

караються штрафом від двох тисяч до чотирьох тисяч неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років. 2. Несанкціоновані перехоплення або копіювання інформації, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, якщо це призвело до її витоку, вчинені особою, яка має право доступу до такої інформації, - караються позбавленням волі на строк до трьох років з позбавленням права обіймати певні посади або займатися певною діяльністю на той самий строк. 3. Дії, передбачені частиною першою або другою цієї статті, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду, - караються позбавленням волі на строк від трьох до шести років з позбавленням права обіймати певні посади або займатися певною діяльністю на строк до трьох років.	інформаційно-телекомунікаційних технологіях, системах і мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї 1. Несанкціоновані зміна, знищення або блокування цифрової інформації, яка оброблюється в інформаційно-телекомунікаційних технологіях, системах і мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї, - караються штрафом від двох тисяч до чотирьох тисяч неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років. 2. Несанкціоноване копіювання цифрової інформації, що обробляється в інформаційно-телекомунікаційних технологіях, системах і мережах, якщо це призвело до її витоку, вчинене особою, яка має право доступу до такої інформації, - караються позбавленням волі на строк до трьох років з позбавленням права обіймати певні посади або займатися певною

	діяльністю на той самий строк. 3. Дії, передбачені частиною першою або другою цієї статті, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду, - караються позбавленням волі на строк від трьох до шести років з позбавленням права обіймати певні посади або займатися певною діяльністю на строк до трьох років.
Стаття 363 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 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, якщо це заподіяло значну шкоду, вчинені особою, яка відповідає за їх експлуатацію, - караються штрафом від двох тисяч до чотирьох тисяч неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк до трьох років з позбавленням права обіймати певні посади чи займатися певною діяльністю на той самий строк.	**Стаття 363** Порушення правил експлуатації інформаційно-телекомунікаційних технологій, систем та мереж або порядку чи правил захисту цифрової інформації, яка в них оброблюється, - Порушення правил експлуатації інформаційно-телекомунікаційних технологій, систем та мереж або
Стаття 363-1	

Перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку 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 електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, - карається штрафом від двох тисяч до чотирьох тисяч неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк до трьох років. 2. Ті самі дії, вчинені повторно або за попередньою змовою групою осіб, якщо вони заподіяли значну шкоду, - караються обмеженням волі на строк до п'яти років або позбавленням волі на той самий строк, з позбавленням права обіймати певні	порядку чи правил захисту цифрової інформації, яка в них оброблюється, якщо це заподіяло значну шкоду, вчинені особою, яка відповідає за їх експлуатацію, - караються штрафом від двох тисяч до чотирьох тисяч неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк до трьох років з позбавленням права обіймати певні посади чи займатися певною діяльністю на той самий строк. **Стаття 363-1** 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, - карається штрафом від однієї

посади або займатися певною діяльністю на строк до трьох років.	тисяч до трьох тисяч неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк до трьох років. 2. Ті самі дії, вчинені повторно або за попередньою змовою групою осіб або якщо вони заподіяли значну шкоду, - карається штрафом від трьох тисяч до п’яти тисяч неоподатковуваних мінімумів доходів громадян або обмеженням волі на строк до п'яти років або позбавленням волі на той самий строк, з позбавленням права обіймати певні посади або займатися певною діяльністю на строк до трьох років.
Частина 2 статті 190 Шахрайство, вчинене повторно, або за попередньою змовою групою осіб, або таке, що завдало значної шкоди потерпілому, - карається штрафом від трьох тисяч до чотирьох тисяч неоподатковуваних мінімумів доходів громадян або виправними роботами на строк від одного до двох років, або обмеженням волі на строк до п'яти	3. Дії, передбачені частиною першою або другою цієї статті, якщо вони спричинила тяжкі наслідки або вчинені з корисливих мотивів, - карається штрафом від п’яти тисяч до семи тисяч неоподатковуваних мінімумів доходів громадян або позбавленням волі на строк від п'яти до 8 років, з позбавленням права обіймати певні посади або займатися певною

років, або позбавленням волі на строк до трьох років.	діяльністю на строк до трьох років. 4. Дії, передбачені частиною першою або другою цієї статті, якщо вони спричинила тяжкі наслідки або вчинені проти інформаційної інфраструктури держави. караються позбавленням волі на строк від 12 до 15 років.
Стаття 185-1 **Відсутня**	**Частина 2 статті 190** 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, - карається штрафом від трьох тисяч до чотирьох тисяч неоподатковуваних мінімумів доходів громадян або виправними роботами на строк від одного до двох років, або обмеженням волі на строк до п'яти років, або позбавленням волі на строк до трьох років.
Частина 2 статті 189 Вимагання, вчинене повторно,	**Стаття 185-1** Крадіжка у сфері обігу

або за попередньою змовою групою осіб, або службовою особою з використанням свого службового становища, або з погрозою вбивства чи заподіяння тяжких тілесних ушкоджень, або з пошкодженням чи знищенням майна, або таке, що завдало значної шкоди потерпілому, -	безготівкових або електронних грошей і віртуальних активів - 1. Крадіжка у сфері обігу безготівкових або електронних грошей та віртуальних активів, вчинена шляхом введення цифрової інформації в інформаційно-телекомунікаційні технології, системи і мережі, - Крадіжка у сфері обігу безготівкових або електронних грошей і віртуальних активів внаслідок іншого втручання в роботу інформаційно-телекомунікаційні технології, системи і мережі, -
Частина 1 статті 194 Умисне знищення або пошкодження чужого майна, що заподіяло шкоду у великих розмірах, -	3. Діяння, передбачене частинами першою – другою цієї статті, вчинене повторно, або за попередньою змовою групою осіб, або таке, що завдало значної шкоди потерпілому, -
Статтю 67 доповнити такими обставинами, що обтяжують покарання 14) 15)	4. Діяння, передбачене частинами першою – другою цієї статті, якщо воно вчинене шляхом модифікації цифрової інформації, -
Відсутні	5. Діяння, передбачене частинами першою – другою, вчинене у великих розмірах або

	організованою групою. **Частина 2 статті 189** Вимагання, вчинене повторно, або за попередньою змовою групою осіб, або службовою особою з використанням свого службового становища, або з погрозою вбивства чи заподіяння тяжких тілесних ушкоджень, або з пошкодженням чи знищенням майна, або таке, що завдало значної шкоди потерпілому, або погроза блокування, видалення, знищення, модифікації, або погроза іншого несанкціонованого втручання в роботу інформаційно-телекомунікаційних технологій, систем і мереж, що може завдати шкоду правам та інтересам потерпілої особи – **Частина 1 статті 194** Умисне знищення або пошкодження чужого майна, що заподіяло шкоду у великих розмірах, або таке, що вчинене шляхом несанкціонованого втручання в роботу

	інформаційно-телекомунікаційних технологій, систем і мереж, - **Статтю 67 доповнити такими обставинами, що обтяжують покарання** 14) заподіяння шкоди інформаційно-телекомунікаційній технології, системи або мережі державного значення, яке має ознаки критичної інфраструктури; 15) предметом кримінального правопорушення виступає цифрова інформація, яка має ознаки державної таємниці.
Закону України «Про основні засади забезпечення кібербезпеки України»	
Стаття 1 **1. У цьому Законі наведені нижче терміни вживаються в такому значенні:** Кіберзлочин (компьютерный злочин) – суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними	**Стаття 1** **1. У цьому Законі наведені нижче терміни вживаються в такому значенні:** Кримінальне правопорушення у кіберпросторі – суспільно небезпечне, протиправне, винне, каране діяння, що посягає та заподіює шкоду різним суспільним відносинам шляхом використання інформаційно-телекомунікаційних

договорами України;	технологій, інформаційно-телекомунікаційних систем та мереж та створюваного ними кіберпростору.
2. У цьому Законі додати наведені нижче терміни вживаються в такому значенні:	**2. У цьому Законі додати наведені нижче терміни вживаються в такому значенні:**
Відсутні	Несанкціоноване втручання – отримання можливості для ознайомлення та (або) використання цифрової інформації, які 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) по за дозволом власника інформаційно-телекомунікаційної технології, системи або мережі; віртуальний простір – це створене комп'ютерними технологіями глобальне комунікативне середовище, в основі якого лежить створення, збереження, упорядкування та обмін інформацією за допомогою інформаційно-телекомунікаційних мереж.

Додаток Г

«ЗАТВЕРДЖУЮ»
Начальник відділу протидії
кіберзлочинам в Сумській області
Департаменту кіберполіції
Національної поліції України

Сергій ВОЛОСОВЕЦЬ

«02» серпня 2023 р.

АКТ

впровадження результатів дисертаційного дослідження

Думчикова Михайла Олександровича

«Концептуальні засади кримінально-правової охорони кіберпростору в Україні»

на здобуття ступеня доктора юридичних наук
за спеціальністю 12.00.08 – кримінальне право та кримінологія; кримінально-виконавче право у практичну діяльність

Комісія у складі:

1. Начальника відділу протидії кіберзлочинам в Сумській області Департаменту кіберполіції Національної поліції України Волосовця Сергія Євгенійовича;

2. Заступника начальника відділу протидії кіберзлочинам в Сумській області Департаменту кіберполіції Національної поліції України Ісакова Василя Андрійовича;

2. Старшого інспектора з особливих доручень відділу протидії кіберзлочинам в Сумській області Департаменту кіберполіції Національної поліції України Бухтіарова Артема Геннадійовича:

цим актом засвідчує, що результати дисертаційного дослідження докторанта Сумського державного університету Думчикова Михайла Олександровича на тему: «Концептуальні засади кримінально-правової охорони кіберпростору в Україні» поданого на здобуття наукового ступеня доктора юридичних наук за спеціальністю 12.00.08 – кримінальне право та кримінологія; кримінально-виконавче право використовуються у практичній діяльності працівників Департаменту кіберполіції Національної поліції України, а також під час проведення занять у системі службової підготовки.

1. _____ **Сергій ВОЛОСОВЕЦЬ**
2. _____ **Василь ІСАКОВ**
3. _____ **Артем БУХТІАРОВ**

Додаток Ґ

АКТ

Думчикова Михайла Олександровича

«Концептуальні засади кримінально-правової охорони кіберпростору в Україні»

на здобуття ступеня доктора юридичних наук
за спеціальністю 12.00.08 – кримінальне право та кримінологія; кримінально-виконавче право у практичну діяльність

Підписано:

Начальником Управління Держспецзв'язку в Сумській Області полковником Віктором ІВАНЮЩЕНКОМ.

Цим актом засвідчую, що результати дисертаційного дослідження докторанта Сумського державного університету Думчикова Михайла Олександровича «Концептуальні засади кримінально-правової охорони кіберпростору в Україні» поданого на здобуття наукового ступеня доктора юридичних наук за спеціальністю 12.00.08 – кримінальне право та кримінологія; кримінально-виконавче право можуть бути застосовані під час проведення занять у системі службової підготовки.

Віктор ІВАНЮЩЕНКО (підпис)

Додаток Д

Міністерство освіти і науки України
Сумський державний університет

ЗАТВЕРДЖУЮ
Проректор з наукової роботи
Сумського державного університету
_____ Анатолій Чорноус
«22» червня 2023 р.

АКТ

про впровадження у наукову діяльність результатів дисертаційного дослідження Думчикова Михайла Олександровича
«Концептуальні засади кримінально-правової охорони кіберпростору в Україні»
на здобуття ступеня доктора юридичних наук
за спеціальністю 12.00.08 – кримінальне право та кримінологія; кримінально-виконавче право

Комісія у складі:

Голова – професор кафедри кримінально-правових дисциплін та судочинства Навчально-наукового інституту права Сумського державного університету, д.ю.н., професор Сухонос Віктор Володимирович;

Члени комісії –

заступник директора Навчально-наукового інституту права з наукової роботи, старший викладач кафедри адміністративного, господарського права, фінансово-економічної безпеки, к.ю.н. Миргород Валерія Валеріївна;

доцент кафедри кримінально-правових дисциплін та судочинства Навчально-наукового інституту права Сумського державного університету, к.ю.н., доцент Янішевська Катерина Дмитрівна.

Комісія склала цей акт з приводу розгляду результатів дисертаційного дослідження Думчикова Михайла Олександровича «Концептуальні засади кримінально-правової охорони кіберпростору в Україні» та їх впровадження у наукову діяльність.

Висновок: комісія вважає, що результати проведеного Думчиковим Михайлом Олександровичем дослідження на тему «Концептуальні засади кримінально-правової охорони кіберпростору в Україні» отримані на основі грунтовного аналізу та вивчення наукової доктрини та положень нормативно-правових актів, що регламентують основні засади та особливості кримінально-правової охорони кіберпростору в Україні. Вони мають грунтовний та аргументований характер і використовувалися при проведенні наукових досліджень у рамках науково-дослідної роботи «Концептуальні засади реформування системи правоохоронних органів в сучасних умовах трансформації нагляду і контролю щодо забезпечення економічної безпеки України» (№ 55.15.02-22/24.3Ф-01), яка розробляються в Навчально-науковому інституті права Сумського державного університету.

Голова комісії Віктор СУХОНОС

Члени комісії Валерія МИРГОРОД

Катерина ЯНШЕВСЬКА

Додаток Е

Міністерство освіти і науки України
Сумський державний університет

ЗАТВЕРДЖУЮ
Перший проректор
Сумського державного університету
Сергій Лєонов
«09» 05 2023 р.

АКТ
про впровадження в освітній процес результатів дисертаційного дослідження
Думчикова Михайла Олександровича
«Концептуальні засади кримінально-правової охорони кіберпростору в Україні»
на здобуття ступеня доктора юридичних наук
за спеціальністю 12.00.08 – кримінальне право та кримінологія; кримінально-виконавче право

Комісія у складі:

Голова – директор Навчально-наукового інституту права Сумського державного університету, д.ю.н., професор, заслужений юрист України Куліш Анатолій Миколайович.

Члени комісії – професор кафедри кримінально-правових дисциплін та судочинства Навчально-наукового інституту права Сумського державного університету, д.ю.н., професор Сухонос Віктор Володимирович;

- професор кафедри адміністративного, господарського права та фінансово – економічної безпеки Навчально-наукового інституту права Сумського державного університету, д.ю.н., професор Старинський Миколо Іванович.

Комісія склала цей акт з приводу розгляду результатів дисертаційного дослідження Думчикова Михайла Олександровича «Концептуальні засади кримінально-правової охорони кіберпростору в Україні» і їх використання в освітньому процесі з дисциплін «Кримінальне право», «Сучасні проблеми кримінального права і процесу», «Основи запобігання кіберзлочинності» кафедри кримінально-правових дисциплін та судочинства, кафедри адміністративного, господарського права та фінансово-економічної безпеки Сумського державного університету.

Висновок: комісія вважає, що результати проведеного Думчиковим Михайлом Олександровичем дослідження ««Концептуальні засади кримінально-правової охорони кіберпростору» отримані на основі ґрунтовного аналізу та вивчення сутності та особливостей кримінально-правової охорони кіберпростору України, мають комплексний характер і використовувалися під час проведення лекцій, семінарських та практичних занять кафедри кримінально-правових дисциплін та судочинства і кафедри адміністративного, господарського права та фінансово-економічної безпеки Сумського державного університету при вивченні

дисциплін «Кримінальне право», «Сучасні проблеми кримінального права та процесу», «Основи запобігання кіберзлочинності», «Основи запобігання злочинності», «Криміналістика»

Акт складений у 2-ч примірниках.

Голова комісії Анатолій КУЛИШ

Члени комісії Віктор СУХОНОС

Микола СТАРИНСЬКИЙ