ХМЕЛЬНИЦЬКА ОБЛАСНА РАДА
ХМЕЛЬНИЦЬКИЙ УНІВЕРСИТЕТ УПРАВЛІННЯ ТА ПРАВА
ІМЕНІ ЛЕОНІДА ЮЗЬКОВА

Кваліфікаційна наукова
праця на правах рукопису

МАЛІЙ МИКОЛА ІВАНОВИЧ

УДК 343.3.7

ДИСЕРТАЦІЯ
ОСОБА КОМП'ЮТЕРНОГО ЗЛОЧИНЦЯ
ЯК ОБ'ЄКТ КРИМІНОЛОГІЧНОГО ДОСЛІДЖЕННЯ

Спеціальність 081 Право
Галузь знань 08 Право

Подається на здобуття ступеня доктора філософії

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело
_____ **М.І.Малій**

Науковий керівник
БІЛЕНЧУК Петро Дмитрович,
кандидат юридичних наук, доцент

Хмельницький – 2023

АНОТАЦІЯ

Малій М.І. Особа комп’ютерного злочинця як об'єкт кримінологічного дослідження. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття освітньо-наукового ступеня доктора філософії за спеціальністю 081 Право. Хмельницький університет управління та права імені Леоніда Юзькова, Хмельницький, 2022.

Дисертація є одним з перших комплексних досліджень особи комп’ютерного злочинця. У дисертації здійснено теоретичне узагальнення та запропоновано нове розв’язання наукового завдання щодо формування, по-перше, теоретико-методологічних засад комплексного дослідження особи комп’ютерного злочинця як об’єкта кримінологічного пізнання, по-друге, поняття і сутності особи комп'ютерного злочинця, по-третє, поняття і структури кримінологічної характеристики особи комп’ютерного злочинця, по-четверте, концептуальних положень нової кримінологічної систематизації і класифікації комп’ютерних злочинців, по-п’яте, шляхів запобігання і протидії кримінальним правопорушенням, що вчиняються особою комп’ютерного злочинця, по-шосте, пріоритетних напрямів протидії кримінальним правопорушенням, що вчиняються комп’ютерними злочинцями, по-сьоме, перспектив дослідження запобігання вчиненню комп’ютерних злочинів з використанням електронного інтелекту в наземному і космічному кіберпросторі.

Це обумовлено тим, що за останні роки відбувся значний ріст світової кіберзлочинності в результаті значного збільшення кількості інтернет-користувачів, що, відповідно, призвело до масового глобального використання і поширення новітніх інформаційних технологій, зокрема, електронного (штучного) інтелекту та несе в собі нові небачені та непрогнозовані кіберзагрози та кібервиклики світовому співтовариству.

Також поруч із тими новими загрозами і викликами для Українського народу та нашої держави України постало тяжке випробування, спричинене військовою агресією з боку Російської Федерації, яка поширилась в наземному, повітряному, космічному та кібернетичному просторах.

Очевидно, що варто звернути особливу увагу на значне збільшення та велику інтенсивність кіберінцидентів в Україні ще до введення воєнного стану, що підтверджується різними вітчизняними та закордонними аналітичними дослідженнями.

Відомо, що для дестабілізації діяльності органів державної влади в ніч з 13 на 14.01.2022р. було здійснено неймовірно масштабну та блискавичну злочинну крекерську кібератаку на надзвичайно важливі сімдесят урядових сайтів України.

Наступною, ще більш масштабною кібератакою в наземному та космічному просторі на важливі державні та приватні об’єкти як України, так і ряду країн-членів Європейського Союзу, стала кібератака, організована Російською Федерацією за годину до початку воєнної агресії проти України.

Це перша в світі така потужна кібератака на рівні держави в електронному, космічному та наземному кіберпросторі, яка передувала повномасштабному сухопутному, повітряному та космічному вторгненню на територію суверенної та незалежної держави України.

Отже, на практиці в умовах воєнного стану існують як тактичні, так і стратегічні задачі пов’язані з необхідністю дослідження особи комп’ютерного злочинця з метою запобігання і протидії злочинності в сфері інформаційних технологій, які потребують постійного дослідження і оперативного розв’язання як на рівні держави, так і на міжнародному, міждержавному рівнях. Очевидно, що оперативне використання знань кримінологічної науки на сьогодні є одним із основних інструментів для миттєвого використання всіх наявних можливостей системи запобігання кіберзлочинності (комп’ютерній злочинності).

Викладене вище дозволяє зробити висновок про те, що наявний сьогодні достатньо потужний рівень сучасних кіберзагроз в електронному світі надзвичайно небезпечних комп'ютерних злочинів як в наземному, так і космічному кіберпросторі потребує негайної розробки пріоритетних напрямів дослідження особи комп'ютерного злочинця з метою запобігання і протидії цим негативним кіберзагрозам, кіберризикам і кібернебезпекам, які реально мають місце в суспільстві.

Вважаємо, що на сучасному етапі цивілізаційного розвитку в Україні одним з пріоритетних вітчизняних напрямів є комплексне дослідження особи комп'ютерного злочинця з метою запобігання комп'ютерній злочинності в наземному, повітряному і космічному кіберпросторі, а також розробка шляхів реформування діяльності правоохоронних органів України з метою забезпечення координації їхніх дій в кіберпросторі, та, відповідно, електронним документуванням цих дій на всіх рівнях в єдиній електронній правоохоронній системі.

Базуючись на даних положеннях, в дисертаційному дослідженні висвітлені засадничі теоретико-методологічні засади пізнання сутності особи комп'ютерного злочинця.

Запропоновано особу комп'ютерного злочинця розуміти як фізичну особу (людину), яка вчиняє кримінальні правопорушення з використанням електронно-обчислювальних машин (комп'ютерів), різного рівня новітніх комп'ютерних засобів і технологій (нанокомп'ютери, портативні комп'ютери, суперкомп'ютери, квантові комп'ютери тощо) та різного виду засобів (електронного, біологічного або нейробіологічного електронного інтелекту тощо), електронних банків даних, систем та комп'ютерних мереж, або інших засобів комп'ютерної інформатизації та різного роду інформаційно-телекомунікаційного обладнання (державного, приватного, наземного, космічного).

В дисертації сформульовано і обгрунтовано поняття фізичної особи комп'ютерного злочинця. Визначено поняття і структура кримінологічної

характеристики особи комп'ютерного злочинця. Запропонована кримінологічна систематизація і класифікація комп'ютерних злочинців.

Вказано шляхи запобігання і протидії кримінальним правопорушенням, що вчиняються особою комп'ютерного злочинця.

Досліджено пріоритетні напрями протидії кримінальним правопорушенням, що вчиняються комп'ютерними злочинцями.

В дисертації особливу увагу звернуто на сучасні проблеми, які пов'язані з впровадженням в освіту, науку і практичну діяльність програм з використанням електронного інтелекту. Тим більше, що сьогодні є очевидні факти використання програмних продуктів на базі електронного інтелекту в злочинних цілях. Тому ця проблематика в даний час є особливо актуальною і характеризується надзвичайною новизною.

В дисертаційному дослідженні наведено теоретичне узагальнення та сформульовано нове вирішення наукового завдання, що полягало у з'ясуванні закономірностей особливостей пізнання характерних рис, ознак, властивостей і манер поведінки особи комп'ютерного злочинця як об'єкта кримінологічного дослідження. Дане дослідження базується на новітніх положеннях теорії кримінології і результатах узагальнення матеріалів вітчизняної і міжнародної практики. Отримані результати дозволяють сформулювати ряд інноваційних теоретичних висновків, а також запропонувати окремі рекомендації по удосконаленню норм чинного законодавства та розробити механізм і методику дослідження особи комп'ютерного злочинця з метою запобігання та протидії вчиненню кримінальних правопорушень, а саме комп'ютерних проступків та комп'ютерних злочинів в сучасному електронному світі.

Головним теоретичним, методологічним і праксеолого-прикладним надбанням дисертаційного дослідження є такі висновки, пропозиції і рекомендації:

1. Комплексний аналіз сутності поняття особи комп'ютерного злочинця дозволив виокремити суттєві риси, ознаки, властивості та манери поведінки, а

саме сформулювати його реальний соціально-правовий, психофізіологічний і інформаційно-комунікаційний портрет.

2. Системний консолідований аналіз рис, ознак, властивостей і манер поведінки комп'ютерних злочинців дозволяє розкрити сутнісні характеристики типології осіб, які вчиняють окремі види комп'ютерних злочинів.

3. Відповідно до вказаної мети були поставлені та вирішені такі завдання: по-перше, окреслено теоретико-методологічні засади дослідження особи комп'ютерного злочинця як об'єкта кримінологічного пізнання; по-друге, сформульовано поняття особи комп'ютерного злочинця; по-третє, визначено структуру кримінологічної характеристики особи комп'ютерного злочинця; по-четверте, здійснено кримінологічну систематизацію і класифікацію комп'ютерних злочинців; по-п'яте, визначено пріоритетні напрями протидії комп'ютерним злочинцям, які вчиняють кримінальні правопорушення; по-шосте, досліджено перспективи і сформульовано напрями протидії вчиненню комп'ютерних злочинів з використанням електронного інтелекту.

На підставі проведеного дослідження запропоновано ряд новацій направлених на удосконалення чинного законодавства, впровадження новітніх пропозицій в освітню, наукову і праксеолого-практичну діяльність.

Ключові слова: комп'ютерний злочинець, комп'ютерна злочинність, наземний і космічний кіберпростір, автоматизовані комп'ютерні системи (комп'ютер), електронні банки даних, електронні мережі, електронна безпека, кібербезпека, кібертероризм.

SUMMARY

Malii Mykola. The person of a computer criminal as an object of criminological research. – Qualifying scientific work on the rights of the manuscript.

Dissertation for the degree of Doctor of Philosophy in the specialty 081 Law. Leonid Yuzkov Khmelnytskyi University of Management and Law, Khmelnytskyi, 2022.

The dissertation is one of the first comprehensive studies of the identity of a computer criminal. The dissertation made a theoretical generalization and proposed a new solution to the scientific task of forming, firstly, the theoretical and methodological foundations of a comprehensive study of the person of a computer criminal as an object of criminological knowledge, and secondly, the concept and essence of the person of a computer criminal , thirdly, the concepts and structures of the criminological characteristics of the person of the computer criminal, fourthly, the conceptual provisions of the new criminological systematization and classification of computer criminals, fifthly, the ways of preventing and countering criminal offenses committed by the person of computer of the computer criminal, sixth, the priority directions of combating criminal offenses committed by computer criminals, seventh, the prospects of researching the prevention of computer crimes using electronic intelligence in terrestrial and space cyberspace.

This is due to the fact that in recent years there has been a significant increase in global cybercrime (computer crime) as a result of a significant increase in the number of internet users, which, accordingly, has led to the massive global use and spread of the latest information technologies, in particular, electronic (artificial) intelligence and carries new unprecedented and unpredictable cyber threats and cyber challenges to the world community.

Also, next to those new threats and challenges for the Ukrainian people and our state of Ukraine, there was a severe test caused by the military aggression of the Russian Federation, which spread in the ground, air, space and cybernetic spaces.

It is obvious that it is worth paying special attention to the significant increase and high intensity of cyber incidents in Ukraine even before the introduction of martial law in Ukraine, which is confirmed by various domestic and foreign analytical studies.

It is known that in order to destabilize the activities of state authorities on the night from January 13 to 14, 2022. an incredibly large-scale and lightning-fast criminal cracker cyber-attack was carried out on extremely important seventy government websites of Ukraine.

The next, even more large-scale cyber attack in terrestrial and outer space on important state and private objects of both Ukraine and a number of member states of the European Union was a cyber attack organized by the Russian Federation an hour before the start of military aggression against Ukraine.

This is the first in the world such a powerful cyberattack at the level of a cybercriminal state in electronic space and terrestrial cyberspace, which preceded a full-scale land, air and space invasion of the territory of the sovereign and independent state of Ukraine.

So, in practice, in the conditions of martial law, there are both tactical and strategic tasks related to the need to investigate the identity of a computer criminal in order to prevent and counter crime in the field of information technologies, which require constant research and operational solutions both at the level of the state, as well as at the international and interstate levels. It is obvious that the operative use of the knowledge of criminological science today is one of the main tools for the immediate use of all available capabilities of the cybercrime (computer crime) prevention system.

The above allows us to conclude that the current sufficiently powerful level of modern cyber threats in the electronic world of extremely dangerous computer crimes both in terrestrial and space cyberspace requires the immediate development

of priority areas of research into the identity of computer criminals in order to prevent and counter these negative cyber threats, cyber risks and cyber dangers that actually exist in society.

Based on the above, we believe that at the current stage of civilizational development in Ukraine, one of the priority national directions is a comprehensive study of the identity of a computer criminal with the aim of preventing computer crime in terrestrial and space cyberspace, as well as the development of ways to reform the activities of law enforcement agencies of Ukraine with in order to ensure coordination of their actions in cyberspace, and, accordingly, electronic documentation of these actions at all levels in a single electronic law enforcement system.

Based on these provisions, the dissertation study highlights the fundamental theoretical and methodological principles of knowing the essence of the identity of a computer criminal.

It is proposed to understand the identity of a computer criminal as a natural person (person) who commits criminal offenses using electronic computing machines (computers), various levels of the latest computer tools and technologies (nanocomputers, portable computers, supercomputers computers, quantum computers, etc.) and various types of means (electronic, biological or neurobiological electronic intelligence, etc.), electronic data banks, systems and computer networks, or other means of computer informatization and various types of information and telecommunication equipment (public, private, terrestrial, space).

The dissertation formulates and substantiates the concept of a physical person of a computer criminal and, secondly, the concept of an electronic person of a computer criminal. The concept and structure of the criminological characteristics of a computer criminal are defined. A proposed criminological systematization and classification of computer criminals.

Ways to prevent and counteract criminal offenses committed by computer criminals are indicated.

The priority areas of combating criminal offenses committed by computer criminals have been studied.

In the dissertation, special attention is paid to the modern problems imposed by the implementation of electronic intelligence in education, science and practical activities. Moreover, today there are obvious facts of the use of electronic intelligence for criminal purposes. Therefore, this issue is currently particularly relevant and is characterized by extreme novelty.

The dissertation study provides a theoretical generalization and formulates a new solution to the scientific task, which consisted in clarifying the regularities of the knowledge of the characteristic features, signs, properties and manners of behavior of a computer criminal as an object of criminological research. This study is based on the latest provisions of the theory of criminology and the results of the generalization of the materials of domestic and international practice. The obtained results make it possible to formulate a number of innovative theoretical conclusions, as well as to offer separate recommendations for improving the norms of current legislation and to develop a mechanism and methodology for investigating the identity of a computer criminal in order to prevent and counteract the commission of criminal offenses, namely computer misdemeanors and computer crimes in today's electronic world.

The main theoretical, methodological and praxeological-applied assets of the dissertation research are the following conclusions, proposals and recommendations:

1. A comprehensive analysis of the essence of the concept of the person of a computer criminal made it possible to single out essential features, signs, properties and manners of behavior, namely to formulate his real socio-legal, psycho-physiological and informational and communication portrait.

2. A systematic consolidated analysis of the traits, characteristics, properties and manners of behavior of computer criminals allows us to reveal the essential characteristics of the typology of persons who commit certain types of computer crimes.

3. In accordance with the specified goal, the following tasks were set and solved: first, the theoretical and methodological principles of the study of the person of a computer criminal as an object of criminological knowledge were outlined; secondly, the concept of the identity of a computer criminal is formulated; thirdly, the structure of the criminological characteristics of the person of the computer criminal is determined; fourthly, a criminological systematization and classification of computer criminals was carried out; fifthly, the priority areas of combating computer criminals who commit criminal offenses are determined; Sixthly, the prospects are explored and the directions of combating the commission of computer crimes using electronic intelligence are formulated.

On the basis of the conducted research, a number of innovations aimed at improving key legislation, introducing the latest proposals into educational, scientific, and praxeological-practical activities have been proposed.

Keywords: computer criminal, computer crime, terrestrial and space cyberspace, automated computer systems (computer), electronic data banks, electronic networks, electronic security, cyber security, cyber terrorism.

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

в яких опубліковані основні наукові результати дисертації:

1. Малій М.І. Інноваційні концепції застосування grid- і blockchain-технологій в юриспруденції. *Актуальні проблеми права України та Польщі:* монографія / Київський університет права НАН України; за заг. ред. проф. Ю.Л. Бошицького та проф. А. Шміта. Київ: Талком, 2020. С. 48-62. URL: http://kul.kiev.ua/images/A/25/Monografia/Polska_monografia_2020.pdf.

2. Малій М.І. Правовий статус саббота та відповідальність перед людством. *Економіка. Фінанси. Право.* 2022. № 8. С. 27-35. http://efp.in.ua/uk/journal-item/335 (DOI: https://doi.org/10.37634/efp.2022.8.6).

3. Борисова Л.В., Біленчук П.Д., Малій М.І., Виноградова В.С. Експертиза як засіб установлення фактів і обставин вчинення

транснаціональних комп'ютерних злочинів. *Криміналістика і судова експертиза*. 2020. Вип. 65. С. 230-239. https://digest.kndise.gov.ua/wp-content/uploads/2020/06/Криміналістика_65_друк_новий-230-239.pdf (DOI: https://doi.org/10.33994/kndise.2020.65.22).

4. Біленчук П.Д., Малій М.І., Сватюк Н.І., Симканич О.І. Кібербезпека радіаційних випробувань космічних апаратів: правові засади, регламентні вимоги та стан їх інноваційного забезпечення. *Наукові праці Національного авіаційного університету. Серія: Юридичний вісник «Повітряне і космічне право»*. 2020. № 4 (57). С. 156-162. http://www.law.nau.edu.ua/images/Nauka/Naukovij_jurnal/2020/4-57/24.pdf (DOI: 10.18372/2307-9061.57.15079).

5. Біленчук П.Д., Малій М.І., Колонюк В.П. Інноваційне науково-технологічне забезпечення правосуддя в еру асиметричної електронної трансформації. *Криміналістика і судова експертиза.* 2021. Вип. 66. С. 70-80. https://digest.kndise.gov.ua/wp-content/uploads/2021/04/Bilenchuk.pdf (DOI: https://doi.org/10.33994/kndise.2021.66.08).

які засвідчують апробацію матеріалів дисертації:

6. Малій М.І. Міжнародні організації з протидії космічній кіберзлочинності. *АЕРО-2019. Повітряне і космічне право:* матеріали всеукраїнської конференції молодих учених і студентів (м. Київ, Національний авіаційний університет, 21 листопада 2019 р.). Том. 1. Тернопіль: Вектор, 2019. С. 216-218.

7. Малій М.І. Особливості кримінолого-криміналістичної характеристики особи електронного зловмисника. *Актуальні проблеми сучасної юридичної науки та практики:* матеріали круглого столу (м. Київ, 1 жовтня 2020 року). Київський університет права НАН України. Київ, Видавництво Ліра-К, 2020. С. 40-45.

8. Малій М.І. Міжнародний досвід запобігання і протидії корупції: системний аналіз діяльності ЛІ КУАН Ю. *Реалізація державної*

антикорупційної політики в міжнародному вимірі: матеріали V Міжнар. наук.-практ. конф. (Київ, 9–10 грудня 2020 р.): у 2 ч. / [редкол.: В. В. Чернєй, С. Д. Гусарєв, С. С. Чернявський та ін.]. Київ, Нац. акад. внутр. справ, 2020. Ч. 2. С. 150-152.

9. Малій М.І. Електронна кіберзлочинність як об'єкт кримінологічного дослідження. *Сучасне право в епоху соціальних змін*: матеріали XI Міжнародної науково-практичної конференції. (м. Київ, Національний авіаційний університет, 26 лютого 2021 р.) Том. 1. Тернопіль: Вектор, 2021. С. 323-325.

10. Малій М.І. Правова відповідальність електронного інтелекту в новому тисячолітті. *Актуальні проблеми сучасної юридичної науки та практики.* Випуск 2: матеріали круглого столу (Київ, 7 жовтня 2021 р.). Київ: Видавництво Ліра-К, 2021. С. 40-54.

11. Біленчук П.Д., Лихова С.Я., Малій М.І. Космічні кіберзагрози в третьому тисячолітті: наукове і правове пізнання. *50 років академічної науки на Закарпатті*: матеріали міжнародної конференції (м. Ужгород, 24-25 травня 2021 року). Укладач: А.М. Завілопуло, д.ф.-м.н. Інститут електронної фізики НАН України. Ужгород, Видавництво «ФОП Сабов А.М.», 2021. С. 283-286.

12. Біленчук П.Д., Близнюк М.М., Кобилянський О.Л., Малій М.І., Пілюков Ю.О., Соболєв О.В. Електронна цивілізація: інноваційне майбутнє України: монографія / за заг. ред. П.Д. Біленчука. Київ: УкрДГРІ, 2018. 284 с.

13. Біленчук П.Д., Кобилянський О.Л., Ковальчук Ю.І., Копчук І.В., Малій М.І., Моргунов С.А., Соболєв О.В., Тимощук С.В. та ін. Е-СУСПІЛЬСТВО: цифрове майбутнє України: монографія / за заг. ред. П.Д. Біленчука. 2-е вид., допов. і переробл. Київ: УкрДГРІ, 2019. 292 с.

14. Біленчук П.Д., Береський Я.О., Кобилянський О.Л., Малій М.І., Перелигіна Р.В. Конвергенція сонячного суспільства знань: креативна освіта і цивілізаційний розвиток: монографія / за заг. ред. П.Д. Біленчука. Київ: УкрДГРІ, 2019. 416 с.

15. Біленчук П.Д., Кобилянський О.Л., Малій М.І. та ін. Правова соціалізація особистості в сучасному світі: людина, суспільство, цивілізація: монографія / за заг. ред. П.Д. Біленчука. Київ: УкрДГРІ, 2020. 204 с.

16. Біленчук П.Д., Кобилянський О.Л., Малій М.І., Перелигіна Р.В., Тарасевич Т.Ю. та ін. Електронне суспільство, електронне право, кібербезпека: стратегія розвитку інноваційної ери: монографія / за заг. ред. П.Д. Біленчука і Т.Ю. Тарасевич. Київ: УкрДГРІ, 2020. 388 с.

17. Біленчук П.Д., Перелигіна Р.В., Малій М.І. Кримінологічна характеристика особи комп'ютерного злочинця. *Кримінологічна теорія і практика: досвід, проблеми сьогодення та шляхи їх вирішення*: матеріали міжвузів. наук.-практ. круглого столу (м. Київ, 22 березня 2019 р.) [редкол. В.В. Чернєй, С.Д. Гусарєв, С.С. Чернявський та ін.]. Київ, Нац.акад.внутр.справ, 2019. С. 144-147.

18. Біленчук П.Д., Малій М.І. Сучасні комп'ютерні злочинці та кібертерористи: новітні технології на службі організованого злочинного світу. *Бизнес и безопасность*. 2019. № 4. С. 2-4.

19. Біленчук П.Д., Малій М.І. Космічна і електронна кіберзлочинність третього тисячоліття: новітні виклики та загрози для людини, держави, цивілізації. *Бизнес и безопасность*. 2019. № 5. С. 18-21.

20. Біленчук П.Д., Малій М.І. Портрет електронного зловмисника. *ООН – гарантування світового мировпорядкування:* матеріали Всеукраїнської науково-практичної конференції ВНЗ «Київський університет ринкових відносин» (м. Київ, 28 жовтня 2020 р.). Київ, «Хай-Тек Прес», 2021. С. 9-12.

21. Біленчук П.Д., Малій М.І. Пріоритетні напрями досліджень психологічного портрету електронного зловмисника. *Актуальні проблеми психологічного забезпечення службової діяльності працівників правоохоронних органів:* зб. тез Міжнар. наук.-практ. конф. (м. Київ, 30 жовтня 2020 р.). Київ, ДНДІ МВС України, 2020. С. 79-81.

22. Біленчук П.Д., Малій М.І. Космічна кіберзлочинність електронної ери асиметричної трансформації. *Актуальні проблеми кримінального права,*

процесу, криміналістики та оперативно-розшукової діяльності: тези IV Всеукраїнської науково-практичної конференції (Хмельницький, 26 лютого 2021 р.). Хмельницький, Вид-во НАДПСУ, 2021. С. 337-340.

23. Біленчук П.Д., Малій М.І. Планетарна електронна кіберзлочинність на шляху до сингулярності. *Злочинність і протидія їй в умовах сингулярності: тенденції та інновації*: зб. тез доп. наук.-практ. конф., присвяч. пам'яті члена Правління Кримінологічної асоціації України, професора Тетяни Андріївни Денисової (м. Харків, 16 квіт. 2021 р.) / МВС України, Харків. нац. ун-т внутр. справ, Кримінол. асоц. України. Харків, ХНУВС, 2021. С. 432-434.

які додатково відображають результати дисертації:

24. Malii M. Prevention of computer crimes electronic intelligence against human, society, state. *Visegrad Journal on Human Rights*. 2021. № 4. С. 143-150.

25. Біленчук П.Д., Малій М.І. Міжнародно-правові і конституційні засади реалізації прав і свобод людини в Україні як контекст для розвитку кримінальної юстиції. *Проблеми підвищення ефективності кримінальної юстиції України:* колективна монографія / Інститут держави і права імені В.М. Корецького НАН України, Київський університет права НАН України; за заг. ред. Ю.С. Шемшученка, Ю.Л. Бошицького. Київ: Видавництво Ліра-К, 2021. С. 509-523.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

АНБ США– Агенство національної безпеки США

ДОТ – довготривала вогнева точка

ДСА України – Державна судова адміністрація України

ЕОМ – електронна обчислювальна машин

ЄВРОПОЛ – Європейське поліцейське управління – установа правопорядку Європейського Союзу

ЄДРСР – Єдиний державний реєстр судових рішень

ЄС – Європейський Союз

ІНТЕРПОЛ – Міжнародна організація кримінальної поліції

КК – Кримінальний кодекс України

МВС – Міністерство внутрішніх справ України

МО України – Міністерство оборони України

МПА – Міжнародна поліцейська асоціація

НАН України – Національна академія наук України

НАТО – військово-політичний союз (North Atlantic Treaty Organization)

НЦБ Інтерполу в Україні – Національне центральне бюро Інтерполу в Україні

ОАЕ – Об’єднані Арабські Емірати

ОБСЄ – Організація з безпеки і співробітництва в Європі

ООН – Організація Об’єднаних Націй

РНБО – Рада національної безпеки і оборони України

СБУ – Служба безпеки України

США – Сполучені Штати Америки – федеративна республіка в Північній Америці

ТОВ – товариство з обмеженою відповідальністю

ФАТФ – Міжнародна група з протидії відмиванню брудних грошей (Financial Action Task Force on Money Laundering)

ФБР – Федеральне бюро розслідувань агенство Міністерства юстиції США

ФРН – Федеративна Республіка Німеччина

ЦК – Цивільний кодекс України

ЦРУ США – Центральне розвідувальне управління США

ЮНЕСКО – Організація Об'єднаних Націй з питаннях освіти, науки і культури (United Nations Educational, Scientific and Cultural Organization)

BBS – дошки електронних об’яв

BEC – інвестиційне кібершахрайство, шахрайство

CCDCOE – Керівний комітет Об’єднаного центру передових технологій з кібероборони НАТО

CNP – кібершахрайство з використанням карти без наявності

COMPAS – програмне забезпечення (Correctional Offender Management Profilingfor Alternative Sanctions), яке використовується в судах та правоохоронних органах більшості штатів США

CONTI – програми-вимагачі Conti Team

COVID-19 – коронавірус 2019 року (SARS-CoV-2, або 2019-nCoV)

CSAM – матеріали про сексуальне насильство над дітьми

CSIS – Центр стратегічних і міжнародних досліджень США

DDoS – розподілена атака на відмову в обслуговуванні

DFF – Фонд майбутнього Дубая

DIFC – Міжнародний фінансовий центр Дубая (ОАЕ)

EAC – компроментація облікового запису електронної пошти

EDRi – Європейська коаліція за цифрові права

EMOTET – назва комп’ютерного вірусу

EMSAT– європейська система мобільного супутникового зв’язку

EuroHPC – Європейське спільне підприємство з високопродуктивних обчислень

FLASH – звіт ІСЗ ФБР США «FBI Liaison Alert System»

ІСЗ – Центр скарг на злочини в інтернеті ФБР США

IC3 RAT – група з повернення активів в Центрі скарг на злочини в інтернеті ФБР США

ICSEDB – міжнародна база даних щодо сексуальної експлуатації дітей

LDCA – випадки жорстокого поводження з дитиною на відстані

LEO – назва підрозділу силових структур інтернет-поліції

LPS – Лабораторія фізичних наук АНБ США

LQS – LPS Qubit Collaboratory, дослідницький центр квантової інформаційної науки на підтримку Національної квантової ініціативи США

NASA (НАСА) – Національне управління з аеронавтики і дослідження космічного простору (National Aeronautics and Space Administration) – агенство уряду США

P2P – однорангові мережі обміну файлами

RAT – група з повернення активів в Центрі скарг на злочини в інтернеті (IC3) ФБР США

ВСТУП

Обґрунтування вибору теми дослідження. Невід'ємним складником розбудови сучасної України як суверенної і незалежної, демократичної, соціальної, правової держави є забезпечення недоторканості і безпеки охоронюваних конституційних прав та законних інтересів людини. Значне місце серед негативних соціальних явищ, що заважають ефективному становленню демократичних інститутів, займає комп'ютерна злочинність. Кіберзагрози, які пов'язані з кібератаками, комп'ютерними терористичними атаками, які здійснюють сьогодні сучасні хакери і крекери (crackers – це фактично «комп'ютерні терористи», «комп'ютерні пірати», «комп'ютерні кібершахраї») турбують не тільки окремі регіони чи держави. Це сьогодні світова проблема. Це проблема безпеки сучасної електронної цивілізації.

На кіберзагрози, які пов'язані з масштабним зростанням комп'ютерної злочинності у світі вказується в Доповіді Генерального секретаря про роботу ООН за 2021 рік. Зокрема, в доповіді зазначено, що оскільки під час пандемії люди стали частіше користуватися інтернетом, тому ООН розширила підтримку, яка надається державам-членам в боротьбі з кіберзлочинністю та онлайновими зловживаннями.

Необхідність боротьби з комп'ютерною злочинністю ставить перед наукою та правозастосовною діяльністю завдання щодо розробки і реалізації нових ідей, інновацій та більш ефективних засобів запобігання цим небезпечним кримінальним явищам. Важливим завданням кримінології є підвищення ефективності запобігання та протидії комп'ютерній злочинності. Оскільки комп'ютерний злочинець є центральною фігурою, яка здійснює зловмисні дії в кіберпросторі, тому дослідження характерних рис, ознак, властивостей та манер його поведінки в процесі вчинення комп'ютерних злочинів є нагальним та своєчасним, теоретично і практично значимим. Значний обсяг нерозкритих комп'ютерних злочинів як в Україні, так і світі

свідчить про те, що особи, які вчиняють комп'ютерні кримінальні правопорушення не виявляються, не затримуються і фактично не несуть кримінальну відповідальність за свої злочинні дії. Тому особливості пізнання особи комп'ютерного злочинця потребують використання новітніх засобів, методів і технологій його дослідження. Вважаємо також, що і наявний рівень нормативного забезпечення цієї пізнавальної діяльності видається недостатнім.

Теоретичним підгрунтям для вивчення зазначених питань стали праці таких відомих вчених України й зарубіжних країн, як В.В. Голіна, Б.М. Головкін, І.М. Даньшин, М.І. Демура, С.Ф. Денісов, Б.В. Дзюндзюк, А.Ф. Зелінський, О.М. Костенко, М.О. Кравцова, В.М. Куц, Р.В. Перелигіна, О.В. Плахотнік, О.Е. Радутний, В.В. Риков, А.В. Савченко, Т.В. Туз, А.В. Титаренко, Ю.Н. Харарі, А.І. Шевченко, К. Шваб та інші.

Разом із тим на даний час у кримінології бракує наукових робіт, присвячених визначенню сутності поняття і характерних ознак, рис, властивостей і манер поведінки особи комп'ютерного злочинця. Окремі аспекти вказаної проблеми висвітлювали у своїх працях такі науковці, як Н.М. Ахтирська, П.Д. Біленчук, І.Г. Богатирьов, Л.В. Борисова, Д.Л. Виговський, В.О. Голубєв, М.В. Гуцалюк, А.П. Закалюк, С.А. Крушинський, В.В. Налуцишин, Л.П. Паламарчук, В.Г. Хахановський та інші. Однак безпосереднє вивчення особи комп'ютерного злочинця як об'єкта кримінологічного дослідження залишилося поза увагою вчених. Нині існує нагальна потреба у формуванні, по-перше, теоретико-методологічних засад дослідження особи комп'ютерного злочинця, по-друге, розробці кримінологічної систематизації і класифікації комп'ютерних злочинців і, по-третє, визначення пріоритетних напрямів використання новітніх даних з метою комплексного дослідження особи комп'ютерного злочинця для запобігання комп'ютерної злочинності в наземному і космічному кіберпросторі. Саме ці обставини зумовлюють актуальність теми даної дисертації.

Зв’язок роботи з науковими програмами, планами, темами. Дисертація виконана в межах науково-дослідної теми кафедри кримінального права та процесу Хмельницького університету управління та права імені Леоніда Юзькова «Забезпечення прав людини у сфері боротьби зі злочинністю» (номер державної реєстрації 0117U000106), а також згідно з планами науково-дослідної роботи Київського університету права Національної академії наук України в межах теми «Державно-правове регулювання суспільних відносин в умовах нових глобалізаційних викликів: вітчизняні та міжнародні реалії» (номер державної реєстрації U11U004745).

Мета і завдання дослідження. Метою дисертаційного дослідження є формування методологічних положень пізнання сутності особи комп’ютерного злочинця як об’єкта кримінологічного дослідження.

Відповідно до вказаної мети були поставлені та вирішені такі завдання:

1) окреслити теоретико-методологічні засади дослідження особи комп’ютерного злочинця як об’єкта кримінологічного пізнання;

2) сформулювати поняття особи комп’ютерного злочинця;

3) визначити структуру кримінологічної характеристики особи комп’ютерного злочинця;

4) здійснити кримінологічну систематизацію і класифікацію комп’ютерних злочинців;

5) визначити пріоритетні напрями протидії комп’ютерним злочинцям, які вчиняють кримінальні правопорушення;

6) дослідити перспективи і сформулювати напрями протидії вчиненню комп’ютерних злочинів з використанням електронного інтелекту.

Об’єктом дослідження є закономірності формування пізнавальних процесів, пов’язаних з дослідженням наземної і космічної комп’ютерної злочинності в кіберпросторі.

Предметом дослідження виступає особа комп'ютерного злочинця як об’єкт кримінологічного дослідження**.**

Методи дослідження. Методологічну основу даної наукової роботи становить система методів наукового пізнання, а також концептуальні положення загальної теорії кримінології. У процесі виконання дисертаційного дослідження використовувалися *загальнонаукові методи: формально-логічний* – при визначенні поняття і сутності особи комп'ютерного злочинця і виокремленні його суттєвих рис, ознак, властивостей та манер поведінки; *функціональний* – для встановлення перспективних можливостей дослідження особи комп'ютерного злочинця; *системно-структурний* – у процесі з'ясування типових видів комп'ютерних злочинів, які вчиняють комп'ютерні злочинці і розроблення їх наукової кримінологічної систематизації та класифікації; *порівняльний* – під час комплексного дослідження кримінологічної класифікації злочинних посягань комп'ютерних злочинців в наземному і космічному кіберпросторі; *історичний* – при аналізі наукових дискусій стосовно визначення поняття і сутності комп'ютерного злочинця як об'єкта кримінологічного дослідження; *догматичний* – при визначенні перспектив дослідження особи комп'ютерного злочинця.

Теоретичним підгрунтям дисертаційного дослідження є наукові праці вчених у галузі філософії, логіки, психофізіології, лінгвістики, кібернетики, інформатики, кібербезпеки, нейробіоніки, кримінального права, кримінології.

Нормативно-правову базу дисертації становлять Конституція України, кримінальне законодавство України, нормативно-правові акти, що регламентують організацію та діяльність правозахисних органів у процесі запобігання та протидії комп'ютерній злочинності.

Емпіричну базу дослідження становлять аналітичні дані доповіді Генерального секретаря ООН «Протидія використанню інформаційно-комунікаційних технологій в злочинних цілях», які сформульовані ним на сімдесят четвертій сесії Генеральної Асамблеї ООН, узагальнення, викладені у звітах ООН, звіті «TheThreat Report, Summer 2022», звітах Інтерполу, звітах Європолу, звітах ФБР США, звітах Національної поліції України), матеріали слідчої та судової практики, рішення (вироки, ухвали) судів загальної

юрисдикції України в кримінальних провадженнях, статистичні та аналітичні узагальнення правоохоронних органів, конкретні приклади вчинення комп'ютерних злочинів в наземному і космічному кібепросторі, власний емпіричний досвід автора.

Наукова новизна одержаних результатів дослідження полягає у тому, що за характером і змістом розглянутих питань, дане дисертаційне дослідження є одним із перших в Україні комплексним монографічним дослідженням теоретичних і практичних питань пізнання сутності особи комп'ютерного злочинця як об'єкта кримінологічного дослідження. Найістотнішими результатами дослідження, що зумовлюють його наукову новизну та визначають внесок автора в розроблення зазначеної проблематики, є такі положення й висновки:

уперше:

1) окреслені теоретико-методологічні засади дослідження особи комп'ютерного злочинця як об'єкта кримінологічного пізнання, утому числі світоглядно-філософські, соціально-правові, інноваційно-комунікаційні і безпекові;

2) запропоновано новітню кримінологічну систематизацію комп'ютерних злочинців, зокрема виокремлено такі групи: хакери, крекери, фрікери, спамери, колекціонери, фішери, кіберплути, кардери, кіберкрукери, кіберсквокери, інсайдери, вірмейкери, кібертерористи, електронні «торгаші» або кіберпірати, спуфери, творці шкідливих комп'ютерних програм, організовані злочинні кіберугрупування, іноземні розвідувальні кіберслужби;

3) з урахуванням реалій інтенсивного розвитку цифрових технологій визначено пріоритетні напрями протидії комп'ютерним злочинцям, які вчиняють кримінальні правопорушення;

удосконалено:

4) визначення особи комп'ютерного злочинця, яка розглядається як фізична особа (людина), яка вчиняє кримінальні правопорушення з використанням електронно-обчислювальних машин (комп'ютерів), різного

рівня новітніх комп’ютерних засобів і технологій (нанокомп’ютери, портативні комп’ютери, суперкомп’ютери, квантові комп’ютери тощо) та різного виду засобів (електронного, біологічного або нейробіологічного електронного інтелекту тощо), електронних банків даних, систем та комп’ютерних мереж, або інших засобів комп’ютерної інформатизації та різного роду інформаційно-телекомунікаційного обладнання (державного, приватного, наземного, космічного);

5) класифікацію комп’ютерних злочинців, зокрема, за віком, за відношенням до жертви злочину, за професійною діяльністю, за параметрами доступу до комп'ютерних систем, мереж, баз даних;

6) кримінологічну характеристику особи комп’ютерного злочинця, що включає такі параметри (ознаки, риси, характеристики): стать, вік, фізичні дані, інтелектуальний розвиток, мотивація, освіта, злочинний досвід, положення в суспільстві, манери поведінки, риси характеру;

7) положення, що стосуються визначення сутності та правового статусу електронної юридичної особи;

набули подальшого розвитку:

8) позиція про те, що одним із пріоритетних напрямів запобігання зловмисним діям комп’ютерних злочинців є необхідність створення загальносвітової Стратегії кібербезпеки відповідних вітчизняних і міжнародних відомств, установ та організацій;

9) система характерних ознак комп’ютерного злочинця;

10) питання протидії міжнародним кримінальним правопорушенням, що вчиняються комп’ютерними злочинцями, у тому числі й в космічному просторі.

Практичне значення одержаних результатів. Викладені в дисертаційному дослідженні положення, висновки і пропозиції можуть бути використані:

– *у правотворчій діяльності* – під час підготовки конвенцій, законів та інших нормативно-правових актів щодо удосконалення відповідальності за

комп’ютерні кримінальні правопорушення, які вчиняються комп’ютерними злочинцями;

– *у практичній* діяльності органів правопорядку – як кримінологічні рекомендації щодо удосконалення діяльності з виявлення і затримання комп’ютерних злочинців та запобігання комп'ютерній злочинності у наземному і космічному кіберпросторі (акт про впровадження міститься в Додатку Б);

– *у науково-дослідницькій діяльності* – як підгрунтя для подальшого розроблення загальнотеоретичних проблем кримінології, а також кібербезпеки та кібероборони;

– *в освітньому процесі* – при викладанні навчальних дисциплін «Кримінологія», «Кримінальне право. Загальна частина», «Кримінальне право. Особлива частина» та «Порівняльне кримінальне право», підготовці підручників, навчальних і довідкових посібників, методичних матеріалів (акт про впровадження міститься в Додатку В).

Апробація результатів дослідження. Дисертаційне дослідження виконано на кафедрі кримінального права та процесу Хмельницького університету управління та права імені Леоніда Юзькова, представлено та обговорено на її засіданнях, схвалено і рекомендовано до захисту. Основні ключові положення й теоретичні висновки дисертаційного дослідження оприлюднені на 11 міжнародних і вітчизняних науково-практичних заходах.

Крім того, впровадження результатів дисертаційного дослідження в освітню, наукову і праксеологічну діяльність здійснювалося кафедрою кримінального права і процесу юридичного факультету Національного авіаційного університету в рамках реалізації положень Меморандуму про співробітництво між Національним авіаційним університетом та правничою компанією ТОВ «АЮР-КОНСАЛТИНГ» та пріоритетних напрямів розвитку інноваційної діяльності університету за темою «Захист прав і свобод людини і громадянина (кримінально-правові аспекти): 01.09.2017-30.06.2022» (Додаток Г).

Особистий внесок здобувача. Усі сформульовані в дисертації положення та висновки ґрунтуються на власних дослідженнях. Новітні ідеї та наукові розробки, що належать співавтору публікацій за темою дисертації, здобувачем не використовувалися.

Публікації. Основні положення та висновки, що сформульовані в дисертації, оприлюднені у 25 наукових публікаціях, з яких 4 статті опубліковано у фахових періодичних виданнях України, 2 статті – в інших вітчизняних виданнях, 1 – у зарубіжних наукових виданнях, 7 – у колективних монографіях, а також тези 11 доповідей на науково-практичних конференціях.

Структура та обсяг дисертації обумовлені метою, завданням та предметом дослідження**.** Дисертація складається із вступу, трьох розділів, що поділені на шість підрозділів, висновків, списку використаних джерел та додатків. Загальний обсяг роботи становить 224 сторінки, з яких основний текст – 164 сторінки, список використаних джерел викладений на 24 сторінках і охоплює 212 найменувань, додатки – на 17 сторінках.

РОЗДІЛ 1
ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ЗАСАДИ ДОСЛІДЖЕННЯ ОСОБИ КОМП'ЮТЕРНОГО ЗЛОЧИНЦЯ

1.1. Теоретико-методологічні засади комплексного дослідження особи комп’ютерного злочинця як об’єкта кримінологічного пізнання

Людство у даний час знаходиться у витоків нових кардинальних інноваційно-комунікаційних, революційно-еволюційних змін, які фундаментально визначають пріоритетні напрями цивілізаційного розвитку в третьому тисячолітті. Очевидно, що за швидкостю, об’ємами, складністю і масштабами фундаментальних змін, людство ще не переживало таких аналогів на своєму тисячолітньому шляху цивілізаційного розвитку. Попередній розвиток світу ще не бачив таких приголомшливих інноваційних соціально-комунікаційних технологічних проривів в найрізноманітніших галузях діяльності з яким зустрінеться нове покоління людей з потужним розвитком цифрової цивілізації [45, с. 25].

Звичайно, що в першу чергу це торкнеться широкомасштабних змін в галузі кібернетики, інформатики, електронного інтелекту, робототехніки, ноозасобів, інтерактивних методів, нанотехнологій, грід-технологій, біотехнології, тривимірного друку, матеріалознавства, накопичення, передачі і збереження енергії, квантових обчислень, електронного-права, електронної-економіки, електронної-інтелектуальної власності, кібербезпеки, електронної кримінології, електронного експертознавства і багатьох інших сфер освітньої, наукової, праксеологічної людської діяльності.

Тому дане дисертаційне дослідження проводиться з метою всебічного дослідження особи комп’ютерного злочинця та направлене на те, щоб сформулювати чіткий орієнтир для кримінологів в електронний (цифровий) час для того, щоб вчасно зорієнтуватися в швидкоплинних змінах, які чекають світову спільноту в близькому майбутньому.

Очевидно, що настав час нам визначити і знайти чіткі перспективи свого майбутнього і мати віру, впевненість, тверді наміри, володіти знаннями, вміннями і навичками вчасно використати революційні інноваційно-комунікаційні технології для того, щоб запобігти і протидіяти комп'ютерній злочинності. Такий прогностичний підхід дозволить якісно змінити сучасний світ і зробити його для людини кращим, безпечним, щасливим, радісним, здоровим, заможним, багатим і успішним.

Дійсно людська цивілізація переживає в даний час унікальні, але разом з тим кардинальні еволюційні зміни, які безпосередньо відбуваються на наших очах. Цікаво, що якщо деякі речі нам колись бачилися як фантастичними, то сьогодні вони стають для нас звичайною реальністю, безпосереднім побутовим явищем нашого повсякденного життя. Це і комп'ютер, і робот-автомобіль, і розумний-годинник, і розумний будинок, і розумне місто, і інтернет-речей, і великі дані, і всесвітня мережа інтернет тощо.

Все це для кожної людини стає вже звичайною буденністю і не викликає якихось яскравих парадоксальних здивувань, але потребує надійного захисту від злочинних кіберпосягань. Фактично без цих речей ми взагалі вже не уявляємо своє життя, свою працю, свій відпочинок, своє навчання і т.п.

Різниця тільки в тому, що всі ці зміни відбуваються сьогодні з шаленою швидкістю і, звичайно, супроводжуються великими інноваційними викликами, ризиками, інколи кіберзагрозами, кібернебезпеками та потужною нечуваною раніше конкуренцією [45, с. 26].

Фактично четверта промислова революція, концептуальні засади якої сформулював засновник і президент Всесвітнього економічного форуму в Женеві-Давосі (Швейцарія) – Клаус Шваб, буквально в найближчі роки з допомогою проривних інновацій внесе кардинальні зміни і буде суттєво впливати на всю інфраструктуру світової культури, освіти, науки, медицини, економіки і політики [208, с. 12].

Всебічний аналіз і узагальнення досвіду та поглядів провідних світових експертів в галузі управління, менеджменту, економіки, інноваційних

технологій і кібербезпеки, а також результати діяльності лідерів потужних міжнародних транснаціональних компаній, корпорацій і установ, дозволив Клаусу Швабу системно структурувати, консолідовано визначити головні тренди і кібербезпекові алгоритми пріоритетного розвитку цифрової цивілізації.

К. Шваб справедливо вказує, що всі новітні ідеї, інновації і наукові досягнення мають одну загальну особливість: вони ефективно використовують всюдипроникливу силу цифрових і інформаційних технологій. Причому все це забезпечується і удосконалюється за допомогою обчислювальних потужностей, системної консолідованої аналітики даних та електронного інтелекту [208, с. 12].

Отже ці світоглядні тенденції електронного цивілізаційного розвитку слід враховувати при дослідженні особи комп'ютерного злочинця як об'єкта кримінологічного пізнання.

Узагальнені і проаналізовані дані результатів діяльності лідерів світових інновацій в цифровому світі дозволяють нам, як вважає К. Шваб, сформулювати мету, завдання і визначити певні орієнтири та висвітлити окремі передбачення і прогнози з метою зміни людської свідомості та окреслити пріоритети реальної готовності жити, вчитися, працювати і відпочивати в новому цифровому суспільстві [208, с. 17-23].

Це обумовлено тим, що світове співтовариство знаходиться сьогодні у підніжжя «Індустрії 4.0», на світанку четвертої промислової революції, яка принесе фундаментальні якісні зміни в наше життя, в нашу культуру, в нашу освіту, в нашу науку, в нашу працю і взагалі в наше міжособистісне спілкування, співпрацю, партнерство, взаємодію і міжнародне порозуміння.

Важливо тільки чітко усвідомити масштаби, швидкість, всеосяжність темпів розвитку і всесвітній розмах колориту «Індустрії 4.0» і четвертої промислової революції. Особливо тут слід звернути увагу на формування Стратегії кібербезпеки в реаліях бурхливого розвитку електронної цивілізації.

Звичайно, що «Індустрія 4.0» дозволить надати людству необмежені можливості пізнання світу, в якому мільярди людей зможуть миттєво комунікувати між собою з допомогою Всесвітньої мережі інтернет, блокчейну, грід-технологій, мобільних пристроїв, Big Data, інтернет-речей. А це значить, що перед світовою спільнотою відкриваються безпрецедентні горизонти у сфері збирання, фіксації, електронного документування, зберігання, обробки, аналізу даних, відомостей, інформації в реальному часі та прийняття швидких змістовних і якісних, креативних рішень. Людина отримує надпотужний і колосальний за об'ємом доступ до світової скарбниці знань, навиків, умінь та різного роду природних ресурсів, в тому числі і людських. Водночас, необмежені можливості використання інноваційно-комунікаційних технологій несуть певні кіберзагрози, які слід враховувати в реальному житті.

Це обумовлено тим, що для вирішення своїх щоденних завдань людина зможе системно і структуровано користуватися цими інноваційно-комунікаційними технологіями, які побудовані на межі переплетень фізики, хімії, біології, нейробіоніки, психофізіології, математики, кібернетики, інформатики, робототехніки і комунікаційних цифрових реалій «Індустрії 4.0». Очевидно, що в майбутньому корінним чином зміниться парадигма (алгоритми і правила) системи виробництва, споживання, транспортування, зберігання і доставки товарів та послуг.

Аналогічні зміни відбудуться і в соціально-комунікаційній сфері (навчанні, праці, відпочинку, самовираженні, міжособистісному спілкуванні тощо).

Суттєві зміни відбудуться на рівні урядових, державних і міждержавних установ і організацій, особливо у сфері комунікаційного управління системами законотворчості, освіти, науки, охорони здоров'я, культури, транспорту, кібербезпеки, житлового і паркового господарства, зберігання довкілля та культурної спадщини, культурних цінностей і мистецьких творів.

Очевидно, що розвиток «Індустрії 4.0» пов'язаний з певними труднощами, невизначеностями, які обумовлені кореляційними складнощами

взаємодії, партнерства, співпраці урядів, освітньої і наукової спільноти, підприємництва та громадянського суспільства не тільки окремих країн, але загалом усього світу. Все залежить від наявності тісної співпраці, порозуміння всіх гравців цивілізованої міжнародної спільноти для досягнення означеної мети зробити світ кращим – щасливим, радісним, заможним, багатим, чесним, справедливим, гуманним і безпечним.

Визначальним, звичайно, тут буде розуміння чіткої мети і завдань, які будуються на загальнолюдських цінностях, звичаях, традиціях світової спільноти. А це значить, що потрібно усвідомити, визначити, окреслити всім гравцям цивілізації комплексне та чітке єдине уявлення потреб залучення і використання інноваційних комунікаційних цифрових технологій з метою зміни і покращення сенсу і сутності життя на землі як для теперішніх, так і для майбутніх поколінь.

Окреслені завдання дозволять намітити план перетворень, які необхідно здійснити з залученням ноозасобів, інтерактивних методів і грід та трансп'ютерних технологій для покращення соціального, культурного, освітнього, наукового, гуманітарного, економічного і безпекового як національного, так і загальносвітового середовища.

Епоха «Індустрії 4.0», очевидно, що буде кардинально іншою в порівнянні з тисячолітньою історією розвитку людини на землі. Завдячуючи використанню арсеналу новітніх технологій людина отримає колосальні можливості для творчої діяльності, але водночас з'являться багато потенційних кіберзагроз, кіберризиків і кібернебезпек. Ці реалії необхідно враховувати уже сьогодні при розробці і конструюванні сучасних надпотужних безпекових засобів, методів і технологій.

Сьогодні як ніколи справедливим є твердження Л.А. Виговського з приводу духовного розвитку самої людини та людства загалом, що розвиток науково-технічного прогресу кардинальним чином змінив розуміння ролі особистості в житті суспільства [86, с. 40].

Як зазначає Л.А. Виговський сьогодні надзвичайно важливу роль починають відігравати системи телекомунікації та освіти, які набувають статусу суспільно значимих й самодостатніх. Телекомунікаційна система докорінно змінює комунікаційні можливості самої людини, оскільки може миттєво надавати їй будь-яку необхідну інформацію без посередництва якихось груп і символічних систем. Використання електронних засобів інформації створює можливість “безпосереднього членства” в групах чи колективах, які мають відповідне радіотехнічне обладнання [86, с. 45].

В зв’язку з цим Ю.Н. Харарі ставить справедливе запитання «якими будуть відносини» між людиною і штучним інтелектом? Чи не стане пересічна людина рабом штучно створених і вічно живих істот із незбагненною свідомістю? [199, с. 4].

Ці питання зобов’язують нас відчути подих нової епохи вже зараз і самому шукати відповіді на непрості запитання, які чекають нас в майбутньому. Очевидно, що ці питання зобов’язують нас аналізувати ескіз майбутнього людства як цілком реальний, хоча і не обов’язково райдужний. Відомо, що на допомогу нам уже зараз приходять різноманітні пристрої зі штучним інтелектом, які успішно вирішують ряд наших завдань.

Тому не випадково застерігає нас Л. Шавалюк про те, що такий стан речей у світі «породжує величезну нерівність, бо ті, хто «на ти» з технологіями, мають зовсім інші перспективи, рівень доходів і соціальний статус, ніж ті, хто далекий від усіляких «комп’ютерних штучок». Це обумовлено також і тим, що «технології суттєво підвищують продуктивність праці», завдяки цьому їх адепти можуть виконувати ту ж саму роботу з меншою кількістю зайнятих, а технологічні гіганти отримують космічні прибутки, які не мають куди дівати. Наслідок – купка людей заробляє мільярди, а решта жорстко конкурує за копійки, що призводить до зростання соціального напруження на осях високий-низький дохід та наявність-відсутність роботи» [206, с. 8].

Відомо, що новітні інформаційно-комунікаційні технології несуть не тільки позитивні зміни в суспільстві, але характеризуються тим, що їх використовують комп'ютерні злочинці в злочинних цілях. Зокрема, в доповіді Генерального секретаря ООН вказано, що питання боротьби з використанням інформаційно-комунікаційних технологій для вчинення злочинів носить надзвичайно багатогранний і складний характер в залежності від різних факторів. До цих факторів відносяться мотиви злочинців, відповідний профіль і вразливі місця потерпілих, методи і технічні засоби, які використовують злочинці, в тому числі конкретні методи маскування їх діяльності, зв'язків зі злочинним контентом (наприклад, матеріалами, які торкаються сексуальної експлуатації дітей) в ході вчинення злочину [179].

Наприклад, в Сполученому Королівстві Великої Британії і Північної Ірландії незважаючи на те, що питання встановлення і затримання комп'ютерних злочинців є пріоритетним завданням, водночас, ще залишається багато проблем стратегічного характеру, зокрема таких:

а) недостатній технічний потенціал для встановлення комп'ютерних злочинців з використанням цифрових технологій, включаючи нестачу співробітників, які володіють достатніми знаннями, навиками і уміннями в галузі інформаційно-комікаційних технологій, а також наявність проблем в затримці таких співробітників на службі, особливо в національних правоохоронних органах;

б) відсутність в ряді країн внутрішнього матеріально-правового законодавства, яке передбачає кримінальну відповідальність за правопорушення, пов'язані з інформаційно-комунікаційними технологіями, що можуть слугувати правовою базою для міжнародного співробітництва шляхом взаємного визнання таких правопорушень (спільного визнання відповідних зловмисних дій злочином);

в) відсутність внутрішнього процесуального законодавства, яке б передбачало гарантії прав людини і режимів нагляду, яке допускає виявлення комп'ютерних злочинців та розслідування злочинів, пов'язаних з

інформаційно-комп’ютерними технологіями та забезпечує допустимість цифрових доказів у суді;

г) проблеми, які потребують підвищення усвідомленості суспільства про необхідність дотримання правил кібербезпеки в зв’язку зі стрімким розвитком злочинів, пов’язаних з інформаційно-комунікаційними технологіями та швидкого повідомлення органів правопорядку про такі дії комп’ютерних злочинців [179].

Ці питання стали теж предметом спеціального обговорення і на наступній сімдесят шостій сесії (A/76/1-2021) Генеральної Асамблеї ООН. Зокрема, заступник Генерального секретаря ООН з питань охорони і безпеки Жіль Мішо у своїй доповіді теж акцентує особливу увагу на тому, що ми працюємо над тим, щоби забезпечити виконання програм Організації Об’єднаних Націй в складних умовах в плані безпеки [99].

Світова практика показує, що кібервійни, кібератаки, кібербулінг, кібертероризм, кіберзлочини в даний час вже набули не тільки транскордонного, транснаціонального, трансконтинентального, планетарного, але і космічного характеру [66, с. 14]. Це зобов’язує міжнародну спільноту, враховуючи можливі глобальні негативні наслідки світового світоупорядкування цього надзвичайно небезпечного соціального явища, постійно здійснювати асиметричний кримінологічний аналіз таких зловмисних намірів комп’ютерних злочинців та контролювати і мінімізувати їх посягання на державні та міждержавні правові, політичні, дипломатичні, освітні, наукові, економічні, екологічні, соціально-комунікаційні відносини [45, с. 7].

Тому очевидно, що розвиток глобальної електронної соціальної комунікації – це головна стратегічна умова формування відносно нової галузі знань і сфери практичної кібербезпекової діяльності в третьому тисячолітті. Очевидно, що сучасний розвиток соціальної мережевої інженерії, яка є «нервовою системою» глобальної електронної комунікації, істотно впливає на стан трансформаційних інноваційних процесів, які сьогодні відбуваються у світі. Тому вважаємо, що дискусія про конвергенцію квантового майбутнього

нині була б неможливою без виникнення і розповсюдження інтернету і розробки нових технологій -grid і blockchain [155; 44, с. 61-80].

Наприклад, вчені справедливо наголошують на тому, що в сучасних умовах глобальна інформаційна мережа надає значні можливості формування в тому числі екологічних знань людини. Основні сайти громадської мобілізації в Україні є соціальні мережі Facebook, Youtube, Instagram, Twitter. Роль цих мереж в об'єднанні та мобілізації громадян у боротьбі для розвитку громадянського суспільства, поширення екологічних знань є надзвичайно великою. Перевага соціальних спільнот як засобу для спілкування за допомогою традиційних ЗМІ полягає у тому, що вони не тільки поширюють екологічну інформацію, а й надають можливість обговорити її, висловити або запропонувати своє бачення вирішення екологічної проблеми. При цьому кожен член в референтній групі, з якою він ідентифікує себе в кіберпросторі, це не лише споживач екологічної інформації, виробленої іншими членами спільноти, але також творець нового контенту, активний суб'єкт спілкування про екологічні проблеми [85, с. 113].

Фактично на даний час чисельність інтернет-користувачів у світовій спільноті зростає за експонентною. Сьогодні уже впевнено можна стверджувати, що людство загалом реально дедалі більше і більше занурюється в інформаційно-комунікаційні глибини електронного цивілізаційного розвитку.

Аналізуючи дану ситуацію Н.М. Ахтирська вказує, що тільки за перше десятиліття XXI століття кількість користувачів інтернету зросла від 350 мільйонів до понад 2 мільярдів. Швидкими темпами змінюються й характеристики комунікаційно-мережевих приладів, їх швидкість та потужність. Закон Мура, емпіричне правило галузі технологій, стверджує, що чіпи процесора – маленькі монтажні плати, що утворюють кістяк будь-якого обчислювального пристрою – стають удвічі швидшими кожних вісімнадцять місяців. А це означає, що в 2025 році комп'ютер працюватиме в 64 рази швидше, ніж в 2013 році. Водночас, залучення значної кількості людей до

світової мережі сприятиме також збільшенню способів вчинення протиправних дій у сфері фінансів, ядерної безпеки, інформаційної безпеки, банківської безпеки, підприємницької діяльності, інтелектуальної власності тощо [32, с. 3].

Це підтверджує і О.В. Зернецька, яка звертає увагу на те, що інтернет сьогодні є конденсованим вираженням глобального полікультурного соціуму в добу глобальної електронної комунікації, яка продукує і транслює нові або оновлені сенси надшвидкими темпами [116, с. 33]. А це значить, що електронна сфера, кіберпростір, електронне право, кіберправо, кіберекономіка, кібербезпека, кіберкримінологія, кіберкриміналістика, кіберекспертологія стають сьогодні надзвичайно пріоритетними об’єктами освітнього, наукового і практичного осмислення та необхідності всебічного пізнання.

Слід зазначити, що розвиток глобальної соціальної електронно-мережевої комунікації в інтернет-середовищі є позитивним підтвердженням того, чому була прийнята країнами «Великої вісімки» в Окінаві у 2000 році Хартія глобального інформаційного суспільства (Окінавська хартія) [119, с. 4]. У нашій державі теж визначені основні стратегічні пріоритети побудови електронного суспільства, які юридично закріплені в Указі Президента України «Про заходи щодо розвитку національної складової глобальної інформаційної мережі та забезпечення широкого доступу до цієї мережі в Україні» [194]. Важливим є те, що у цьому правничому документі передбачається удосконалення правового регулювання діяльності суб’єктів інформаційних відносин, виробництва, використання, поширення та зберігання електронної інформаційної продукції, захисту прав на інтелектуальну власність, посилення юридичної відповідальності за порушення порядку доступу до електронних інформаційних ресурсів усіх форм власності, за умисне поширення комп’ютерних вірусів тощо. У зв’язку зі створенням нових інноваційних електронних продуктів та розширення електронних послуг, що надаються в Україні, виникла необхідність прийняття сучасних правових норм, які б регулювали ці суспільні відносини. Тому з

метою більш детального врегулювання правових відносин в соціально-комунікаційній сфері були прийняті Закон України «Про електронні довірчі послуги» від 5 жовтня 2017 року [107] і Закон України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 року [109].

У зазначених вітчизняних і міжнародних правових документах чітко вказується, що розвиток електронних комунікацій, мережі інтернет та інформаційних grid- і blockchain-технологій свідчить про високий рівень інтелектуального потенціалу людини, суспільства, держави, цивілізації, а також прагнення до удосконалення правового регулювання суспільних відносин в електронному просторі, поліпшення використання наукових досліджень у повсякденному житті для спілкування, обміну мріями, думками, ідеями, інноваціями, «ноу-хау», поглядами, творчим та інтелектуальним надбанням в освітній, науковій і праксеологічній діяльності. Водночас, як стверджує Джаред Коен, засновник і директор наукового центру GoogleIdeas, інтернет є невловимим і таким, що без зупину змінюється, щосекунди стає все більшим і складнішим. Це джерело колосального добра і страхітливого зла. Інтернет – це найграндіозніший в історії унікальний експеримент, де криється анархія і безпорядок. Ця нова здатність вільного самовияву та безперешкодного руху інформації створила багатий віртуальний ландшафт. Брак всебічного надійного і ефективного контролю призводить до інтернет-тероризму, інтернет-злочинності, інтернет-шахрайства, залякування і переслідування, створюються сайти груп ненависті та форуми, де спілкуються терористи. І це тільки початок [209, с. 9].

Очевидно, що сьогодні перед світовою цивілізацією в галузі кіберпростору виникли грандіозні можливості і одночасно нові кібервиклики, кіберзагрози і кібернебезпеки, які потребують негайного вирішення. Фактично для цивілізованого світу необхідне нове «Сінгапурське чудо».

Варто зазначити, що міжнародний досвід діяльності органів державної влади провідних країн світу по протидії корупції свідчить про те, що здійснити

це чудо (подолання корупції) при бажанні можна реально дуже просто і надзвичайно швидко на прикладі діяльності Лі Куан Ю [156, с. 151].

Про реальний стан небезпечних зловмисних дій комп'ютерних злочинців свідчать опубліковані звіти Інтерполу, Європолу, Федерального бюро розслідувань США і Національної поліції України за 2021 рік. А це значить, що є багато питань до сучасного стану законодавчого забезпечення запобігання і протидії комп'ютерній злочинності, а також необхідності професійної підготовки кадрів в галузі кібербезпеки тощо.

Слід зазначити, що технологічні та юридичні питання, які виникають в процесі установлення осіб, які вчиняють комп'ютерні кримінальні правопорушення, вимагають спеціальної професійної підготовки як освітян, науковців, так і практичних співробітників правоохоронних органів. Наприклад, у США атторнеї федерального рівня, які залучають до встановлення осіб, які вчиняють комп'ютерні злочини, щорічно проводять спеціальний недільний курс підвищення кваліфікації, який організовується як державними, так і приватними організаціями. Причому працівники усіх правоохоронних підрозділів федерального рівня проходять відповідні тренування з кібербезпеки. На даний час в США створено національний центр кібернетичної підготовки, де проводиться початкове навчання працівників правоохоронних органів федерального рівня, окремих штатів і місцевого рівня зі спеціалізацією по виявленню і затриманню комп'ютерних злочинців з метою запобігання комп'ютерних злочинів. У апараті Міністра юстиції – Генерального атторнея США створено і функціонує спеціальний відділ дослідження осіб, які вчиняють комп'ютерні злочини, та забезпечення захисту інтелектуальної власності у складі 18 прокурорів. ФБР США теж на рівні штатів сформувало відділення по захисту критичної інфраструктури США від незаконного проникнення комп'ютерних злочинців в автоматизовані комп'ютерні системи, електронні банки даних та електронні мережі.

Очевидно, що дійсно настав уже час суттєво переглянути не тільки кадрову політику в галузі інформаційно-комунікаційних технологій, але також

удосконалити як вітчизняне, так і міжнародне законодавство в галузі кібербезпеки з метою дієвого запобігання і протидії комп'ютерній злочинності. Це обумовлено тим, що згідно річного звіту Інтерполу за 2021 рік особливої уваги сьогодні потребують такі питання, які пов'язані, по-перше, з основними базами даних, по-друге, з необхідністю радикальних дій по протидії кібертероризму, по-третє, з кіберзахистом вразливих спільнот, по-четверте, з гарантуванням безпеки кіберпростору, по-п'яте, зі стриманням незаконних ринків, по-шосте, з підтриманням екологічної безпеки, по-сьоме, зі сприянням глобальній цілісності, по-восьме, з управлінням кіберзахистом, по-дев'яте, із забезпеченням безпечного розвитку людських ресурсів, по-десяте, із формуванням надійної системи кіберзахисту фінансових ресурсів партнерів і донорів [3].

У річному звіті Європолу за 2021 рік теж сформульовані висновки щодо оцінки реальних кіберзагроз організованої злочинності, яка діє в інтернеті. Основними ключовими висновками Європолу за 2021 рік в галузі кіберзлочинності є наступні: наскрізна кіберзлочинність; кіберзалежна злочинність; сексуальне насильство в інтернеті; онлайн-шахрайство; темні мережі (DarkWeb) [14].

Надзвичайно цікавим є звіт ФБР США за 2021 рік, який висвітлює основні кіберзагрози, що здійснюють комп'ютерні злочинці в кіберпросторі. Згідно зі звітом ФБР США за 2021 рік основними кіберзагрозами були наступні: 1) компроментація ділової електронної пошти (BEC); 2) ІСЗ команда відновлення активів. ІСЗ RAT заморожено 328,32 мільйона доларів США із 443,48 мільйонів доларів США загального збитку; 3) шахрайство з конфіденційною інформацією або романні шахрайства; 4) криптовалюта (віртуальна валюта). У 2021 році ІСЗ отримав 34202 скарги, пов'язані з використанням певного типу криптовалюти, як от Bitcoin, Ethereum, Litecoin або Ripple; 5) програми-вимагачі. У 2021 році ІСЗ отримав 3729 скарг, визначених як програми-вимагачі з скоригованими збитками понад 49,2 мільйона доларів. У 2021 році зареєстровано жертви від даних програм-

вимагачів із критично важливого сектору інфраструктури США. У травні 2021 року ІСЗ опублікував звіт FBI Liaison Alert System (FLASH), у якому повідомляється, що ФБР ідентифікувало щонайменше 16 атак програм-вимагачів CONTI, націлених на мережі охорони здоров'я США та служби швидкого реагування, включаючи правоохоронні органи, служби екстренної медичної допомоги, диспетчерські служби 911 центрів муніципалітетів протягом останнього року; 6) шахрайство з технічною підтримкою [13].

У звіті роботи системи виявлення вразливостей і реагування на кіберінциденти та кібератаки за 2021 рік, який підготовлений Оперативним центром реагування на кіберінциденти державного центру кіберзахисту Державної служби спеціального зв'язку та захисту інформації України теж звертається особлива увага на те, що сучасні комп'ютерні злочинці використовують різні засоби, методи і технології для вчинення комп'ютерних злочинів. Серед найбільш небезпечних посягань комп'ютерні злочинці використовують, зокрема, такі способи: шкідливе підключення; сканування; фішинг; компроментація системи; саботаж/шкідливі дії; несанкціонований доступ до інформації; несанкціонована модифікація; шахрайський сайт та багато інших [113].

У звіті Національної поліції України про результати роботи у 2021 році теж є розділ, який присвячений діяльності кіберполіції, які забезпечували встановлення осіб, що вчиняють комп'ютерні злочини. Зокрема, в даному звіті акцентована увага на тому, що «у 2021 році задокументовано майже вдвічі більше злочинів, учинених з використанням високих інформаційних технологій. Зокрема, у майже півтора рази зросла динаміка реєстрації злочинів у банківській сфері та на третину – у сфері комп'ютерних систем. Кіберполіцейські у 2021 році ініціювали проведення 9 міжнародних поліцейських операцій та взяли участь у 8 таких заходах на запрошення іноземних колег. Як приклад, минулого року встановлено трьох громадян України, підозрюваних у створенні вірусу «EMOTET». Через незаконні дії цих громадян потерпілим завдано збитків на суму близько 2 млрд. доларів США.

Крім того, встановлено шістьох громадян України, які за допомогою шкідливого програмного забезпечення «Ransomware» завдали компаніям Республіки Корея та США збитків на загальну суму 500 млн. доларів США.

Водночас, кіберполіцейські продовжують тримати прямий зв'язок з громадянами. Так, у 2021 році по допомогу до кіберполіції звернулося понад 190 тис. громадян. Переважна більшість телефонувала до call-центру, водночас, громадяни активно подавали звернення і через форми електронного запиту». Згідно положень Звіту Національної поліції України про результати роботи у 2021 році в Україні виявлено такі посягання комп'ютерних злочинців. У 2020 році виявлено 5240 комп'ютерних злочинців, а у 2021 році відповідно виявлено 10020 комп'ютерних злочинців. Серед них у 2020 році у банківській сфері – 2110, пов'язаних з онлайн шахрайствами – 1355, у сфері комп'ютерних систем – 1461, та, відповідно у 2021 році у банківській сфері – 3049, пов'язаних з онлайн шахрайствами – 1928, у сфері комп'ютерних систем – 1981 [112].

Слідча, експертна і судова практика українських правоохоронних органів, які забезпечують запобігання кіберзлочинності, теж свідчить, що кількість кримінальних правопорушень, вчинюваних з використанням електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, у тому числі тяжких, середньої тяжкості, невеликої тяжкості в Україні постійно зростає. Якщо у 2016 році в Україні було зареєстровано лише 818 таких комп'ютерних злочинів, то уже в 2017 році було зареєстровано понад 2514 кримінальних правопорушень, а станом на початок серпня 2022 року вже зареєстровано аж 1945 даних кримінальних правопорушень [103]. Судова статистика показує, що тенденції вчинення комп'ютерних злочинів в Україні і світі у 2022 році з використанням інформаційних технологій стрімко зростає. Більше того, багато розслідувань комп'ютерних злочинів уповноваженими органами України були зупинені у зв'язку з необхідністю виконання процесуальних дій в межах міжнародного

співробітництва. А це значить, що такі комп'ютерні злочини будуть розслідуватися роками.

Очевидно, що наявні в органах правосуддя дані не у повній мірі відображають реальний сьогоднішній стан рівня комп'ютерної злочинності у сфері інформаційних технологій в Україні. З огляду на це, як справедливо зазначає Н.М. Ахтирська, сьогодні потребують суттєвих змін закони і відомчі нормативно-правові акти, що регулюють юридичну відповідальність за вчинення кримінальних правопорушень з використанням комп'ютерних засобів, удосконалення процесуального законодавства щодо збору доказів, розширення міжнародного співробітництва під час кримінального провадження, а також підготовку кадрів для розслідування кіберзлочинів [32, с. 5]. Адже відомо, що в Україні спеціальна професійна вузівська підготовка кадрів в галузі кібербезпеки для органів правосуддя, адвокатури і кіберполіції здійснюється не у достатньому обсязі. Це обумовлено тим, що сучасні прокурори, судді, кіберполіцейські і адвокати фактично не володіють достатніми правовими, технічними, кримінологічними, криміналістичними і експертними знаннями в цій швидко ростучій галузі електронного цивілізаційного розвитку [67, с. 57-62].

Виходячи з того, що в Україні поки що не достатньо ведеться базова професійна підготовка з метою запобігання і протидії комп'ютерній злочинності, вважаємо за доцільне створити в закладах вищої освіти системну підготовку відповідних кадрів.

Такі інновації теж сформульовані в Угоді про асоціацію України з Європейським Союзом, в якій чітко визначено, що боротьба з кіберзлочинністю є пріоритетним елементом безпекової політики [193], задля чого на загальнодержавному рівні доцільно вжити низку законодавчих, організаційних, кадрових, освітніх, правових та ресурсних заходів. Актуальність вказаних питань знайшла своє відображення в Стратегії національної безпеки України, відповідно до якої, зокрема, необхідно підвищити спроможність правоохоронних органів щодо запобігання, протидії

та розслідування кіберзлочинів; створити систему підготовки кадрів у сфері кібербезпеки, кіберкримінології, кіберкриміналістики та кіберекспертології; здійснювати міжнародне співробітництво у сфері забезпечення кібербезпеки [195].

Тому, вважаємо, що особливої уваги сьогодні потребують питання, які пов'язані з розвитком грід- і блокчейн-технологій, введенням в обіг криптовалюти, перспектив ефективного використання Всесвітньої павутини – інтернету, соціальних мереж, комп'ютерних ігор, введенням процедури біометричних паспортів (ID-карток), створенням нових інноваційних стартапів, формуванням банків віртуальної власності, перспектив подальшого розвитку інтернет-речей, електронної комерції, обов'язкового гарантування конституційного права людини на інформацію і забезпечення надійної інформаційної кібербезпеки та реальних механізмів відшкодування завданої шкоди у кіберсфері [46, с. 16-17]. Викладене вище дозволяє зробити висновок, що усі ці проблемні питання (загрози, ризики і небезпеки в кіберпросторі) потребують правового, освітнього, наукового забезпечення з метою всебічного вивчення особи комп'ютерного злочинця як об'єкта кримінологічного дослідження. Тому саме ці важливі питання і є предметом даного кримінологічного дослідження. Виходячи з даних позицій, здійснений нами аналіз стану і тенденцій розвитку інформаційно-комунікаційних технологій в Україні і світі дозволяє зробити важливий висновок щодо необхідності удосконалення чинного законодавства, розширення організаційно-технічного і ресурсного забезпечення освітньої та наукової діяльності по запобіганню та протидії комп'ютерній злочинності в епоху формування четвертої промислової революції, Індустрії 4.0 та розвитку суспільства знань [46, с. 16-17].

Підводячи підсумки, слід зазначити, що кіберзлочинність і кібертероризм (як складова частина кіберзлочинності) – це сучасні надзвичайно небезпечні кіберзагрози ефективного розвитку суспільства, держави, цивілізації. Тому вважаємо, що особливої уваги сьогодні потребують

розширення мережі кримінологічних наукових досліджень щодо питань, які торкаються комп’ютерних злочинів, що вчиняються комп’ютерними злочинцями.

Зазначене вище дозволяє окреслити ряд пріоритетних напрямів, які доцільно здійснити на даному етапі розвитку електронної цивілізації. Серед найбільш важливих питань, які потребують наукового осмислення є такі: визначення поняття та сутності фізичної особи комп’ютерного злочинця; дослідження структури кримінологічної характеристики особи комп’ютерного злочинця; розробка правових і наукових засад дослідження кримінологічного портрету комп’ютерного злочинця; формування кримінологічної типології особи комп'ютерного злочинця; розробка структури і основних елементів систематизації та класифікації комп’ютерних злочинців; проведення міжнародного та вітчизняного порівняльного аналізу кримінологічної класифікації та характеристики комп'ютерних злочинців; визначення поняття, сутності та загальної характеристики кримінологічних засобів дослідження комп’ютерного злочинця; визначення можливостей використання новітніх засобів, методів і технологій для кримінологічного дослідження особи комп’ютерного злочинця; виявлення причин та умов розвитку комп’ютерної кіберзлочинності, а також розробки праксеологічних заходів по її запобіганню та протидії; розробка теоретичних основ нової галузі знань – соціально-комунікаційної електронної інженерії особистості комп’ютерного злочинця; формування концептуальних засад правового, кримінологічного, освітнього і праксеологічного забезпечення дослідження особи комп’ютерного злочинця як об’єкта кримінологічного пізнання; удосконалення законодавчого врегулювання правових відносин в соціально-комунікаційній індустрії з метою запобігання комп’ютерних злочинів в кіберпросторі; розробка нових засобів, методів, програм і технологій в галузі комп’ютерної діагностики особи комп’ютерного злочинця; формування стратегії, тактики і мистецтва використання даних про особу комп’ютерного злочинця для запобігання і протидії злочинності в кіберпросторі; розробка системи пріоритетних

напрямів запобігання комп’ютерній злочинності в наземному і космічному просторі на основі вивчення даних про особу комп’ютерного злочинця; дослідження можливостей використання новітніх засобів ідентифікації особи комп’ютерного злочинця для запобігання кримінальних правопорушень в кіберпросторі; розробка концептуальних засад запобігання вчиненню комп’ютерних злочинів електронним інтелектом проти людини, суспільства, держави; здійснення аналізу стану і тенденцій криміногенного впливу комп’ютерної злочинності у галузі соціально-комунікаційної індустрії на засади цивілізаційного розвитку суспільства [149, с. 275-295].

На завершення слід зазначити, що окреслені вище пріоритетні напрямки фактично і являють собою світоглядно-філософську, соціально-правову, інноваційно-комунікаційну і безпекову наукову базу, яка дозволяє здійснити всебічне консолідоване асиметричне дослідження особи комп’ютерного злочинця як об’єкта кримінологічного пізнання.

1.2. Поняття і сутність особи комп'ютерного злочинця

Аналізуючи та оцінюючи небезпеку протиправних діянь для світового співтовариства як відображення об’єктивної дійсності та міжнародної практики запобігання і протидії кіберзлочинам, вчені прийшли до висновку, що кількість діянь, які сприймаються міжнародною спільнотою злочинами в XXI столітті, збільшилася. У 20-х роках XX століття частина юристів-міжнародників виступали за прийняття міжнародного кодексу, де були б перелічені найбільш серйозні порушення міжнародного права і встановлені санкції за діяння, що мають ознаки міжнародної суспільної загрози з їх поділом на дві групи: міжнародні злочини і «правопорушення міжнародного характеру, стосовно яких має місце конфлікт національних юрисдикцій або складно визначити територіальну юрисдикцію певних держав». Міжнародна конференція з уніфікації кримінального законодавства, яка проходила ще у 1927 році у Варшаві, до міжнародних злочинів віднесла такі правопорушення:

піратство; підробка металевих грошей і державних цінних паперів; торгівля рабами; торгівля жінками і дітьми; умисне застосування будь-яких засобів, що здатні спричинити суспільну небезпеку; торгівля наркотиками; торгівля порнографічною літературою; інші злочини, які передбачені міжнародними конвенціями. Тому очевидно, що сьогодні є нагальна потреба у подальшому поглибленні досліджень міжнародної та регіональної юрисдикції, щодо засадничих положень соціально-комунікаційного права, інформаційного права, електронного права, електронної економіки, електронного інтелектуального права, кібербезпеки, кіберкримінології з метою підсилення ефективності запобігання і протидії протиправним діям (кібертероризму, кіберзлочинності) у сфері інформаційних технологій [54].

Очевидно, що злочини міжнародного характеру, до яких відносяться діяння, що посягають на інтереси декількох держав, які вчиняються особами (групами осіб) не у зв'язку з політикою будь-якої держави, а всупереч законодавству і правопорядку своєї держави заради досягнення власних протиправних цілей також являють міжнародну суспільну загрозу.

Аналіз основних міжнародних документів правового регулювання використання інформаційних технологій для вчинення комп'ютерних дозволяє зробити висновок про те, що для ефективної діяльності з метою запобігання і розслідування міжнародних (транскордонних, трансконтинентальних, транснаціональних) комп'ютерних злочинів необхідно: усунути норми «подвійного права»; удосконалити протокол офіційної правової допомоги для ефективного запобігання і розслідування злочинів та вирішення проблеми оперативного отримання із-за кордону вилучених й збережених на час надання правової допомоги комп'ютерної інформації в документованому вигляді для використання як доказу; передбачити канал зв'язку для забезпечення обслуговування невідкладних запитів у будь-який проміжок часу в усіх часових поясах з метою удосконалення системи слідчих й оперативно-розшукових заходів, які стосуються інтересів декількох держав; запровадити системи ідентифікації для сприяння пошуку особи

комп’ютерного злочинця за декілька секунд з метою отримання незаперечних доказів його злочинної діяльності; забезпечити обмін адресами операторів мережі/постачальників послуг мережі; укласти між державами відповідні угоди про надання правової допомоги при вчиненні злочинів у галузі інформаційних технологій [54, с. 121].

Таким чином, здійснений в даному дисертаційному дослідженні аналіз основних міжнародних документів, які забезпечують правове регулювання використання інформаційних технологій, дає підстави зробити висновок, що кінцевою метою кожного комп’ютерного кримінального правопорушення є отримання інформації, яка зберігається, передається, обробляється на комп’ютері у будь-якому вигляді (закодована або ні) та вміщує дані про сфери людської діяльності, а також запропоновані шляхи для ефективної діяльності по запобіганню і розслідуванню транскордонних, трансконтинентальних, транснаціональних, планетарних комп’ютерних злочинів [47, с. 14-15].

Варто зазначити, що сьогодні слідчий не в змозі відстежувати усі технологічні зміни в сфері інформаційних технологій і для дослідження слідів комп’ютерних кримінальних правопорушень особливу увагу належить приділяти використанню можливостей експертизи комп’ютерних систем і машинних носіїв [79, с. 233].

Викладене вище свідчить, що саме інноваційний цивілізаційний безпековий розвиток людства став сьогодні тією рушійною силою, яка звернула особливу зацікавленість на необхідність кримінологічного дослідження сутності поняття особи комп'ютерного злочинця, який сьогодні є ключовим об’єктом кримінологічної характеристики найпоширеніших і найнебезпечніших у світі комп’ютерних злочинців.

Провідний український кримінолог А.П. Закалюк справедливо зазначає, що основним предметом кримінології є злочинність. Інші елементи предмета кримінології так чи інакше тісно пов'язані з її основним предметом — злочинністю, є похідними від нього. Тому їх вивчення допомагає глибше і всебічно визначити основний предмет науки кримінології, зрозуміти його

сутність, закономірності прояву, існування та технології запобігання злочинності в сучасних умовах. Слід зазначити, що до елементів предмета кримінології, що органічно пов'язані зі злочинністю, належать мотиви і механізми діяльнісних проявів характерних рис, ознак особи злочинця, а також такі елементи як детермінація злочинності та злочинних проявів, запобігання дії цих детермінантів і тим самим запобігання злочинності загалом [105, с. 21].

Як стверджує В.М. Куц сьогодні консолідованого поняття злочинності та його визначення, що відображало б сутність, зміст та інші суттєві аспекти цього явища, в кримінології поки що не надано [151, с. 34], але це якраз потребує і зумовлює проводити подальші нові наукові дослідження в цій галузі знань.

На думку А.П. Закалюка, злочинність – це феномен суспільного життя у виді неприйнятної та небезпечної для суспільства масової, відносно стійкої, різнообумовленої кримінальної активності частини членів цього суспільства [105, с. 139]. Варто зауважити, що це один із багатьох наукових підходів до розуміння і визначення сутності злочинності у вітчизняній кримінології, який охарактеризований В.В. Голіною і Б.М. Головкіним як «особистісно-активнісний» [145, с. 54].

Справедливим є також твердження В.В. Голіни та Б.М. Головкіна про те, що одним із основних елементів предмету кримінології є особа злочинця. Оскільки злочинець, як особа засуджена судом за вчинення злочину, – це суспільна більш менш соціалізована людина, то в сучасній кримінології особа злочинця на різних рівнях наукової абстракції досліджується не як уроджена злочинна особа з певною генетично закладеною злочинною програмою, а як продукт недостатньої соціалізації і негативного соціального впливу. Фундаментальним у вітчизняній та й світовій кримінології є положення, що майбутнім злочинцем особа стає внаслідок слабкої позитивної соціалізації. Кримінологія досліджує особу злочинця як поняття високої наукової абстракції, як узагальнений тип певної частини чи групи злочинів і як конкретного злочинця. У межах цього елемента вивчається співвідношення

соціального і біологічного в особі злочинця, дається кримінологічна характеристика та створюється типологія злочинців [144, с. 9].

На сьогодні проведено досить багато досліджень та опубліковано достатньо наукових праць на тему пізнання сутності особи злочинця [121, с. 249]. Крім того, сьогодні існує багато описових, поведінкових, структурних і морально-юридичних визначень поняття сутності як особи, так і особи комп'ютерного злочинця. Водночас в кримінологічній літературі, на думку А.Ф. Зелінського, досі немає одноманітного і чіткого визначення характерних рис, ознак, індивідуальних елементів поняття особи, яке б претендувало на всебічну характеристику особи [114, с. 53].

Зокрема, О.М. Джужа, В.В. Василевич, В.В. Чернєй, С.С. Чернявський визначають особу злочинця як систему соціально-демографічних, соціально-рольових, кримінально-правових, морально-психологічних та інших властивостей осіб, які вчиняють злочини. Злочин виступає не тільки як зовнішній акт, але і як акт вольовий, свідомий, вільно обраний. Це наслідок досить складного процесу, в якому зовнішні обставини пов'язані з внутрішніми умовами. Щоб пізнати причини злочинності, необхідно розкрити механізм злочинної поведінки, а це неможливо зробити, не вивчивши особу злочинця, вплив її властивостей та особливостей на протиправну поведінку [148, с. 15].

На думку інших вчених, будучи різновидом особи взагалі, особа злочинця має загальні ознаки (стать, вік, фах, освіту, соціальний статус тощо), а також властиві лише їй ознаки, які проявляють характер і ступінь її суспільної небезпеки та, відповідно, вказані групи ознак у своїй сукупності становлять структуру особи злочинця [146, с. 81].

Ю.А. Чаплинська особу злочинця (елемента криміналістичної характеристики) визначає як сукупність соціально значущих ознак і відносин, які характеризують винну в порушенні кримінального закону людину, в поєднанні з іншими умовами та обставинами, що впливають на її злочинну поведінку. Створення криміналістичного «портрету» є досить важливим для

всього процесу розслідування. У будь-якому випадку, він надає змогу висунути певні версії та здійснювати розшук особи, що зникла з місця події, а також можливості якісного проведення подальших слідчих (розшукових) дій [203, с. 183].

Цікавою є думка Б.М. Головкіна та О.В. Лисодєда, які вважають, що термін «особистість злочинця» доцільно вживати на індивідуальному рівні, так би мовити адресно, стосовно конкретних осіб, які вчинили ті чи інші злочини. На загальнотеоретичному рівні є сенс використовувати поняття «особа злочинця». Воно охоплює сукупність усіх ознак і властивостей (демографічних, біосоціальних, психофізіологічних, морально-психологічних, кримінально-правових та ін.), що усебічно характеризують злочинця, як члена суспільства і суб'єкта протиправної поведінки. На відміну від цього, поняття особистість злочинця відображає його соціальну властивість, внутрішній світ і виражається в індивідуально-психологічних ознаках, що обумовлюють мотивацію та спрямованість злочинної поведінки. Указані ознаки не можна дослідити методом спостереження. Потрібно спиратися на офіційні документи (висновки експертів, характеристики), а також на результати спеціальних психологічних досліджень, що дозволяють встановити і розкрити індивідуально-психологічні риси, ознаки і властивості злочинців, охарактеризувати потрібнісно-мотиваційну, емоційно-вольову, ціннісно-нормативну сфери особистості. Отже, на рівні кримінологічної теорії доцільно використовувати поняття «особа злочинця», що позначає увесь контингент злочинців, охоплює їх характеристику, тоді як поняття «особистість злочинця» застосовується на рівні окремих категорій злочинців, наприклад: «особистість кіберзлочинця», «особистість домашнього кривдника», «особистість корупціонера», «особистість терориста», а також на індивідуальному рівні, зокрема, «особистість крадія», «особистість маніяка», «особистість шахрая», «особистість ґвалтівника» і так далі [91, с. 43].

В.Г. Лукашевич та К.В. Калюга справедливо стверджують, що сучасна злочинність – це "тихі" паперові (мереживі) дії – вони не залишають слідів, чи

явних слідів. Тобто формально все відбувається за законом. Раніше особа злочинця – це "злочинці громили", а зараз там інтелект (в тому числі з залученням штучного інтелекту), і вони значно ефективніші. Тому і підходи (прийоми, методи) до розкриття та розслідування таких злочинів повинні бути зовсім інші. Справи треба по іншому вивчати, залучати відповідних фахівців, застосовувати інші криміналістичні методи [153, с. 204].

Відзначимо, що згідно із Законом України «Про внесення змін до деяких законодавчих актів України щодо спрощення досудового розслідування окремих категорій кримінальних правопорушень» № 2617-VIII від 22 листопада 2018 р. було внесено зміни до КК України [52], відповідно до яких було введено новий термін «кримінальне правопорушення» та запроваджена нова класифікація кримінальних правопорушень, які поділяються на кримінальні проступки і злочини [53, с. 11]. Тому виникає питання, наскільки коректно вживати термін «особа злочинця» щодо усіх кримінальних правопорушень, а не лише щодо злочинів. У наукових працях використовується також термін «особа кримінального правопорушника»

Вважаємо, що оригінальною є наукова позиція С.А. Крушинського та В.В. Налуцишина відносно того, що варто розрізняти такі поняття, як «суб’єкт кримінального правопорушення» і «особа злочинця (кримінального правопорушника)» [150, с. 49].

При цьому, якщо проаналізувати санкції статей розділу XVI Особливої частини КК України, то можна дійти до висновку, що відповідно до вимог ст. 12 КК України лише склад кримінального правопорушення, передбачений ч. 1 ст. 361 КК України, є кримінальним проступком, а решта є злочинами. Тому, у тому числі, зважаюи на це, у цій роботі ми будемо використовувати традиційний термін «особа злочинця».

В юридичній літературі традиційно вказується, що наука кримінологія вивчає особу злочинця з різних позицій. І.М. Даньшин, В.В. Голіна, М.Ю. Валуйська визначають, що отримання кримінологією наукових знань про злочинність, особу злочинця, кримінальну детермінацію має на меті

належне забезпечення щодо розробок і впровадження у практику боротьби зі злочинністю оптимальних заходів її запобігання в Україні [143, с. 3]. Варто зауважити, що кримінологія вивчає особу злочинця з наступних позицій: по-перше, як елемент кримінологічної характеристики злочину; по-друге, як об'єкт і суб'єкт тактичної взаємодії під час запобігання, протидії злочинам [31, с. 38].

Крім того в кримінологічній науці досліджується поведінка злочинця під час вчинення злочину (механізм і спосіб вчинення), який містить органічно взаємопов'язані елементи внутрішньої (психічної) та зовнішньої (фізичної) діяльності [133, с. 7]. Фактично такі знання, які пов'язані з пізнанням сутності особливих рис і ознак особи комп'ютерного злочинця дозволяють прокурору, слідчому, судді так спланувати й організувати запобігання та протидію злочину, «що всі дії, які будуть проводитися в його рамках, будуть максимально ефективними, а розслідування в цілому буде успішним» [171, с. 31-34].

Слід погодитися з думкою А.П. Закалюка, який стверджує, що у правовій науці, у тому числі і у науці кримінології, уявлення про особу сформовано тільки на підставі загального поняття про неї, яке розроблено у філософії та психології [105, с. 234-235]. Слід зазначити, що в українській мові термін «особа» має два значення. Перше – це особа як діяльнісна самодостатня людина, суб'єкт суспільної активності та діяльності, учасник цих процесів та суспільних утворень. Цьому значенню відповідає російський термін «лицо», а в англійській мові «person». Термін «особа» має й друге значення, зокрема для виділення у людини тієї змістовної якості, яка у соціальному відношенні становить її власну ідентичність (власне Я), яке відрізняє від інших людей та осіб і визначає її ставлення до суспільства, його відносин, правових і етичних норм, що регулюють суспільну життєдіяльність. Іншими словами, це соціальна якість особи. У російській мові терміну «особа» у цьому значенні відповідає термін «личность», а в англійській мові «personality». Що стосується української мови, то – термін «особа» зазвичай об'єднує два російські терміни

«лицо» і «личность», або англійські терміни «person» та «personality». Така етимологія терміна «особа» часто викликає непорозуміння, зокрема, при спеціальному науковому використанні, коли потрібно відділити особу від її соціальної якості. Через це, як вважає А.П. Закалюк, в українській науковій літературі останніх десятиріч, у тому числі в кримінології, поряд з терміном «особа» використовують термін «особистість» для визначення соціальної складової особи [105, с. 234-235]. Такий термін, на наш погляд, є необхідним і правомірним, а тому будемо використовувати надалі терміни «особа» та «особистість» у їх чітко визначеному сутністному значенні.

Варто зазначити, що, на думку Д.Л. Виговського та Т.І. Нікіфорової виникає необхідність більш глибокого вивчення особистості не лише злочинця, а й жертви вчиненого ним злочину [84, с. 178].

Водночас, І.М. Даньшин вважає, що в структурі поняття особи злочинця слід включати такі елементи: біологічну, психологічну та соціальну їх складові. Зокрема, до біологічної складової слід віднести анатомо-фізіологічні, генетичні, нервово-мозкові та інші властивості організму, а також прояви складного механізму успадкування; до психологічної складової – її відчуття, сприйняття, переживання; вольові, інтелектуальні та емоційні особливості, темперамент і характер; до соціальної складової – суспільної сутності, яка складається під впливом суспільства, членом якого вона є [142, с. 34-35].

Аналізуючи безпосередньо структуру особи злочинця, А.П. Закалюк вважає, що вона включає наступні елементи: 1) соціальну характеристику особи злочинця (її особистість): ознаки формування соціалізації особи; ознаки соціального статусу та соціальних ролей; безпосередні ознаки спрямованості особистості; 2) біосоціальні ознаки особи: демографічні ознаки, які мають соціальне і психологічне значення; 3) психофізіологічні особливості, зокрема, стан здоров’я та психологічні риси; 4) взаємозв’язок між вчиненням злочину та особою, яка його вчинила [105, с. 258].

Формулюючи основні положення сутності особи злочинця А.Ф. Зелінський вважає, що питання про характеристику та її основні

елементи особи злочинця можна ставити тільки тоді, коли дана особа буде визнана судом винною у вчиненні злочину, тобто такої, що вчинила систему суспільно небезпечних дій, передбачених кримінальним законом і спрямованих на реалізацію єдиного мотиву [115, с. 56].

Справедливим є твердження С.А. Крушинського та В.В. Налуцишина про те, що без відповідної особи, яка вчиняє кримінальне правопорушення, останнє не може мати місця, для характеристики будь-якого кримінального правопорушення та його складу. Значну увагу слід приділяти суб'єкту, який його вчинив [150, с. 49].

Варто ще раз підкреслити та погодитись з думкою С.А. Крушинського та В.В. Налуцишина, які рекомендують розрізняти поняття «суб'єкта кримінального правопорушення» і «особи злочинця (кримінального правопорушника)». Суб'єкт кримінального правопорушення як кримінально-правове поняття за своїм змістом окреслюється законодавчими ознаками (статус фізичної особи, осудність і вік). Ці ознаки мають кримінально-правове значення, оскільки відсутність хоча б однієї з них означає відсутність складу кримінального правопорушення в цілому. Натомість, термін «особа злочинця» є більш широким і, крім ознак суб'єкта кримінального правопорушення, охоплює ще низку інших характеристик, які виходять за межі складу кримінального правопорушення, однак враховуються судом при призначенні покарання у разі засудження такої особи [150, с. 49].

Таким чином, сьогодні в кримінологічній літературі розглядаються різні думки стосовно сутності змісту самого поняття особа злочинця. В зв'язку з цим С.Ф. Денисов справедливо вказує, що особа злочинця є достатньо складним феноменом, інтегруючим і багатовекторним поняттям [96, с. 154], а тому потребує більш грунтовного системного асиметричного аналізу.

На думку Д.Л. Виговського термін «особа злочинця», по-перше, не зовсім відповідає закладеному в нього змісту, з погляду етимологічних його особливостей. Це пов'язано з некоректним перекладом українською російського терміна «личность преступника». Слово «личность» може бути

перекладене і як «особа», і як «особистість». Але в цьому конкретному випадку більшість науковців веде мову про сукупність рис характеру злочинця, його психологічних схильностей, звичок і особливостей. При цьому цей злочинець, зазвичай, є одиницею абстрактною, без згадки реальної людини «особа насильницького злочинця», «особа корисливого злочинця» тощо. Натомість «особа» - це конкретний індивід, член суспільства. По-друге, таке некоректне використання терміна стало традиційним в українській кримінологічній науці, що нівелювало можливі помилки в розумінні сутності «особи злочинця».

На думку вченого, використання терміну «особистість злочинця» є більш коректним, з погляду формальних правил, але через розповсюдженість і загальновживаність терміна «особа злочинця» як синонімічного терміну «особистість злочинця», використання обох цих термінів є припустимим і не може призвести до помилкового уявлення про предмет наукової дискусії [82, с. 145].

Відомо, що перше в Україні дослідження портрета комп'ютерного злочинця здійснене ще у 1997 році [56]. Дану працю побудовано на основі узагальнення вітчизняного та зарубіжного досвіду дослідження характерних рис і ознак особи комп'ютерного злочинця. Крім того в даному дослідженні розкривається сутність поняття особи комп'ютерного злочинця, розкрита характеристика особи комп'ютерного злочинця та сформульована класифікація комп'ютерних злочинців, які вчиняли злочини 25 років тому.

Водночас, судова статистика свідчить про стрімке зростання кількості вчинених комп'ютерних злочинів в світі за останні роки. Виходячи з даних позицій, вважаємо, що комп'ютерні злочинці, які вчиняють комп'ютерні злочини сьогодні у Всесвітній мережі інтернет потребують спеціального і більш детального наукового дослідження. Особливо нагальними питаннями при дослідженні особи комп'ютерного злочинця, це вивчення його особистих якостей, психофізіологічних особливостей, індивідуальних рис та ознак,

притаманних саме йому та закономірностей манер його поведінки при вчиненні комп'ютерних злочинів.

Так, заступник директора Федерального бюро розслідувань Пол Аббат (Paul Abbate) наголошує на тому, що у 2021 році в Сполучених Штатах Америки спостерігалося безпрецедентне зростання кібератак і зловмисної кіберактивності. Про це йдеться в аналітичному звіті Центру скарг на злочини в Інтернеті ФБР (IC3), який надає американській громадськості прямий вихід для повідомлення про кіберзлочини в режимі онлайн. Так, у 2021 році IC3 продовжувала отримувати рекордну кількість скарг від американської громадськості: 847 376 скарг, що на 7% більше, ніж у 2020 році, з потенційними збитками, що перевищили 6,9 мільярда доларів. Серед отриманих у 2021 році скарг програми-вимагачі, схеми компрометації бізнес-електронної пошти (BEC) і злочинне використання криптовалюти є одними з найбільш повідомлених інцидентів. У 2021 році схеми компрометації бізнес-електронної пошти призвели до 19 954 скарг зі скоригованими втратами майже 2,4 мільярда доларів [13].

Статистика ФБР США свідчить, що комп'ютерні злочинці постійно удосконалюють свою діяльність, кількість скарг про факти вчинення кіберінцидентів, кіберзлочинів, кібератак постійно зростає. Про це свідчать також дані, які опубліковані у Звіті Національної поліції України. Тому зростає потреба безпосереднього дослідження осіб, які вчиняють кібератаки, кіберзлочини тощо.

Очевидно, що чітке наукове визначення сутності даного поняття, отримане в результаті здійсненого дослідження, дасть дослідникам зрозуміти суть та наповненість того, що саме включається у поняття «особа комп'ютерного злочинця».

Висвітлюючи характеристику особи, яка вчиняє злочини з використанням інформаційних технологій, Л.П. Паламарчук справедливо відмічає її основні ознаки, основною з яких є те, що у цю злочинність втягнуто широке коло осіб, від професіоналів до дилетантів. Причому даний автор

зазначає, що комп’ютерні правопорушники мають різний соціальний статус і різний рівень освіти (навчання, виховання тощо) [166, с. 8].

Дійсно, досліджуючи та аналізуючи поняття особи комп’ютерного злочинця за останні двадцять п’ять років (1997-2022 р.р.) не можна констатувати, що сьогодні «портрет особи комп’ютерного злочинця» має однакові ознаки та вичерпний їх перелік. Перш за все, це обумовлено науково-технічним розвитком, а також залежить від рівня освіченості та обізнаності комп’ютерного злочинця в роботі технічних пристроїв (комп’ютерів, телефонів, планшетів, інших гаджетів) та рівня електронного доступу до них (санкціонованого чи несанкціонованого). Тільки виходячи з таких позицій, можливо сформувати сутність поняття особи комп’ютерного злочинця і систематизувати та класифікувати осіб, які вчиняють комп’ютерні кримінальні правопорушення.

Сама дефініція сутності «особи комп’ютерного злочинця» – очевидно умовна і, оскільки може розглядатися як низка характеристик, ознак, рис, відомостей та манери поведінки під час вчинення комп’ютерного кримінального правопорушення, що мають фундаментальне значення для запобігання, протидії та розслідування комп’ютерних кримінальних правопорушень.

В процесі розвитку науки кримінології та дослідження саме сутності поняття особи комп’ютерного злочинця, науковці-дослідники в залежності від рівня інноваційного розвитку суспільства вкладали у дане поняття в різні роки різні сутнісні значення. Це обумовлено тим, що стрімкий розвиток інформаційно-телекомунікаційних технологій та впровадження їх в освіту, науку і практику постійно змінювало і види комп’ютерних злочинів, а також виявляло нові характерні риси, ознаки та індивідуальні властивості комп’ютерних злочинців.

Зважаючи на те, що сьогодні окремим розділом XVI КК України визначено склади кримінальних правопорушень у сфері використання ЕОМ (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку,

особливої уваги сьогодні потребують питання, які пов’язані з дослідженням, по-перше, визначення сутності поняття комп’ютерного злочинця, по-друге, формулювання основних елементів кримінологічної характеристики особи комп’ютерного злочинця, по-третє, визначення типологічних ознак і рис особи комп’ютерного злочинця, по-четверте, розкриття характерних ознак портрета комп’ютерного злочинця, і, по-п’яте, окреслення структури систематизації і класифікації комп’ютерних злочинців.

Водночас, наукові кримінологічні дослідження і судова практика дозволяють зробити висновок, що сьогодні комп’ютерні злочини фактично можуть здійснювати фізичні особи (комп’ютерні злочинці) з допомогою автоматизованих інформаційно-комунікаційних систем наділених електронним інтелектом.

Очевидно, що стосується сутності поняття електронного інтелекту і можливості його використання для вчинення комп’ютерних злочинів, то ці питання потребують особливої уваги оскільки ні в кримінологічній літературі, ні в чинному законодавстві України, Європи і світу в науковому плані не досліджені, та юридично в законодавсті не закріплені. А це значить, що новітні розробки по створенню електронного (штучного) інтелекту несуть не тільки користь суспільству, але і величезні кіберзагрози, кіберризики і кібернебезпеки.

Проведені нами дослідження свідчать, що за статистичними даними найбільшу частку комп’ютерних злочинів (73,8% від загальної кількості) становить саме вчинення діянь, передбачених ст. 361 КК України «Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп’ютерів), автоматизованих систем, комп’ютерних мереж чи мереж електрозв’язку» [64, с. 14-15]. Зокрема протягом 2014-2017 р.р. Державним центром кіберзахисту та протидії кіберзагрозам Державної служби спеціального зв’язку та захисту інформації України було зареєстровано 792 випадки (216 - 234 щороку) різних типів посягань на інформацію, що обробляється засобами ЕОМ (кіберзагроз). Серед них необхідно виокремити

такі: 82 - несанкціоноване втручання, 97 - DDoS-атака, 149 - поширення шкідливого програмного забезпечення, 353 - фішинг (інтернет-шахрайство), 45 - APT-атака (несанкціоноване втручання до інформаційних систем потерпілого шляхом встановлення прихованого доступу до них з метою використання або контролю в майбутньому) та 65 інших видів, до яких належать «ботнет» мережі (мережа комп'ютерів, заражених шкідливими програмами), експлуатація уразливості системи (використання недоліків у комп'ютерній системі, завдяки яким можна навмисно порушити її цілісність, що призведе до неправильної роботи [64, с. 14-15].

Також варто зазначити, що Оперативним центром реагування на кіберінциденти Державного центру кіберзахисту Державної служби спеціального зв'язку та захисту інформації України підготовлено та опубліковано «Звіт роботи системи виявлення вразливостей і реагування на кіберінциденти та кібератаки» за 2021 рік, в якому висвітлюються статистика зібраних та опрацьованих даних, категорії та типи подій інформаційної безпеки, ключові кіберзагрози, а також надано рекомендації щодо підвищення рівня кіберзахисту комунікаційних систем всіх форм власності [167].

Так, згідно з аналітичними даними Оперативного центру реагування на кіберінциденти Державного центру кіберзахисту Державної служби спеціального зв'язку та захисту інформації України за 2021 рік зафіксовано неймовірну кількість подій, які отримали статус «підозрілих», а саме: 41 мільйон підозрілих подій інформаційної безпеки, та, відповідно, опрацьовано 160 тисяч критичних подій, в результаті чого виявлено та задокументовано 147 кіберінцидентів [167].

Вище наведена статистика зібраних та опрацьованих даних представлена згідно з Переліком категорій кіберінцидентів, схваленого Національним координаційним центром кібербезпеки при Раді національної безпеки та оборони України (протокол № 18 засідання Національного координаційного центру кібербезпеки при Раді національної безпеки і оборони України від 25 жовтня 2021 р.), та включає такі категорії подій ІБ:01. шкідливий

(образливий) вміст; 02. шкідливий програмний код; 03. збір інформації зловмисником; 04. спроби втручання; 05. втручання; 06. порушення доступності; 07. порушення властивостей інформації; 08. шахрайство; 09. відома вразливість та 10. інше [167].

Також в даному аналітичному звіті кіберінциденти розподілено по типах подій з відповідною статистикою, а саме: 01.01. спам (8000); 02.01. зараження шкідливим програмним забезпеченням (20000); 02.02 розповсюдження шкідливого програмного забезпечення (20000); 02.03 командно-контрольний центр (260000); 02.04 шкідливе підключення (300000); 03.01 сканування (300000); 03.03 фішинг (300000); 04.01 спроба експлуатації вразливості (80000);04.02 спроби авторизації/входу в систему (25000); 05.01 компрометація облікового запису (8000); 05.02 компрометація системи (250000); 06.01 атака на відмову в обслуговуванні (10000); 06.02 саботаж/шкідливі дії (300000); 06.03 збій (5000); 07.01 несанкціонований доступ до інформації (300000); 07.02 несанкціонована модифікація (270000); 08.01 шахрайський сайт (300000); 09.01 вразливість (300000); 10.01 невизначений інцидент (300000) [167].

Варто також зазначити, що засобами Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки забезпечується цілодобовий моніторинг кіберпростору, аналіз і передання телеметричної інформації про події інформаційної безпеки, які фіксуються на об’єктах кіберзахисту і можуть мати негативний вплив на їх стале функціонування.

Відповідно до зібраних статистичних даних, найбільше кіберінцидентів стосувалися шкідливого програмного коду (28%), збору інформації зловмисниками (18%) та шахрайства (6%).

Як зазначає керівник Державного центру кіберзахисту Державної служби спеціального зв’язку та захисту інформації України А.П. Кузміч, уніфікація категорій та єдина система передачі інформації дала можливість більш ефективно та злагоджено працювати основним суб'єктам національної системи кібербезпеки України, а сам перелік категорій кіберінцидентів був

розроблений на основі рекомендацій Національного координаційного центру кібербезпеки при Раді національної безпеки та оборони України [1].

Також варто звернути особливу увагу на значне збільшення та велику інтенсивність кіберінцидентів в Україні, що підтверджується різними вітчизняними та закордонними аналітичними дослідженнями. Так, наприклад, керівник Державного центру кіберзахисту Державної служби спеціального зв'язку та захисту інформації України А.П. Кузміч стверджує, що країна-агресор Російська Федерація здійснює кібератаки переважно на державні органи влади України, та у сукупності з інформаційною війною, вони мають на меті завдати значної шкоди державному устрою та економіці України. За перші чотири місяці 2021 року Командою реагування на комп'ютерні надзвичайні події України CERT-UA (спеціалізованим структурним підрозділом Державного центру кіберзахисту Державної служби спеціального зв'язку та захисту інформації України) було зафіксовано 178 кібератак (за весь попередній 2020 рік було зафіксовано загалом 261 кібератаку), які за сукупністю технічних методів і організаційних заходів можна віднести до країни-агресора Російської Федерації [29].

В звіті «The Threat Report, Summer 2022» фахівці компанії Trellix Threat Labs заявляють, що наприкінці січня 2022 року війна Російської Федерації з Україною стала каталізатором розділення кіберзлочинців на тих, які підтримують збройну агресію, та на тих які проти неї. А також можемо побачити співпрацю російських та українських злочинців-вимагачів заради фінансової вигоди. Наприклад, свідомий вибір сторони став найбільш очевидним у програмі-вимагачі Conti Team, коли злочинці-вимагачі публічно висловлювали свою підтримку уряду Російської Федерації та підтримку їхніх дій [27].

Наприкінці другого кварталу 2022 року кіберфахівці Trellix Threat Labs спостерігали за діями злочинців-вимагачів пов'язаних з Conti Team, та зважаючи на те, що жодних членів цієї злочинної групи не було заарештовано представниками правоохоронних органів Російської Федерації, дійшли

висновку, що це свідчить про формування гібридної злочинної групи, яка може атакувати цілі, вибрані урядом, але з підтриманням правдоподібного заперечення даної злочинної групи після посиленого фінансування [27]. Фактично ми ведемо мову про «державу-кіберзлочинця», як дивно б це не звучало.

Фахівці компанії Trellix спільно з співробітниками Центру стратегічних і міжнародних досліджень США (CSIS) дійшли основного висновку у звіті «In the Crosshairs: Organizations and Nation-State Cyber Threats», що межа між державними та недержавними комп'ютерними злочинцями продовжує стиратися [5].

Значне збільшення облікованої кількості та різкий приріст динаміки комп'ютерних злочинів відображено також в звіті Національної поліції України про результати роботи у 2021 році. З метою протидії комп'ютерній злочинності в Національній поліції функціонує підрозділ кіберполіції, фаховими співробітниками якого за 2021 звітний рік задокументовано майже вдвічі більше злочинів, учинених з використанням високих інформаційних технологій. Зокрема, у майже півтора рази зросла динаміка реєстрації злочинів у банківській сфері, та на третину – у сфері комп'ютерних систем [112].

Варто зазначити, що періодичне обмеження соціальної активності громадян України у зв'язку з посиленням карантиних заходів спровокувало збільшення на 42 % шахрайств, пов'язаних з використанням електронно-обчислювальної техніки (ч.ч. 3, 4 ст. 190 КК України). Так, у 2021 році підрозділом кіберполіції зафіксовано понад 190000 звернень громадян України, в тому числі через форми електронного запиту. В результаті проведених розслідувань правоохоронними органами задокументовано 10020 кіберзлочинів, серед яких найбільш поширеними є такі: у банківській сфері – 3049; пов'язані з онлайн-шахрайством – 1928; у сфері комп'ютерних систем – 1981. Наприклад, фахівцями кіберполіції в ході міжнародної поліцейської операції затримано трьох громадян України, підозрюваних у створенні вірусу «EMOTET». Через зловмисні незаконні дії даних громадян потерпілим завдано

значних збитків на суму близько 2 млрд. доларів США. Крім того, співробітниками правоохоронних органів також затримано шістьох громадян України, які за допомогою шкідливого програмного забезпечення «Ransomware» завдали компаніям Республіки Корея та США збитків на загальну суму 500 млн. доларів США [112].

Сьогодні справедливими є твердження В.В. Налуцишина та С.А. Крушинського, що законодавці всіх європейських країн включили норми про відповідальність за комп'ютерні злочини до своїх кримінальних кодексів. Також вони вважають, що розвиток та подальше вдосконалення вітчизняного законодавства про відповідальність за злочини у сфері комп'ютерної інформації та протидії їм, неможливі без використання досвіду застосування кримінального законодавства країн Європейського Союзу [164, с. 445].

Важливим висновком на основі аналізу запобігання та протидії комп'ютерній злочинності в державах Європейського Союзу, як зазначають вчені, є позитивий досвід ряду держав Європейського Союзу щодо притягнення до відповідальності юридичних осіб за посягання на системи автоматизованої обробки даних [164, с. 448].

І. Бірюк вказує на те, що комп'ютерні злочини – це одна з найдинамічніших груп суспільно небезпечних посягань. Практика свідчить, що швидко збільшуються показники поширення комп'ютерних злочинів, а також постійно зростає їх суспільна небезпечність. Очевидно, що це зумовлено прискореним розвитком науки й технологій у сфері комп'ютеризації, інформатизації, а також постійним і стрімким розширенням сфери застосування комп'ютерної техніки [77, с. 175-177].

Дещо іншу позицію займають Я.С. Яценко, К.Ю. Ісмайлов, які погоджуються з визначенням Ю. Батурина, що кіберзлочинність – це злочинність у так званому «віртуальному просторі» [212, с. 54-55]. Ю. Батурин вважає, що віртуальний простір – це інформаційний простір, що моделюється за допомогою комп'ютера, у якому перебувають відомості про особу, предмети, факти, події, явища і процеси, представлені в математичному,

символьному або будь-якому іншому вигляді, й рухи, що перебувають у процесі, по локальних і глобальних комп’ютерних мережах, або відомості, що зберігаються в пам’яті будь-якого фізичного або віртуального пристрою, а також іншого носія, спеціально призначеного для їхнього зберігання, обробки й передачі [38, с. 2].

М.В. Салтевський визначає комп'ютерний злочин – як протиправне використання засобів електронно-обчислювальної техніки: великих, середніх та малих машин, у тому числі персональних комп'ютерів, програмних засобів, технологій та комунікативних систем зв'язку з корисливою метою [183, с. 3]. Водночас дані автори не розкривають сутнісні характеристики особи комп’ютерного злочинця.

На наш погляд цікавою є позиція Б.В. Дзюндзюка, який визначає, що кіберзлочинець – це злочинець, який вчиняє свої злочини у «віртуальному просторі» за допомогою комп’ютера та виходу до інтернету з метою досягнення своїх власних інтересів [98].

Слід зазначити, що донедавна у вітчизняному законодавстві було відсутнє взагалі чітке нормативне визначення поняття «кіберзлочинність», «комп’ютерний злочинець» або «кіберзлочин». Зокрема, у КК України у розділі XVI визначено лише перелік кримінальних правопорушень у сфері використання ЕОМ (комп’ютерів), систем та комп’ютерних мереж. А в Законі України «Про національну безпеку України» [108] серед основних реальних та потенційних загроз національній безпеці України передбачені тільки основні засади спрямування державної політики у сферах національної безпеки і оборони на забезпечення кібербезпеки України.

Сьогодні варто зазначити, що поняття особи комп’ютерного злочинця фактично схоже з поняттям особи кіберзлочинця, адже по суті дані поняття розкривають один і той самий зміст, що полягає у стилістиці вчинення людиною комп’ютерного злочину, але на нашу думку поняття особи комп’ютерного злочинця є значно ширшим і більш досконалим. В даному випадку така стилістика прослідковується саме у застосуванні, зокрема,

засобів комп'ютерної інформатизації ЕОМ (комп'ютерів), систем та комп'ютерних мереж.

Кримінологічні дослідження особи комп'ютерного злочинця обмежуються головним чином тими особливостями людини, які необхідні для використання з метою протидії, запобігання, профілактики, попередження й розслідування цих злочинів [76, с. 145]. Кримінологія вивчає, в першу чергу, «професійні» звички злочинців, які проявляються, в основному, в певних способах і прийомах вчинення злочинів, що залишають на місці вчинення злочинів характерний спосіб, метод вчинення злочину, дії (modus operandi), профіль злочинця, «почерк» злочинця, слідову картину, типовий портрет злочинця. Це обумовлено тим, що результати кожної злочинної діяльності містять специфічні сліди людини (ідеальні і матеріальні, звичайні і електронні), яка їх залишила. Тому виявлення на місці вчинення злочину речових доказів, електронних слідів злочину проливає світло на відомості як про деякі особисті соціально-психофізіологічні ознаки, риси, звички, манери поведінки злочинця, так і про його злочинний досвід, професію, соціальні і професійні знання, навички, уміння, стать, вік, особливості взаємодії з потерпілим. Тому, очевидно, що формування банку типових моделей різних категорій злочинців, вивчення загальних рис цих людей дозволяє оптимізувати процес виявлення кола осіб, серед яких варто вести пошук злочинця [64, с.14-15].

Виходячи з положень чинного законодавства, М.О. Кравцова вважає, що фактично кримінально-правовий обсяг поняття «кіберзлочинність» складають злочини, передбачені ст.ст. 361, 361-1, 361-2, 362, 363, 363-1 КК України. На її думку під кіберзлочинністю слід розуміти соціально-правовий феномен, що проявляється в забороненій законом про кримінальну відповідальність предметній діяльності (кримінальній активності) частини населення з використанням ЕОМ (комп'ютерів), телекомунікаційних систем, комп'ютерних мереж і мереж електрозв'язку [137, с. 19].

Окремим заходом запобігання вчиненню кіберзлочинів, вчені вважають, виявлення та запобігання діяльності кібертерористів, тобто осіб, які використовують комп’ютерну техніку, пристрої та мережі для вчинення терористичних актів [141, с. 408].

Як зазначає М.О. Кравцова важливим напрямом діяльності щодо протидії вчиненню кіберзлочинів слід також визначити виявлення осіб, які вчиняють або схильні до вчинення кіберзлочинів, індикаторами поведінки яких є систематичний перезапис даних без необхідності, заміна або видалення даних, поява фальшивих записів, випадків, коли оператор системи без об’єктивних підстав починає працювати наднормово, персонал заперечує проти здійснення контролю за записом даних, фіксуються постійні скарги користувачів баз даних або власників щодо помилок та затримок у роботі системи тощо [138, с. 164].

Підсумовуючи вище викладене, слід зазначити, що методика дослідження особи комп’ютерного злочинця, по-перше, базується на тому, що аналізуються матеріали слідчої, судової і експертної практики щодо вчинених злочинів з використанням електронно-обчислювальних машин, комп’ютерів, електронних баз даних, та інформаційно-комунікаційних комп'ютерних мереж і мереж електрозв’язку. По-друге, оскільки комп’ютерні злочинці є поширеною групою осіб покоління «digital-nature», які достатньо професійно володіють спеціальними знаннями, комп’ютерними технологіями для вчинення комп’ютерних злочинів в кіберпросторі, то дослідженню підлягають як світоглядно-філософські, морально-психологічні, психофізіологічні, соціально-комунікаційні, інноваційно-аналітичні, безпекові, так і юридично значимі риси, ознаки, звички, властивості, манери поведінки особи комп’ютерного злочинця.

Враховуючи викладене, робимо висновок, що **особа комп’ютерного злочинця** – це фізична особа (людина), яка вчиняє кримінальні правопорушення з використанням електронно-обчислювальних машин (комп’ютерів), різного рівня новітніх комп’ютерних засобів і технологій

(нанокомп’ютери, портативні комп’ютери, суперкомп’ютери, квантові комп’ютери тощо) та різного виду засобів (електронного, біологічного або нейробіологічного електронного інтелекту тощо), електронних банків даних, систем та комп’ютерних мереж, або інших засобів комп’ютерної інформатизації та різного роду інформаційно-телекомунікаційного обладнання (державного, приватного, наземного, космічного).

На завершення важливо підкреслити також і те, що як справедливо зазначає А.В. Титаренко, комп’ютерна злочинність сучасного світу не знає кордонів. Віртуальні злочини є транснаціональними не лише тому, що для комп’ютерних мереж не існує кордонів, а й через відсутність цілісної законодавчої бази щодо кримінальної відповідальності суб’єктів таких злочинів. Проблема комп’ютерної злочинності набирає оберти і в Україні. У зв’язку з цим у правоохоронних органів виникло доволі широке коло завдань, які мають переважно технічний та процесуальний характер. Одне з таких завдань повязане із відсутністю чіткої класифікації злочинів, вчинених у сфері використання ЕОМ (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку, а також у недостатній підготовці слідчих для проведення огляду місць вчинення злочинів з використанням комп’ютерної техніки [188, с. 160].

І з цим не можна не погодитись, адже стрімкий розвиток у сфері створення новітніх автоматизованих комп’ютерних систем, засобів електронного інтелекту, електронних банків даних, інформаційно-комп’ютерних мереж та сучасних комп’ютерних технологій породжує й розвиток та удосконалення діяльності криміногенного світу (комп’ютерних злочинців), що в свою чергу пов'язаний і з проблематикою необізнаності кадрів правоохоронних органів щодо запобігання та протидії розвитку комп’ютерній злочинності.

Висновки до розділу 1

1. Особа комп'ютерного злочинця як об'єкт кримінологічного дослідження тісно взаємопов'язана перш за все з безпосередньою подією вчинення комп'ютерного злочину. Тому вважаємо, що сама дефініція сутності «особи комп'ютерного злочинця» – очевидно умовна і, оскільки може розглядатися як низка характеристик, ознак, рис, відомостей та манери поведінки під час вчинення комп'ютерного злочину, що мають фундаментальне значення для запобігання, протидії та розслідування комп'ютерних злочинів стосовно осіб, які вчинили дане кримінальне правопорушення. Водночас, слід зазначити, що на законодавчому рівні поняття сутності особи, що вчинила саме комп'ютерний злочин фактично і юридично відсутнє.

2. Особливо небезпечним сьогодні є можливість використання організованими злочинними угрупуваннями (хакерами, крекерами, фрікерами, спуферами, колекціонерами, кіберплутами, інсайдерами, терористами, піратами, шахраями) новітніх розробок в злочинних цілях, які уже сьогодні несуть надзвичайно потужну загрозу та небезпеку соціально-комунікаційним системам і мережам, автоматизованим базам та банкам даних і критичній інфраструктурі держави загалом.

3. Для ефективної діяльності з метою запобігання і розслідування міжнародних (транскордонних, трансконтинентальних, транснаціональних) комп'ютерних злочинів необхідно: усунути норми «подвійного права»; удосконалити протокол офіційної правової допомоги для ефективного запобігання і розслідування злочинів та вирішення проблеми оперативного отримання з-за кордону вилучених й збережених на час надання правової допомоги комп'ютерної інформації в документованому вигляді для використання як доказу; передбачити канал зв'язку для забезпечення обслуговування невідкладних запитів у будь-який проміжок часу в усіх часових поясах з метою удосконалення системи слідчих й оперативно-

розшукових заходів, які стосуються інтересів декількох держав; запровадити системи ідентифікації для сприяння пошуку особи комп'ютерного злочинця за декілька секунд з метою отримання незаперечних доказів його злочинної діяльності; забезпечити обмін адресами операторів мережі/постачальників послуг мережі; укласти між державами відповідні угоди про надання правової допомоги при вчиненні злочинів у галузі інформаційних технологій.

4. За результатами дослідження пропонуємо визначення особи комп'ютерного злочинця як фізичної особи (людини), яка вчиняє кримінальні правопорушення з використанням електронно-обчислювальних машин (комп'ютерів), різного рівня новітніх комп'ютерних засобів і технологій (нанокомп'ютери, портативні комп'ютери, суперкомп'ютери, квантові комп'ютери тощо) та різного виду засобів (електронного, біологічного або нейробіологічного електронного інтелекту тощо), електронних банків даних, систем та комп'ютерних мереж, або інших засобів комп'ютерної інформатизації та різного роду інформаційно-телекомунікаційного обладнання (державного, приватного, наземного, космічного).

РОЗДІЛ 2
КОМП'ЮТЕРНИЙ ЗЛОЧИНЕЦЬ ЯК ОБ'ЄКТ СИСТЕМНОГО КРИМІНОЛОГІЧНОГО ДОСЛІДЖЕННЯ

2.1. Поняття і структура кримінологічної характеристики особи комп'ютерного злочинця

Аналізуючи поняття і сутність кримінологічної характеристики особи комп'ютерного злочинця, вважаємо, що доцільно користуватися як новітніми, так традиційними засобами, методами, методиками і технологіями пізнання сутності соціальних явищ. Вагомий внесок у формування продуктивних методологічних принципів пізнання соціальних явищ, в тому числі і кримінологічних явищ внесли Чезаре Беккарія, Юрій Блувштейн, Джонн Локк, Артур Шопенгауер, Огюст Кант, Еміль Дюркгейм, Анатолій Закалюк, Олександр Костенко, Зігмунд Фрейд та багато інших як вітчизняних, так і зарубіжних філософів, психологів та кримінологів.

О.М. Костенко і Р.В. Перелигіна вважають, що під методом кримінологічного дослідження слід розуміти узгоджену з принципом кримінологічного пізнання сукупність прийомів, що застосовуються для пізнання злочинності, її причин і умов, особистості злочинця і розробки заходів протидії злочинності [136, с. 6].

Очевидно, що комп'ютерний злочинець як об'єкт системного консолідованого асиметричного кримінологічного дослідження повинен вивчатися за допомогою новітньої системи засобів, методів, методик і технологій. Дана система засобів необхідна для зібрання, обробки, аналізу і інтерпретації кримінологічно значущої інформації про характерні ознаки і риси, манери поведінки особи комп'ютерного злочинця. На даний час для здійснення кримінологічних досліджень характерних рис і ознак та манер поведінки особи комп'ютерного злочинця використовуються такі групи

засобів і методів збирання інформації: 1) документальний метод; 2) опитування; 3) спостереження; 4) експеримент [136, с. 6].

Водночас, в процесі кримінологічного дослідження характеристики особи комп'ютерного злочинця активно використовуються засоби і методи обробки, аналізу, упорядкування та інтерпретації зібраної кримінологічної інформації. Такий арсенал засобів, методів, методик і технологій кримінологічного дослідження характеристики особи комп'ютерного злочинця необхідний для одержання нових теоретичних і практичних висновків з метою запобігання і протидії сучасній комп'ютерній злочинності.

Тому в даному підрозділі нами зроблена спроба застосувати сучасний арсенал наукових засобів і методів, методик і технологій для пізнання сутності та розкриття структури кримінологічної характеристики особи комп'ютерного злочинця. Водночас, звертаємо увагу на те, що ці питання є достатньо складними, дискусійними, полемічними, оскільки системно є малодослідженими як у вітчизняній, так і зарубіжній кримінологічній літературі.

Виходячи з даних позицій, перейдемо до більш детального розгляду і висвітлення поняття і сутності кримінологічної характеристики особи комп'ютерного злочинця. Слід акцентувати увагу на тому, що особа комп'ютерного злочинця досліджується різними юридичними науками: філософією права, кримінологією, криміналістикою тощо.

Водночас, кримінологічні дослідження особи комп'ютерного злочинця обмежуються головним чином тими рисами, ознаками, властивостями і особливостями манер поведінки людини, які необхідні для використання отриманих даних з метою запобігання і попередження комп'ютерних злочинів.

Відомо, що кримінологічна наука в першу чергу досліджує характерні «професійні» звички комп'ютерних злочинців, які проявляються, в основному, в певних способах і прийомах вчинення комп'ютерних злочинів та проступків, оскільки такі злочинці залишають на місці вчинення кримінальних правопорушень характерний «почерк», тобто відображають безпосередній

«портрет» комп’ютерного злочинця. Це обумовлено тим, що в результаті кожної злочинної діяльності комп'ютерний злочинець залишає свої матеріальні і ідеальні сліди [50].

Тому очевидно, що виявлення на місці вчинення комп’ютерного злочину як звичайних (сліди рук, ніг, голосу, запаху і т.п.), так особливо електронних речових доказів проливають світло як на відомості про деякі його особисті соціально-психологічні риси, ознаки, властивості, манери поведінки, так і на відомості про його злочинний досвід, професію, соціальні і професійні знання в галузі кібернетики, інформатики, стать, вік, особливості взаємодії з потерпілим в реальному житті та кіберпросторі.

Транснаціональний та транскордонний характер злочинності, специфіка утворення електронних слідів поза юрисдикцією держави зумовлюють необхідність розвитку міжнародного співробітництва, формування уніфікованого міжнародного законодавства щодо використання електронних доказів у кримінальному судочинстві.

Кримінологічні дослідження особи комп’ютерного злочинця базуються в основному на двох особливо значимих специфічних групах відомостей. По-перше, це відомості про особу невідомого комп’ютерного злочинця. Такі відомості будуються в основному на основі залишених комп’ютерним злочинцем матеріальних слідах як на місці події комп’ютерного злочину, так і ідеальних слідах відображених в пам'яті свідків, потерпілих тощо. Очевидно, що такі відомості дозволяють сформулювати уяву про загальні риси, ознаки та манери поведінки комп’ютерного злочинця. По-друге, це відомості, які характеризують риси, ознаки та манери поведінки для встановлення відомого комп’ютерного злочинця. Очевидно, що в даній ситуації досліджуються відомості не тільки про ціннісні орієнтації, особливості антисуспільних поглядів, але і про те, яка інформація є найбільш характерною для досліджуваної особи комп’ютерного злочинця. З цією метою вивчаються особливості поведінки комп’ютерного злочинця до, під час і після вчинення комп’ютерного злочину, його зв’язках з потерпілим.

Очевидно, що врахування таких відомостей про особу комп’ютерного злочинця можуть бути покладені в основу систематизації і класифікації комп’ютерних злочинців [81, с. 30]. Вважаємо, що формування банку типових моделей поведінки окремих категорій комп’ютерних злочинців, дозволяє не тільки їх систематизувати і класифікувати по окремих параметрах, категоріях, групах, але і оптимізувати сам процес виявлення слідової картини, способів вчинення комп’ютерних злочинів, а також більш детально дослідити системи безпеки безпосередньо об’єкту кібернападу чи кіберпосягання.

Аналізуючи характерні риси, ознаки, відомості та манери поведінки особи комп'ютерного злочинця, слід звернути особливу увагу на основну ознаку, яка характеризує даний вид злочину. Це обумовлено тим, що сьогодні в комп’ютерну злочинність втягнуто фактично надзвичайно широке коло комп’ютерних зловмисників, від висококваліфікованих комп’ютерних фахівців – хакерів і суперкрекерів, до звичайних професійно не підготовлених дилетантів. Цікавим є також і той факт, що в комп’ютерну злочинність залучаються комп’ютерні злочинці з усіх сфер як звичайної, так і високопрофесійної діяльності. Очевидно, що комп’ютерні злочинці є вихідцями з освітнього середовища (школярі, студенти, викладачі), зі сфери науки (програмісти, дизайнери, інженери тощо), а також практики, які надають сервісні послуги тощо. Причому комп’ютерні злочинці характеризуються різними рівнями освіти, науковими здобутками та практичної професійної комп’ютерної діяльності.

Вважаємо, що з метою більш глибокого та всебічного кримінологічного асиметричного дослідження таких осіб необхідно достатньо чітко і впевнено знати, хто ж вони – комп'ютерні злочинці [55, с. 15]. Сучасний системний аналіз комп’ютерних кримінологічних досліджень здійснений освітянами і науковцями в цій галузі знань дозволяє всебічно сформулювати реальний «портрет», а також соціальний «профіль» типового комп'ютерного злочинця.

Тому вважаємо, що особливо важливо розглянути більш детально як загальні характерні риси, ознаки та манери поведінки комп'ютерного

злочинця, так і індивідуальні психофізіологічні ознаки, властивості особи конкретного комп’ютерного злочинця.

Слід зазначити, що майбутній комп’ютерний злочинець практично знайомиться з комп'ютером ще у дитячому віці. Фактично з дитинства він обожнює комп’ютер. Для нього комп’ютер і автоматизована комп'ютерна система – це загадка, таємниця, яку необхідно всебічно пізнати, дослідити та всебічно і ефективно використовувати для вирішення власне поставленої мети. Тому такі особистості вже у школі, а пізніше у закладах вищої освіти досконало і всебічно вивчають основи комп'ютерної науки: кібернетики, інформатики, електроніки тощо. В більшості випадків майбутні комп’ютерні злочинці набувають фахових комп’ютерних знань ще у школі, коледжі, інституті або в університеті. Відомо, що самостійне вивчення можливостей комп’ютерних технологій і автоматизованих комп’ютерних систем комп’ютерним злочинцем теж є надійним фундаментом для вчинення в майбутньому комп’ютерних злочинів.

Дослідження наукових літературних джерел і аналіз вітчизняної, а також зарубіжної практики показує, що вік комп'ютерних злочинців в основному коливається в досить широких межах (в середньому 13-45 років). Проведені дослідження показують, що на момент вчинення злочину вік 33 % злочинців не перевищував 20 років, 13 % - були старші 40 років і 54 % - мали вік від 20 до 40 років [56, с. 9]. Таким чином, сучасні комп’ютерні злочинці – це не завжди зовсім молоді особи, як вважали раніше.

Відомо, що біля 83 % осіб даної категорії (злочинці, які були заарештовані в Сполучених Штатах Америки за комп'ютерні злочини) - це чоловіки, але слід зауважити, що сьогодні уже доля жінок швидко зростає через професійну орієнтацію деяких нових спеціальностей та посад, які заповнюють в основному жінки (секретар, програміст, бухгалтер, дизайнер, фінансист, економіст, менеджер, касир, контролер, ділознавець, тощо). Водночас, слід звернути увагу і на те, що розмір ресурсних збитків від комп’ютерних злочинів, які вчиняють чоловіки, у чотири рази більший, чим

від злочинів, що вчиняють жінки. За даними соціологів США приблизно третина комп'ютерних злочинців становлять жінки [56, с. 10].

Що стосується освітньої професійної підготовки, то більшість комп'ютерних злочинців у віці від 14 до 21 навчаються у коледжі або інституті чи університеті. Про це свідчить і той факт, що більшість комп'ютерних вірусів сьогодні створюється саме студентами-хакерами у період літніх або зимових канікул [127, с. 117]. Також відомо, що сучасні комп'ютерні злочинці у школах, коледжах, інститутах і університетах добре навчаються по ряду комп'ютерних дисциплін (основи інформатики, кібернетики, електроніки), але можуть фактично відставати в освітній підготовці по ряду інших галузей знань. Практика свідчить, наприклад, що значна частка комп'ютерних програмістів не вміє добре писати і оформляти документацію, або інколи має достатньо слабо розвинуті мовні чи риторичні знання, уміння і навики.

Водночас, слід акцентувати особливу увагу на тому, що комп'ютерні злочинці володіють достатньо високим коефіцієнтом інтелекту (IQ), як правило, вище за середнього, оскільки високий рівень інтелекту обов'язково необхідний для написання складної компактної комп'ютерної програми чи вміння проникати в таємниці електронного всесвіту. Практика показує, що 77 % комп'ютерних злочинців, які вчиняли комп'ютерні злочини, мали середній рівень інтелектуального розвитку, 21 % - вище середнього і тільки 2 % - нижче середнього. Важливо акцентувати увагу ще і на рівень освітньої підготовки комп'ютерних злочинців. Зокрема, 20 % комп'ютерних злочинців мали середню освіту, 20 % - середню спеціальну і 40 % вищу [177, с. 16-19]. Це свідчить про достатньо потужні професійні здібності, знання, навики і уміння комп'ютерних злочинців.

Що стосується рівня спеціальної професійної комп'ютерної освіти комп'ютених злочинців то він є теж достатньо широкий. Фактично сучасні комп'ютерні злочинці є такі особи, які володіють як мінімальними знаннями, навиками, уміннями користувача комп'ютера чи автоматизованих

комп’ютерних систем, так і є достатньо висококваліфікованими, високоосвіченими комп’ютерними фахівцями в галузі кібернетики, інформатики, кібербезпеки тощо. Кримінологічні дослідження засвідчують, що 52 % комп’ютерних злочинців мали спеціальну професійну комп’ютерну підготовку в галузі автоматизованої обробки комп’ютерної інформації, 97 % - були службовцями державних установ і організацій, які в процесі професійної діяльності використовували автоматизовані комп'ютерні системи, автоматизовані електронні банки даних і інформаційні комп’ютерні технології в своїх професійних виробничих процесах, а 30 % з них мали безпосереднє відношення до експлуатації та сервісного обслуговування засобів автоматизованих систем, електронних банків даних і комп'ютерної техніки [38, с. 271]. Вважаємо, що з дослідницької позиції цікавим є і той факт, що з кожної тисячі комп'ютерних злочинів тільки сім вчинені професійними програмістами [177, с. 16-19]. Судова статистика підтверджує, що в окремих випадках комп’ютерні злочинці, які вчинили комп'ютерні злочини, взагалі не мали спеціального професійного технічного досвіду в галузі автоматизованих комп’ютерних систем, комп’ютерних мереж і електронних баз даних.

Вважаємо, що слід особливо звернути увагу і на те, що особистими психофізіологічними особливостями, ознаками і рисами, які характеризують особу комп'ютерного злочинця являються, по-перше, достатньо активна життєва позиція, по-друге, специфічність, оригінальність (нестандартність) мислення і нетипові манери поведінки, по-третє, чутливість, обережність, уважність і водночас зухвалість здійснюваних злочинних дій: кіберпосягань, кібератак тощо. Як правило комп’ютерні злочинці зосереджують свою увагу на вчиненні комп’ютерних злочинів, які передбачають розуміння, передбачення і управління автоматизованими комп’ютерними системами і інформаційно-технологічними процесами. Вважаємо, що такий виважений ретельний підхід до вчинення комп’ютерних злочинів є основою їх спеціальної комп’ютерної компетенції та професійної майстерності. Відомо, що комп’ютерні злочинці відзначаються надзвичайною обережністю,

уважністю і професійною пильністю, оскільки їх злочинні дії достатньо виважені, витончені, досконалі, хитромудрі, оскільки супроводжуються відмінним маскуванням своїх зловмисних дій [49, с. 216-218].

Що стосується особистих людських психофізіологічних ознак, рис, манер поведінки і характеристик – то це як правило, достатньо яскрава, мисляча й творча особистість, дійсно великий і уважний професіонал своєї справи, який реально здатний іти на неймовірно зухвалий, зловмисний, науковий та технічний виклик і пізнати, зламати і отримати цінну інформацію з автоматизованої комп’ютерної системи. Водночас, це людина, яка достатньо серйозно боїться втратити свій значний накопичений професійний авторитет серед колег або соціальний статус у своєму колективі. Водночас, комп’ютерні злочинці стараються бути втаємничими, оскільки достатньо серйозно бояться на роботі сторонніх глузувань. Крім того зовні манери поведінки комп’ютерних злочинців рідко відрізняється від встановлених у державі, колективі, соціальних, звичаєвих та правових норм поведінки. Ще однією важливою характерною ознакою є те, що комп'ютерні злочинці у своїй більшості випадків взагалі не мають кримінального минулого. Це ускладнює органам правосуддя виявляти осіб, які вчиняють комп’ютерні злочини.

Слід звернути особливу увагу і на те, що, як правило, значна частина комп'ютерних злочинів вчиняється комп’ютерними злочинцями індивідуально. Водночас, судова статистика свідчить, що сьогодні має місце негативна тенденція співучасті комп’ютерних злочинців в забезпеченні діяльності організованих злочинних організацій з метою вчинення групових кіберпосягань. Зокрема, статистичні дані свідчать, що 38 % комп’ютерних злочинців діяли самостійно, індивідуально без співучасників, але 62 % комп’ютерних злочинців вчиняли комп’ютерні злочини в складі організованих злочинних груп і потужних криміногенних співтовариств [165, с. 12-13].

Дійсно, комп’ютерні злочинці, які вчиняють комп’ютерні злочини в складі організованих злочинних груп, є достатньо технічно і технологічно оснащені, оскільки мають на своєму озброєнні достатньо дорогі, престижні,

науково місткі й могутні сучасні автоматизовані комп'ютерні системи, інформаційно-комунікаційні технології та новітні комп’ютерні програми. Це дозволяє їм використовувати прогресивні новітні технології для вчинення різних видів комп’ютерних злочинів. Причому сучасні автоматизовані комп’ютерні системи і засоби телекомунікації сьогодні створюють реальні прагматичні можливості для вчинення комп’ютерних злочинів дистанційно, оскільки регіони їх впливу є достатньо широкими. Сьогодні вже відомо, що такі комп’ютерні злочини можуть вчинятися уже за межами країни безпосереднього перебування комп’ютерного злочинця.

Тобто комп’ютерні злочинці уже діють сьогодні як на регіональному, загальнодержавному, так і на транскордонному, транснаціональному, трансконтинентальному і планетарному рівні. Сьогоднішні юридичні факти свідчать і про те, що комп’ютерна злочинність уже вийшла з наземного рівня, оскільки є випадки вчинення таких злочинів в космічному кіберпросторі.

Небезпечним є і те, що сьогодні велика кількість сучасних комп'ютерних злочинців – це фактично керівники різних установ, організацій і відомств всіх рангів. Статистично це більше 25 % комп’ютерних злочинців. Вважаємо, що це обумовлено тим, що керівником, є, як правило, спеціаліст більш високого класу, який володіє достатніми професійними знаннями, навиками, уміннями. Крім того, такі керівники мають безпосередній доступ до широкого кола таємних відомостей організації і, звичайно, володіють кодами доступу до автоматизованих комп’ютерних систем установи, де вони працюють. Важливим є і те, що керівники установ і організацій згідно з посадовими інструкціями мають право і зобов’язані давати відповідні вказівки та розпорядження і безпосередньо не відповідати за технологічні процеси, які пов’язані з роботою комп'ютерної техніки [129, с. 18-20].

Тому, розглядаючи сутність ознак і рис комп'ютерного злочинця В.Б. Вехов вважає, що кримінологічну характеристику його особи слід вважати поняттям комплексним, системним в широкому значенні цього слова,

хоча з деяким поділом на самостійні відокремлені групи по ряду специфічних рис та ознак [81, с. 28-39].

Аналіз досліджень, проведених Ю.М. Батуріним, В.П. Веховим, П.Б. Гудковим та іншими дослідниками [38; 48; 81; 55; 92], дають можливість сформулювати основні риси, ознаки, манери поведінки і властивості окремих груп людей, які реально схильні до вчинення комп'ютерних злочинів.

В.Б. Вехов вважає, що до першої групи комп'ютерних злочинців слід відносити осіб, які характеризуються сталим поєднанням професіоналізму у галузі комп'ютерної техніки і комп'ютерного програмування з елементами своєрідного фанатизму, творчості і винахідливості [81, с. 31]. На думку Ю.М. Батурина і А.М. Жодзинського ці комп'ютерні злочинці сприймають можливість використовувати засоби комп'ютерної техніки як своєрідний технологічний виклик їх творчим і професійним знанням, умінням і навикам [40, с. 158]. Саме це, як вважає В.Б. Вехов, є у соціально-психологічному плані стимулюючим фактором, своєрідним детонатором, мотивацією для вчинення різних зловмисних дій, більшість з яких мають ярко виражений злочинний характер. За наявними у провідних спецслужбах світу даними, комп'ютерних злочинців, хакерів і крекерів широко використовують організовані злочинні організації для проникнення в зарубіжні і вітчизняні автоматизовані комп'ютерні системи [81, с. 28-39].

Аналізуючи риси, ознаки, манери поведінки і властивості типових комп'ютерних злочинців першої групи В.Б. Вехов вказує на наступні особливості, які характеризують осіб даної категорії: по-перше, це відсутність у них чітко продуманого плану підготовки до вчинення злочину; по-друге, специфічність, оригінальність і нетиповість способу вчинення комп'ютерного злочину; по-третє, використання в якості інструментів, знарядь для вчинення комп'ютерного злочину побутових технічних засобів, пристроїв і предметів (звичайних комп'ютерів тощо); по-четвертих, неприйняття заходів власної безпеки з метою приховування факту здійсненого ними комп'ютерного

злочину; в-п’ятих, вчинення пустотливих нетипових дій на місці події вчинення комп’ютерного злочину [81, с. 28-39].

Підводячи підсумки всебічного аналізу рис, ознак, манер поведінки і характерних властивостей комп’ютерних злочинців першої групи, слід віддати належне, що це особи, які фактично не завжди прагнуть реально вчинити комп’ютерний злочин. Для них це спочатку забава, безкорислива гра, яка викликана спортивним інтересом, азартом, фанатизмом з метою подолання таємничого, загадкового комп’ютерного монстра. В процесі такої гри першопочатківці-комп’ютерні злочинці спочатку набувають професійний досвід, а пізніше у них виникає особиста зацікавленість у цьому виді діяльності. Тому безкорислива гра любителів-першопочатківців поступово набуває нову сутність, тобто уже злочинну якість. На нашу думку, для комп’ютерних злочинців цієї групи важливо не тільки поєднувати свої захоплення володіння комп’ютерною технікою, але можливість використовувати свої професійні знання, навики і уміння з метою реального отримання матеріальної винагороди. Цим вдало користуються організовані злочинні угрупування, які запрошують молодих талановитих комп’ютерних геніїв для співробітництва з метою вчинення різних видів комп’ютерних злочинів. Таким чином, спостерігається поступовий процес переродження талановитого юнака любителя початківця-програміста у більш досвідченого професійно-орієнтованого комп’ютерного злочинця.

Підсумовуючи аналіз характерних ознак комп’ютерних злочинців першої групи, можна стверджувати, що якщо не вести профілактичну діяльність з цими особами, то тут зароджується фактично плідне підгрунтя для майбутніх комп’ютерних злочинців.

Що стосується другої групи комп'ютерних злочинців, то до них відносяться особи, які страждають новим видом психічних захворювань – інформаційними хворобами, комп'ютерними фобіями. Даний новий вид захворювань сьогодні визивається систематичними порушеннями інформаційного режиму людини: інформаційним перевантаженням,

інформаційним голодом, збоями темпоритму, інформаційним шумом, тощо. Ці психофізіологічні процеси сьогодні значно впливають на школярів, студентів та інших осіб, які постійно працюють з комп’ютерами, гаджетами тощо. Дослідженням даних надзвичайно небезпечних професійних психічних захворювань займається порівняно нова і молода галузь медицини – інформаційна медицина [197, с. 250; 198, с. 290].

Спеціальна комісія Всесвітньої організації здоров'я (ВОЗ), яка узагальнила всі наявні в її розпоряджені матеріали про психофізіологічний вплив автоматизованих комп’ютерних систем, різного роду комп'ютерних терміналів на здоров'я їх користувачів визнала небезпеки, які чекають людство в електронну еру. Причому комісія ВОЗ чітко вказала на суттєві негативні наслідки для здоров'я людини, якщо вона часто і довго працює з персональним комп'ютером. Фактично ці психічні захворювання сьогодні є наочними і становлять об'єктивну реальність [174 с. 527].

Проведені дослідження, здійснені на основі всебічного аналізу емпіричних даних, свідчать про те, що комп'ютерні злочини, які вчиняються комп’ютерними злочинцями даної групи, в основному пов'язані з небезпечними злочинними діями, які направлені на фактичне фізичне знешкодження або значне пошкодження засобів комп'ютерної техніки потерпілої сторони інколи без наявності якого небудь продуманого злочинного умислу, з частковою або повною втратою контролю над своїми психічними діями [81, с. 28-39]. Очевидно, що ця друга група комп’ютерних злочинців є достатньо небезпечною, оскільки їх дії є неконтрольованими.

Третю групу комп’ютерних злочинців формують уже певною мірою підготовлені комп’ютерні фахівці, які ситуаційно, технологічно і вірогідно мотивовано мають реальну можливість фахово, професійно вчинити комп’ютерний злочин. Це обумовлено тим, що, по-перше, такі комп’ютерні злочинці мають можливість безпосереднього доступу до автоматизованих комп’ютерних систем, електронних банків даних і електронних мереж. По-друге, такі особи ілюзорно вважають, що технологічне використання

можливостей кіберпростору – це безкарна справа. По-третє, відсутність безпосереднього особистого контакту комп'ютерного злочинця в кіберпросторі з потерпілою жертвою злочинних дій фактично створює умови і надає можливість вчинити комп'ютерний злочин таємно і не бути за це виявленим, затриманим і покараним. І, по-четверте, оскільки комп'ютерні злочинці цієї категорії вважають, що встановити їх електронні сліди зловмисних дій складно, тому вони дійсно не в повній мірі розуміють, що вони дійсно вчинили комп'ютерний злочин в кіберпросторі і надіються, що їх злочинні дії технологічно не будуть задокументовані і за це вони не понесуть взагалі заслужене покарання. Вчиненню комп'ютерних злочинів фактично сприяє недолуге законодавство про кримінальну відповідальність за такі зловмисні дії.

Статистика розкриття комп'ютерних злочинів в Україні, Європі і світі є теж реальним фактом того, що більшість таких професійних комп'ютерних злочинців фактично ніколи не встановлюються органами правопорядку. Розкриття таких злочинів складає всього 1 % від кількості вчинюваних в реальності. Тому вважаємо, що базовим підгрунтям для аналізу характерних рис і ознак комп'ютерного злочинця цієї групи є, зокрема, обгрунтоване міркування І.Г. Богатирьова. Даний дослідник вважає, що можна виокремити такі типи злочинців: 1) з агресивно-зневажливим ставленням до людини та її найважливіших благ (життя, здоров'я, честі, гідності тощо); 2) з корисливо-егоїстичною мотивацією, пов'язаною з ігноруванням принципу соціальної справедливості та чесної праці; 3) з індивідуалістично-анархічним ставленням до різних соціальних інститутів, своїх громадських, службових, сімейних та інших обов'язків; 4) з легковажно-байдужим ставленням до дотримання правил техніки безпеки, що проявляється у вчиненні необережних злочинів. За другим критерієм І. Г. Богатирьов поділяє злочинців на послідовно-криміногенний, ситуативно-криміногенний і ситуативний типи. Для послідовно криміногенного типу є характерним те, що вчинення злочину зумовлене звичним стилем поведінки особи і є наслідком стійких

антисуспільних установок та орієнтацій суб'єкта. Для злочинця ситуативно-криміногенного типу вчинення злочину великою мірою обумовлено несприятливою ситуацією та певною мірою – попереднім антисуспільним способом життя особи. Представниками ситуаційного типу злочин вчиняється під вирішальним впливом ситуації, що виникла не з їх вини [147, с. 87].

Очевидно, що різноманітність комп'ютерних злочинів, які вчиняють комп'ютерні злочинці даної групи повністю вкладається у вище сформульованих І.Г. Богатирьовим критеріях. Підтвердженням цьому є і показники звітності Державної судової адміністрації України (ДСА України) щодо вчинених злочинів даної категорії.

За даними Звіту про склад засуджених за 2021 рік (форма № 7) місцевими судами України за злочини у сфері використання електронно-обчислювальних машин (комп'ютерів) систем та комп'ютерних мереж (ст.361-ст.363-1 КК України) було засуджено 76 осіб (також деякі засуджені особи перебували в складі злочинних груп – 9). Усі з них – громадяни України. Серед них 15 жінок, що становить 19,8 %. З них 2 – належать до вікової категорії осіб – 16 до 18 років; 14 – з 18 до 25 років; 23 – від 25 до 30 років; 35 – від 30 до 50 років; 2 – від 50 до 65 років; 0 – від 65 років і старше.

За заняттям на час вчинення злочину засуджені класифікуються таким чином: 1) робітники – 7; 2) державні службовці – 1; 3) інші службовці – 3; 4) військовослужбовці – 2; 5) приватні підприємці – 4; 6) студенти навчальних закладів – 4; 7) інші заняття – 12; 8) пенсіонери, в тому числі інваліди – 1; 9) безробітні – 1; 10) працездатні особи, які не працюють та не навчаються – 41. Відомості щодо освіти: 1) повна вища освіта – 26, що складає 34,32 %; 2) базова вища – 7; 3) професійно-технічна – 13; 4) повна загальна середня – 13; базова загальна середня – 17 [111].

Дані звітності свідчать, що найбільшу питому вагу серед комп'ютерних злочинів складають шахрайства, вчинені з використанням електронно-обчислювальної техніки, кібернасильства – доведення до самогубства, погрози

позбавлення життя, порушення недоторканості приватного життя, незаконний обіг зброї, наркотичних і психотронних речовин, порнографії тощо [89, с. 116].

Наприклад, середній вік комп'ютерних злочинців, які вчинили комп'ютерне шахрайство коливається від 18 до 26 років. Характерним тут є те, що 91 % комп'ютерні шахрайства вчиняють чоловіки [168, с. 106]. Водночас, переважно жінки віком від 18 до 22 років вчиняють комп'ютерні злочини у формі виготовлення і збуту порнографічної продукції [204].

Статистичні дані і наукові дослідження дозволяють стверджувати, що комп'ютерні злочинці даної групи є достатньо молодими за віком. Оскільки 48 % від усіх користувачів інтернету становлять молоді особи віком від 14 до 24 років, то очевидно справедливим буде вважати, що сучасна комп'ютерна злочинність набуває ознаки ювенальної [168, с. 106; 93, с. 4].

Тенденції сьогодні такі, як стверджує О.Є. Коваль, що основну вікову групу комп'ютерних злочинців сьогодні складають особи від 14 до 21 року [125, с. 189]. Але очевидно, що більшість комп'ютерних злочинів, які вчиняють комп'ютерні злочинці третьої групи становлять особи віком до 45 років.

Хоча відомо, що характерною ознакою комп'ютерного злочинця є його любов до комп'ютера ще з дитинства, але сьогодні практично всі верстви населення є повноправними користувачами комп'ютерних технологій і мережі інтернет. Тому у кожного користувача комп'ютера, як зазначає Л.В. Борисова, є «унікальний за своєю суттю мотив – інтелектуальна боротьба між людиною і комп'ютерною системою» [78, с. 76].

Підводячи підсумки аналізу даної групи комп'ютерних злочинців, можна стверджувати про майбутні прогностичні масштабні зміни в структурі комп'ютерної злочинності, які несуть великі загрози для суспільства, держави, цивілізації.

До найбільш небезпечної четвертої групи відносяться професійні комп'ютерні злочинці з яскраво вираженою корисливою і корисливо-насильницькою метою, так звані «профі-крекери». На відміну від першої

групи «любителів-початківців», другої специфічної групи «хворих», достатньо небезпечної третьої групи фахівців комп’ютерної справи, злочинці четвертої групи характеризуються професійно-орієнтованим систематичним багатократним вчиненням комп'ютерних злочинів з обов'язковим виконанням злочинних дій, які направлені на підготовку, втаємничене вчинення та їх безпосереднє латентне приховування. Особи цієї групи володіють достатньо сталими злочинними навиками, знаннями і уміннями.

Дослідження показують, що злочинці цієї групи, як правило, є членами добре озброєних і організованих, мобільних і технологічно якісно оснащених новітнім висококласним обладнанням і спеціальною технікою (нерідко оперативно-технічного характеру) злочинних груп і криміногенних співтовариств. Осіб, які входять до їх складу, загалом можна охарактеризувати як висококваліфікованих спеціалістів з вищою юридичною, економічною (фінансовою) і технічною освітою. Справедливо вважає Н.М. Ахтирська, що саме ця група злочинців і представляє собою основну загрозу для людей, суспільства і держави, оскільки є реальним потужним кадровим ядром комп'ютерної злочинності як в якісному, так і кількісному плані [32, с.5]. Практика показує, що на долю цих комп’ютерних злочинців приходиться максимальна кількість особливо небезпечних посягань, наприклад, розкрадань грошових коштів у великих та надзвичайно великих розмірах і різного роду посадових злочинів, які вчиняються з використанням засобів комп'ютерної техніки.

Очевидно, що комп’ютерні злочинці, які виконують завдання організованих злочинних груп і організацій, складають групу спеціалістів-професіоналів у галузі засобів комп'ютерної техніки. Тому узагальнені емпіричні дані, які приведені В.Б. Веховим, дозволяють визначити наступну соціально-психологічну і кримінологічну характеристику комп’ютерних злочинців, які входять в структуру організованих злочинних організацій. Узагальнений аналіз незалежних характеристик комп’ютерних злочинців даної категорії свідчить про те, що, як правило, комп’ютерні злочинці цієї групи

достатньо фахово підготовлені, оскільки це «майстри своєї справи», так як мають достатні розумові і професійні здібності. При цьому, вони мають деякий своєрідний «спортивний» інтерес, азарт і фанатизм. Тому нові заходи із забезпечення кібербезпеки комп'ютерних систем і комп’ютерних мереж ними сприймаються у психофізіологічному плані, - як своєрідний виклик особі, а тому вони намагаються будь-якою ціною знайти ефективний підхід, розробити оптимальні засоби і методи доступу та несанкціонованого втручання в автоматизовані банки даних, чим довести свою зухвалість, неперевершеність в професійній майстерності [81, с. 28-39].

Відомим є той факт, що професійні програмісти фахівці в галузі інформаційно-комунікаційних технологій мають можливість мігрувати по світу і приймати запрошення злочинних угруповань для вчинення злочинів. Очевидно, що цих злочинців майже неможливо спіймати, оскільки комп’ютерна операція-кібератака ретельно планується і триває декілька хвилин. Приміщення, звідки виконує свою роботу крекер, знімається на вигадане ім'я.

Таким чином, для представників четвертої групи комп’ютерних злочинців характерними рисами і ознаками є наступні: по-перше, крекери – це спеціалісти вищого класу (High Tech Anarchisns); по-друге, крекери мають на озброєнні надсучасне технічне, технологічне, програмне комп’ютерне та інформаційно-телекомунікаційне забезпечення; по-третє, крекери достатньо потужно гарно організовані; по-четверте, у своїй структурі крекери мають чітко налагоджений порядок та контроль обміну як відкритою, так і таємною інформацією; по-п’яте, крекери добре організаційно та криптологічно законспіровані; по-шосте, крекери володіють достатньо високим рівнем організації, співпраці, взаємодії, комунікації та кооперації.

Підводячи підсумки викладеного, вважаємо, що характерними рисами, ознаками, властивостями комп’ютерного злочинця є наступні:

1) комп’ютерні злочинці вчиняють, як правило, міжнародні (транскордонні, транснаціональні, трансконтинентальні, планетарні, а інколи

космічні) комп'ютерні злочини, які виходять за рамки кордонів однієї держави;

2) комп'ютерні злочинці володіють знаннями й навичками в сфері інформаційних технологій (користуються таємними кодами, паролями для вчинення комп'ютерних злочинів);

3) комп'ютерні злочинці користуються сучасними технологіями, оскільки вчиняють комп'ютерні злочини дистанційно, а тому є великі труднощі у встановленні місцезнаходження як самого комп'ютерного злочину (електронні сліди таких злочинів можуть бути встановлені в різних установах, країнах і континентах), так і місце безпосереднього перебування комп'ютерного злочинця в момент вчинення протиправної злочинної дії;

4) комп'ютерні злочинці при вчиненні комп'ютерних злочинів працюють так, що фактично неможливо в реальному масштабі часу спостерігати і документувати електронні сліди (докази) візуально;

5) комп'ютерні злочинці в процесі вчинення комп'ютерних злочинів використовують такі безпекові процедури: різні засоби, способи і технології криптографічного шифрування інформації; засоби, призначені для виготовлення ключових даних або ключових документів та управління ключовими даними, що використовуються в методах комп'ютерного захисту інформації; засоби захисту від несанкціонованої модифікації чи нав'язування неправдивої інформації, що фактично реалізують алгоритми криптографічного перетворення інформації, у тому числі комп'ютерні технології імітозахисту та електронного підпису, а також засоби розмежування доступу до ресурсів автоматизованих комп'ютерних систем, електронних баз даних, електронних комунікаційних мереж, в яких реалізовані криптоалгоритми;

6) комп'ютерні злочинці володіють достатньо потужними криптологічними засобами (апаратними, програмними, апаратно-програмними), криптологічними алгоритмами і криптологічними автоматизованими комп'ютерними системами захисту конфіденційної інформації, яка отримана в процесі вчинення комп'ютерних злочинів;

7) з метою забезпечення власної безпеки комп’ютерні злочинці використовують різні засоби захисту своїх автоматизованих комп'ютерних систем (ключові дані, системи управління ключовими даними, технічні засоби, спеціальні інформаційно-телекомунікаційні системи) від несанкціонованого зовнішнього проникнення з метою отримання інформації;

8) комп’ютерні злочинці вчиняють комп’ютерні злочини таким чином, що інколи просто неможливо встановити чіткі зв’язки між ланками електронних слідів у цілісній системі комп’ютерних (електронних) доказів;

9) оскільки комп’ютерні злочинці вміло користуються можливостями всесвітньої електронної мережі інтернет, то це дозволяє їм широко використовувати піратське програмне забезпечення, займатися промисловим шпигунством, торгувати зброєю, наркотиками, здійснювати вторгнення до телефонних мереж та незаконно торгувати послугами зв’язку тощо;

10) характеризуючи риси, ознаки і властивості комп’ютерних злочинців, їх можна систематизувати і класифікувати на чотири основні групи: «любителі-початківці», «хворі», «професіонали», «супер професіонали»:

- комп’ютерні злочинці – «любителі-початківці» - це особи, які характеризуються сталим поєднанням первинних елементів професіоналізму у галузі комп’ютерної техніки і комп’ютерного програмування з елементами своєрідного дитячого захоплення, спортивного азарту, фанатизму і винахідливості. Такі особистості не завжди прагнуть вчинити комп’ютерний злочин, оскільки для них це забава, безкорислива гра, яка викликана спортивним інтересом, азартом, фанатизмом, але в ряді випадків приводить до вчинення ними комп'ютерних злочинів;

- комп’ютерні злочинці – «хворі» - це особи, які страждають новим видом психічних захворювань – інформаційними хворобами, комп’ютерними фобіями;

- комп’ютерні злочинці – «професіонали» - це фахово підготовлені професіонали своєї справи, які технологічно та ситуаційно мають реальну можливість вчиняти комп’ютерні злочини;

- комп'ютерні злочинці – «супер професіонали» - це, по-перше, найбільш небезпечні високопрофесійні комп'ютерні злочинці з яскраво вираженою корисливою і корисливо-насильницькою метою злочинних дій; по-друге, це профі-крекери – спеціалісти вищого класу в галузі володіннями знаннями, навиками і уміннями вчинення потужних, як наземних, так і космічних комп'ютерних злочинів (кібератак, кібертерористичних актів тощо); по-третє, профі-крекери мають на озброєнні надсучасне технологічне та комп'ютерне програмне забезпечення; по-четверте, «профі-крекери» у своїй структурі мають чітко налагоджений порядок та контроль обміну як відкритою, так прихованою, таємною інформацією, по-п'яте, «профі-крекери» достатньо потужно з позиції управління злочинною діяльністю гарно організовані; по-шосте, «супер-крекери» добре організаційно, оперативно-технологічно та криптологічно законспіровані; по-сьоме, «супер-крекери» володіють достатньо високим рівнем знань, навиків і умінь організації комунікації та кооперації в процесі вчинення комп'ютерних злочинів.

2.2. Кримінологічна систематизація і класифікація комп'ютерних злочинців

У числі важливих питань, пов'язаних з удосконаленням діяльності по запобіганню комп'ютерній злочинності, заслуговує на особливу увагу всебічне вивчення осіб комп'ютерних злочинців та їх кримінологічної систематизації і класифікації.

Як вказує О.Г. Старіш, сьогодні реальних сподівань на спрощення середовища існування людства уже немає, оскільки цивілізація розвивається у напрямку ускладнення, насамперед, у сфері інформаційній, включаючи соціально-комунікаційну і комп'ютерно-технологічну їх складову [187, с. 3].

За цих обставин, вірогідно, адекватним підходом може бути лише комплексне, системне і всестороннє консолідоване пізнання особи

комп’ютерного злочинця саме в контексті його походження і прояву в реальних криміногенних ситуаціях.

Відповідно, комп’ютерний злочинця як об’єкт системного кримінологічного дослідження доцільно розглядати і вивчати у взаємозв’язку з його оточенням, зрозуміти причини його появи та розвитку, а це означає необхідність з’ясування всіх характерних його ознак, рис, властивостей і манер поведінки. При цьому дане дослідження потрібно здійснювати систематизовано, в певній послідовності, з використанням наукових засобів систематизації і класифікації, лише тоді воно дасть максимально наближений до реальності, а не тільки до уяви дослідника, результат [187, с. 3].

Це обумовлено тим, що сучасний інформаційний кіберпростір, електронні інформаційні ресурси та величезні інформаційні потоки, які сформувалися в епоху стрімкого розвитку інформаційно-комунікаційних технологій уже не дозволяють виявляти і досліджувати нові риси, ознаки, властивості, манери поведінки комп’ютерних злочинців традиційними засобами пізнання. Таким чином, звичайні аналітичні засоби і методи пізнання окремих наукових дисциплін, які раніше використовувались для вивчення окремих подій, явищ і процесів, в тому числі, і особи комп’ютерного злочинця тепер уже не відповідають вимогам сучасної науки інформатики, кібернетики, нейробіоніки та нової галузі знань – кіберкримінології. Тому на порядок денний постало питання розробити нову парадигму засобів, методів і технологій для дослідження особи комп’ютерного злочинця, яка б відповідала вимогам і потребам сучасної науки кримінології та допомагала розібратись в усіх як горизонтальних, так і вертикальних зв’язках між відокремленими подіями, явищами і процесами [187, с. 4].

Системологічні дослідження сьогодні використовуються практично в усіх галузях знань: так, в технічних науках мова йде про системотехніку, в кібернетиці – системне управління, в соціології – структурно-функціональний підхід, в суспільних науках і кримінології – системологію [187, с. 4-5].

Слід зазначити, що саме методологія наукового пізнання є багатоплановим і багатоаспектним системоутворюючим філософським фундаментом дослідження сутності особи комп'ютерного злочинця. Очевидно, що ступінь та глибина пізнання сутності та характерних рис, ознак, властивостей і манер поведінки особи комп'ютерного злочинця залежить головним чином, від правильного застосування витоків історіографії, джерелознавства, теорії, методології і праксеології такого дослідження.

На думку О.Г. Старіш, системне мислення вказує на нові перспективи в дослідженні природи і людини, створені техніки та нового суспільного життя. Воно являє собою також новий спосіб організації досліджень завдяки використанню таких понять, як система, системні властивості і відношення [187, с. 8]. Вважаємо, що сьогодні асиметричний консолідований системний підхід у кримінологічній науці фактично перетворився в об'єктивну необхідність і потребу, реальну складову багатьох новітніх напрямів кримінологічних досліджень, зокрема, і всебічного пізнання особи комп'ютерного злочинця.

Відомо, що сам термін «система» з'явився ще у Древній Греції приблизно в V столітті до нової ери і мав початкове значення: поєднання, організм, організація, союз, лад. Сьогодні термін система, на думку О.Г. Старіш – це відокремлена сукупність взаємодіючих між собою елементів, яка утворює деяку цілісність, володіє певними інтегральними властивостями, що дозволяє їй виконувати в середовищі визначену функцію [187, с. 8].

Таким чином методологія системного аналізу, на думку В.І. Ярошовця, займає важливе місце в розробці системних уявлень, становленні системного підходу, формуванні парадигми сучасних наукових досліджень для розв'язання пізнавальних завдань з використанням системи комунікацій [211, с. 87].

Вище викладене свідчить, що сьогодні істотне місце в сучасній кримінологічній науці займає системний підхід, асиметричний консолідований

аналіз, хоча його єдиного трактування даних термінів в науці поки що немає, оскільки кожний дослідник по-своєму розуміє його зміст.

О.Г. Старіш вважає, що системний підхід – це напрямок методології спеціально-наукового пізнання і соціальної практики, в основі якого лежить дослідження об’єктів як систем. На практиці ідеї системного підходу кристалізуються в методологічних засобах системного аналізу [187, с. 134].

Тому вважаємо, що при проведенні наукових кримінологічних досліджень особи комп’ютерного злочинця слід використовувати системний асиметричний підхід і ретельно підходити до питання вибору засобів, методів, методик і технологій дослідження.

Таким чином розглянутий вище світоглядний шар знань, ідей, концепцій, методологій дозволяє нам сформулювати систему засобів наукового пізнання, які стануть орієнтиром, наріжним каменем для пізнання сутності особи комп’ютерного злочинця, а також формулювання наукових засад систематизації та класифікації комп’ютерних злочинців, виходячи з їх професійної злочинної орієнтації.

Вище викладене дає можливість нам перейти до ретельного розгляду кримінологічної систематизації і класифікації комп’ютерних злочинців. Слід зазначити, що в кримінологічній літературі дослідники пропонують різні підходи до систематизації і класифікації комп'ютерних злочинців [81, с. 31].

Проведені соціологічні і кримінологічні дослідження, зокрема в Австралії, Великій Британії, Канаді, США, ФРН, Україні дозволяють, по-перше, систематизувати і класифікувати комп'ютерних злочинців за віком на три великі категорії: комп’ютерні злочинці віком 10-16 років – в більшості випадків займаються комп’ютерними злочинами з використанням телефонів, мережі інтернет, кредитних карток та автоматів по видачі готівки (хакери, фрікі, колекціонери); комп’ютерні злочинці віком 17-25 років – займаються комп'ютерним хакерством і крекерством (хакери, крекери, кіберплути, творці вірусних програм); комп’ютерні злочинці віком 26-55 років – використовують

комп'ютери для корисливих цілей та шпигунства (кіберплути, кібертерористи, крекери, кібершахраї, кіберпірати) [56].

Проведені дослідження дозволяють зробити висновок, що з віком ускладнюється професійний рівень технічних завдань, що вирішються в інформаційно-комунікаційній сфері, а мотивація стає більш раціональною і більш небезпечною.

По-друге, що стосується відношення до жертви, всіх комп'ютерних злочинців умовно можливо поділити на чотири великі групи: 1) це зовсім сторонні особи, які, як правило, ніколи не мали ніяких стосунків з державою-жертвою, фірмою-жертвою чи потерпілою особою; 2) це сторонні особи, які володіють деякою інформацією про державу-жертву, фірму-жертву, потерпілу особу, в тому числі звільнені з даної фірми-жертви працівники; 3) це співробітники, які займають у фірмі-жертві відповідальні посади, які безпосередньо не пов'язані з використанням автоматизованих комп’ютерних систем та засобів обчислювальної техніки; 4) це співробітники, які безпосередньо користуються автоматизованими електронними комп’ютерними системами і комп’ютерними мережами, автоматизованими електронними банками даних і зловживають своїм професійним службовим становищем.

По-третє, згідно з даними судової статистики комп’ютерних злочинців можна умовно класифікувати, базуючись на їхній професійній діяльності: 1) це керівники установ, відомств і організацій (начальники, директори, управляючі департаментів, управлінь, відділів, служб і т.п.); 2) це співробітники, які забезпечують економічну і фінансову стабільність відомств, установ і організацій (керівники і співробітники банківського і небанківського сектору економіки, управляючі банків і страхових компаній, бухгалтери, економісти, фінансисти, табельщики, контролери, нормувальники тощо); 3) це фахівці, які забезпечують правову, організаційну, технологічну і безпекову сферу відомств, установ і організацій (інженери, оператори, програмісти, менеджери, юристи, адвокати, фахівці сервісних служб, працівники служб безпеки тощо).

Приведені вище аналітичні дані вказують на те, що центральним питанням є те, яка основна доля комп’ютерних злочинців сьогодні є найбільш небезпечною для людини, суспільства і держави. Виходячи з даних позицій, слід зазначити, що в літературі зустрічаються різні підходи щодо аналізу і класифікації таких комп’ютерних злочинців.

Так, наприклад, В.Б. Вехов вважає, що всіх комп'ютерних злочинців можливо умовно класифікувати на дві основні групи, виходячи з системної класифікаційної ознаки професійної категорії осіб, які мають безпосередній доступ до засобів автоматизованих комп'ютерних систем, електронних мереж і електронних банків даних згідно їх службових (посадових) інструкцій: по-перше, це внутрішні користувачі; по-друге, це зовнішні користувачі, яким надано право звертатися до автоматизованої комп’ютерної інформаційної системи, або посередника за отриманням необхідної йому інформації і має можливість користуватися нею [81, с. 31; 38, с. 271].

Виходячи з даних позицій, вважаємо, що за параметрами доступу до комп'ютерних систем, мереж, баз даних можливо класифікувати таких користувачів на дві основні групи (види): офіційно зареєстровані (санкціоновані, законні) і незареєстровані (несанкціоновані, незаконні).

Реальна судова статистика вчинення комп’ютерних злочинів свідчить, що основна небезпека в плані вчинення такого злочину, в більшості випадків, виходить безпосередньо від внутрішніх користувачів (тобто своїх співробітників) і ними фактично вчиняється 94 % комп’ютерних злочинів, тоді як зовнішніми користувачами вчиняється - тільки 6 %, при цьому 70 % - це клієнти-користувачі комп'ютерної системи, а 24 % - обслуговуючий персонал [130, с. 3-6; 178, с. 9-11; 205].

В зв’язку з цим Ю.М. Батурин вважає, що комп’ютерних злочинців можливо класифікувати на підставі функціональної категорії осіб, яким надана можливість доступу до засобів комп'ютерної техніки в установі, відомстві чи організації. Таким чином внутрішніх комп’ютерних злочинців умовно можливо класифікувати на три основні групи. До першої групи, на його думку,

відносяться комп’ютерні злочинці, які вчинили комп'ютерні злочини, побудовані на основі використання можливостей комп’ютерних програмних засобів установи, відомства чи організації, в яких вони безпосередньо працюють. Такими комп’ютерними злочинцями є оператори ЕОМ, касири, бухгалтери, економісти, фінансисти, нормувальники, табельщики, оператори бензозаправочних станцій, продавці, оператори електронних периферійних засобів, оператори-програмісти (системні і прикладні), інженери-системщики та інженери-програмісти, тощо.

До другої групи відносяться комп’ютерні злочинці, які вчинили комп'ютерні злочини, що базувалися на використанні автоматизованих апаратних засобів комп'ютерної техніки установ, відомств чи організацій в яких ці особи працюють. До цієї групи відносяться: оператори автоматизованих засобів зв'язку і телекомунікацій, інженери по термінальному обладнанню, фахівці по комп'ютерному аудиту, інженери по електронному обладнанню, інженери-зв'язківці.

До третьої групи, як вважає Ю.М. Батурин, відносяться комп’ютерні злочинці, які вчинили комп'ютерні злочини на базі непрямого доступу до засобів комп'ютерної техніки. Як правило, такі комп’ютерні злочини вчиняють ті комп’ютерні злочинці, хто безпосередньо займається організаційно-управлінськими питаннями: керуванням автоматизованою комп'ютерної системою або електронною мережею, керування операторами автоматизованих комп’ютерних систем, керування автоматизованими базами даних, керівництвом процесу розробки програмного забезпечення. Це в основному головні (старші) інженери, програмісти, зв'язківці; керівники і начальники різних служб і відділів (зокрема, комп’ютерно-технологічний, інформаційно-аналітичний); співробітники служб безпеки, менеджери, тощо [38, с. 271].

Що ж стосується комп’ютерних злочинців з числа зовнішніх користувачів, то ними, як свідчить практика, найчастіше є особи, які всебічно і достатньо повно володіють інформацією стосовно реальної професійної

діяльності потерпілої сторони (фірми-жертви). Таких організацій, відомств і установ жертв комп’ютерного злочину є достатньо багато. Це настільки велика кількість комп’ютерних злочинців, що практично не може бути піддана якійсь об'єктивній систематизації чи класифікації. Такими комп’ютерними злочинцями можуть бути будь-які, навіть випадкові особи. Практика показує, що такими комп’ютерними злочинцями можуть бути представники організацій, які займаються сервісним обслуговуванням, ремонтом, конструюванням і розробкою технічних та програмних засобів комп'ютерної техніки, представники різних контролюючих і владних органів, клієнти і просто хакери [38, с. 271].

Таким чином, проведений вище системний асиметричний аналіз комп’ютерних злочинців, які вчиняють комп’ютерні злочини як поодинці, так і в структурі організованих злочинних груп, дозволяє класифікувати їх за метою, цілями, формами, засобами, методами, технологіями та сферою їх злочинної діяльності. Таким чином комп’ютерних злочинців можна умовно систематизувати і класифікувати на такі окремі групи і підгрупи: хакери, крекери, фрікери, спамери, колекціонери, фішери, кіберплути, кардери, кіберкрукери, кіберсквокери, інсайдери, вірмейкери, кібертерористи, електронні «торгаші» або кіберпірати, спуфери, творці шкідливих комп’ютерних програм, організовані злочинні кіберугрупування, іноземні розвідувальні кіберслужби, держави-кіберзлочинці.

Нижче системно розглянемо більш детально класифікацію комп’ютерних злочинців, які вчиняють усталені різновиди комп’ютерних злочинів в сучасному електронному світі.

Достатньо велику групу комп’ютерних злочинців складають хакери. Практика показує, що це найбільш поширена спільнота комп’ютерних злочинців, а тому риси, ознаки, властивості, манери поведінки даних осіб розглянемо більш детально.

Очевидно, що сам факт історичної появи комп'ютерної злочинності у суспільстві більшість дослідників пов'язують з діяльністю так званих

«хакерів» (англ. hacker) – тобто звичайних користувачів автоматизованих обчислювальних комп’ютерних систем, електронних баз даних і мереж ЕОМ, які професійно займаються пошуком і розробкою незаконних засобів, методів і технологій отримання несанкціонованного, неправомірного (самовільного) доступу до засобів електронної комп'ютерної техніки і електронних баз даних, а також їх несанкціоноване проникнення і використання з корисливою злочинною метою [55, с. 16].

В юридичні літературі, а також у засобах масової інформації таких комп’ютерних злочинців називають по різному: «кібертерористами», «кіберзлочинцями», «комп'ютерними взломщиками», «електронними злодіями або електронними шахраями», «електронними торгашами або піратами», «одержимими програмістами», «електронними бандитами», «злодіями з електронними ломиками і відмичками», тощо. Водночас слід зазначити, що сам термін «хакер» не завжди раніше сприймався як синонім комп'ютерного злочинця. Таким чином, фактично дослівно слово «хакер» означає, що це трудівник, найманий працівник. Відомо, що первісно так називали комп’ютерних програмістів, які розробляли комп’ютерні програми без спеціальної попередньої підготовки та швидко, якісно і оперативно вносити відповідні виправлення, зміни до комп’ютерних програм, котрі тоді ще не мали спеціальної документації. Нижче розглянемо більш детально в історичному аспекті саме походження сутності терміну «хакер».

Фактично термін «хакер» вперше почав використовуватись на початку семидесятих років минулого століття у Масачусетскому технологічному інституті США по відношенню до молодих програмістів, які проектували різні апаратні засоби для ЕОМ та намагались сконструювати перші персональні комп'ютери. Водночас, коли у Сполучених Штатах Америки з’явились перші великі ЕОМ, комп’ютерні компанії дозволяли студентам безкоштовно працювати і користуватися їхніми можливостями. Відомо, що як правило, комп’ютерні компанії США, для цього відводили певні нічні години і таких студентів, які працювали на ЕОМ, стали звати хакерами. Практично студенти

мали можливість залишатись працювати на ЕОМ на всю ніч. Але для цього окремі групи студентів розподілялись працювати по змінах. Наприклад, одна група студентів мала можливість працювати на ЕОМ, але для цього мала відповідний квант часу, наприклад, з 1 до 2 години ночі. Друга група студентів мала час для праці з 3 до 4 години ночі, третя група з 5 до 6 години і т.п. Після закінчення комп'ютерного програмування на ЕОМ, студенти-хакери залишали розроблені ними власні комп'ютерні програми у шухлядах, які знаходилися біля ЕОМ. Причому кожен студент з іншої групи, який працював на цій ЕОМ, мав реальну можливість заглянути при цьому в записи своїх друзів програмістів. Відомо, що досить часто студенти брали чужі нотатки з комп'ютерного програмування та вносили до них свої відповідні зміни, уточнення, покращення, виправлення, намагаючись удосконалити результати комп'ютерного програмування своїх друзів. Водночас, студенти-хакери не псували програми своїх друзів-хакерів, але і не намагались спеціально захистити свої комп'ютерні програми від інших однодумців-хакерів. Студенти вважали, що усі комп'ютерні програми, які вони розробляли, повинні бути призначені для спільного користування всіма членами суспільства. Фактично хакери вірили в те, що автоматизовані комп'ютерні системи, комп'ютерні мережі і електронні бази даних це ключ до повного визволення людини, оскільки здобутки і знання людства повинні бути загальнодоступними для всіх людей земної планети. Отже думки, мрії, ідеї, інновації та уявлення хакерів про пріоритетні напрями шляхів розбудови суспільства та роль у ньому автоматизованих комп'ютерних систем, комп'ютерних мереж, електронних баз даних та інформаційних технологій знайшли своє відображення у вигляді визначення розроблених хакерами специфічних маніфестів та звернень до світової спільноти. Неможливо заперечувати, що деякі з цих світоглядних положень, які розробили хакери, мали, окрім науково-технічних та філософських аспектів, і звичайне суто соціальне забарвлення. Очевидно, що деякі із запропонованих маніфестів хакерів й досі можливо знайти на дошках

електронних об'яв (BBS) у великих автоматизованих комп'ютерних мережах і електронних базах даних.

Вважається, що взірцем типового хакера був Роберт Морріс (Robert Morris), аспірант Cornell University, яким було написано відомого черв'яка інтернету. Комп'ютерну програму-черв'яка створив Р. Морріс тоді коли йому було всього 22 роки. Друзі та вчителі характеризували його психофізіологічний портрет як приємного зовні, але водночас надзвичайно сором'язливого, та чітко сфокусованого у наукові дослідження вченого. Заради справедливості слід зазначити, що реально Р. Морріс не простий звичайний типовий хакер, а дійсно видатний комп'ютерний програміст. Підтвердженням цього є те, що до нього за допомогою у питаннях комп'ютерного програмування часто зверталися не тільки студенти, друзі, однодумці, але, навіть, викладачі Cornel Universiti університету. Однак, його характерною психофізіологічною рисою було те, що він не міг чітко зосередитися на вивченні тих предметів, які були для нього нецікавими. Тому під час навчання вже у Harvard University через те, що у нього були погані оцінки з таких нецікавих предметів, його фактично звільнили на рік від навчання. Водночас, у Р. Морріса була чітка мета – написати таку комп'ютерну програму-черв'яка, яка буде фактично символізувати «надію вищого розуму», «надію інтелекту», «взірець творчої думки». За свідченням друзів психофізіологічний портрет Р. Морріса можна описати наступним чином: він реально оперний фанатик, оскільки надзвичайно хвилюється, коли телефонує до невідомої раніше особи. Причому Р. Морріс при цьому відчуває складнощі в процесі підтримки розмови з незнайомими особами. З позиції психології – це типовий інтроверт. Водночас, Р. Морріс надзвичайно нетипова, нестандартна, але цікава і талановита особистість. Він багато читає унікальних наукових праць і художніх творів світового рівня. Наприклад, під час обшуку в офісі Р. Морріса співробітники ФБР США знайшли у нього книги Вірджинії Вульф, Редьярда Кіплінга та Володимира Набокова.

Підсумовуючи викладене, можна стверджувати, що хакери – це особи, які достатньо фахово володіють комп’ютерним програмним забезпеченням. Причому на самому нижньому рівні можемо виділити тих хакерів, які як раз і займаються цим – «зламують». Очевидно, що такий хакер – це людина, яка зламує різні інтернет-ресурси, роблячи їх публічними для всього суспільства. Завдяки діяльності таких хакерів у звичайних інтернет-користувачів з’являються можливості отримати торрент-посилання, кряки новинок відеоігор, безкоштовні ключі для ліцензійних комп’ютерних програмних компонентів. Але як правило, такі хакери здійснюють злами не для власної вигоди. Хакери такого типу здійснюють несанкціонований доступ в автоматизовану комп'ютерну систему для власного аматорського спортивного інтересу, азарту, професійного саморозвитку в цій галузі знань. Мета таких хакерів показати себе як професійного знавця автоматизованих комп’ютерних систем, електронних мереж і електронних банків даних, тобто позиціонувати себе як потужного комп’ютерного фахівця в галузі кібернетики, інформатики, нейробіоніки з метою покрасуватися перед оточуючими друзями, колегами, однодумцями. В останньому випадку в інтернеті з’являються спеціальні хакі, підписані хакерами за типом hackMr.N. Як правило, на даному рівні хакери професійного розвитку практично знаходиться недовго. Хакери такого типу розвиваються далі, оскільки поглиблюють свої знання з метою всебічного освоєння комп’ютерного програмного забезпечення. Оволодівши професійними знаннями, такі хакери перетворюють свою забаву в працю над дійсно цікавими й складними кіберпроектами. Ряд хакерів не досягають вершин професійної майстерності і опускають руки при різних бар’єрах, труднощах в робочому процесі.

Підсумовуючи викладене, можна зазначити, що в більшості випадків хакери – це достатньо знані фахівці комп’ютерної техніки, які допомагають корпоративним компаніям або окремим фізичним особам захищати комерційну, особисту інформацію. Водночас, такі хакери володіють

специфічними комп’ютерними знаннями і легко можуть стати комп’ютерними злочинцями.

Тому наступний рівень професійного комп’ютерного розвитку займають хакери-майстри, тобто професіонали у галузі кібербезпеки, які забезпечують захист комп’ютерної інформації від несанкціонованого доступу. Тому тлумачення слова «хакер» в цьому випадку наступне: це фахівець, який займається всебічним вивченням інтернет-простору з метою пошуку різних схем і шляхів обходу ресурсних кіберобмежень. А знаходячи такі прогалини в комп'ютерних програмах, намагається розробити свою власну більш потужну концепцію захисту такої комп’ютерної програмної дірки. Подібне значення слова «хакер» в таких випадках дуже часто прирівнюють до системного комп’ютерного адміністратора. На цьому етапі хакеру вже неважлива його репутація в інтернет-просторі. Тому хакери такого типу взагалі особливо не бажають показувати свої здобутки в пізнанні особливостей електронної мережі. На цьому етапі хакери займаються системним аналізом кіберпростору через реальну потребу простого особистого професійного інтересу з метою покращення своїх професійних знань, навиків, умінь в кіберпросторі.

Таким чином, можна тлумачити сутність хакера-майстра, що це комп’ютерний зломщик, який спеціалізується на інформаційно-комунікаційній комп’ютерній сфері, з високим рівнем професійних знань, умінь, навиків, який реально здатний зламувати кіберзахист та нелегально проникати практично до любої інформаційної автоматизованої комп’ютерної системи чи мережі. Слід зазначити, що для роботи хакера-майстра притаманні, зокрема, такі риси, ознаки, манери поведінки, які характеризують його особистість: по-перше, хакер-майстер повинен бути професійно грамотним, високо ерудованим, швидко вміти усвідомлювати і миттєво досліджувати щоденні нові науково-технологічні та комп’ютерні програмні нововведення, а для цього хакер-майстер має одразу розробляти сучасні методики адміністрування нових її компонентів; по-друге, характерними ознаками хакера-майстра є терплячість і прагнення знайти якомога більше новітньої інформації про сучасні наукові

досягнення в цій галузі знань. Очевидно, що перед безпосередньою початковою діяльністю хакер-майстер спочатку проводить всебічний системний попередній консолідований аналіз, діагноз автоматизованої комп'ютерної системи. Із різного роду літературних джерел, реєстрів, електронних банків даних, каталогів, закритих і відкритих наукових джерел хакер-майстер віднаходить важливу інформацію про досліджуваний електронний ресурс; по-третє, хакер-майстер використовує різного роду комп'ютерні технологічні програмні коди, технічні нестандартні рішення. Хакери-майстри все це здійснюють для прагматичного досягнення визначених цілей проникнення в автоматизовану комп'ютерну систему своєї жертви. Часом хакеру-майстру, щоб отримати достовірну інформацію досліджуємого об'єкта, доводиться озброюватися забороненими чинним законодавством незаконними засобами, методами і технологіями, такими як прослуховування клієнта, підключення до панелі управління його веб-сайтом чи навіть до веб-камери ноутбука тощо.

Розглядаючи ідеологію діяльності хакерів та етику манер поведінки справжніх хакерів, слід зазначити, що вони базуються на наступних загальних принципах: по-перше, хакери взагалі вважають, що автоматизовані комп'ютерні системи – це потенційний інструмент для народу, а тому вони не повинні бути власністю тільки окремих відомств, установ і організацій, а також заможних осіб або інших привілейованих верств населення, і тим більш такий інструмент не повинен використовуватися для досягнення їх приватних інтересів; по-друге, на думку хакерів, інформація, яка знаходиться в кіберпросторі, теж належить усім громадянам. Це обумовлено тим, що більшість хакерів починали свій життєвий професійний шлях в кіберпросторі з університетського навчання. Тому хакери вважають, що оскільки завдання університету надавати і розповсюджувати знання безкоштовно, а не приховувати їх. Виходячи з таких міркувань хакери, вже не будучи студентами, продовжують дотримуватися цієї позиції. Щоправда, є тільки невелика кількість хакерів, які допускають навмисне змінення або

знешкодження файлів, або їх секретну (таємну, приховану) модифікацію; по-третє, на думку хакерів, комп’ютерний код – це загальнонародне надбання. Отже гарним кодом мають можливість користуватися усі люди планети, а поганий код необхідно змінити, покращити, виправити. Крім того хакери вважають, що доступ до комп’ютерного коду повинен бути вільним для усіх громадян, а комп’ютерні програми не повинні бути захищені авторським правом та захистом від несанкціонованого копіювання. Причому хакери дотримуються тієї позиції, що все комп’ютерне програмне забезпечення повинно бути безоплатним. На їх думку, таке програмне забезпечення може вільно копіюватися та розповсюджуватися незважаючи на авторське право чи право власності. Виходячи з цих позицій, на думку хакерів, схеми комп’ютерного захисту від несанкціонованого копіювання повинні бути повністю знищені; по-четверте, хакери вважають, що комп’ютерне програмування – це професійний різновид мистецтва, зміст якого та його краса полягають у компактному кодуванні, коли комп’ютерна програма компактна, проста і займає невелику кількість рядків. На думку хакерів, головна мета – зробити таку комп’ютерну програму, яка може здійснювати те, що не може інша програма, а також повинна швидко взаємодіяти з іншими комп’ютерними програмами. Така комп’ютерна програма повинна швидко входити до інших програм, мати можливість маніпулювати файлами так, як раніше вважалося неможливим; по-п’яте, хакери взагалі вважають, що комп'ютер це звичайна жива істота. Оскільки хакери мають суспільні та приватні стосунки з комп'ютерами, то вони доброзичливо доглядають за ними, люб’язно співчувають їм як людині. Відомо, що хакери практично живуть комп’ютерним програмуванням, оскільки фактично можуть працювати всю ніч над цікавим комп’ютерним проектом. Причому хакери реально займаються комп’ютерним програмуванням по 80-100 годин на тиждень.

Водночас, слід зазначити, що з поширенням сфери застосування автоматизованих комп'ютерних систем у державних установах, комерційних відомствах і загалом суспільстві, ентузіазм хакерів в останні роки дещо спадав.

Це привело до того, що раніше розроблені ідеї хакерства, які закріплені в їхніх маніфестах, стали втрачати свою прогресивну спрямованність, яку мали на самому її початку. Вийшло так, що ідеалістичні уявлення студентів-хакерів про вільний доступ до інформації, яка зберігається в автоматизованих комп’ютерних системах, ввійшли у конфлікт з бурхливим науково-технічним прогресом та економічним розвитком суспільства і стали своєрідною формою протесту проти соціальної несправедливості. Цим у деякій мірі можливо пояснити початок створення хакерами антисоціальних і достатньо небезпечних комп'ютерних вірусів, шкідливих комп’ютерних програм, а також ігнорування ними загально прийнятих законодавчо визначених норм і правил користування автоматизованими комп'ютерними системами, електронними базами даних і електронними інформаційно-комунікаційними мережами.

Підводячи підсумки, можна стверджувати, що хакери – це особи, які отримують задоволення від несанкціонованого вторгнення та всебічного вивчення великих автоматизованих комп’ютерних систем, електронних мереж і електронних баз даних за допомогою арсеналу комп’ютерних засобів, методів і технологій телефонних ліній та національних і всесвітніх комп'ютерних мереж. Сьогодні хакери – це фактично комп'ютерні хулігани, комп'ютерні злочинці, комп’ютерні електронні корсари, які без дозволу власника незаконно проникають в чужі інформаційні мережі не тільки для забави чи гри, але і для вчинення зловмисних дій. У значній мірі їх приваблює реальна можливість подолання значних труднощів в електронному світі. На їх думку, чим складніша електронна комп’ютерна система, тим привабливішою вона є для хакера. Слід акцентувати увагу ще і на тому, що хакери – це прекрасні професійні знавці електронних комп’ютерних систем, електронних баз даних і електронних мереж сучасної інформаційної техніки. Сьогодні фактично за допомогою телефону і домашніх комп'ютерів вони підключаються до електронних комп’ютерних мереж, які пов'язані з державними та комерційними установами, банками та страховими компаніями, науково-дослідними та університетськими центрами, військовими об'єктами. Прийнято

вважати, що хакери, як правило, не роблять значної шкоди автоматизованій комп’ютерній системі та електронним базам даних. Однак психологія хакера полягає в тому, що несанкціоноване проникнення в державну чи приватну електронну систему чи електронну базу даних дозволяє йому насолоджуватися не тільки від почуття своєї влади, зверхності над автоматизованою комп'ютерною системою, електронними базами даних, але можливість отримувати за це винагороду.

При розгляді загальної характеристики хакерів-початківців і хакерів-майстрів сьогодні слід виділити ще і різні типи та підвиди хакерів, які сьогодні вчиняють різноманітні види комп’ютерних злочинів.

Підводячи підсумки розгляду мети, засобів, методів і технологій діяльності такого виду комп’ютерних злочинців, слід акцентувати увагу ще і на наступних важливих характеристиках хакерів.

По-перше, хакери – це особи, які отримують несанкціонований доступ до автоматизованих комп’ютерних систем, з метою отримання конфіденційної інформації шляхом комп’ютерного подолання захисту програмного забезпечення. Виходячи з даних позицій, хакерів, які спеціалізуються на такій протиправній діяльності, умовно можна поділити на крекерів – осіб, які здійснюють зламування шляхом самостійної розробки відповідних комп’ютерних програм з комерційною метою, а також скрипткідів – тобто осіб, які використовують для зламування захисту програмного забезпечення напрацювання інших хакерів та хакерів – вандалів, метою яких є зламування комп’ютерного захисту [149, с. 286; 189, с. 201; 36, с. 90; 139, с. 76].

По-друге, найбільш небезпечною групою комп’ютерних злочинців є крекери. Очевидно, що це більш серйозні фахові правопорушники, які здатні спричинити будь-яку значну шкоду комп’ютерній системі. Сучасні крекери (crackers – це фактично «комп’ютерні терористи», «комп’ютерні пірати», «комп’ютерні кібершахраї») фактично викрадають інформацію, викачуючи за допомогою комп'ютера цілі інформаційні електронні банки даних, змінюють та псують комп’ютерні файли. Очевидно, що з технічного боку це набагато

складніше здійснити у порівнянні з тим, що роблять звичайні хакери [55, с. 16].

Практика свідчить, що за декілька годин, не докладаючи особливих зусиль, будь-який крекер-технік середньої руки може пограбувати банк даних французького комісаріату з атомної енергії і отримати найконфіденційніші відомості, наприклад, таємний проект створення лазера чи програму будівництва ядерного реактора [39, с. 30].

Так, наприклад, американський крекер Річард Чешир, якого запросили в Мюнхен на нараду експертів з охорони відомостей в комп'ютерах, на очах фахівців забезпечив собі доступ спочатку в німецьку, потім в американську інформаційні мережі, а звідти проник в один із найважливіших стратегічних комп'ютерів США [70, с. 10].

Вважаємо, що детальний аналіз рис, ознак, відомостей і манер поведінки хакерів, здійснений нами вище, необхідний для більш всебічної систематизації і класифікації окремих наступних груп комп’ютерних злочинців. Підсумовуючи викладене, зазначимо, що хакери є достатньо потужними особами, які створюють дієву платформу для формування класифікації різновидів інших різновидів груп комп’ютерних злочинців. Нижче продовжимо розгляд класифікації цих груп комп’ютерних злочинців згідно з реальними показниками їх безпосередньої злочинної діяльності.

Важливою другою групою комп’ютерних злочинців є інсайдери. Сутність слова інсайдер походить від англійського inside – всередині. Таким чином, інсайдер, це особа, яка володіє інформацією «з внутрішніх джерел», оскільки може краще оцінити, проаналізувати, спрогнозувати реальний стан в державі, установі, відомстві чи організації, ніж будь-який інший фахівець, який, як правило, користується зовнішньою інформацією для здійснення експертних висновків. Що стосується інсайдерів – комп’ютерних злочинців, то вони характеризуються достатньо потужними даними, рисами, ознаками, манерами поведінки, оскільки мають безпосередній доступ до будь-якої важливої прихованої, секретної, конфіденційної, закритої інформації. Це, як

правило, посадові особи вищого рангу – керівники державних і корпоративних установ, відомств і організацій. Відомо, що з позиції науки кримінології інсайдери, по-перше, це будь-яка особа (юридична чи фізична), яка має реальний доступ до таємної, прихованої, латентної, закритої, конфіденційної інформації про діяльність державних, комерційних чи приватних відомств, установ і організацій, яка знаходиться в автоматизованій комп'ютерній системі, електронній комп'ютерній мережі чи електронному банку даних в силу свого службового (посадового) становища або родинних зв'язків, по-друге, це фізична особа, що в силу свого службового становища має доступ до важливої (секретної, конфіденційної, закритої) інформації, яка є недоступною для широкого загалу. Очевидно, що такі комп'ютерні злочинці є надзвичайно небезпечними, оскільки володіють інформацією з перших джерел.

Вважається, що початком обговорення на рівні наукових та правлячих організацій щодо внутрішніх загроз є проєкт «Інсайдерське дослідження загроз», який у 2002 році розпочали Програма CERT Інституту програмної інженерії Університету Карнегі-Меллона і Національний центр оцінки загроз (NTAC) Секретної служби США (USSS). Уперше був здійснений комплексний аналіз внутрішніх загроз на основі досвіду NTAC у поведінковій психології та технічного досвіду CERT з питань безпеки. Команда проєкту CERT акцентувала увагу на важливість використання реальних даних для створення моделі внутрішньої загрози — складних взаємодій, відносного ступеня ризику та непередбачених наслідків політики, практики, технологій, внутрішніх психологічних проблем та організаційної культури з часом. Таким чином було започатковано проєкт MERIT (Management and Education of the Risk of Insider Threat) – «Управління та навчання ризику внутрішньої загрози». В даному дослідженні було проаналізовано 150 інсайдерських кіберзлочинів у секторах критичної інфраструктури США. Подальша робота CERT включала детальне групове моделювання та аналіз 54 випадків внутрішнього IT-саботажу із 150 випадків. Інсайдерський IT-саботаж включає інциденти, в яких основною метою інсайдера було саботувати певний аспект організації або завдати

конкретної шкоди особі. У цьому документі описано сім загальних спостережень щодо внутрішнього IT-саботажу на основі емпіричних даних і результатів дослідження та описано модель системної динаміки проблеми внутрішнього IT-саботажу, яка розробляє складні взаємодії в домені та непередбачувані наслідки організаційної політики, практики, технологій і культури на поведінку інсайдерів [17].

Третю групу комп'ютерних злочинців складають телефонні кібершахраї – фрікери. Фрікі (phone+break=phreak) – це комп'ютерні злочинці, які спеціалізуються на використанні телефонних систем з метою уникнення від оплати телекомунікаційних послуг. Фрікери отримують насолоду від подолання труднощів технічного плану. Тому у своїй злочинній діяльності фрікери використовують спеціальне технологічне обладнання («чорні» та «блакитні» скрині), які генерують спеціальні тони виклику для телефонних мереж. На сьогодні, фрікери переважно орієнтуються на отримання кодів комп'ютерного доступу, крадіжках телефонних карток та номерів комп'ютерного доступу, з метою віднести платню за телефонні розмови на рахунок іншого абонента. Досить часто фрікери займаються прослуховуванням телефонних розмов.

До окремої четвертої групи комп'ютерних злочинців слід віднести колекціонерів. Фактично колекціонери (codes kids) – це комп'ютерні злочинці, які колекціонують та використовують комп'ютерні програми, які перехоплюють різні паролі, а також коди телефонного виклику та номери приватних телефонних компаній, які мають вихід до загальної електронної мережі. Як правило, молодші за хакерів та фрікерів. Практично колекціонери обмінюються програмним комп'ютерним забезпеченням, паролями, кодами, номерами, але не торгують ними.

До наступної п'ятої групи комп'ютерних злочинців слід віднести спуферів. Відомо, що спуфери використовують різні технічні можливості, для зламу кіберзахисту чужих комп'ютерів з метою викрадання конфіденційної інформації. Цим способом скористався знаменитий хакер Кевін Митник ще у

1995 році, коли він зламав кіберзахист домашнього комп'ютера експерта по комп'ютерній безпеці ФБР США Цутому Шимомури [25].

Окрему шосту групу комп'ютерних злочинців являють спамери. Фактично спамери – це комп'ютерні злочинці, які здійснюють розсилку спаму – кореспонденції, яку адресати не висловили бажання отримувати, з метою поширення порнографічних творів, комп'ютерних вірусів або виведення з ладу поштового сервісу тощо [36, с. 90].

До достатньо небезпечної сьомої групи комп'ютерних злочинців слід віднести кібершахраїв, яких прийнято називати «фішерами». Таким чином фішери – це такі кібершахраї, які спеціалізуються на фішингу – спеціальному виді кібершахрайства, метою якого є отримання комп'ютерного доступу до конфіденційних секретних даних користувачів, логінів, паролів шляхом направлення повідомлення з пропозицією підтвердити дані облікового запису (онлайн-аукціони, лотереї, банківські і страхові послуги, інтернет-магазини тощо) з прямим посиланням на сайт, використання на якому особою його логіну та паролю дозволяє отримати доступ до її акаунту, банківського рахунку або персональних даних. Характерною ознакою таких сайтів є їх подібність до загальновідомих інтернет-ресурсів [149, с. 286; 36, с. 90].

Наступну, восьму групу комп'ютерних злочинців складають кардери. Відомо, що кардери – це комп'ютерні злочинці, які здійснюють викрадення номерів кредитних електронних карт з подальшим отриманням доступу до банківських рахунків осіб, чиї паролі, номери і коди електронних карт були викрадені [189, с. 201; 41, с. 85].

До окремої дев'ятої групи комп'ютерних злочинців слід віднести кіберплутів. Фактично кіберплути (cybercrooks) – це такі комп'ютерні злочинці, які спеціалізуються на фінансових розрахунках. Кіберплути використовують автоматизовані комп'ютерні системи для крадіжки грошей, отримання номерів електронних кредитних карток та іншої цінної фінансово-економічної інформації. Отриману інформацію кіберплути потім продають іншим особам. Відомо, що кіберплути досить часто контактують з

організованою комп'ютерною злочинністю. (Коди PBX можуть продаватись за 200-500 доларів США, як і інші види інформації неодноразово. Популярним товаром є кредитна інформація, інформаційні бази правоохоронних органів та інших державних установ, відомств і організацій) [56].

Десяту групу становлять комп'ютерні злочинці – кіберкрукери, які є достатньо небезпечним їх видом. Це обумовлено тим, що кіберкрукери – це комп'ютерні злочинці, які спеціалізуються на несанкціонованому проникненні в автоматизовані комп'ютерні системи та електронні мережі фінансово-банківських установ і закриті комп'ютерні системи і електронні мережі, електронні бази даних державних органів з метою перепродажу отриманих персональних даних [87].

До одинадцятої групи комп'ютерних злочинців слід віднести вірмейкерів – творців комп'ютерних вірусних програм. Дійсно, до вірмейкерів (вексерів) відносяться досить небезпечна група комп'ютерних злочинців, які розробляють комп'ютерні віруси. Отже вірмейкери – це надзвичайно небезпечні творці комп'ютерних вірусів [139, с. 76].

Дванадцяту групу комп'ютерних злочинців являють кіберсквотери. Фактично група кіберсквотерів – це комп'ютерні злочинці, які здійснюють захоплення доменних імен з корисливих мотивів [41, с. 85].

До тринадцятої групи комп'ютерних злочинців слід віднести електронних піратів, електронних шахраїв або кіберторгашів. Відомо, що кібертограші або електронні пірати (wares dudes) – це комп'ютерні злочинці, які спеціалізуються на збиранні та торгівлі піратським програмним забезпеченням. Ці комп'ютерні злочинці вчиняють також злочини, які пов'язані із порушенням авторського права. На сьогоднішній день це дуже чисельна група комп'ютерних злочинців. Кількість піратських BBS має співвідношеня до хакерських як 20 до 1 [64, с. 14-15].

Чотирнадцяту групу надзвичайно небезпечних комп'ютерних злочинців являють кібертерористи. Сучасні кібертерористи фактично спеціалізуються на віртуальному терорі. Про дану загрозу вказує також і заступник Генерального

секретаря ООН, який очолює контртерористичне управління, В. Воронков, який зазначає, що ми повинні зберегти пильність і єдність та передбачити прогресуючу комплексну загрозу, яка створюється терористами [99]. Для запобігання злочинним діям терористів ООН здійснено 68 активних програм і проектів на загальну суму в 63 млн. долл. США з метою надання державам-членам підтримки в здійсненні Глобальної контртерористичної стратегії [99].

Слід зазначити, що серед комп'ютерних терористів певну частку складають люди, які пройшли спеціальну комп'ютерну підготовку, спрямовану на здійснення комп'ютерної терористичної діяльності.

А. Політті зазначає, що комп'ютерний тероризм тісно пов'язаний з організованою злочинністю і корупцією. За деякими даними щорічно в світі відмивається 300 – 500 мільярдів доларів (з яких 30-40% походять від наркотиків, а решта є прибутком від фіскальних порушень, контрабанди зброєю, тероризму, шахрайства) [172, с. 22-23].

Загальна характеристика та тенденції розвитку комп'ютерного тероризму свідчить про багато різновидів злочинних зазіхань, які вчиняють комп'ютерні терористи. Серед найбільш відомих способів комп'ютерного тероризму є такі: несанкціонований доступ до інформації в автоматизованих комп'ютерних системах; кібервійни у віртуальному просторі (інформаційні війни); крадіжки грошей та матеріальних цінностей щодо інформації, яка циркулює в електронній (комп'ютерній) формі; шахрайство в інтернеті; транскордонне «нелегальне інформаційне брокерство»; організоване «комп'ютерне піратство»; шахрайство з кредитними картками; шахрайство в інтернет-торгівлі; шкідливі комп'ютерні програми (віруси); підробка грошей та цінних паперів; несанкціонований доступ до глобальних банківських комп'ютерних систем; крадіжки інтелектуальної власності; застосування комп'ютерних технологій для вимагання; шантаж; імітація у стільникових телефонах; дитяча порнографія; відмивання грошей тощо [128, с.37].

До п'ятнадцятої групи входять комп'ютерні злочинці, які характеризуються надзвичайно небезпечними злочинними діями в

кіберпросторі. Це – крекери. Крекери (crackers) – це фактично «комп'ютерні терористи», «комп'ютерні пірати», «комп'ютерні кібершахраї», що професійно спеціалізуються на вторгненні в автоматизовані комп'ютерні системи, електронні банки даних і соціально-комунікаційні електронні комп'ютерні мережі з метою заволодіння конфіденційною інформацією. Крекери – це «супер-професіонали», які здатні завдати будь-якої шкоди автоматизованій комп'ютерній системі і електронній комп'ютерній мережі, викрасти інформацію (ресурси, кошти) з електронних банків даних, змінити та зіпсувати відомості, дані у відповідності зі своїми інтересами. Зазвичай, це високопрофесійні комп'ютерні програмісти, які створюють різного роду комп'ютерні програми, комп'ютерні віруси та інші програмні продукти для реалізації масштабних злочинних дій. Крекери співпрацюють з організованими злочинними групами, спецслужбами та іншими відомствами, установами і організаціями, які потребують висококваліфікованих фахівців в галузі інформатики, кібернетики, нейробіоніки тощо.

До наступної шістнадцятої групи комп'ютерних злочинців слід віднести творців шкідливих комп'ютерних програм. Відомо, що творці шкідливих комп'ютерних програм фактично наносять непоправимі збитки як людині, так і державним та корпоративним установам. Сьогодні шкідливі комп'ютерні програми, які розроблені комп'ютерними злочинцями, дозволяють здійснювати кібератаки та фактично призводять до великих і менших комп'ютерних епідемій [80, с. 73]. В даний час спостерігається стрімкий ріст шкідливих програм, які переслідують певні як політичні, так і комерційні цілі – крадіжку конфіденційних даних, фінансових коштів, різного роду ресурсів (матеріальних і інтелектуальних), паролів доступу до інтернету, а також інші зловмисні дії, які спричиняють матеріальну шкоду користувачам.

До сімнадцятої групи комп'ютерних злочинців слід відносити організовані злочинні угрупування, які використовують потужні комп'ютерні системи для вчинення білокомірцевих комп'ютерних злочинів.

Вісімнадцяту групу комп'ютерних злочинців являють іноземні розвідувальні служби, які використовують сучасні автоматизовані комп'ютерні системи, електронні банки даних і електронні мережі для здійснення несанкціонованого збору конфіденційної інформації та кібератак.

Наприклад, нещодавно офіційно підтверджено на міжнародному рівні Високим представником Європейського Союзу Жозепом Боррелем, який заявив, що 24 лютого 2022 року, за годину до початку повномасштабного вторгнення Російської Федерації в Україну, країна-агресор, а саме конкретно та безпосередньо Російська Федерація здійснила масовану кібератаку на супутникову мережу KA-SAT, що керується Viasat, яка, в свою чергу, спричинила масштабні збої у зв'язку між багатьма державними органами, підприємствами та користувачами в Україні і в низці держав-членів ЄС [24]. Це перша в світі така потужна кібератака, яка вчинена на високому рівні в електронному космічному та наземному кіберпросторі, яка передувала незаконному повномасштабному сухопутному та повітряному військовому вторгненню на територію суверенної та незалежної держави України.

Так, зовсім недавно, а саме наприкінці другого кварталу 2022 року кіберфахівці Trellix Threat Labs спостерігали за діями злочинців-вимагачів пов'язаних з Conti Team, та зважаючи на те, що жодних членів цієї злочинної групи не було заарештовано представниками правоохоронних органів Російської Федерації, дійшли висновку, що це свідчить про формування гібридної злочинної групи, яка може атакувати цілі, вибрані урядом, але з підтриманням правдоподібного заперечення даної злочинної групи після посиленого фінансування [27].

Також варто зазначити, що фахівці компанії Trellix спільно з співробітниками Центру стратегічних і міжнародних досліджень США (CSIS) дійшли основного висновку у звіті «In the Crosshairs: Organizations and Nation-State Cyber Threats», що межа між державними та недержавними комп'ютерними злочинцями продовжує стиратися [5].

Підводячи підсумки проведеної нами систематизації і класифікації комп’ютерних злочинців, слід відмітити, що сучасні комп'ютерні злочинці є фахівцями своєї сфери, оскільки відмінно знають автоматизовані обчислювальні комп’ютерні системи, електронні мережі, електронні банки даних, віртуозно володіють комп’ютерним програмуванням. Причому слід особливо акцентувати увагу на тому, що дії сучасних комп’ютерних злочинців досить обачливі, втаємничені, розумні, засекречені, продумані, оскільки супроводжуються прекрасним маскуванням, особливо у випадках вчинення комп’ютерних злочинів з метою особистого матеріального збагачення, або якщо вони носять політичний характер.

Здійснений вище аналіз дозволяє зробити висновок, що серед комп'ютерних злочинців є представники усіх груп традиційної класифікації: білокомірцевого, організованого і загальнокримінального злочинного світу. Як правило, комп’ютерні злочинці працюють як у самих організаціях, відомствах і установах, проти яких вони вчиняють комп’ютерні злочини, так і поза їх межами. Причому комп’ютерні злочинці вчиняють комп’ютерні злочини як поодинці, так і у групі зловмисних співучасників. Важливо звернути увагу на те, що провідне місце де зловмисно діють кіберзлочинці – це забезпечення антисоціальної і надзвичайно небезпечної діяльності організованих злочинних груп. Тобто сьогодні надзвичайно небезпечною є організована комп’ютерна злочинність. Це обумовлено тим, що по-перше, злочинна діяльність мафіозних злочинних структур є часткою великомасштабного бізнесу; по-друге, із організацій, відомств і установ, які використовують автоматизовані комп'ютерні системи, значно легше, простіше і зручніше «витягувати» (викрадати) гроші, ресурси, персональні дані також за допомогою автоматизованої комп'ютерної техніки; нарешті, по третє, оскільки сьогодні сили служб кібербезпеки і кіберполіції використовують автоматизовані комп'ютерні технології для боротьби із комп’ютерною злочинністю, то, відповідно, щоб попередити стеження і розгадати плани правоохоронців, білокомірцева організована кіберзлочинність широко використовує таку

могутню зброю, як автоматизовані комп’ютерні системи, автоматизовані бази даних та електронні наземні і космічні мережі.

Висновки до розділу 2

1. Особа комп’ютерного злочинця як об’єкта системного консолідованого асиметричного криміналогічного дослідження повинна вивчатися з допомогою новітньої системи засобів, методів, методик і технологій. Дана система засобів необхідна для зібрання, обробки, аналізу і інтерпретації кримінологічно значущої інформації про характерні ознаки і риси, манери поведінки особи комп’ютерного злочинця. На даний час для здійснення кримінологічних досліджень характерних рис і ознак та манер поведінки особи комп’ютерного злочинця використовуються такі групи засобів і методів збирання інформації: 1) документальний метод; 2) опитування; 3) спостереження; 4) експеримент, засоби і методи обробки, аналізу, упорядкування та інтерпретації зібраної кримінологічної інформації.

2. Кримінологічні дослідження особи комп’ютерного злочинця базуються в основному на двох особливо значимих специфічних групах відомостей. По-перше, це відомості про особу невідомого комп’ютерного злочинця. Такі відомості будуються в основному на основі залишених комп’ютерним злочинцем матеріальних слідах як на місці події комп’ютерного злочину, так і ідеальних слідах відображених в пам'яті свідків, потерпілих тощо. Очевидно, що такі відомості дозволяють сформулювати уяву про загальні риси, ознаки та манери поведінки комп’ютерного злочинця. По-друге, це відомості, які характеризують риси, ознаки та манери поведінки для встановлення відомого комп’ютерного злочинця. Очевидно, що в даній ситуації досліджуються відомості не тільки про ціннісні орієнтації, особливості антисуспільних поглядів, але і про те, яка інформація є найбільш характерною для досліджуваної особи комп’ютерного злочинця. З цією метою

вивчаються особливості поведінки комп’ютерного злочинця до, під час і після вчинення комп’ютерного злочину, його зв’язках з потерпілим.

3. Особу комп’ютерного злочинця як об’єкт системного кримінологічного дослідження доцільно розглядати і вивчати у взаємозв’язку з його оточенням, зрозуміти причини його появи та розвитку, а це означає необхідність з’ясування всіх характерних його ознак, рис, властивостей і манер поведінки. При цьому дане дослідження потрібно здійснювати систематизовано, в певній послідовності, з використанням наукових засобів систематизації і класифікації, лише тоді воно дасть максимально наближений до реальності, а не тільки до уяви дослідника, результат.

4. Комп’ютерних злочинців можна умовно систематизувати і класифікувати на такі окремі групи і підгрупи: хакери, крекери, фрікери, спамери, колекціонери, фішери, кіберплути, кардери, кіберкрукери, кіберсквокери, інсайдери, вірмейкери, кібертерористи, електронні торгаші або кіберпірати, спуфери, творці шкідливих комп’ютерних програм, організовані злочинні кіберугрупування, іноземні розвідувальні кіберслужби.

5. Серед комп'ютерних злочинців є представники усіх груп традиційної класифікації: білокомірцевого, організованого і загальнокримінального злочинного світу. Як правило комп’ютерні злочинці працюють як у самих організаціях, відомствах і установах, проти яких вони вчиняють комп’ютерні злочини, так і поза їх межами. Причому комп’ютерні злочинці вчиняють комп’ютерні злочини як поодинці, так і у групі зловмисних співучасників. Важливо звернути увагу на те, що провідне місце де зловмисно діють кіберзлочинці – це забезпечення антисоціальної і надзвичайно небезпечної діяльності організованих злочинних груп.

6. Сучасні комп'ютерні злочинці є фахівцями своєї сфери, оскільки відмінно знають автоматизовані обчислювальні комп’ютерні системи, електронні мережі, електронні банки даних, віртуозно володіють комп’ютерним програмуванням. Причому слід особливо акцентувати увагу на тому, що дії сучасних комп’ютерних злочинців досить обачливі, втаємничені,

розумні, засекречені, продумані, хитрі, оскільки супроводжуються прекрасним маскуванням, особливо у випадках вчинення комп'ютерних злочинів з метою особистого матеріального збагачення, або якщо вони носять політичний характер.

7. Комп'ютерні злочинці сьогодні спеціалізуються на вчиненні таких зловмисних дій: втручання або перехоплення (незаконний доступ, перехоплення, викрадення часу); зміна або пошкодження інформації («логічна бомба», «троянський кінь», «програми-віруси», «черв'яки»); комп'ютерне шахрайство (шахрайство з автоматами на видачі готівки, комп'ютерна підробка, шахрайство з ігровими автоматами, шахрайство шляхом неправильного вводу/виводу або маніпуляції програмами, шахрайство з платіжними засобами, телефонне шахрайство); несанкціоноване копіювання (несанкціоноване тиражування комп'ютерних ігор, несанкціоноване тиражування програмного забезпечення, несанкціоноване тиражування напівпровідникової продукції); комп'ютерний саботаж (саботаж технічного забезпечення, саботаж програмного забезпечення); злочини, які пов'язані з використанням комп'ютерів (незаконне використання дошки електронних оголошень (BBS), викрадення комерційної таємниці, зберігання або розповсюдження матеріалів, які є об'єктом судового переслідування) тощо.

РОЗДІЛ 3
ШЛЯХИ ЗАПОБІГАННЯ І ПРОТИДІЇ КРИМІНАЛЬНИМ ПРАВОПОРУШЕННЯМ, ЩО ВЧИНЯЮТЬСЯ ОСОБОЮ КОМП'ЮТЕРНОГО ЗЛОЧИНЦЯ

3.1. Пріоритетні напрями протидії кримінальним правопорушенням, що вчиняються комп'ютерними злочинцями

Сьогодні розвиток автоматизації, комп'ютерізації, інформатизації усіх сфер суспільного життя надає нові можливості для розвитку національної освіти, науки і практики. Водночас, поширення інформаційних технологій, як свідчить статистика, має й свій негативний аспект: це відкриває шлях до антисоціальної та злочинної поведінки. Це обумовлено тим, що автоматизовані комп'ютерні системи містять у собі нові й дуже досконалі можливості для вчинення невідомих раніше комп'ютерних правопорушень, а також для вчинення традиційних злочинів, але нетрадиційними новітніми електронними засобами, методами і технологіями. Консолідований асиметричний аналіз феномену космічних і наземних кіберзагроз, здійснюваних комп'ютерними злочинцями, проведений нами на основі використання новітніх ноозасобів пізнання та доказування свідчить про необхідність проведення спеціальних кримінологічних досліджень як космічної, так і наземної кіберзлочинності, оскільки такі криміногенні явища загрожують національній безпеці України. Вважаємо, що сучасний стан законодавчого врегулювання запобігання і протидії зловмисним діям комп'ютерних злочинців є недостатнім, а тому потребує прийняття відповідних конвенцій і законів як на світовому, так і на загальнодержавному рівні.

Проведений нами консолідований асиметричний аналіз сучасного стану кіберзагроз, які завдають комп'ютерні злочинці, свідчить, що здійснювані

ними комп'ютерні злочини завдають великих соціальних і економічніх збитків, оскільки сьогодні суспільство стає все більш і більш залежним від роботи автоматизованих комп'ютеризованих систем у різноманітних сферах суспільного життя – від керування рухом космічних станцій, літаків і потягів, освітнього і наукового забезпечення, а також до медичного обслуговування та національної безпеки. Іноді навіть невеличкий збій у функціонуванні таких автоматизованих комп'ютерних систем, електронних банків даних і електронних мереж може привести до реальної загрози життю людей. Очевидно, що стрімке зростання глобальних комп'ютерних мереж, а також можливість комп'ютерних злочинців підключення до них через звичайні телефонні лінії та електронні засоби доступу посилюють можливості їх використання для злочинної діяльності.

Відомо, що частіше від наземних і космічних зловмисних дій комп'ютерних злочинців страждають більш розвинуті в технологічному відношенні країни, однак й інші держави, з початком впровадження процесу автоматизації, комп'ютеризації, інформатизації стають, так би мовити, «родючим ґрунтом» для вчинення таких комп'ютерних злочинів. Зокрема, глобальна комп'ютерна мережа інтернет сьогодні надає реальну можливість комп'ютерному злочинцю увійти до будь-якої державної, відомчої чи приватної (комерційної) автоматизованої комп'ютерної системи, електронного банку даних, електронної мережі в тому числі й військової, до того ж, це можливо зробити майже з будь-якої точки світу. У порівнянні із США національна кібербезпека України поки що залежить від автоматизованих комп'ютерних систем, електронних банків даних і електронних мереж значно менше. Водночас, на сьогодні ми стикаємося зі зловмисними діями комп'ютерних злочинців в основному у банківській, страховій, фінансово-кредитній сфері тощо. Але очевидно, що в недалекому майбутньому такі комп'ютерні злочинці можуть вчинити такі зловмисні дії, що дозволять привести до всесвітніх глобальних катастроф – ядерних, екологічних,

біологічних, політичних, економічних, фінансових, телекомунікаційних, транспортних тощо.

Судова практика засвідчує, що введення сучасної автоматизованої комп'ютерної системи управління повітряним, морським, залізничним, автомобільним рухом, поширення автоматизованої телекомунікаційної мережі, впровадження в банківській галузі системи електронних платежів, використання комп'ютерів у діяльності суду, прокуратури, правоохоронних органів та керуванні військами значно розширили сферу діяльності для хакерів і крекерів [43, с. 16-17].

Протягом останніх років нами вивчалися проблеми, пов'язані з бурхливим розвитком феномена, відомого в усьому світі під назвою «комп'ютерна злочинність». Вважаємо, що на сьогоднішній день це поняття включає всі протизаконні дії, при яких електронне опрацювання інформації було знаряддям їх вчинення або їх об'єктом. Таким чином, у це коло небезпечних проблем потрапили не тільки комп'ютерні злочини, які безпосередньо пов'язані з використанням комп'ютерів, але й такі, як фінансове шахрайство з кредитними магнітними картками, злочини в галузі телекомунікацій (фінансове шахрайство з оплатою міжнародних телефонних переговорів), злочинне використання банківської мережі електронних платежів, комп'ютерне програмне «піратство», шахрайство з використанням ігрових автоматів та багато інших злочинів. До цієї групи ризикових питань також відносяться такі проблеми, які пов'язані з протиправним використанням електронних доказів комп'ютерного походження.

Аналіз статистичних даних дозволяє зробити висновок, що сьогодні типовими і найбільш небезпечними комп'ютерними злочинами, які вчиняються комп'ютерними злочинцями не тільки в Україні, але в Європі та світі є наступні: 1) втручання або перехоплення (незаконний доступ, перехоплення, викрадення часу; 2) зміна або пошкодження інформації («логічна бомба», «троянський кінь», програми-віруси, «черв'яки»); 3) комп'ютерне шахрайство (шахрайство з автоматами на видачі готівки,

комп’ютерна підробка, шахрайство з ігровими автоматами, шахрайство шляхом неправильного вводу/виводу або маніпуляції з програмами, шахрайство з платіжними засобами, телефонне шахрайство тощо); 4) несанкціоноване копіювання (несанкціоноване тиражування комп’ютерних ігор, несанкціоноване тиражування програмного забезпечення, несанкціоноване тиражування напівпровідникової продукції); 5) комп’ютерний саботаж (саботаж технічного забезпечення, саботаж програмного забезпечення); 6) злочини, пов’язані з комп’ютерами (незаконне використання дошки електронних оголошень, викрадення комерційної таємниці, зберігання або розповсюдження матеріалів, які є об’єктом судового переслідування).

Вважаємо, що сьогодні комп’ютерна злочинність – це міжнародне (транскордонне, транснаціональне, трансконтинентальне, планетарне) наземне і космічне явище, рівень якого тісно пов’язаний з науковим, освітнім, військовим, економічним рівнем розвитку суспільства в різних державах та регіонах, а також можливостями користування Всесвітньою мережею інтернет. При цьому очевидно, що менш розвинуті в науково-технічному і технологічному відношенні країни завдяки продуктивній діяльності міжнародних правоохоронних організацій мають можливість використати досвід більш розвинутих країн щодо встановлення особи комп’ютерного злочинця з метою запобігання та протидії комп’ютерним злочинам. Причому тенденції розвитку мережі інтернет сприяють комп’ютерним злочинцям, які вчиняють комп’ютерні злочини. Хоча наявні кіберзасоби та кіберзаходи направлені для встановлення комп’ютерних злочинців є різні. Водночас, в більшості випадків ці кіберзасоби базуються на єдності інформаційно-телекомунікаційної технологічної бази, яка дозволяє швидко встановлювати комп’ютерних злочинців.

Відомо, що сьогодні активно використовують комп’ютерні злочинці Всесвітню павутину (WorldWideWeb - WWW) – інтернет (від англ. internet). Це обумовлено тим, що інтернет – це всесвітня система взаємосполучення

комп’ютерних мереж, що базуються на відповідних комплексах протоколів, якими мають можливість користуватися і комп’ютерні злочинці. Сьогодні інтернет складається з мільйонів глобальних і локальних, публічних і приватних, урядових і комерційних, наукових і освітніх мереж, пов’язаних між собою з використанням різноманітних дротових, бездротових і оптичних технологій. Ця всесвітня мережа мереж становить фізичну основу для розміщення величезної кількості банків електронної інформації на своїх електронних ресурсах.

Відомо, що інтернет сьогодні відкрив кіберпростір для реалізації тих ідей, інновацій, що раніше були просто нейздійсненими. Це дозволило людям різних країн спілкуватися без обмежень, одночасно збиратися в новій віртуальній реальності. Одночасно слід зазначити, що віртуальний світ сповнений небезпеки, оскільки тут діють різноманітні хакери і крекерські злочинні угрупування. Для виявлення і затримання комп’ютерних злочинців, а також з метою запобігання кіберзлочинності в інтернет-просторі створено спеціальний орган – інтернет-поліцію. Слід зазначити, що інтернет-поліція – це повноправна силова структура, яка забезпечує кібербезпеку мережі інтернет від зловмисних дій комп’ютерних злочинців та здійснює заходи по боротьбі з інтернет-злочинністю. У цілому, інтернет-поліція складається з силових структур, урядовців та волонтерів більше ніж 70 країн світу. Тісна співпраця інтернет-поліції та урядових структур у повній мірі сприяє виявленню і затриманню комп’ютерних злочинців, причому місце знаходження такого зловмисника або підозрюваного значення не має, оскільки віртуальний світ існує без кордонів.

Інтернет-поліція структурно складається з трьох основних підрозділів. Підрозідл LEO (силові структури) об’єднує представництва інтернет-поліції всіх країн-членів віртуального світу. Цивільний підрозділ об’єднує всі волонтерські формування країн-членів віртуального світу. Підготовчий підрозділ забезпечує навчання новачків-кіберполіцейських. Керівництво даним підрозділом покладено на LEO.

Інтернет-поліція займається виявленням комп'ютерних злочинців та запобіганням інтернет-злочинності. Спеціально підготовлені офіцери інтернет-поліції володіють сучасними технологіями виявлення та затримання хакерів і крекерів, які зловмишляють у віртуальноиу інтернет-просторі.

Інтернет-поліція займається дослідженням різноманітних дій комп'ютерних зловмисників: починаючи з незначних, таких як образа в чаті або електронному листі, закінчуючи виявленням і затриманням комп'ютерних злочинців, які займаються незаконним транспортуванням наркотиків, нелегальною проституцією, викраденням людей та кібертероризмом у віртуальному світі.

База даних інтернет-поліції містить інформацію про всі кіберінциденти і вчинені інтернет-злочини, починаючи з 1986 року. Це значною мірою сприяє швидко виявляти зловмисні дії комп'ютерних злочинців, встановлювати і аналізувати нові види інтернет-злочинів та поліпшує оперативність прийняття запобіжних дій здійснюваних інтернет-поліцейськими [135, с. 36-37].

Розглянемо нижче більш детально характерні риси і ознаки комп'ютерної злочинності. Вважаємо, що серед них слід виокремити наступні: це як правило, міжнародний наземний або космічний характер комп'ютерного злочину (виходить за рамки кордону однієї держави – має ознаки транскордонного, транснаціонального, трансконтинентального, планетарного характеру); значні технологічні труднощі у визначені «місцезнаходження» комп'ютерного злочину; слабкі зв'язки між ланками в системі пізнання і доказування безпосереднього факту вчинення комп'ютерного злочину; неможливість реально спостерігати й фіксувати докази візуально; широке використання комп'ютерними злочинцями засобів кодування і криптологічного шифрування інформації.

У зв'язку з цим сьогодні освітяни, науковці, громадськість усе більше цікавиться цими питаннями, оскільки кожний власник або користувач комп'ютера - це потенційний потерпілий, якого можуть очікувати тяжкі наслідки в разі вчинення комп'ютерного злочину, особливо в

загальнодержавному, комерційному та промисловому секторі, де можливі великі економічні, політичні, фінансові та військові втрати. Фактично комп'ютерні злочинці за допомогою міжнародних автоматизованих комп'ютерних мереж - типу інтернет - широко розповсюджують свій кримінальний досвід, не звертаючи увагу на національні кордони, що вимагає відповідних кроків кооперації від Інтерполу, Європолу, МПА, ФАТФ, поліцейських установ, служб кібербезпеки, протидіючих цим комп'ютерним злочинам. Все це вимагає взаємодії, співпраці та оперативного обміну інформацією про комп'ютерні злочини між різними службами кіберзахисту.

Важливо зазначити також і те, що із розвитком глобальних автоматизованих комп'ютерних мереж набула поширення практика промислового комп'ютерного шпигунства. Саме тому, проблеми розробки систем кіберзахисту та збереження державної, службової, професійної, судової, банківської, адвокатської, нотаріальної, лікарської та комерційної таємниці набувають нині надзвичайно особливого значення. Сьогодні багато проблем виникає в зв'язку з крадіжками товарів, продуктів, послуг, зокрема вторгнення до автоматизованих банків даних, телефонних мереж та незаконна торгівля послугами зв'язку. Небезпечним є те, що інтернет сьогодні широко використовують торгівці піратським комп'ютерним програмним забезпеченням, порнографією, зброєю, торгівлею людьми та наркотиками для ведення справ, обміну інформацією, координації дій. Автоматизовані комп'ютерні системи, комп'ютерні мережі та автоматизовані банки даних, державних і комерційних відомств та установ, окрім всього, сьогодні стають об'єктом нападу кібертерористів.

Підтвердженням юридичних фактів негативного впливу комп'ютерних злочинців на телекомунікаційне обладнання є нещодавня заява глави Космічного командування Збройних сил США, генерала Джеймса Дікінсона про те, що поведінка певних країн у космосі стає «дедалі більш ворожою» та періодично виникають спроби перешкоджання GPS-сигналам. На його думку,

кібератаки на GPS вже стали «повсякденням людей і націй у всьому світі» [23].

Також варто зазначити, що Високий представник Європейського Союзу Жозеп Боррель офіційно підтвердив на міжнародному рівні, що 24 лютого 2022 року, за годину до початку повномасштабного вторгнення Російської Федерації в Україну, країна-агресор здійснила масовану кібератаку на супутникову мережу KA-SAT, що керується Viasat, яка, в свою чергу, спричинила масштабні збої у зв'язку між багатьма державними органами, підприємствами та користувачами в Україні і в низці держав-членів ЄС [24]. Це перша в світі така потужна кібератака на рівні держави в електронному космічному та наземному кіберпросторі, яка передувала повномасштабному сухопутному та повітряному вторгненню на територію суверенної та незалежної України.

Варто звернути особливу увагу і на те, що історичною подією для України стало підтримання 4 березня 2022 року Керівним комітетом Об'єднаного центру передових технологій з кібероборони НАТО (CCDCOE) Заявки України на приєднання, яку було подано Національним координаційним центром кібербезпеки при РНБО України ще в серпні минулого року. Приєднання України до CCDCOE є значним досягненням для нашої держави в частині посилення міжнародної взаємодії в сфері кібербезпеки та кібероборони, а також важливим кроком на шляху вступу України до НАТО [196].

Важливі результати використання новітніх засобів пізнання для здійснення наукових досліджень («Електронне судочинство і кібербезпека», «Електронне кримінальне провадження», «Особа комп'ютерного злочинця як об'єкт кримінологічного дослідження» та ін.), отримані нами в рамках «Меморандуму про співробітництво між Національним авіаційним університетом та правничою компанією ТОВ «АЮР-КОНСАЛТИНГ». Результати використання новітніх засобів пізнання для дослідження особи комп'ютерного злочинця систематизовано та реалізовано в освітньо-

дослідницькому та праксеологічному проєкті кафедри кримінального права та процесу юридичного факультету Національного авіаційного університету за темою «Захист прав і свобод людини і громадянина (кримінально-правові аспекти): 01.09.2017- 30.06.2022» (Додаток Г).

Викладене вище дозволяє зробити висновок про те, що наявний сьогодні достатньо потужний рівень сучасних кіберзагроз в електронному світі надзвичайно небезпечних комп'ютерних злочинів як в наземному, так і космічному кіберпросторі потребує негайної розробки Концепції стратегії кібербезпеки України, а також пріоритетних напрямів наукових досліджень з метою запобігання і протидії цим негативним кіберзагрозам, кіберризикам і кібернебезпекам, які реально мають місце в суспільстві.

Вважаємо, що одним із пріоритетних напрямів запобігання зловмисним діям комп'ютерних злочинців - це формування і створення загальносвітової Стратегії кібербезпеки відповідних вітчизняних і міжнародних установ по запобіганню кіберзлочинності у наземному і космічному кіберпросторі.

Одним з пріоритетних вітчизняних напрямів запобігання зловмисних дій комп'ютерних злочинців в наземному і космічному кіберпросторі це розробка шляхів реформування діяльності органів кримінальної поліції України на сучасному етапі цивілізаційного розвитку.

Базуючись на вище викладеному, вважаємо, що на сучасному етапі цивілізаційного розвитку в Україні в першу чергу потребують суттєвого реформування органи кримінальної кіберполіції. Про це свідчать і результати діяльності Національної поліції України за 2021 рік (Додаток Д).

Сьогодні варто зазначити, що 23.11.2001 р. історичною подією для цивілізованого світу стало підписання важливого правничого документу в Будапешті Конвенції про кіберзлочинність [131] державами-членами Ради Європи та іншими державами, які усвідомлювали глибокі зміни, спричинені розвитком електронної ери і переходом всіх сфер життя на електронні (цифрові) технології, конвергенцію і глобалізацію комп'ютерних мереж.

Зазначимо, що наша держава долучилась до даної визначної міжнародної ініціативи 07.09.2005 р., ратифікувавши Законом України [110] Конвенцію про кіберзлочинність, норми якої згідно зі ст. 9 Конституції України стали частиною національного законодавства України [134].

Беручи до уваги чинні правові положення Конвенції про кіберзлочинність та враховуючи значне зростання динаміки кіберзлочинності в світі, наказом МВС України № 581 від 24.11.2010 р. [161] було організовано діяльність Департаменту боротьби з кіберзлочинністю і торгівлею людьми МВС України, а також підрозділів боротьби з кіберзлочинністю і торгівлею людьми в ГУМВС та УМВС.

Через п’ять років згідно з наказом Національної поліції України від 07.11.2015 р. №10 «Про затвердження Штату Департаменту кіберполіції Національної поліції України» передбачено залучення в штат чотирьохсот фахівців з кібербезпеки. Пізніше згідно з наказом Національної поліції України від 10.11.2015 р. №85 було затверджено Положення про Департамент кіберполіції Національної поліції України [60, с. 26].

Аналізуючи стан практичної діяльності Департаменту кіберполіції Національної поліції України з моменту створення до середини 2022 року, нами встановлено відсутність чіткої налагодженої організаційно-правової, інформаційно-комунікаційної та процесуальної взаємодії між Головним управлінням та регіональними відділеннями Національної поліції на всій території України в ході реагування на кіберінциденти. Багаторічний консолідований системний асиметричний аналіз діяльності кіберполіції України свідчить про відсутність дієвої реєстрації кіберінцидентів, а також неналежне правове забезпечення запобігання та протидії кіберзлочинів відповідно до засадничих положень чинного законодавства України.

Вважаємо, що пріоритетним напрямом суттєвого посилення запобігання комп’ютерних злочинів в мережі інтернет і встановлення осіб, які їх вчинили на вітчизняному рівні – це, по-перше, створення Департаменту стратегічних розслідувань Національної поліції України [162]. Відповідно до затвердженого

Положення основними завданнями цього департаменту є: реалізація повноважень Національної поліції України в частині боротьби з організованою злочинністю, злочинністю в органах державної влади та місцевого самоврядування, протидії корупції, захисту прав і свобод людини і громадянина та об'єктів права власності від протиправних посягань, а саме: 1) виявлення, припинення і попередження незаконної діяльності суспільно небезпечних організованих груп і злочинних організацій, у тому числі в органах державної влади та місцевого самоврядування, які впливають на криміногенну ситуацію в державі та в окремих її регіонах; 2) здійснення заходів, спрямованих на координацію діяльності органів (підрозділів) поліції у сфері боротьби з тероризмом відповідно до компетенції, визначеної законодавством України; 3) протидія корупції серед посадових осіб, на яких поширюється дія Закону України «Про запобігання корупції», вжиття заходів з метою виявлення корупційних правопорушень і правопорушень, пов'язаних з корупцією, та їх припинення відповідно до законодавства України; 4) здійснення оперативно-розшукової діяльності, спрямованої на здобуття інформації про криміногенні процеси в злочинному середовищі, пов'язані з протиправною діяльністю окремих осіб та злочинних угруповань, схеми легалізації (відмивання) доходів, одержаних злочинним шляхом; 5) організація та здійснення відповідно до законодавства України заходів захисту працівників ДСР, інших органів та підрозділів Національної поліції України, забезпечення безпеки учасників кримінального судочинства, членів їх сімей та близьких родичів цих осіб.

По-друге, створення підрозділів поліції спеціального призначення «Корпус оперативно-раптової дії» [163]. Виходячи з положень закріплених у відомчому нормативному акті основними функціями цього підрозділу Національної поліції України є: 1) організація, спільно з керівниками ГУНП, діяльності управлінь «КОРД» ГУНП. Координація та контроль щодо виконання цими підрозділами визначених завдань та функцій, а також щодо дотримання нормативно-правових актів та організаційно-розпорядчих актів

Національної поліції України у сфері протидії злочинності; 2) здійснення заходів у сфері протидії злочинності, які пов'язані з підвищеною загрозою для життя і здоров'я поліцейських, високою ймовірністю збройного опору та передбачають, що поліцейські повинні мати високий рівень фізичної підготовленості, професійної майстерності та вміння впевнено діяти в екстремальних умовах; 3) участь у плануванні, організації та забезпеченні професійного навчання поліцейських Департаменту та управлінь «КОРД» ГУНП.

Таким чином, удосконалення правового, законодавчого і організаційно-управлінського забезпечення запобігання комп'ютерній злочинності з метою встановлення осіб, які вчиняють комп'ютерні правопорушення в Україні є надзвичайно актуальним і своєчасним пріоритетним напрямом.

Вважаємо, що ці знання особливо необхідні сьогодні, оскільки сучасні комп'ютерні злочинці використовують можливості мережі інтернет у своїх злочинних цілях.

Відомо, що інтернет є не тільки засобом передачі інформації в усіх професійних сферах, але став глобальною електронною мережею, світовою павутиною, яка стосується усіх аспектів нашого життя. Із розвитком сучасних комп'ютерних технологій тісно пов'язана і кіберзлочинність та кібертероризм, тобто злочини, що вчиняються з допомогою мережі інтернет. За статистикою Американського Інституту Комп'ютерної Безпеки (Computer Security Institute) збитки від злочинів, що вчиняються за допомогою комп'ютерних технологій, з кожним роком зростають. Так сукупний збиток від таких злочинів у США тільки за 5 років з 2017 р. по 2021 р. склав вже більше 18,7 мільярдів доларів США. За даними експертів тільки у 2021 році втрати комерційних структур через інтернет склали понад 6,9 мільярдів доларів [11].

Викладене вище свідчить, що Україна сьогодні не здатна протистояти цьому злу самостійно. Нагальною є активізація міжнародного співробітництва на рівні міжнародно-правового регулювання. Приєднання України до страсбургської Конвенції щодо попередження кіберзлочинів (Draft

Conventionon Cyber-crime) [8] є важливим кроком, спрямованим проти загрози поширення кіберзлочинів у сферах державного та приватного сектору економіки. Наша держава також здійснює ряд необхідних заходів щодо нормативно-правового регулювання запобігання і протидії комп'ютерній злочинності, прикладом чого є Указ Президента від 31 липня 2000 року «Про заходи щодо розвитку національної складової глобальної інформаційної мережі інтернет та забезпечення широкого доступу до цієї мережі в Україні» [194], а також розділ 16 Кримінального кодексу України «Кримінальні правопорушення у сфері використання електро-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж [140]. Нещодавно прийняті також два важливі закони, зокрема, Закон України «Про основні засади забезпечення кібербезпеки України» №2163-VIII від 5 жовтня 2017 року [109] і Закон України «Про електронні довірчі послуги» №2155-VIII від 5 жовтня 2017 року [107]. Очевидно, що ці нормативні акти загалом урегульовують ряд правовідносин в електронній (цифровій) сфері. Водночас вважаємо, що для більш креативного здійснення державної правової регуляції в електронній (цифровій) галузі України слід постійно та оперативно вдосконалювати законодавство.

Проведений нами аналіз дозволив виявити та підтвердити юридичний факт вчинення комп'ютерними злочинцями першого в Україні космічного кіберзлочину, який нещодавно вже розглянутий в українському суді [185, с. 14-31].

Даний перший космічний кіберзлочин був вчинений комп'ютерними злочинцями на наземній території і космічному просторі України, а також на наземних територіях та космічному просторі семи держав світу (на чотирьох континентах – Американському, Африканському, Євразійському та Європейському) з допомогою використання потужних інструментів міжнародних автоматизованих комп'ютерних систем супутникового зв'язку та державних і приватних наземних станцій електрозв'язку ще в жовтні 2018 року [152, с. 9-17].

Варто особливо звернути увагу на те, що офіційні письмові, електронні та особисті звернення жертви кіберінциденту до державних установ України та законодавчо визначених відповідних правоохоронних органів (до Уповноваженого Верховної Ради України з прав людини, до Голови Верховного Суду України, до Голови Апеляційного господарського суду та інших місцевих апеляційних та касаційних інстанцій України, до Генерального прокурора України, до голови Ради національної безпеки і оборони України, до Міністра внутрішніх справ України, до керівництва Департаменту контррозвідувального захисту інтересів держави у сфері інформаційної безпеки Служби безпеки України, до голови Департаменту у сфері захисту персональних даних, до керівництва Департаменту Кіберполіції Національної поліції України, до керівництва Департаменту кіберполіції Київського управління кіберполіції Національної поліції України, до десяти районних управлінь поліції міста Києва, Головного управління Національної поліції України до Департаменту у сфері захисту персональних даних) щодо встановлення особи комп'ютерного злочинця, а також з метою запобігання даного кіберінциденту жодних реальних результатів не дали. Ці звернення жертви кіберінциденту згідно зі ст.ст. 1, 3, 5 Конституції України та іншого чинного законодавства не зобов'язали виконати норми закону щодо реакції державних та відповідних правоохоронних органів хоча б спроби встановлення особи комп'ютерного злочинця, а також розпочати запобігання, протидію та розслідування даного кіберзлочину. Аналіз фактичних документів реагування правоохоронних органів на вчинений кіберінцидент свідчить, що дані державні відомства і установи приховують зловмисні дії комп'ютерних злочинців і тим самим порушують чинне законодавство та надають практично типові шаблонні відписки і цими протиправними діями покривають комп'ютерних злочинців. Цікавим є і те, що законодавчо визначені правоохоронні органи, які зобов'язані реагувати на кіберінциденти, фактично заяви про кіберінцидент не реєструють в Єдиному реєстрі досудового розслідування. Водночас, слід зазначити, що якщо в поодиноких випадках ці

правоохоронні органи і реєструють такі заяви про кіберінцидент, то їх слідчі не здійснюють встановлення особи комп'ютерного злочинця і, відповідно, не розслідують дані комп'ютерні злочини, а кримінальні провадження необгрунтовано та безпідставно, а значить протизакронно закривають. Це свідчить про реальні юридичні доказові факти вчинення кримінальних правопорушень посадовими особами цих правоохоронних органів.

З цією метою здійснений нами системний аналіз матеріалів судових засідань даного комп'ютерного злочину свідчить, що жодна правнича служба кібербезпеки шести держав світу і України, а також їх безпекових телекомунікаційних установ (операторів космічних телекомунікацій, операторів магістральних телекомунікаційних мереж супутникового зв'язку, операторів наземних телекомунікаційних служб) фактично не зреагували на даний кіберінцидент і не застосували засоби щодо встановлення особи комп'ютерного злочинця і, відповідно, не сприяли запобіганню та протидії вчинення даного комп'ютерного злочину. Це фактично свідчить про те, що державні і відповідні безпекові правоохоронні органи семи країн світу не зацікавилися злочинною дією електронних зловмисників, оскільки не виявили комп'ютерних злочинців, не запобігли, не задокументували і не здійснили відповідні правничі, технологічні, безпекові заходи щодо запобігання та протидії цим кіберінцидентам (космічним і наземним кібератакам, кіберзагрозам, кіберзлочинам) здійсненим в електронному кіберпросторі [59, с. 283-286].

Важливо акцентувати увагу ще і на тому, що даний трафік кібератак здійснювався комп'ютерними злочинцями понад 24 години підряд (в період з 14.10.2018 р. по 18.10.2018 р.).

Відомо, що зовсім недавно, а саме вніч з 13 на 14 січня 2022 р. було здійснено неймовірно масштабну та блискавичну злочинну крекерську кібератаку на надзвичайноважливі урядові сайти України. Причому, на головних сторінках атакованих сайтів було розміщено повідомлення провокаційного характеру [124].

Варто також зауважити, що ця кібератака була здійснена комп'ютерними злочинцями на сімдесят державних сайтів України. Дана кібератака була здійснена саме після вдалого запуску українського супутника «Січ 2-30» і виведеного на орбіту Землі [74, с. 12-13]. Відомо, що фактично до переліку атакованих сайтів потрапили установи кричичної інфраструктури України, а саме: Кабінету Міністрів України, Міністерства закордонних справ, загальноукраїнського порталу Дії, Державної казначейської служби, Державної служби України з надзвичайних ситуацій, Міністерства освіти і науки, Міністерства енергетики та інші.

Це свідчить про те, що такі кібератаки здійснені комп'ютерними злочинцями з наземних та космічних сфер фактично порушують конституційні права людини, суспільства, держави, а також є особливо небезпечними для гарантування миру, безпеки людства та міжнародного правопорядку.

Вважаємо, що сьогодні українським державним та правоохоронним органам необхідно консолідувати свої зусилля з метою встановлення осіб, які вчиняють такі зловмисні дії, а також здійснити заходи по запобіганню, протидії, розслідуванню вчинених наземних та космічних кіберзлочинів. З цією метою необхідно: по-перше, забезпечити обов'язкову та миттєву реєстрацію кіберзлочинів в Єдиному реєстрі досудових розслідувань згідно положень чинного законодавства; по-друге, налагодити тісну співпрацю з відповідними безпековими міжнародними органами світу (ООН, ОБСЄ, ЮНЕСКО, ФАТФ, МПА, Інтерпол, Європол) і державними безпековими установами (Великої Британії- Мі5, Мі-6; США – АНБ, ЦРУ, ФБР; України – РНБО та інших країн), а також з освітніми та науковими установами (університетами, інститутами, академіями, коледжами, безпековими науково-дослідними інститутами). Для цього необхідно розробити і реалізувати не тільки в освіті, науці, але і на практиці стратегічні кроки щодо прийняття відповідних безпекових управлінських стратегічних та тактичних рішень по встановленню осіб, які вчиняють комп'ютерні злочини; по-третє, забезпечити якісне та блискавичне запобігання, протидію, розслідування не тільки

надзвичайно небезпечних кіберзлочинів, але і всіх наявних кіберзлочинів без винятку [61; 62; 63].

Крім вітчизняних пріоритетних напрямів удосконалення діяльності по встановленню осіб, які вчиняють зловмисні дії в кіберпросторі, а також здійсненню заходів по запобіганню комп'ютерної злочинності в наземному і космічному просторі заслуговують на увагу питання, які потребують реформування міжнародних безпекових установ і організацій, що забезпечують кібербезпеку в кіберсфері і кіберпросторі загалом.

Відомо, що починаючи з 1991 року при Генеральному секретаріаті Інтерполу діє робоча група з проблем запобігання комп'ютерної злочинності, яка вивчає цей вид злочинів у різних країнах світу, розробляє стратегічні і тактичні кримінологічні рекомендації, допомагає в стандартизації національних законодавств, напрацьовує методологічний досвід запобігання і протидії комп'ютерним злочинам [159, с. 216]. За час свого існування вказана робоча група створила сучасну класифікацію комп'ютерних злочинів, розробила уніфіковану форму повідомлення (запиту) про такі комп'ютерні злочини, працює над створенням нового довідника «Комп'ютери та злочини», намагаючись стандартизувати засоби, методи та процедури запобігання комп'ютерних злочинів в різних країнах світу, щорічно організує навчальні курси по підготовці і перепідготовці національних кадрів фахівців у галузі запобігання кіберзлочинності та кібербезпеки [65, с. 18].

Особлива увага в даному аспекті приділяється саме питанням міжнародного співробітництва з метою швидкого встановлення і затримання комп'ютерних злочинців. У багатьох країнах з метою швидкого затримання комп'ютерних злочинців, а також для запобігання і протидії цьому виду комп'ютерних злочинів створені відповідні спеціалізовані підрозділи. Дані підрозділи займаються виявленням комп'ютерних злочинців, а також здійснюють запобігання, протидію, розслідування комп'ютерних злочинів та збором іншої безпекової інформації з цього питання на національному рівні. Саме такі спеціалізовані національні поліцейські підрозділи утворюють

головне ядро сил протидії міжнародній комп'ютерній злочинності. Такі підрозділи вже створені та діють тривалий час у Сполучених Штатах Америки, Канаді, Великобританії, Німеччині, Швеції, Швейцарії, Бельгії, Японії, Португалії, Австрії, Польщі та багатьох інших країнах світу.

Для того, щоб інформація з інших країн світу швидко та в доступній формі (мова повідомлення, типовий портрет комп'ютерного злочинця, специфічні терміни, коди злочинів тощо) надходила до національних спеціалізованих підрозділів (якщо таких немає, то до інших компетентних органів), а також для оперативного обміну такої інформації між країнами і діють такі кібербезпекові служби під організаційним керівництвом Інтерполу та Європолу. Слід зазначити, що така системна кримінологічна діяльність в Інтерполі та Європолі працює цілодобово. Причому генеральний секретаріат Інтерполу ще в 1994 році рекомендував усім країнам-членам організації створити національний центральний консультативний пункт з проблем запобігання комп'ютерній злочинності (national central referemce poiпt) та закріпити конкретних співробітників для роботи з інформацією про комп'ютерні злочини. Аналогічні завдання здійснені і Європолом. На даний час в європейських країнах уже створено такі пункти й надіслано інформацію до Генерального секретаріату Інтерполу. Ці пункти створені, як правило, в апаратах національних бюро Інтерполу, чи в спеціалізованих підрозділах, які займаються встановленням комп'ютерних злочинців, а також запобіганням комп'ютерної злочинності, або протидією і розслідуванням економічних злочинів.

На базі НЦБ Інтерполу в Україні такий пункт теж був створений ще 26 років тому (17 вересня 1996 року). Це дало можливість накопичити матеріал про законодавче регулювання та організаційний досвід реальних можливостей затримання комп'ютерних злочинців з метою запобігання комп'ютерної злочинності в різних країнах світу, а також підготувати ряд систематизованих інформаційно-аналітичних оглядів і методичних рекомендацій із вказаних питань, ознайомити співробітників прокуратури,

МВС України з цим новим для нашої країни видом комп'ютерних злочинів. Такі узагальнення дозволили внести конкретні пропозиції з удосконалення чинного кримінального законодавства.

Водночас, викликає занепокоєння той факт, що необхідність всебічного дослідження особи комп'ютерного злочинця з метою запобігання і протидії комп'ютерним злочинам в Україні ще не має достатньої правової, інформаційно-аналітичної, організаційної, освітньої, наукової, кадрової та праксеологічної підтримки. По-перше, не створена дієва нормативно-правова база, оскільки чинне законодавство нашої держави (зокрема, Кримінальний і Кримінальний процесуальний кодекси України та інші Закони України в галузі кібербезпеки) й досі не відповідають рекомендаціям Ради Європи, які були прийняті з питань запобігання і протидії комп'ютерним злочинам. По-друге, не прийняте рішення про створення потужного науково-дослідницького центру з консолідованого системного асиметричного аналізу тенденцій розвитку кіберзагроз (кіберзлочинності, кібертерористичних актів, кібератак тощо) як у космічному, так і наземному кіберпросторі. По-третє, відсутнє держзамовлення на підготовку необхідних фахівців для запобігання, протидії, розслідування електронних злочинів в наземному і космічному кіберпросторі.

На нашу думку, необхідно терміново розробити та прийняти на державному рівні національну програму з кібербезпеки України з метою протидії наземним і космічним кіберзагрозам і кібератакам, що забезпечить належний рівень правового забезпечення організації питань щодо діагностики, аналізу, прогнозування, попередження, запобігання, викриття та розслідування такого небезпечного явища в суспільстві, якими є сьогодні комп'ютерні злочини.

Очевидно, що сучасний етап розвитку електронної цивілізації потребує також розробки відповідних нормативно-правових актів (конвенцій, угод тощо) для запобігання і протидії міжнародному кібертероризму, який є одним із надважливих пріоритетних напрямів запобігання сучасному глобальному міжнародному кібертероризму.

Відомо, що у сучасних умовах стрімкий розвиток інформаційних технологій у світі та необхідність обміну інформацією через використання глобальної інформаційної мережі інтернет реально створюють сприятливий клімат як для наземних, так і космічних електронних злочинних посягань як традиційного, так і терористичного характеру: незаконного доступу до державних та приватних комп'ютерних баз даних; баз даних фінансово-кредитних установ (внутрішніх банківських комп'ютерних систем); телефонних комунікацій; комп'ютерних систем підприємств; наукових установ і навчальних закладів; привласнення коштів з банківських рахунків інших осіб, у тому числі й на території інших держав світу. Нещодавні кібератаки, здійснені на Пентагон, трубопровідні транспортні мережі та інші держустанови критичної інфраструктури США, відключення систем електропостачання в західних регіонах України, блокування діяльності аеропорту у Варшаві тощо уже конкретно свідчать про реально існуючі наземні й космічні електронні терористичні кіберзагрози, кіберризики і кібернебезпеки міжнародного маштабу в кібепросторі. Світова практика свідчить, що кібервійни, кібератаки, кібербулінг, кібертероризм, кіберзлочини на сьогодні вже набули не тільки транскордонного, транснаціонального, трансконтинентального, планетарного, але й космічного характеру [66, с. 14-15].

Це зобов'язує міжнародну спільноту, враховуючи можливі глобальні негативні наслідки для світового правопорядку цього надзвичайно небезпечного соціального явища [70, с. 9-12], постійно аналізувати, моніторити, прогнозувати такі можливі зловмисні наміри та контролювати й мінімізувати посягання на державні та міждержавні правові, політичні, дипломатичні, освітні, наукові, економічні, екологічні, соціально-комунікаційні відносини.

Слід зазначити, що з метою подолання таких надзвичайно небезпечних кіберзагроз в Європі ще в 2001 році був прийнятий базовий правовий документ для запобігання і протидії міжнародному кібертероризму та

кіберзлочинності на території європейських країн. Зокрема, була прийнята Конвенція Ради Європи про кіберзлочинність від 23.11.2001 р. та додаткові протоколи до неї від 28.01.2003 р. та від 17.11.2021 р. Очевидно, що сьогодні ця європейська конвенція є потужним фундаментом і дієвим правничим документом для використання, подальшої розробки й удосконалення відповідного чинного законодавства з кібербезпеки в європейських країнах. Водночас вважаємо, що на наш погляд, ряд положень даної конвенції сьогодні вже теж потребують удосконалення, наповнення її новими ідеями, інноваціями, обумовленими сучасними тенденціями цивілізаційного розвитку електронної комунікації в світі.

Сьогодні Н.М. Ахтирська вчасно звертає увагу на те, що усвідомлюючи глибокі зміни, спричинені переходом на цифрові технології, конвергенцію і глобалізацію комп'ютерних мереж, держави-члени Ради Європи визнали необхідність спільної кримінальної політики, спрямованої на захист суспільства від кіберзлочинності, шляхом створення відповідного законодавства і налагодження міжнародного співробітництва. Таке рішення було зумовлене необхідністю зупинення дій, спрямованих проти конфіденційності, цілісності і доступності комп'ютерних систем, мереж і комп'ютерних даних, а також зловживання такими системами, мережами і даними, шляхом встановлення кримінальної відповідальності за таку поведінку, надання повноважень, достатніх для ефективної боротьби з такими кримінальними правопорушеннями шляхом сприяння їхньому виявленню, розслідуванню, як на національному, так і на міжнародному рівнях, і укладення домовленостей щодо швидкого і надійного міжнародного співробітництва [34, с. 188].

Н.М. Ахтирська була безпосереднім учасником конференції Ради Європи, присвяченій 20-річчю Будапештської конвенції, яка відбулася в листопаді 2021 р., де було зазначено про необхідність забезпечення виконання конвенційних положень шляхом створення загальної системи моніторингу, розробки нових юридичних обов'язкових стандартів, що зумовлені новими

викликами. 17.11.2021 р. Комітет міністрів Ради Європи прийняв Другий додатковий протокол до Конвенції про кіберзлочинність, який скерований на розширення міжнародного співробітництва та розкриття електронних доказів. Протокол скерований на вирішення низки питань, зокрема: 1) як домогтися більш ефективного використання облікового запису або інтернет-протоколу, який використовується для вчинення злочину; 2) як та на яких умовах здійснювати співробітництво з постачальником послуг, який перебуває на території іншої держави, для одержання електронних доказів; 3) як без зволікань домогтися розкриття даних, включаючи дані про зміст, від іншої держави в надзвичайних ситуаціях; 4) як зробити міжнародне співробітництво більш ефективним та чи можна надати правоохоронним органам додаткові інструменти для збору електронних доказів [34, с. 190].

Відомо, що нині низка провідних країн світу для забезпечення миру, безпеки людства та міжнародної кібербезпеки цивілізації створили власні безпекові космічні відомства, установи та організації. Так, наприклад, у Сполучених Штатах Америки в 2019 році створено космічні сили. В Японії нещодавно оголошено про формування космічних військ. А в Україні вже довгий час діє Центр космічного спостереження, а також здійснюються інші творчі пошуки для забезпечення кібербезпеки нашої країни [58, с. 18-19].

Вважаємо, що важливим пріоритетом дослідження даних про особу комп’ютерного злочинця з метою запобігання комп’ютерної злочинності – це постійний консолідований асиметричний аналіз, моніторинг вітчизняної і міжнародної судової практики про реальні факти вчинення комп’ютерних злочинів і вивчення характерних ознак, рис, манер поведінки осіб, які вчинили дані комп'ютерні злочини.

Це обумовлено тим, що міжнародна судова практика свідчить про факти вчинення комп’ютерними злочинцями не тільки наземних комп’ютерних злочинів, але і космічних.

Директор Управління з питань космічного простору Сімонетта Ді Піппо вважає, що сьогодні неможливо заперечувати те значення, яке космос має для

нашого повсякденного життя. В цьому зв'язку важливо зберегти можливість стабільного використання космосу в довгостроковій перспективі і при цьому забезпечити його більш широку доступність. Адже думаючи про майбутнє ми повинні думати про космос [99].

Підтвердженням цієї ідеї є те, що в 2020 році в космос було запущено рекордну кількість об'єктів і супутників. Це еквівалентно 10 відсоткам всіх зареєстрованих космічних об'єктів за всю історію освоєння космосу. Водночас, такий стрімкий розвиток подій створює не тільки можливості для побудови кращого майбутнього, але і проблеми, які пов'язані з безпекою, надійністю і екологічністю освоєння космічного простору [99].

Здійснюваний нами аналіз даних міжнародної судової практики щодо зловмисних дій комп'ютерних злочинців, свідчить про реальні факти вчинення космічних кіберзлочинів в світі. Зокрема, нещодавно стало відомо, що NASA розслідує перший у світі комп'ютерний злочин, вчинений комп'ютерними зловмисниками у космосі (космічному кіберпросторі). Підґрунтям цього розслідування стало те, що потерпіла Н. заявила про космічний комп'ютерний злочин, вчинений з космічної орбіти Землі американською астронавткою К., яка перебувала в той час на космічній станції [72, с. 2-4]. Про цей реальний юридичний факт правового спору двох суб'єктів конфліктної ситуації, який, ймовірно, став одним з перших комп'ютерних злочинів, вчинених у космосі, нещодавно повідомило авторитетне видання The New York Times [18].

Разом із тим, сьогодні органам правопорядку і громадськості вже відомі реальні випадки про вчинення комп'ютерними злочинцями різних криміногенних зловмисних дій, які відбувалися довгий час в космічному просторі. Так, наприклад, відомо, що десять років тому (ще у 2011-му) Національне управління з аеронавтики і дослідження космічного простору (англ. National Aeronautics and Space Administration - NASA) - агенство уряду США, засноване 1958 року для здійснення досліджень у галузі аеронавтики й космічних польотів та підпорядковується безпосередньо Президенту США), організувало спецоперацію, спрямовану на вивчення неправомірних

кримінологічних дій вдови американського космічного інженера, яка хотіла, порушуючи норми міжнародного космічного права, продати місячний камінь. А в 2013 році російський супутник зазнав аварії, оскільки був пошкоджений після його зіткнення з уламками китайського супутника, зруйнованого в ході випробування космічної ракети ще в 2007-му. У 2017 році австрійський бізнесмен подав до суду на компанію з космічного туризму, намагаючись повернути свій депозит за заплановану ним поїздку на космічному кораблі, яка з різних об'єктивних і суб'єктивних причин була заблокована й не просувалася, тобто по факту не була реалізована [69, с. 432].

Аналізуючи різні ситуації, які відбуваються сьогодні в космічному кіберпросторі, директор Центру глобального космічного права Клівлендського державного університету (США) Марк Сундал на основі проведених досліджень зловмисних злочинних дій, вчинених у космосі комп'ютерними злочинцями, справедливо зазначає таке: «Те, що він знаходиться в космосі, не означає, що він не підкоряється закону» [101, с.197]. За його словами, однією з потенційних фактичних проблем, які можуть виникнути у зв'язку з будь-яким космічним кримінальним злочином або космічним судовим процесом з приводу використання комп'ютерними злочинцями як наземних, так і позаземних банківських електронних комунікацій, є відкриття закритих даних і, вірогідно, що співробітники НАСА будуть побоюватися, наприклад, відкрити високочутливі режимні втаємничені комп'ютерні мережі, автоматизовані системи й засекречені бази даних для перевірки звичайними, не допущеними до секретності юристами (слідчими, прокурорами, суддями, адвокатами та іншими правозахисниками). Але такі юридичні питання в майбутньому, на переконання М. Сундала, будуть звичайно, неминучими й потребуватимуть обов'язкових прозорих механізмів реалізації правовідносин, оскільки вже незабаром люди проводитимуть більше часу у космосі [184]. Такі дослідницькі космічні проекти здійснюються сьогодні і в Україні.

Іншою реальною небезпекою вчинення зловмисних електронних дій комп'ютерними злочинцями у космічному електронному кіберпросторі, яка

вже сьогодні реально присутня на горизонті – це можливість комп'ютерних злочинців здійснювати електронні інформаційні кібератаки з космосу на наземні фізичні об'єкти. Автори звіту «The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation» [26] справедливо попереджають, що сучасні ноозасоби і грід-технології електронного інтелекту дозволяють уже зараз безперешкодно проникати як у системи космічних та наземних установ і організацій, зокрема, космічних станцій, безпілотних автомобілів, безпілотних літаків, поїздів, кораблів тощо. А це дозволяє реально управляти ними по спеціальному коду з метою вчинення зловмисних дій комп'ютерними злочинцями, що сприяє реальній можливості здійснювати не тільки розкрадання майна, ресурсів, коштів, але й також можливості вчинення від наземних, так і до космічних кіберзагроз у вигляді епідемій, аварій та катастроф, а можливо і різного роду космічних військових кібероперацій.

Ще одним небезпечним прикладом вчинення космічних чи наземних електронних зловмисних дій комп'ютерних злочинців може бути використання «армій дронів», які за допомогою новітніх грід-технологій розпізнавання обличчя, голосу, запаху, особливих рис та манер поведінки тощо можуть вбивати людей, наголошується в цьому дослідженні. Таким чином, уже сьогодні існує реальна загроза створення в дослідницьких лабораторіях й використання як на Землі, так і в космічному кіберпросторі (близькому і далекому) електронних роботів-убивць.

У даному узагальненому науковому звіті «The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation» також описується можливий сценарій, в якому електронний робот-прибиральник офісів на ім'я SweepBot, оснащений спеціальною вибуховою бомбою, проникає в міністерство фінансів та «губиться» серед інших автоматизованих керованих машин такого ж виробника. Причому даний електронний робот-зловмисник спочатку поводиться в новому середовищі достатньо акуратно, ввічливо і природньо – збирає сміття, підмітає коридори, доглядає за вікнами, аж поки

автоматизована комп'ютерна програма для розпізнавання обличчя не зафіксує індивідуальні риси, ознаки певної особи, визначеної комп'ютерними зловмисниками, і не запустить код відповідного пускового електронного механізму вибухового пристрою. Очевидно, що інколи прихований вибуховий електронний пристрій може вбивати не тільки розпізнану зловмисником-роботом певну особу, але й спричиняти поранення працівників, які можуть випадково знаходитися поруч або бути неподалік.

Таким чином, швидкий розвиток індустрії електронного інтелекту засвідчує те, що сьогодні це уже не просто науково-фантастична літературна історія-передбачення, а уже дійсно створена об'єктивна реальність, тобто існує конкретна технологічна кібернебезпека і кіберзагроза подальшого цивілізаційного розвитку в космічному кіберпросторі. Очевидно, що ці обставини зобов'язують відповідні світові та регіональні аналітичні установи з наземної та космічної електронної кібербезпеки уже сьогодні приступити до розробки і впровадження кібербезпекової стратегії, тактики і мистецтва запобігання та протидії таким електронним злочинам [101, с.199].

Нещодавно з метою реалізації стратегічних завдань запобігання і протидії космічній кіберзлочинності та формування надійної космічної кібербезпеки в Об'єднаних Арабських Еміратах (ОАЕ) влада Дубая оголосила про створення першого у світі космічного суду для врегулювання майбутніх цивільних правовідносин та запобіганню зловмисних дій комп'ютерних правопорушників в космічному кіберпросторі на орбіті Землі.

Дійсно, на сайті Міжнародного фінансового центру Дубая (DIFC) зазначається, що у 2021 році суди Міжнародного фінансового центру Дубая і Фонд майбутнього Дубая (DFF) приступили до реалізації нової правничої ініціативи «Суди майбутнього», створюючи та впроваджуючи перший у світі космічний суд.

У повідомленні вказується, що новий арбітражний космічний суд ОАЕ буде спеціалізуватися на космічній діяльності в основному приватних компаній, на розбіжностях з приводу купівлі супутників або неправомірного

зіткнення космічних пристроїв (космічних апаратів, супутників, міжнародних космічних станцій) на навколоземній орбіті. Таке рішення продиктовано прогресом в космічній галузі, який був досягнутий Об'єднаними Арабськими Еміратами в останні роки. Це обумовлено також і тим, що інші країни, такі як США, Китай, розробили новітні проривні технології в космічній галузі [152, с.12].

Слід також зазначити, що космічна галузь у світовому правничому контексті досліджується і регулюється міжнародним космічним правом. На даний час вся діяльність в космічному просторі регулюється міжнародними конвенціями та резолюціями, в тому числі Договором ООН щодо мирного використання космосу, який набрав чинності ще у 1967 році [75, с. 157]. Зокрема відомо, що крім того деякі держави також підписали між собою двосторонні або багатосторонні угоди для забезпечення правового регулювання своєї космічної діяльності. Це обумовлено також і тим, що донедавна космічна сфера близького і далекого космосу була фактично майже виключно пререгативою провідних країн світу і потужних державних організацій тільки деяких країн, а зараз же для засвоєння космічного простору залучаються уже і приватні компанії. Зокрема, в Україні теж ведуться творчі пошуки в даному напряму [75, с. 158]. Аналіз наземних і космічних кіберзагроз, які вчиняють комп'ютерні злочинці свідчить про нові факти вчинення комп'ютерних злочинів в наземному і космічному кіберпросторі.

Юридичні факти свідчать про вчинення зловмисних дій комп'ютерними злочинцями в космічному просторі вже з території України [185, с. 14-31]. Так на основі аналізу судової практики нашої країни нами встановлений юридичний факт вчинення комп'ютерними злочинцями першого в Україні космічного електронного кіберзлочину, який нещодавно (3 березня 2021 р.) вже розглянутий в українському суді.

Вважаємо, що небезпечність вчинення комп'ютерними злочинцями такого роду електронних наземних і космічних комп'ютерних злочинів пов'язано з тим, що такі дії комп'ютерних зловмисників уже сьогодні несуть

загрозу цивілізації, оскільки можуть бути здійснені як проти миру, безпеки людства, так і реально впливати на міжнародний правопорядок та інші охоронювані законом про кримінальну відповідальність об’єкти.

Важливо наголосити ще і на тому, що даний перший космічний кіберзлочин був вчинений комп’ютерними злочинцями не тільки на наземній території України, але і на наземних територіях та космічних просторах загалом семи держав світу (причому на різних континентах) з допомогою використання потужних інструментів міжнародних систем супутникового зв’язку (європейської системи мобільного супутникового зв’язку EMSAT, глобальної ORATION TECHNOLOGIES, а також супутникової технології на базі міжнародної супутникової мережі GLOBALSTAR) та наземних станцій електрозв’язку ряду країн світу в жовтні 2018 року. Цікаво, що даний трафік кібератак комп’ютерні злочинці здійснювали посекундно понад 24 години підряд [185, с. 14-31].

Причому цікавим є те, що ці наземні і космічні електронні кібератаки комп’ютерні злочинці здійснювали з інтервалом інколи до секунди, а в більшості випадків тривалістю від однієї, двох, трьох, чотирьох та більше секунд та загальною тривалістю електронного кібернападу більше 24 годин (в період з 14 жовтня 2018 р. по 18 жовтня 2018 р.) на території як Буркіна-Фасо, Сьєрра-Леоне, Мальдів, Сполучених Штатів Америки, Російської Федерації, Куби та України.

Як було встановлено в судовому засіданні, жодна служба кібербезпеки не зацікавилася злочинною дією електронних зловмисників, оскільки не виявили, не запобігли, не задокументували і не здійснили відповідних технологічних профілактичних безпекових заходів щодо запобігання та протидії цим космічним кібератакам, кіберзагрозам, кіберзлочинам, здійсненим в наземному і космічному кіберпросторі в період з 14 по 18 жовтня 2018 р.

Підводячи підсумки викладеного вище, слід зазначити, що, очевидно, сьогодні сформулювати конкретний дієвий прогноз подальшого чіткого

розвитку реальних сценаріїв використання комп'ютерними злочинцями технологічних можливостей електронного інтелекту і електронного наземного та космічного кіберпростору в зловмисних цілях як теоретично, так і практично достатньо складно.

Водночас, вважаємо, що важливо уже сьогодні відповідним безпековим міжнародним органам світу (ООН, ОБСЄ, ЮНЕСКО, ФАТФ, МПА, Інтерполу, Європолу) та окремих державних установ (Великої Британії – Мі-5, Мі-6; Канади – кінної поліції; США – АНБ, ЦРУ, ФБР; України – РНБО та інших країн), освітнім та науковим установам приступити до розробки та реалізації в освіті, науці і на практиці наступних стратегічних кроків і прийняття відповідних безпекових управлінських тактичних рішень, а саме:

– розробити міждержавні стандарти з метою формування засобів і методів запобігання комп'ютерній злочинності з метою забезпечення кібербезпеки наземного та космічного кіберпростору для гарантування невідчужуваних та непорушних конституційних прав та свобод людини і громадянина;

– розробити та прийняти чітку і надійну міждержавну кібербезпекову правову базу (Конвенцію ООН) реальних можливостей використання наземного і космічного кіберпростору (близького і далекого) та електронного інтелекту в освітній, науковій і праксеологічній діяльності з метою запобігання і протидії можливим електронним кіберзагрозам, кібератакам, кіберзлочинам, кібервикликам і кібернебезпекам;

– акцентувати увагу розробників новітніх кібербезпекових електронних ноозасобів, креативних методів і грід-технологій електронного інтелекту на те, що необхідно технологічно запобігти та протидіяти можливим кіберзагрозам неправомірного використання космічного простору і електронного інтелекту в різних сферах наземної та космічної життєдіяльності [201, с. 236-240];

– відповідним міжнародним безпековим організаціям, відомствам і установам світу розробити впорядковану правову, організаційну і технологічну систему запобігання і протидії шкідливому використанню

космічного простору і електронного інтелекту як на національному, регіональному, так і на міждержавному (світовому) рівнях (транскордонному, транснаціональному, трансконтинентальному, планетарному, космічному (близький космос, далекий космос) [101, с. 195-200];

– створити міжнародне об'єднання потужних провідних електронних держав світу для формування, розробки і впровадження єдиних запобіжних безпекових стандартів надання електронних довірчих послуг на всій земній кулі [120, с. 29-71];

– зебезпечити впровадження в космічну діяльність новітніх розробок в галузі дослідження особи комп'ютерного злочинця з метою запобігання комп'ютерній злочинності та кібербезпеці здійснених науковцями Національного авіаційного університету спільно з Інститутом електронної фізики НАН України [75, с. 156-162; 54], Національним космічним агенством України та правничою компанією «АЮР-КОНСАЛТИНГ» [160].

3.2. Перспективи дослідження запобігання вчиненню комп'ютерних злочинів з використанням електронного інтелекту

В сучасних умовах стрімкий розвиток ноозасобів і ноотехнологій, грід і блокчейн інформаційних технологій в світі та потреба необхідності цілодобового обміну інформацією з допомогою використання глобальної інформаційної мережі інтернет створюють сприятливий клімат для здійснення злочинних посягань не тільки зі сторони фізичних осіб – комп'ютерних злочинців, але і з допомогою використання сучасних можливостей електронного інтелекту організаціями в злочинних цілях.

Справедливим сьогодні є твердження Д.Л. Виговського, у системі протидії злочинності як сукупності заходів, спрямованих на максимально можливе зниження рівня злочинності (в ідеалі – її подолання), важливе місце має попереднє діагностування найбільш важливих напрямків діяльності. Іншими словами, перш ніж здійснювати заходи, спрямовані на усунення

детермінант конкретних видів злочинності і репресивного впливу на осіб, що вчиняють кримінальні правопорушення в даній сфері, варто визначитись: які саме види злочинності опиняються в зоні особливої уваги суб'єктів протидії злочинності? Закони формальної логіки дозволяють визначитись з окремими видами злочинності, як більш суспільно-небезпечними. Очевидним видається, що більш суспільно-небезпечним може бути той вид злочинності, який являє собою сукупність кримінальних правопорушень, з більш високим рівнем суспільної небезпечності. Відтак, окремим мірилом (втім - не єдиним!) рівня суспільної небезпечності окремого виду злочинності є підвищений рівень суспільної небезпечності окремих кримінальних правопорушень, що в сукупності й складають вказаний вид злочинності [83, с. 48].

Вважаємо, що українські реалії потребують інноваційного розвитку [42, с. 14-15], а питання глобальної цифрової комунікації в контексті сталого розвитку світу потребують спеціального наукового дослідження, зокрема, формування концептуальних засад правового статусу взаємовідносин людини і робота [45, с. 9; 200].

Дійсно слово «робот» використовується уже сто років та вважається звичайний терміном. Водночас, слід зауважити, що сьогодні ведуться активні широкомасштабні дослідження з метою створення та розвитку роботів з електронним інтелектом в Великій Британії, КНР, США, Японії та інших провідних країнах світу.

Новий інноваційно-технологічний етап електронного розвитку спричинив масове поширення та використання новітніх автоматизованих комп'ютерних телекомунікаційних технологій в усіх сферах людського існування. Виходячи з цих тенденцій по особливому гостро постає питання використання електронного інтелекту в правотворчій, правозахисній та судовій діяльності державних органів влади та міжнародних, міждержавних правових структурах, інституціях, різного роду відомствах, установах, організаціях, та, зокрема, в кримінальному праві більшості держав світу. Враховуючи тенденції розвитку правової науки щодо надання електронному

інтелекту правового статусу «особи», або «електронної особи», виникає небезпека постановки даної «особи» в один суспільний ряд з людиною. Тому сьогодні не випадково свідоме людство насторожує можливе поетапне надання прав і свобод електронному інтелекту та можливе зрівняння даних прав в майбутньому з правами людини, що стає значною небезпекою, загрозою для людства як з позицій правового, так і суспільно-етичного характеру. В будь-якому варіанті правового розвитку суспільства безпосередньо «електронна особа», її творці, її власники, її користувачі мають і будуть в повній мірі нести кримінальну відповідальність за вчинення комп'ютерних злочинів з використанням електронного інтелекту або ним самим як «особою». Вважаємо, що сьогодні основоположною безпековою задачею правотворців та правозахисників є недопущення порушення конституційних прав і свобод людини, суспільства та держави з боку «електронної особи» створеної на базі електронного інтелекту. На ранніх етапах розвитку правової бази регулюючої даний тип правовідносин між людиною та роботом або програмою з електронним інтелектом необхідно обов'язково передбачити чіткі законодавчі «правові процедури», «правові безпекові механізми», «правові запобіжники» для унеможливлення використання електронного інтелекту для здійснення злочинних цілей проти людини, суспільства та держав світу [157, с. 40-54].

Так в чому все ж таки полягає реальна небезпека використання електронного інтелекту для розвитку електронної цивілізації? Фахівці стверджують, що електронний інтелект, потрапивши в руки зловмисників, може фактично знизити, а інколи можливо і знищити реально створені захисні безпекові перешкоди, перепони для проведення руйнівних хакерських та крекерських кібератак.

Оскільки Україна має потужний інтелектуальний потенціал вчених в галузі правознавства, математики, кібернетики, інформатики, біоніки і нейробіоніки, тому потрібно створювати унікальні автоматизовані комп'ютерні системи з елементами електронного (штучного) інтелекту. Це

дозволить впроваджувати створені системи на базі електронного інтелекту для пізнання різних проривних напрямів, починаючи від близького і далекого космосу і до вивчення морських глибин.

Очевидно, що нове бачення використання можливостей електронного інтелекту в освіті, науці і практиці дозволить активно використовувати ці системи і технології як для вивчення особи комп'ютерного злочинця, зокрема, так і для запобігання та протидії комп'ютерній злочинності взагалі.

Такий підхід дозволить зберегти як нашу країну, так і цивілізацію від кібератак і кіберзлочинців. Це обумовлено тим, що сьогодні людство і цивілізація загалом уже фактично залежать від протиправних дій однієї особи або від групи осіб, які часом не прогнозовані у своїх злочинних вчинках.

Сьогодні Україна прагне стати повноправним членом Європейського Союзу, тому в швидкому майбутньому наша країна буде долучена до європейської суперкомп'ютерної інфраструктури світового рівня.

Відомо, що Рада міністрів Європейського Союзу у вересні 2018 року офіційно підтримала плани Комісії щодо спільного інвестування з державами-членами у створення європейської суперкомп'ютерної інфраструктури світового рівня, та, відповідно, Рада з питань конкурентоспроможності прийняла Регламент про створення Європейського спільного підприємства з високопродуктивних обчислень (EuroHPC) – нової юридичної та фінансової структури, яка об'єднає ресурси з 25 європейських країн, побудує суперкомп'ютерну інфраструктуру та інфраструктуру даних, а також підтримуватиме дослідження та інновації в даній галузі за участю вчених, підприємств і промисловості. Бюджет Європейського спільного підприємства складатиме 1 мільярд євро, половина з бюджету ЄС, а половина – профінансують європейські країни-члени. Додаткові ресурси на суму понад 400 мільйонів євро надійдуть від приватних партнерів [10].

У багатьох провідних країнах світу також активно ведуться дослідження з метою створення квантового комп'ютера нового покоління. Це обумовлено тим, що керівники багатьох країн світу усвідомлюють і визнають той

важливий фактор про те, що перевага, пріоритет буде на боці тієї країни, де створять новітній інноваційний квантовий продукт – електронний інтелект.

Так, у лютому 2020 року уряд Великої Британії заявив, що інвестує (у співпраці з Microsoft) у проект по створенню суперкомп'ютера для прогнозування метеорологічною службою погоди у Великобританії 1,2 мільярда фунтів стерлінгів, який використовуватиме служби хмарних обчислень Microsoft Azure та інтегруватиме суперкомп'ютери Hewlett Packard Enterprise (HPE) Cray. Даний суперкомп'ютер матиме понад 1,5 мільйона процесорних ядер і понад 60 петафлопсів – або 60 квадрильйонів (60 000 000 000 000 000) обчислень за секунду [7]. Підтвердженням успішного фінансування даного проекту є інформація на сайті Уряду Великої Британії [2].

В жовтні 2021 року стало відомо, що у КНР науковці із Національної лабораторії фізичних наук Хефей Китайського університету науки і технологій, яку очолює Цзянь-Вей Пань, побудували два перші у світі програмовані квантові комп'ютери Zuchongzhi 2.1 та Jiuzhang 2 (фотонний), які в 10 млн разів потужніші за будь-який суперкомп'ютер. Квантові комп'ютери виконують завдання, неможливі для суперкомп'ютерів, лише за одну годину [191].

Також відомо, що Лабораторія фізичних наук (LPS) Агентства національної безпеки США в квітні 2021 року запустила LPS Qubit Collaboratory (LQC), дослідницький центр квантової інформаційної науки на підтримку Національної квантової ініціативи США [19].

Відомо, що в серпні 2022 року дослідницькій групі з Японії під керівництвом аспіранта Єлай Чу, доцента Сільвена де Леселека та професора Кенджі Оморі з Інституту молекулярних наук Національного інституту природничих наук вдалося створити найшвидший у світі двокубітний затвор, фундаментальна операція, важлива для квантових обчислень, яка виконується лише за 6,5 наносекунд (нано = одна мільярдна секунди). Цей надшвидкий квантовий комп'ютер, який використовує надшвидкісні лазери для

маніпулювання холодними атомами, захопленими оптичним пінцетом, очікується, що це абсолютно нове апаратне забезпечення квантового комп’ютера, яке долає обмеження типів надпровідних і захоплених іонів, які зараз розробляються [4].

Відомо, що американський концерн IBM розмістив у Німеччині найпотужніший комерційний квантовий комп'ютер в Європі. Процедура запуску системи IBM Quantum System One відбулася в дата-центрі концерну в Енінгені (Ehningen) 15 червня 2021 р. У церемонії взяли участь генеральний директор IBM Арвінд Крішна, канцлерка Німеччини Анґела Меркель (Angela Merkel), а також представники Товариства імені Фраунгофера - найбільшого європейського об'єднання інститутів прикладних досліджень. Це перший такий комерційний квантовий суперкомп'ютер, представлений за межами США з процесором в 27 кубітів [192].

Слід також зазначити, що над дослідженням розвитку інноваційних електронних технологій в Україні, зокрема програм електронного інтелекту, з метою використання їх в кримінальному праві для аналізу, прогнозування та упередження злочинності, а також запобіганням вчиненню комп’ютерних злочинів з використанням електронного інтелекту та безпосередньо самостійно електронним інтелектом (як «електронною особою») проти людини, суспільства, держави тривалий час працюють такі науковці, як О.В. Плахотнік, О.Е. Радутний та інші [169; 176].

Аналіз наукової літератури, яка присвячена використанню електронного інтелекту свідчить, що сьогодні особливої уваги потребують дослідження практики використання електронного (штучного) інтелекту для реалізації освітніх, наукових, праксеологічних завдань, в тому числі, і в галузі юриспруденції (судах, прокуратурі, правоохоронних органах тощо) в провідних державах світу та, зокрема, застосування новітніх автоматизованих комп’ютерних технологій як в правотворчій, так і правозахисній діяльності, а також в новітньому електронному судочинстві. На разі необхідно провести аналіз перспектив застосування електронного інтелекту у цивільному,

адміністративному, господарському, кримінальному провадженні України (наприклад, цивільне електронне провадження, адміністративне електронне провадження, господарське електронне провадження, кримінальне електронне провадження), а також доцільно здійснити розгляд реальної можливості і правових наслідків вчинення кримінального правопорушення самим електронним інтелектом як «електронною особою» в майбутньому [16].

Якщо ж користуватися визначенням, що інтелект людини – це система алгоритмів, створених її свідомістю, то ця система свідомістю і контролюється. Очевидно, що якщо ж ми нехтуємо таким засадничим принципом, то створюватимемо штучний інтелект, який може вийти з під контролю людини. Дійсно це можливо за якихось особливих технічних проблем, зокрема, виходу з ладу конденсатора чи транзистора, коли штучна система діятиме вже зовсім інакше, ніж від неї очікують. У такому разі неконтрольовану штучну систему повинен хтось зупинити [117].

Відповідно до основоположного принципу вираженого та закріпленого у ст. 3 Конституції України людина, її життя і здоров'я, честь і гідність, недоторканість і безпека визнаються в Україні найвищою соціальною цінністю. Права і свободи людини та їх гарантії визначають зміст і спрямованість діяльності держави. Держава відповідає перед людиною за свою діяльність. Утвердження і забезпечення прав і свобод людини є головним обов'язком держави [134]. Ст. 1 Загальної декларації прав людини передбачає, що усі люди народжуються вільними і рівними у своїй гідності та правах. Вони наділені розумом і совістю і повинні діяти у відношенні один до одного в дусі братерства [104]. Конвенція про захист прав людини і основоположних свобод свідчить про те, що людство, нації, держави світу виражають свою суверенну волю і високо цінують саме життя людини, її права і свободи [102]. Тобто використання новітніх технологій не повинно порушувати усього спектру прав людей і прав громадян різних країн світу.

В XXI столітті очевидним є той факт, що новітні ідеї, інновації, знання, наукові розробки швидко і потужно увірвалися в наше життя і стали новою

рушійною силою для розбудови інноваційного цивілізаційного розвитку світу в епоху «Індустрії» 4.0», «Четвертої промислової революції» [208], «Суспільства знань» [186], «Індустрії інтелекту», «Сонячної індустрії знань», «Глобальної інноваційної сонячної комунікації» [90] та «Конвергенції сонячного суспільства знань» [53].

Дослідженнями в напрямку створення електронного інтелекту та різноманітними на перший погляд фантастичними та неймовірними можливостями його застосування, вчені активно займаються даним феноменом, починаючи ще з 50-х років минулого XX століття фактично з появою у світі перших комп'ютерів.

В зв'язку з цим, О.О. Подгаєцький зазначає, що історія створення електронного інтелекту бере свій початок ще у 1950 році, коли британський учений Алан Тюрінг вперше опублікував статтю під назвою «Чи може машина мислити?» [28], в якій описує так званий «Тест Тюрінга» - процедуру, за допомогою якої можна буде визначити момент, коли машина зрівняється в плані розумності з людиною. В Україні такі дослідження розпочаті вже у 1960 році на базі Інституту кібернетики Національної академії наук України в місті Києві (на той час даний інститут очолював академік В.М. Глушков). Для реалізації цієї ідеї в Інституті кібернетики НАН України було створено новий відділ біологічної кібернетики, керівником якого призначено М.М. Амосова. На основі проведених досліджень академік М.М. Амосов вважав, що вивчення питання електронного інтелекту базується на межі наук: фізіології, психології, техніки та філософії, а також присвятив дослідженню даній тематиці ряд наукових праць та велику частину свого життя [170, с. 48-54].

Що стосується історичних віх розвитку досліджень електронного інтелекту, то тут слід звернути увагу на те, що, як відмічає В.В. Риков, визначення штучного (електронного) інтелекту було сформовано Джоном Маккарті ще у 1956 році під час його виступу на науковій конференції в Дартмунському університеті. На його думку, штучний інтелект – це сукупність

наук і методів, здатних опрацьовувати дані для розроблення надскладних комп'ютерних завдань [180].

Аналізуючи дану проблему, О.В. Плахотнік вважає, що штучний (електронний) інтелект визначається як сукупність наукових методів, теорій та технік, мета яких – відтворити машиною когнітивні здібності людини. Також він стверджує, що у світі існує ряд юридичних сервісів/систем, що використовують штучний інтелект у різних сферах професійної юридичної діяльності: 1) у Франції – Doctrine.fr (пошукова система), Prédictice (аналітика, крім кримінальних справ), Case Law Analytics (аналітика, крім кримінальних справ), Juris Data Analytics – Lexis Nexis (пошукова система, аналітика, крім кримінальних справ); 2) у Великій Британії – Luminance (аналітика), HART – Harm Assessment Risk Tool (аналітика, кримінальні справи, оцінка ризику шкоди); 3) у Сполучених Штатах Америки – Watson/Ross – IBM (аналітика), Lex Machina – Lexis Nexis (аналітика), COMPAS – Correctional Offender Management Profiling for Alternative Sanctions використовуються судами США для оцінки ймовірності вчинення підсудним рецидиву злочинів та аналізу попередніх проступків; 4) в Аргентині – Prometea (аналітика, цивільні та адміністративні справи); 5) у Китайській Народній Республіці – Compulsory Similar Cases Search and Reporting Mechanism (аналітика) застосовується у Верховному народному суді Китайської Народної Республіки. Найбільш потужні системи з визначеного переліку працюють у судах і поліції та допомагають суддям приймати процесуальні рішення [169, с. 46-57].

Так, наприклад, дещо інше визначення сутності поняття терміну штучний інтелект надає Т.В. Туз, який стверджує, що штучний (електронний) інтелект – це штучно створена людиною система, здатна обробляти інформацію, яка до неї надходить, а також пов'язує її із знаннями, якими вона вже володіє, і відповідно дозволяє формувати своє власне уявлення про об'єкти пізнання [190].

Слід зазначити, що розпорядженням Кабінету Міністрів України від 2 грудня 2020 року №1556-р схвалено та затверджено «Концепцію розвитку

штучного інтелекту в Україні». В даній Концепції штучний (електронний) інтелект визначається як організована сукупність інформаційних технологій, із застосуванням якої можливо виконувати складні комплексні завдання шляхом використання системи наукових методів досліджень і алгоритмів опрацювання інформації, отриманої або самостійно створеної під час роботи, а також формувати та використовувати власні бази знань, моделі прийняття рішень, алгоритми роботи з інформацією та визначати способи досягнення поставлених завдань [181].

На даний час група науковців під керівництвом директора Інституту проблем штучного інтелекту НАН України і МО України А.І. Шевченка приступили до розробки Стратегії розвитку штучного інтелекту в Україні. До розробки цієї Стратегії долучаються понад 120 докторів наук, серед яких – завідувачі кафедр штучного інтелекту вищих навчальних закладів. В основу даної стратегії береться до уваги Концепція створення штучного інтелекту, яку розробило Міністерство цифрової трансформації України. Водночас, слід зазначити, що Концепція, яка розроблена Міністерством цифрової трансформації України, передбачає використання тільки іноземних програм, алгоритмів тощо. Тому в Проєкті Стратегії розвитку штучного інтелекту в Україні на 2022 – 2030 р.р. [210], на погляд А.І. Шевченка, необхідно мати власні наукові розробки українських вчених, освітян і практиків (програми, алгоритми, «роботи», тощо).

Варто зазначити, що наукові розробки роботів з елементами штучного інтелекту було здійснено в Україні півтора десятиліття тому і демонструвалися на великій науковій виставці CeBIT у німецькому місті Ганновері.

Цікавим є також те, що самохідні роботи з елементами штучного інтелекту були виготовлені на замовлення різних фірм, зокрема й спецорганів України. Наприклад, був створений робот з власною енергетичною установкою для пошуку мін. Причому даний робот знайшовши міну, він у реальній обстановці визначає, що з нею робити: знешкодити, підірвати, чи залишити біля неї знак-прапорець. Фактично всі дії, які необхідно здійснити,

робот виконує самотужки. Таким чином, це перші унікальні українські розробки, які сконструйовані з елементами штучного інтелекту.

Сьогодні перед українськими дослідниками стоїть важливе завдання – створити машину нового покоління з елементами штучного інтелекту. Тому авторський колектив, який розробляє Стратегію розвитку штучного інтелекту в Україні представив саме таку концептуальну схему прийняття рішень, дій електронним інтелектом виходячи з раніше означених завдань.

Також постає завдання про необхідність розробки і затвердження Верховною Радою України, Указом Президента України або Кабінетом Міністрів України Стратегії розвитку розвитку штучного інтелекту в Україні, адже сьогодні вже більше 50 провідних країн світу розробили та затвердили на законодавчому рівні власні національні стратегії розвитку штучного інтелекту.

В нашому дослідженні вважаємо за доцільне використовувати поняття електронний інтелект. Водночас відомо, що такі дослідники як М.І. Демура [95], О.В. Плахотнік [169], О.Е. Радутний [175; 176], В.В. Риков [180], Т.В. Туз [190] та інші у своїх працях використовують термін штучний інтелект.

Очевидно, що з розвитком наукових досягнень змінюється і сутність поняття штучний інтелект, який сьогодні слід трактувати, на наш погляд, як електронний інтелект. Зокрема, директор Інституту проблем штучного інтелекту НАН України А.І. Шевченко і МО України теж вважають, що сьогодні доцільно вживати такий термін, як інтелект машини, або електронний інтелект. Тому погоджуємося з думкою А.І. Шевченка про те, що сьогодні ми не маємо права пов’язувати ці новостворені автоматизовані комп’ютерні системи (інтелект машини, електронний інтелект) з інтелектом людини, якщо ми не знаємо, що це таке [117].

Очевидним є той факт, що потужний розвиток наукових досягнень в новому тисячолітті засвідчує, що особливо небезпечним сьогодні є можливість використання організованими злочинними угрупуваннями (хакерами, крекерами, фрікерами, спуферами, колекціонерами, кіберплутами, інсайдерами, терористами, піратами, шахраями) новітніх розробок

електронного інтелекту в злочинних цілях. Як стало відомо, що новітні засоби, методи і грід та блокчейн-технології електронного інтелекту уже сьогодні несуть надзвичайно потужну загрозу та небезпеку соціально-комунікаційним системам і мережам, автоматизованим базам та банкам даних і критичній інфраструктурі держави загалом. Зокрема, англійські і американські вчені справедливо стверджують, що електронний інтелект в скорому майбутньому може стати небезпечною зброєю в руках інсайдерів, хакерів і крекерів, електронних піратів, кібершахраїв, кібертерористів та кіберзлочинців, а також організованих злочинних груп і іноземних розвідувальних спеціальних служб. Про ці загрози, виклики і небезпеки зазначено в опублікованому днями стосторінковому дослідженні The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation [26]. Тому очевидно, що постає справедливе запитання: так в чому ж саме полягає реальна загроза світові з боку електронного інтелекту та електронного (комп'ютерного) злочинця і як цьому можна сьогодні реально запобігти, зарадити чи протидіяти?

Звіт, в якому висвітлюються реальні загрози використання можливостей електронного інтелекту для людства, був підготовлений групою з 26 провідних дослідників електронного інтелекту – відомих вчених Кембриджського, Оксфордського і Стенфордського університетів, а також експертів Electronic Frontier Foundation та OpenAI та представників інших авторитетних дослідницьких відомств, установ і організацій.

Очевидно, що реальна небезпека для розвитку електронної цивілізації полягає в тому, що сучасні можливості використання електронного інтелекту в освіті, науці і практиці стають більш могутніми, широкомасштабними і потужними. У зазначеному вище дослідженні визначаються три основні напрями, для яких існує найбільше викликів, ризиків, загроз і небезпек – це цифрова (електронна) безпека, фізичні об'єкти та політична сфера [44, с. 23-26].

Відомо, що сучасні ноозасоби і ноотехнології, грід- і блокчейн-технології електронного інтелекту уже сьогодні можуть виявити критичні

помилки і недоліки програмного забезпечення та швидко вибирати потенційних жертв для вчинення різного роду як загальнокримінальних, так і білокомірцевих фінансових та економічних злочинів. Більше того, сучасні ноозасоби і грід-технології електронного інтелекту можуть сприяти використанню соціальної інженерії як методу кібератаки. Це обумовлено тим, що інформація отримана з інтернету про персональні дані тої чи іншої людини, суспільства чи держави «може бути використана для автоматизованого створення шкідливих сайтів/посилань чи електронних листів, на які, швидше за все, відповідатиме потенційна жертва, адже вони надходитимуть вірогідно від справжніх людей та імітуватимуть їхній стиль спілкування», – стверджують фахівці, які підготували даний звіт [26].

Більше того подальший розвиток і удосконалення ноозасобів і грід-технологій електронного інтелекту, на думку авторів даного дослідження, може призвести до того, що переконливі чат-боти зможуть долучати людей до тривалих діалогів, таким чином збільшуючи рівень довіри до себе, або навіть набувати вигляду реальних людей у відеочаті.

Іншою реальною небезпекою в кіберпросторі, яка з’являється на горизонті, це можливість кібератаки на фізичні об’єкти. Автори звіту справедливо попереджають, що ноозасоби і грід-технології електронного інтелекту можуть безперешкодно проникати як у автоматизовані системи державних і комерційних установ, так і безпілотних автомобілів, так і безпілотних літаків, поїздів, кораблів, реально управляти ними та призводити по спеціальному коду для розкрадання майна, ресурсів, коштів, але і до аварій та катастроф. Ще одним прикладом може бути використання «армій дронів», які за допомогою технології комп’ютерного розпізнавання обличчя можуть вбивати людей, наголошується у дослідженні. Таким чином існує реальна загроза створення роботів-вбивць, роботів-кіберзлочинців [154, с. 324].

Таким чином, можна стверджувати, що діяльність електронних (комп’ютерних) злочинців стала надзвичайно небезпечною, оскільки вчинювані ними комп’ютерні злочини сьогодні вже набули транскордонного,

транснаціонального, трансконтинентального, планетарного характеру, а тому міжнародна спільнота, враховуючи можливі глобальні негативні наслідки цього соціального явища, намагається постійно контролювати і мінімізувати їх посягання на державні, міжнародні та міждержавні політичні, дипломатичні, економічні, екологічні відносини [45, с. 7].

Аналізуючи дану проблему, О.Е. Радутний вважає, що є питання, по-перше, про роль та місце штучного (електронного) інтелекту (artificial intelligence) в системі суспільних правовідносин, які захищаються кримінальним правом, по-друге, це зв'язок інформаційної безпеки з дослідженнями штучного інтелекту та їх результатами, і, по-третє, про можливість і доцільність визнання штучного інтелекту, що фізично втілений в об'єкт робототехніки, об'єктом та/або суб'єктом кримінально-правових правовідносин. На його думку наукові досягнення у розвитку штучного інтелекту можуть бути використані для вчинення злочинів, в тому числі в сфері інформаційних відносин, або сам він може являти безпосередню загрозу охоронюваним правам та законним інтересам людини, суспільства та держави [176, с. 124-132].

На наш погляд, цікавою є також думка О.В. Радутного, що штучний (електронний) інтелект, так само як і людина, може мати здатність усвідомлювати фактичну сторону того, що відбувається, усвідомлювати суспільну небезпечність свого діяння, яке реалізується в інформаційному просторі або завдяки роботизованим консолям, пристроям або механізмам – в оточуючому матеріальному середовищі (тобто, оцінювати за шкалою «добре – нейтральне – погане»), та, без сумніву, буде мати можливість за конкретних умов здійснювати певний вибір між тими чи іншими варіантами поведінки та здатність керувати своєю поведінкою (сьогодні це є однією з головних умов проведення штучним інтелектом хірургічних операцій, допуску його до керування безпілотними транспортними засобами тощо). Але саме через такі ознаки в теорії кримінального права прийнято описувати фізичну особу в якості суб'єкта злочину (ст.ст. 18, 19 КК України): 1) здатність усвідомлювати

фактичну сторону; 2) здатність усвідомлювати суспільну небезпечність свого діяння та його наслідків; 3) можливість за конкретних умов здійснення певного вибору між різними варіантами та здатність керувати своєю поведінкою [175].

Як зазначає М.І. Демура, сьогодні досить поширеним і вже загальновідомим інструментом використання штучного (електронного) інтелекту, який спрямований на попередження кримінального правопорушення або так званим інструментом «профілактичної поліцейської діяльності». Відомо, що Європейська етична хартія про реальні можливості використання штучного (електронного) інтелекту у судовій системі та її середовищі називає «список заборони на виліт», який фактично являє собою додаток для аналізу «великих даних», що збирає і аналізує дані про потенційних терористів з метою запобігання вчиненню актів, або ж алгоритми, що використовуються для виявлення фактів шахрайства або відмивання грошей. Очевидно, що використання штучного (електронного) інтелекту на стадії досудового слідства з метою розслідування кримінальних правопорушень є позитивним явищем. Сьогодні можливості електронного інтелекту активно застосовуються тоді коли у правоохоронних органів вже є достатньо наявна інформація про вчинення кримінального правопорушення і для цього потребується інструмент для аналізу великої кількості даних. Для прикладу, такі інструменти, як Connect, який використовується британською поліцією для аналізу мільярдів даних, отриманих в ході фінансових операцій для виявлення кореляцій або схем операцій, або для цих цілей використовується Міжнародна база даних щодо сексуальної експлуатації дітей (ICSEDB), яка керована Інтерполом. Дана система допомагає виявляти жертв та / або злочинців за допомогою аналізу, наприклад, меблів та інших предметів в зображеннях насильства або аналізу фонового шуму на відео. Такі електронні інструменти виявилися особливо ефективними в запобіганні та протидії транскордонній і транснаціональній злочинності. Так, наприклад, за допомогою програми Connect пошук з дуже високим рівнем складності та

обсягу даних, для якого раніше були потрібні місяці складних досліджень, тепер може бути виконаний фактично за лічені хвилини і з достатньо високою вірогідністю отриманих результатів [95, с. 26].

Варто також зазначити, що у Сполучених Штатах Америки уже понад 20 років використовується в судах та правоохоронних органах більшості штатів програмне забезпечення COMPAS (Correctional Offender Management Profilingfor Alternative Sanctions), яке розроблене ще в 1998 році на основі використання електронного інтелекту для оцінки потенційного ризику рецидиву злочинів [21].

Відомо, що серед науковців Сполучених Штатів Америки влітку 2016 року виникла наукова дискусія про електронний інструмент, який використовується в судах Сполучених Штатів Америки по всій країні для прийняття рішень про звільнення під заставу та винесення вироку. На думку американських фахівців, ця суперечка торкається деяких достатньо великих проблем кримінального правосуддя, що стоять перед нашим (американським) суспільством. І все це торкається алгоритму, який називається COMPAS та використовується по всій країні для вирішення питання, чи підсудні особи, які очікують суду, і наскільки вони небезпечні, щоб їх можна було звільнити під заставу. Аналізуючи ці питання ще у травні 2016 року слідча інформаційна організація ProPublica стверджувала, що COMPAS упереджено ставиться до темношкірих обвинувачених. Компанія Northpointe, штат Мічиган, яка створила даний електронний інструмент, надала свій власний звіт, в якому ставиться під сумнів аналіз наданий організацією ProPublica. У відповідь ProPublica спростувала дане заперечення, на основі чого академічні дослідники вступили в запеклу дискусію. Зокрема Wonkblog цієї газети зважує, що навіть Верховний суд Вісконсіна зробив посилання на дані суперечки в своєму недавньому рішенні, що підтримували використання COMPAS у вироку [9].

Електронний інтелект сьогодні активно використовується і в інших країнах світу. Але незважаючи на різні погляди електронний інтелект активно впроваджується в різні галузі юридичної діяльності.

Так, зокрема, в Китайській Народній Республіці вперше допоміжні технології штучного (електронного) інтелекту були використані в Шанхайському проміжному народному суді № 2 ще в 2019 році, повідомляє інформаційне видання LegalDaily. Наприклад, "Стенограма та представлення доказів тривали разом із ходом судового розгляду. Система 206 реалізувала повний цикл підготовчої допомоги та всебічно переглядала докази, відіграючи активну роль у неупередженому правосудді", - сказав заступник голови інформаційного відділу Шанхайського народного суду Ву Хайін. Відомо, що "Система 206 є інтегрованою допоміжною системою штучного інтелекту для кримінальних справ. Вона може допомогти судді виявити факти, посвідчити докази, захистити право на оскарження та неупереджено здійснювати правосуддя у судовому процесі, щоб запобігти незаконному засудженню громадян у кримінальних справах", - сказав Го Вейцин, голова Шанхайського проміжного народного суду № 2, а також головний суддя у справі про пограбування та вбивство [15].

Дискусії з цього питання тривають і досі в різних країнах світу. Так, наприклад, відомим юридичним фактом також є те, що американець відбув покарання цілий рік у в'язниці за безпідставним звинуваченням у вбивстві. Єдиний доказ проти нього – «думка» штучного (електронного) інтелекту. Судова практика свідчить, що громадянин США Майкл У. майже рік провів у в'язниці за звинуваченням у вбивстві, яке було засноване виключно на доказах, представлених системою з алгоритмами штучного (електронного) інтелекту. Слід зазначити, що результати експертизи, які базуються на даних рішення ShotSpotter, яка фіксує постріли зі зброї в містах США, судді ставлять під сумнів далеко не вперше [118, с. 63].

Разом з тим С.Ф. Денисов та В.Г. Павлов звертають особливу увагу на повідомлення інформаційного видання Technology Review, що вже через 60

років штучний інтелект стане значною загрозою для людства. Дослідники стверджують, що до 2022 року штучний інтелект буде мислити приблизно на 10 % як людина, до 2040 року – на 50 %, до 2075 року – процеси мислення неможливо буде відрізнити від людських. До таких умовиводів прийшов шведський вчений, професор Оксфордського університету Нік Бостром (Niklas Boström), який пропонує бути більш обережними, оскільки вважає його занадто загрозливим для людства (проблемою контролю над штучним інтелектом займаються у світі приблизно шість дослідників, питаннями його створення – десятки і сотні тисяч) [97].

Проведений нами неупереджений асиметричний аналіз тенденцій розвитку електронного інтелекту теж свідчить про реальність таких загроз, ризиків і небезпек.

Таким чином здійснивши системний аналіз інноваційних наукових досягнень у сфері створення електронного інтелекту та пов’язавши його можливості зі зберігання та аналізу масиву великих даних, а також консолідованої обробки масивів інформації та, відповідно, прийняття оперативних управлінських рішень на їх основі, ми не виключаємо реальність масового розповсюдження даних щодо інтенсивно розвиваючихся технологій в житті нашого суспільства та, відповідно, застерігаємо людство, суспільство, держави світу від масових правопорушень фундаментальних конституційних прав людини.

Тому вважаємо, що настав час на основі узагальнених результатів впровадження інноваційних технологій електронного інтелекту в реальне життя людства сформувати на науковому рівні концептуальні засади правового статусу взаємовідносин людини і робота.

Серед перших історичних кроків законодавчого врегулювання питання правового статусу роботів з електронним інтелектом або його елементами можна віднести Резолюцію Європейського Парламенту від 16 лютого 2017 року з рекомендаціями Комісії з цивільно-правових норм з робототехніки (2015/2103 (INL), яка містить пропозицію включити в законодавство

Європейського Союзу поняття “розумний робот”, потребу розробити систему реєстрації таких роботів, а також визначити правовий статус роботів як електронної особи (електронної особистості) [12].

У зв’язку з цим справедливим є зауваження Г.О. Андрощука про те, що після довгих років дискусій і обговорень Європейський Союз нарешті розпочав роботу над правовим регулюванням використання штучного інтелекту. Так, лише 21 квітня 2021 року Європейська комісія представила проект нових правил у цій сфері [22]. Тим часом Європейська коаліція за цифрові права (EDRi) разом з 61 іншою громадською організацією, в т.ч. Amnesty International, German Digitale Freiheit і Польським фондом Panoptykon, направили відкритий лист комісарам ЄС, включаючи Маргрет Вестагер, що відповідає за цифрові справи, і Віру Юрову, комісара ЄС з цінностей і прозоростей. Автори відкритого листа, а саме шістдесят дві громадські організації, закликали Європейську комісію заборонити використання в ЄС технологій штучного (електронного) інтелекту, яка порушує права людини і дозволяє, наприклад, масове спостереження за жителями: "Ми хочемо, щоб новий регламент встановив «червону межу» і ввів абсолютну заборону на використання технологій, що обмежують права людини" [30].

На сьогодні існують різні позиції вчених з приводу визначення правосуб’єктності роботів або програм з електронним інтелектом в системі правовідносин. Концепція правосуб’єктності робота (як потенційного суб’єкта права) є абсолютно новою і зовсім не вивченою на сьогоднішній день ні в літературі, ні в законодавстві. Також дана концепція породжує можливий новий вид суб’єкта права.

Зокрема, Крістофер О. Хернес робить припущення, що якщо штучний (електронний) інтелект повинен нести юридичну відповідальність за свої дії, тоді він повинен мати фізичну, юридичну та цифрову ідентичність, подібну людині. Якщо у штучного інтелекту є ті ж юридичні обов’язки, що і у людини, хіба в нього не повинні бути такі ж юридичні права, як у людини ? [6].

Схожої позиції притримується і О.А. Баранов, який вказує на необхідність визнання роботів зі штучним інтелектом суб'єктами суспільних відносин, а саме "еквівалентами фізичної особи" [37, с. 78].

Натомість Є.О. Харитонов, О.І. Харитонова пропонують визнати роботів зі штучним інтелектом квазі-юридичною особою з "кіберздатністю", яка може реалізовуватися за допомогою не лише правочинів, а й юридичних вчинків [202, с. 44].

Аналіз положень чинного законодавства України, проведений Т.Г. Катковою, дає змогу дійти висновку про правове регулювання, яке ґрунтується на першій гіпотезі: робот зі штучним інтелектом – об'єкт суспільних відносин – власність фізичної або юридичної особи; не є та не може бути окремим самостійним суб'єктом суспільних відносин. Зважаючи на викладене вище, штучний (електронний) інтелект потрібно сприймати як джерело підвищеної небезпеки та розглядати з урахуванням всіх специфічних умов відповідальності за завдану шкоду з боку саме джерела підвищеної небезпеки, що вже встановлено нормами чинного законодавства України. У разі закріплення в майбутньому національним законодавством України особливого статусу робота як самостійного суб'єкта правовідносин, питання відповідальності за помилки штучного (електронного) інтелекту підлягатиме коригуванню, оскільки запровадження статусу «електронної особи», як окремого різновиду страхування, впровадження додаткових критеріїв розподілу відповідальності між виробником і власником, а також пошук відповідей на всі інші можливі виклики, які виникатимуть у процесі подальшого використання штучного інтелекту в різних сферах людської діяльності, зумовить відповідні дії. Так, якщо розглядати правосуб'єктність «електронної особи» як індивідуального суб'єкта, аналогічного людині, то надання їй такого правового статусу є важливим кроком на шляху до отримання повного набору конституційних («людських») прав, що може породжувати в подальшому інші проблеми: наприклад щодо того, чи можуть до суб'єктів штучного інтелекту застосовуватися такі конституційні гарантії як

право не бути у рабстві. Одним із аргументів проти наділення штучного інтелекту правовим статусом «електронної особи» є його обмежена вразливість до покарання. На її думку хоча сучасні корпорації також наділяються правосуб'єктністю, не дивлячись на це, вони не можуть бути, наприклад, позбавлені волі, на них можуть бути накладені фінансові санкції [123, с. 48].

Таким чином, дослідивши зазначені ідеї та концепції науковців у визначеній науковій сфері, щодо перспектив розвитку використання електронного інтелекту вважаємо, що найбільш прийнятною для подальшого дослідження та розвитку із запровадженням в перспективі у чинне законодавство є концепція визначення сутності правового статусу робота або програми з електронним інтелектом як «електронної юридичної особи», яка може мати схожість з юридичною особою в тому сенсі, що обидві є для їх власників засобом досягнення певної мети, цілі в різних сферах людської діяльності в тому числі і для вчинення комп'ютерних злочинів та існують і створюються виключно в інтересах їх власників або творців. Вважаємо, що робот, будучи наділеним правовим статусом «електронної юридичної особи», не набуває прав і обов'язків аналогічних правам і обов'язкам людини чи громадянина, а власник/засновник - розробник робота створює юридичну фікцію, контроль над якою він зобов'язаний безпосередньо здійснювати та нести за його дії повну юридичну відповідальність.

Що стосується поняття «електронної особи» або «електронної юридичної особи» на даний момент в законодавствах країн світу взагалі відсутні визначення. Дані правові визначення необхідно надавати спільним міжнародним колективом науковців з різних галузей науки та техніки та обов'язково на чолі з провідними правниками світу, адже це неймовірно складне завдання.

Відомо, що сьогодні фактично процесом створення та діяльності «електронного інтелекту» - «електронної юридичної особи», незалежно від форм власності, керує людина або група осіб. Водночас, також залишається на

сьогодні поза увагою вчених можливість впливу електронного інтелекту на різні суспільні процеси. А це значить, що потребує дослідження його правової чи позаправової сутності і діяльності.

Очевидно, що електронна юридична особа жодним чином не повинна прирівнюватися з людиною у правах, тобто вона не може мати правовий статус людини чи фізичної особи та, відповідно, мати права людини чи фізичної особи, які чітко визначені в чинному законодавстві. Тому вважаємо, що тут необхідним є обов'язково повний правовий міжнародний, міждержавний, державний та суспільний контроль за діяльністю «електронної юридичної особи». Виходячи з даних позицій, на нашу думку обов'язково потрібно внести до чинного законодавства пропозиції щодо створення нової форми професійної діяльності як «електронна юридична особа» і, як наслідок, повну юридичну відповідальність за діяльність «електронної юридичної особи» покласти виключно на власників, акціонерів та розробників даної «електронної юридичної особи» [16, с. 143-150].

Вважаємо, що запропонована нами концепція визнання робота або програми з електронним інтелектом «електронною юридичною особою» обов'язково повинна враховувати всі три підходи до розвитку електронного суспільства – це світоглядно-філософський, інноваційно-комунікаційний і безпековий, які водночас обов'язково повинні доповнювати один одного. Перший – це світоглядно-філософський, в якому висвітлюються основи становлення і розвитку правового, наукового і ресурсного забезпечення захисту прав людини в сучасному світі. Другий – аналітичний (інноваційно-комунікаційний), який дає змогу оцінити сутнісні ознаки розробки і впровадження інноваційної комунікації (електронної юридичної особи) в електронний простір і створити умови захисту прав людини, суспільства, держави, цивілізації в кіберпросторі. Даний підхід дозволяє осмислити реальні можливості використання можливостей електронного інтелекту та сприяє розробці прагматичних рекомендацій з метою підвищення ефективності захисту прав людини в електронному просторі. Третій – безпековий. Він

допомагає визначити ймовірність здійснення запропонованих законодавчих змін та передбачити і запобігти настання можливих загроз, ризиків та небезпек від дій електронного інтелекту для людини, суспільства і держави. Такий прагматичний підхід також пропонує конкретні реальні безпекові механізми, процедури, запобіжники і заходи, засоби, методи, технології запобігання і протидії цим небезпекам та загрозам [45, с. 27].

Тому в даному дослідженні пропонуються ідеї та інновації щодо необхідності створення правоохоронними органами високотехнологічної системи на базі електронного інтелекту, яка б дозволяла заздалегідь розпізнавати і прогнозувати варіативність злочинних дій комп'ютерних злочинців в різних життєвих ситуаціях.

Така новітня електронна система діагностики і прогнозування поведінки особи комп'ютерного злочинця дозволить вчасно запобігати, а в разі необхідності протидіяти злочинним намірам цих осіб.

Вважаємо, що уже сьогодні є нагальна потреба у подальшому поглибленні наукових досліджень міжнародної та регіональної юрисдикції, щодо засадничих положень соціально-комунікаційного права, інтелектуального права, інноваційного права, інформаційного права, електронного права, кіберправа, електронної економіки, електронного інтелектуального права, кібербезпеки, кіберкримінології, кіберкриміналістики, кіберекспертології, кібердетективознавства з метою підсилення ефективності запобігання і протидії протиправним діям комп'ютерних злочинців (кібертероризму, кібершахрайству, кіберзлочинності) в кіберпросторі і інтернет просторі та у сфері соціально-комунікаційних інформаційних технологій [173, с. 20].

Зокрема, актуальними є питання створення сучасного вчення про систему криміналістичних засобів наукового забезпечення доказознавства, яке б являло собою систему наукових принципів та практичних рекомендацій, спрямованих на ефективне розв'язання означених завдань [73, с. 72].

На наш погляд надзвичайно важливими та своєчасними для безпечного розвитку світового суспільства сьогодні є висловлювання старшого розвідника-аналітика та технічного директора Агенства національної безпеки Сполучених Штатів Америки Давида Т. Мура про те, що наші часи вимагають свіжого, критичного мислення з боку тих, хто відповідає за виявлення і попередження загроз, а також з боку тих, хто протидіє цим загрозам [94, с. 8].

Таким чином концепція визнання робота або програми з електронним інтелектом «електронною юридичною особою» обов'язково повинна враховувати небезпеку постановки людством, суспільством, державами даної «електронної особи» в один суспільний ряд з людиною при використанні електронного інтелекту в правотворчій, правозахисній та судовій діяльності державних органів влади та міжнародних, міждержавних правових структурах, інституціях, відомствах, установах, організаціях, та, зокрема, в кримінологічних дослідженнях і кримінальному праві більшості держав світу [158, с. 31].

Вище наведену наукову позицію підтримують В. Папаконстантінов, П. Герт, які справедливо вважають, що це може стати історичною нагодою для юристів Європи знову змінитися на краще, взяти на себе роль міжнародного лідера та створити нові правила та нові принципи, які є найкращою надією людства в сьогоднішньому технологічному Армагедоні. Парламентська комісія Європейського Союзу з приводу розгляду правового статусу електронного інтелекту повинна зробити стрибок віри в право, в дотримання якісної оцінки правових, моральних задач, які існують, та замість того, щоб латати старі латки існуючої правової бази, вирішити питання щодо надання електронному інтелекту статусу юридичної особи [20].

Підсумовуючи вище викладене, вважаємо, що сьогодні основоположною законодавчою інновацією, задачею, орієнтиром для всіх правотворців та правозахисників в світі є недопущення можливих тенденцій порушення прав і свобод людини, суспільства та держави з боку злочинних дій «електронної особи» створеної на базі електронного інтелекту.

Висновки до розділу 3

1. Аналіз статистичних даних дозволяє зробити висновок, що сьогодні типовими і найбільш небезпечними комп'ютерними злочинами, які вчиняються комп'ютерними злочинцями не тільки в Україні, але в Європі та світі є наступні: а) втручання або перехоплення (незаконний доступ, перехоплення, викрадення часу; б) зміна або пошкодження інформації («логічна бомба», «троянський кінь», програми-віруси, «черв'яки»); в) комп'ютерне шахрайство (шахрайство з автоматами на видачі готівки, комп'ютерна підробка, шахрайство з ігровими автоматами, шахрайство шляхом неправильного вводу/виводу або маніпуляції з програмами, шахрайство з платіжними засобами, телефонне шахрайство тощо); г) несанкціоноване копіювання (несанкціоноване тиражування комп'ютерних ігор, несанкціоноване тиражування програмного забезпечення, несанкціоноване тиражування напівпровідникової продукції); д) комп'ютерний саботаж (саботаж технічного забезпечення, саботаж програмного забезпечення); е) злочини, пов'язані з комп'ютерами (незаконне використання дошки електронних оголошень, викрадення комерційної таємниці, зберігання або розповсюдження матеріалів, які є об'єктом судового переслідування).

2. Сьогодні комп'ютерна злочинність – це міжнародне (транскордонне, транснаціональне, трансконтинентальне, планетарне) наземне і космічне явище, рівень якого тісно пов'язаний з науковим, освітнім, військовим, економічним рівнем розвитку суспільства в різних державах та регіонах. При цьому очевидно, що менш розвинуті в науково-технічному і технологічному відношенні країни завдяки продуктивній діяльності міжнародних правоохоронних організацій мають можливість використати досвід більш розвинутих країн для запобігання та протидії комп'ютерним злочинам. Причому тенденції, розвитку комп'ютерної злочинності, злочинні кіберзасоби

та кіберзаходи по запобіганню є в різні відрізки часу однаковими для різних країн, що базується на єдності технологічної бази цих комп'ютерних злочинів.

3. Наявний сьогодні достатньо потужний рівень сучасних кіберзагроз в електронному світі надзвичайно небезпечних комп'ютерних злочинів в кіберпросторі потребує негайної розробки нової концепції Стратегії кібербезпеки України, а також пріоритетних напрямів наукових досліджень з метою запобігання і протидії цим негативним кіберзагрозам, кіберризикам і кібернебезпекам, які реально мають місце в суспільстві.

4. Проведений нами аналіз дозволив виявити та підтвердити юридичний факт вчинення комп'ютерними злочинцями першого в Україні космічного кіберзлочину, який нещодавно вже розглянутий в українському суді.

5. Викликає занепокоєння той факт, що необхідність всебічного дослідження особи комп'ютерного злочинця з метою запобігання і протидії комп'ютерним злочинам в Україні ще не має достатньої правової, інформаційно-аналітичної, організаційної, освітньої, наукової, кадрової та праксеологічної підтримки. По-перше, не створена дієва нормативно-правова база, оскільки чинне законодавство нашої держави (зокрема, Кримінальний і Кримінальний процесуальний кодекси України та інші Закони України в галузі кібербезпеки) й досі не відповідають рекомендаціям Ради Європи, які були прийняті з питань запобігання і протидії комп'ютерним злочинам. По-друге, не прийняте рішення про створення потужного науково-дослідницького центру з консолідованого системного асиметричного аналізу тенденцій розвитку зловмисних дій, які вчиняють кіберзлочинці (кіберзлочини, кібертерористичні акти, кібератаки тощо) як у космічному, так і наземному кіберпросторі. По-третє, відсутнє держзамовлення на підготовку необхідних фахівців для запобігання, протидії, розслідування електронних злочинів в наземному і космічному кіберпросторі.

6. Актуальною постає проблема вчинення кримінальних правопорушень з використанням можливостей електронного інтелекту. Разом з тим подальші розробки і розвиток електронного інтелекту надасть можливість

використовувати ці системи і технології як для вивчення особи комп’ютерного злочинця, зокрема, так і для запобігання та протидії комп’ютерній злочинності загалом. Запропоновано використовувати поняття «електронної юридичної особи», яка у жодному разі не повинна прирівнюватися до людини в правах, тобто вона не може мати правовий статус фізичної особи.

ВИСНОВКИ

У дисертаційному дослідженні наведено теоретичне узагальнення та сформульовано нове вирішення наукового завдання, що полягало у з'ясуванні закономірностей, особливостей пізнання характерних рис, ознак, властивостей і манер поведінки особи комп'ютерного злочинця як об'єкта кримінологічного дослідження. Дане дослідження базується на новітніх положеннях теорії кримінології і результатах узагальнення матеріалів вітчизняної і міжнародної практики. Одержані результати дозволяють сформулювати низку теоретичних висновків відносно особи комп'ютерного злочинця з метою запобігання та протидії вчинення комп'ютерних злочинів в сучасному електронному світі.

Головним теоретичним, методологічним і праксеолого-прикладним надбанням дисертаційного дослідження є такі висновки, пропозиції і рекомендації:

1. Особа комп'ютерного злочинця – це фізична особа (людина), яка вчиняє кримінальні правопорушення з використанням електронно-обчислювальних машин (комп'ютерів), різного рівня новітніх комп'ютерних засобів і технологій (нанокомп'ютери, портативні комп'ютери, суперкомп'ютери, квантові комп'ютери тощо) та різного виду засобів (електронного, біологічного або нейробіологічного електронного інтелекту тощо), електронних банків даних, систем та комп'ютерних мереж, або інших засобів комп'ютерної інформатизації та різного роду інформаційно-телекомунікаційного обладнання (державного, приватного, наземного, космічного).

2. Комплексний аналіз сутності поняття особи комп'ютерного злочинця дозволив виокремити суттєві риси, ознаки, властивості та манери поведінки, а саме сформулювати його реальний соціально-правовий, психофізіологічний та інформаційно-комунікаційний портрет. Соціально-правовий, психофізіологічний і інформаційно-комунікаційний портрет сучасного

комп'ютерного злочинця характеризується наступними параметрами (ознаками, рисами, характеристиками): 1) стать – комп’ютерні злочинці це переважно чоловіки, але водночас сьогодні кількість жінок постійно збільшується; 2) вік – найбільш активний період злочинної діяльності від 15 до 45 років; 3) фізичні дані – у фізичному відношенні, як правило, слабо розвинутий: худорлявий, або навпаки, інколи має зайву вагу; 4) інтелектуальний розвиток – коефіцієнт інтелектуального розвитку, як правило, вище за середній; 5) мотивація: спортивний інтерес, азарт, гра, жарт; самореклама або самоствердження; хворобливий стан; персональна помста; антисоціальна спрямованість; отримання злочинної матеріальної вигоди; 6) освіта – у переважної більшості комп’ютерні злочинці мають вищу або середню спеціальну комп’ютерну освіту. На практиці відомі випадки, коли комп’ютерний злочинець взагалі не мав ніякого комп’ютерно-технічного досвіду; 7) злочинний досвід – комп’ютерні злочинці, як правило, не мають злочинного минулого; 8) положення у суспільстві – комп’ютерним злочинцем можуть бути школярі, студенти, відповідальні працівники (керівники) державних відомств, установ і організацій, комерційних установ або приватних фірм. Важливим для комп’ютерного злочинця є добре володіти комп’ютером та мати безпосередній доступ до автоматизованих комп'ютерних систем, електронних банків даних та електронних інформаційно-комунікаційних мереж; 9) манери поведінки – комп’ютерний злочинець, як правило, зовнішньо не відхиляється від прийнятих у суспільстві норм етичної і правової поведінки. Дані особи побоюються втрати авторитету серед одногрупників, співробітників і взагалі в структурі певної соціальної групи; 10) риси характеру – комп’ютерний злочинець в більшості випадків за складом характеру «інтроверт», оскільки він є дуже егоїстичним, завжди потребує до себе особливої уваги з боку колег і однодумців, він є уважним, спостережливим, винахідливим, фактично це яскрава особистість, а також бажаний працівник.

3. Системний консолідований аналіз рис, ознак, властивостей і манер поведінки комп’ютерних злочинців дозволяє розкрити сутнісні характеристики типології осіб, які вчиняють окремі види комп’ютерних злочинів, а саме: 1) операційні комп’ютерні злочини можуть вчиняти в основному оператори автоматизованих комп’ютерних систем, електронних банків даних та електронних мереж; оператори автоматизованих периферійних комп’ютерних пристроїв і інформаційно-комунікаційних систем; оператори, які обслуговують лінії телекомунікацій; 2) комп’ютерні злочини, які вчинені з використанням комп’ютерного програмного забезпечення вчиняють переважно комп'ютерні злочинці, які володіють новітніми колекціями комп’ютерного програмного забезпечення; системні комп’ютерні програмісти; прикладні комп’ютерні програмісти; висококваліфіковані користувачі автоматизованих комп’ютерних систем, електронних банків даних і електронних мереж; 3) комп’ютерні злочини вчиняють комп’ютерні злочинці, які мають можливість входу до апаратної частини автоматизованих комп'ютерних систем - це в основному: інженери-системщики; інженери, які мають комп'ютерний доступ до територіальних (регіональних) автоматизованих комп’ютерних пристроїв; інженери зв'язківці; інженери-електронщики; 4) комп’ютерні злочини вчиняють комп’ютерні злочинці, які займаються організаційною управлінською роботою з метою надійного забезпечення діяльності автоматизованих комп’ютерних систем, електронних банків даних і електронних мереж: це особи, які забезпечують керування комп'ютерними мережами; це особи, які забезпечують керування керування комп’ютерними операторами; це особи, які забезпечують керування електронними базами даних; це особи, які забезпечують керування роботою по розробці і використанню програмного забезпечення; 5) комп’ютерні злочини вчиняють також такі особи: це обслуговуючий персонал автоматизованих комп'ютерних систем, електронних банків даних і електронних мереж; працівники, які забезпечують діяльність служби кібербезпеки автоматизованих комп'ютерних систем, електронних банків даних і електронних мереж;

працівники, які забезпечують контроль за функціонування автоматизованих комп'ютерних систем, електронних банків даних і електронних мереж; 6) комп’ютерні злочини також вчиняють працівники, які займаються сервісним обслуговуванням автоматизованих комп'ютерних систем, електронних баз даних та електронних мереж, а також працівники, які забезпечують сервісний ремонт автоматизованих комп'ютерних систем, електронних банків даних, електронних мереж; 7) комп’ютерні злочини вчиняють також такі особи, як: учні старших класів та студенти закладів вищої освіти; викладачі середніх освітніх закладів та професорсько-викладацький склад закладіввищої освіти; безробітні; особи без постійного місця перебування; кібергастролери.

4. Методика дослідження особи комп’ютерного злочинця, по-перше, базується на тому, що аналізуються матеріали слідчої, судової і експертної практики щодо вчинених злочинів з використанням електронно-обчислювальних машин, комп’ютерів, електронних баз даних, та інформаційно-комунікаційних комп'ютерних мереж і мереж електрозв’язку. По-друге, оскільки комп’ютерні злочинці є поширеною групою осіб покоління «digital-nature», які достатньо професійно володіють спеціальними знаннями, комп’ютерними технологіями для вчинення комп’ютерних злочинів як в наземному, так і космічному кіберпросторі, то дослідженню підлягають як світоглядно-філософські, морально-психологічні, соціально-комунікаційні, інноваційно-аналітичні, безпекові, так і юридично значимі риси, ознаки, звички, властивості, манери поведінки особи комп’ютерного злочинця.

5. Характерними рисами, ознаками, властивостями комп’ютерного злочинця є наступні: 1) комп’ютерні злочинці вчиняють, як правило, міжнародні (транскордонні, транснаціональні, трансконтинентальні, планетарні, а інколи космічні) комп’ютерні злочини, які виходять за рамки кордонів однієї держави; 2) комп’ютерні злочинці користуються таємними кодами, паролями для вчинення комп’ютерних злочинів; 3) комп’ютерні злочинці користуючись сучасними технологіями оскільки вчиняють

комп’ютерні злочини дистанційно, а тому є великі труднощі у встановленні місцезнаходження як самого комп’ютерного (електронні сліди таких злочинів можуть бути встановлені в різних установах, країнах і континентах) злочину, так і місце безпосереднього перебування комп’ютерного злочинця в момент вчинення протиправної злочинної дії; 4) комп’ютерні злочинці при вчиненні комп’ютерних злочинів працюють так, що фактично неможливо в реальному масштабі часу спостерігати і документувати електронні сліди (докази) візуально; 5) комп’ютерні злочинці в процесі вчинення комп’ютерних злочинів використовують такі безпекові процедури: різні засоби, способи і технології криптографічного шифрування інформації; засоби, призначені для виготовлення ключових даних або ключових документів та управління ключовими даними, що використовуються в методах комп’ютерного захисту інформації; засоби захисту від несанкціонованої модифікації чи нав’язування неправдивої інформації, що фактично реалізують алгоритми криптографічного перетворення інформації, у тому числі комп’ютерні технології імітозахисту та електронного підпису, а також засоби розмежування доступу до ресурсів автоматизованих комп’ютерних систем, електронних баз даних, електронних комунікаційних мереж у яких реалізовані криптоалгоритми; 6) комп’ютерні злочинці володіють достатньо потужними криптологічними засобами (апаратними, програмними, апаратно-програмними), криптологічними алгоритмами і криптологічними автоматизованими комп’ютерними системами захисту конфіденційної інформації, яка отримана в процесі вчинення комп’ютерних злочинів; 7) з метою забезпечення власної безпеки комп’ютерні злочинці використовують різні засоби захисту своїх автоматизованих комп'ютерних систем (ключові дані, системи управління ключовими даними, технічні засоби, спеціальні інформаційно-телекомунікаційні системи) від несанкціонованого зовнішнього втручання з метою отримання інформації; 8) комп’ютерні злочинці вчиняють комп’ютерні злочини таким чином, що інколи просто неможливо встановити чіткі зв’язки між ланками електронних слідів у цілісній системі комп’ютерних (електронних) доказів; 9) оскільки

комп’ютерні злочинці вміло користуються можливостями всесвітньої електронної мережі інтернет то це дозволяє їм широко використовувати піратське програмне забезпечення, займатися промисловим шпигунством,оргувати зброєю, наркотиками, здійснювати вторгнення до телефонних мереж та незаконно торгувати послугами зв’язку тощо; 10) характеризуючи риси, ознаки і властивості комп’ютерних злочинців їх можна систематизувати і класифікувати на чотири основні групи: «любителі-початківці», «хворі», «професіонали», «супер професіонали»; 11) комп’ютерні злочинці – «любителі-початківці» - це особи, які характеризуються сталим поєднанням первинних елементів професіоналізму у галузі комп’ютерної техніки і комп’ютерного програмування з елементами своєрідного дитячого захоплення, спортивного азарту, фанатизму і винахідливості. Такі особистості не завжди прагнуть вчинити комп’ютерний злочин, оскільки для них це забава, безкорислива гра, яка викликана спортивним інтересом, азартом, фанатизмом, але в ряді випадків приводить до вчинення ними комп'ютерних злочинів; 12) комп’ютерні злочинці – «хворі» - це особи, які страждають новим видом психічних захворювань – інформаційними хворобами, комп’ютерними фобіями; 13) комп’ютерні злочинці – «професіонали» - це фахово підготовлені професіонали своєї справи, які технологічно та ситуаційно мають реальну можливість вчиняти комп’ютерні злочини; 14) комп’ютерні злочинці – «супер професіонали» - це, по-перше, найбільш небезпечні високопрофесійні комп’ютерні злочинці з ярко вираженою корисливою і корисливо-насильницькою метою злочинних дій; по-друге, це профі-крекери – спеціалісти вищого класу в галузі володіннями знаннями, навиками і уміннями вчинення потужних, як наземних, так і космічних комп’ютерних злочинів (кібератак, кібертерористичних актів тощо); по-третє, профі-крекери мають на озброєнні надсучасне технологічне та комп’ютерне програмне забезпечення; по-четверте, «профі-крекери» у своїй структурі мають чітко налагоджений порядок та контроль обміну як відкритою, так прихованою, таємною інформацією, по-п’яте, «профі-крекери» достатньо потужно з позиції

управління злочинною діяльністю гарно організовані; по-шосте, «супер-крекери» добре організаційно, оперативно-технологічно та криптологічно законспіровані; по-сьоме, «супер-крекери» володіють достатньо високим рівнем знань, навиків і умінь організації комунікації та кооперації в процесі вчинення комп'ютерних злочинів.

6. Комп'ютерних злочинців можна умовно систематизувати і класифікувати на такі окремі групи і підгрупи: 1) хакери; 2) інсайдери; 3) телефонні кібершахраї – фрікери; 4) колекціонери; 5) спуфери; 6) спамери; 7) фішери; 8) кардери; 9) кіберплути; 10) кіберкрукери; 11) вірмейкери; 12) кіберсквотери; 13) електронні пірати або «кіберторгаші»; 14) кібертерористи; 15) крекери; 16) творці шкідливих комп'ютерних програм; 17) організовані злочинні угрупування; 18) іноземні розвідувальні служби.

7. Серед комп'ютерних злочинців є представники усіх груп традиційної класифікації: білокомірцевого, організованого і загальнокримінального злочинного світу. Як правило комп'ютерні злочинці працюють як в самих організаціях, відомствах і установах, проти яких вони вчиняють комп'ютерні злочини, так і поза їх межами. Причому комп'ютерні злочинці вчиняють комп'ютерні злочини як поодинці, так і у групі зловмисних співучасників. Важливо звернути увагу на тому, що провідне місце де зловмисно діють хакери і крекери, фрікери і спамери, колекціонери і фішери, кіберплути і кардери, кіберкрукери і кібersквокери, інсайдери і вірмейкери, кібертерористи і електронні торгаші або кіберпірати, спуфери і творці шкідливих комп'ютерних програм тощо – це забезпечення антисоціальної і надзвичайно небезпечної діяльності організованих злочинних груп.

8. Вітчизняний та міжнародно-правовий порівняльний аналіз кримінологічної та кримінально-правової характеристики типових видів злочинних дій комп'ютерних злочинців в кіберпросторі дозволяє зробити наступні висновки: а) сучасний стан зловмисних дій, які вчиняють комп'ютерні злочинці, свідчить про появу зовсім нових видів кримінальних посягань, за вчинення яких наразі не забезпечено можливість притягнення до

кримінальної відповідальності; б) класифікація та коди різновидів комп'ютерних злочинів, які закріплені в чинному законодавстві Ради Європи потребують удосконалення шляхом внесення нових змін і доповнень; в) кримінологічна і кримінально-правова характеристика комп'ютерних злочинів повинна відповідати тим тенденціям, які пов'язані зі значним зростанням вітчизняної, європейської і світової кіберзлочинності (комп'ютерної злочинності) в результаті збільшення кількості інтернет-користувачів (людей, машин, роботів), що, відповідно, призвело до масового глобального використання і поширення новітніх інформаційних технологій, зокрема, електронного (штучного) інтелекту та несе в собі нові небачені та непрогнозовані кіберзагрози та кібервиклики світовому співтовариству; г) дослідження кримінологічної і кримінально-правової характеристики окремих видів злочинної діяльності комп'ютерних злочинців у кіберпросторі слід враховувати також поруч із тими новими загрозами і викликами для Українського народу та нашої держави України. Ці всі пропозиції і рекомендації слід враховувати при розробці положень нових галузей знань – кримінального електронного права України та електронної кримінології.

10. Вважаємо, що важливо уже сьогодні відповідним безпековим міжнародним органам світу (ООН, ОБСЄ, ЮНЕСКО, ФАТФ, МПА, Інтерполу, Європолу) та окремих державних установ (Великої Британії – Мі-5, Мі-6; Канади – кінної поліції; США – АНБ, ЦРУ, ФБР; України – РНБО та інших країн), освітнім та науковим установам (університетам, інститутам, академіям, коледжам, безпековим науково-дослідним інститутам) приступити до розробки та реалізації в освіті, науці і на практиці наступних стратегічних кроків і прийняття відповідних безпекових управлінських тактичних рішень, а саме:

– розробити міждержавні стандарти з метою формування засобів і методів запобігання комп'ютерній злочинності з метою забезпечення кібербезпеки наземного та космічного кіберпростору для гарантування

невідчужуваних та непорушних конституційних прав та свобод людини і громадянина:

– розробити прийняти чітку і надійну міждержавну кібербезпекову правову базу (Конвенцію ООН) реальних можливостей використання наземного і космічного кіберпростору (близького і далекого) та електронного інтелекту в освітній, науковій і праксеологічній діяльності з метою запобігання і протидії можливим електронним кіберзагрозам, кібератакам, кіберзлочинам кібервикликам і кібернебезпекам;

– акцентувати увагу розробників новітніх кібербезпекових електронних ноозасобів, креативних методів і грід-технологій електронного інтелекту на те, що необхідно технологічно запобігти та протидіяти можливим кіберзагрозам неправомірного використання космічного простору і електронного інтелекту в різних сферах наземної та космічної життєдіяльності;

– відповідним міжнародним безпековим організаціям, відомствам і установам світу розробити впорядковану правову, організаційну і технологічну систему запобігання і протидії шкідливому використанню космічного простору і електронного інтелекту як на національному, регіональному, так і на міждержавному (світовому) рівнях (транскордонному, транснаціональному, трансконтинентальному, планетарному, космічному (близький космос, далекий космос));

– створити міжнародне об’єднання потужних провідних електронних держав світу для формування, розробки і впровадження єдиних запобіжних безпекових стандартів надання електронних довірчих послуг на всій земній кулі;

– забезпечити впровадження в космічну діяльність новітніх розробок в галузі дослідження особи комп’ютерного злочинця з метою запобігання комп’ютерній злочинності та кібербезпеки здійснених науковцями Національного авіаційного університету спільно з Інститутом електронної фізики НАН України, Національним космічним агенством України та правничою компанією «АЮР-КОНСАЛТИНГ».

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. 41 млн підозрілих подій та 147 кіберінцидентів – річний звіт ДЦКЗ. URL: https://cip.gov.ua/ua/news/321f4bf8 (дата звернення 01.10.2022).

2. £1.2 billion for the world's most powerful weather and climate supercomputer. Press release. URL: https://www.gov.uk/government/news/12-billion-for-the-worlds-most-powerful-weather-and-climate-supercomputer (дата звернення 01.10.2022).

3. Annual Report 2021. *Interpol.* URL: https://www.interpol.int/en/content/download/17965/file/INTERPOL%20Annual%20Report%202021_EN.PDF (дата звернення 01.10.2022).

4. Breakthrough for the realization of ultrafast quantum computers: the world's fastest 2-Qubit gate between two single atoms. *National Institutes of Natural Sciences.* URL: https://www.eurekalert.org/news-releases/960886 (дата звернення 01.10.2022).

5. Center for Strategic and International Studies (CSIS) Report Launch: Organizations and Nation-State Cyber Threats in the Crosshairs. URL: https://www.csis.org/events/report-launch-organizations-and-nation-state-cyber-threats-crosshairs (дата звернення 01.10.2022).

6. Christoffer O. Hernaes. Artificial Intelligence, Legal Responsibility and Civil Rights. URL: https://techcrunch.com/2015/08/22/artificial-intelligence-legal-responsibility-and-civil-rights (дата звернення 01.10.2022).

7. Cody Godwin. Met Office and Microsoft to build climate supercomputer. URL: https://www.bbc.com/news/technology-56840169 (дата звернення 01.10.2022).

8. Convention on Cyber-crime. URL: http://www.interlex.it/testi/cybercr25.htm (дата звернення 01.10.2022).

9. Corbett-Davies S., Pierson E., Feller A., Goel Sh. A computer program used for bail and sentencing decisions was labeled biased against blacks. It's

actually not that clear. URL: https://www.washingtonpost.com/news/monkey-cage/wp/2016/10/17/can-an-algorithm-be-racist-our-analysis-is-more-cautious-than-propublicas (дата звернення 01.10.2022).

10. Council backs Commission's plans to invest €1 billion in world-class European supercomputers. URL: https://ec.europa.eu/commission/presscorner/detail/en/IP_18_5864 (дата звернення 01.10.2022).

11. Cyber Security Institute. URL: https://cybersecurityinstitute.co.za/?fbclid=IwAR2RrZgNYYEXFfORI6ni83PgrJ1ww5zB8DuzfAgX3YI8Pw75uUgt7U2NKbA (дата звернення 01.10.2022).

12. European Parliament Resolution of 16 February 2017 with recommendations to the Commission on Civil Law Rules on Robotics. URL: https://www.europarl.europa.eu/doceo/document/TA-8-2017-0051_EN.html (дата звернення 01.10.2022).

13. Internet Crime Report 2021. *Federal Bureau of Investigation.* URL: https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf (дата звернення 01.10.2022).

14. Internet Organised Crime Threat Assessment (IOCTA) 2021. *Europol.* URL: https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2021 (дата звернення 01.10.2022).

15. Jiang Wei. China uses AI assistive tech on court trial for first time. URL: http://www.chinadaily.com.cn/a/201901/24/WS5c4959f9a3106c65c34e64ea.html (дата звернення 01.10.2022).

16. Malii M. Prevention of computer crimes electronic intelligence against human, society, state. *Visegrad Journal on Human Rights*. 2021. № 4. С. 143-150.

17. Moore A.P., Cappelli D.M., Trzeciak R.F. The “Big Picture” of Insider IT Sabotage Across U.S. Critical Infrastructures. *Insider Attack and Cyber Security*. 2007. P. 17–52. URL: https://doi.org/10.1007/978-0-387-77322-3_3 (дата звернення 01.10.2022).

18. NASA Astronaut Anne McClain Accused by Spouse of Crime in Space. URL: https://www.nytimes.com/2019/08/23/us/astronaut-space-investigation.html (дата звернення 01.10.2022).

19. NSA Launches LPS Qubit Collaboratory. Press release. URL: https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/2570949/nsa-launches-lps-qubit-collaboratory (дата звернення 01.10.2022).

20. Papakonstantinou V., Hert P. Refusing to award legal personality to AI: Why the European Parliament got it wrong. *European Law Blog.* URL: https://europeanlawblog.eu/2020/11/25/refusing-to-award-legal-personality-to-ai-why-the-european-parliament-got-it-wrong (дата звернення 01.10.2022).

21. Practitioner's Guide to COMPAS Core. URL: https://s3.documentcloud.org/documents/2840784/Practitioner-s-Guide-to-COMPAS-Core.pdf (дата звернення 01.10.2022).

22. Proposal for a regulation of the European Parliament and of the Council «Laying down harmonised rules on artificial intelligence (Artificial intelligence act) and amending certain union legislative acts». URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1623335154975&uri=CELEX%3A52021PC0206 (дата звернення 01.10.2022).

23. Russia takes battle into space and targets GPS in Ukraine. URL: https://www.thetimes.co.uk/article/russia-takes-battle-into-space-and-targets-gps-in-ukraine-qzvkg6ljd (дата звернення 01.10.2022).

24. Russian cyber operations against Ukraine: Declaration by the High Representative on behalf of the European Union. *Council of the EU.* URL: https://www.consilium.europa.eu/en/press/press-releases/2022/05/10/russian-cyber-operations-against-ukraine-declaration-by-the-high-representative-on-behalf-of-the-european-union (дата звернення 01.10.2022).

25. Shimomura T., Markoff J. Takedown: the pursuit and capture of Kevin Mitnick, America's most wanted computer outlaws-by the man who did it. Hyperion Press, 1996. 336 p.

26. The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation. URL: https://img1.wsimg.com/blobby/go/3d82daa4-97fe-4096-9c6b-376b92c619de/downloads/MaliciousUseofAI.pdf?ver=1553030594217 (дата звернення 01.10.2022).

27. The Threat Report, Summer 2022. *Trellix Threat Labs*. URL: https://www.trellix.com/en-us/assets/docs/threat-reports/trellix-atr-report-summer-2022.pdf (дата звернення 01.10.2022).

28. Turing A.M. Computing Machinery and Intelligence. *Mind. A quarterly review of psychology and philosophy*. Vol. LIX. № 236 (October 1950). P. 433–460.

29. Андрій Кузміч: кількість кібератак з Росії за чотири місяці цього року майже сягнула показника за весь минулий рік. *Державна служба спеціального зв'язку та захисту інформації України.* URL: https://cip.gov.ua/ua/news/andrii-kuzmich-kilkist-kiberatak-z-rosiyi-za-chotiri-misyaci-cogo-maizhe-syagnula-pokaznika-za-ves-minulii-rik (дата звернення 01.10.2022).

30. Андрощук Г. Використання в ЄС штучного інтелекту потребує обмежень. *Юридична газета.* URL: https://yur-gazeta.com/golovna/vikoristannya-v-es-shtuchnogo-intelektu-potrebue-obmezhen.html (дата звернення 01.10.2022).

31. Антонян Ю.М. Еникеев М.И., Эминов В.Е. Психология преступления и наказания. М.: Пенатес-Пенаты, 2000. 454 с.

32. Ахтирська Н.М. Актуальні проблеми розслідування кіберзлочинів: навч. посіб. К.: ВПЦ «Київський університет», 2018. 229 с.

33. Ахтирська Н.М. Міжнародний досвід використання цифрової інформації у кримінальному судочинстві. *Юридичний науковий електронний журнал*. 2019. № 4. С. 221-224. URL: http://lsej.org.ua/4_2019/61.pdf (дата звернення 01.10.2022).

34. Ахтирська Н.М. Одержання доказів в електронній формі в світлі другого додаткового протоколу до конвенції про кіберзлочинність. *Криміналістика і судова експертиза*. 2022. Випуск 67. С. 188-200. URL:

https://digest.kndise.gov.ua/wp-content/uploads/2022/08/Akhtyrska67.pdf (дата звернення 01.10.2022).

35. Ахтирська Н.М., Неділько Я.В. Криміналістична характеристика: особа кіберзлочинця. *Юридичний науковий електронний журнал*. 2019. № 1. С. 171-175. URL: http://www.lsej.org.ua/1_2019/47.pdf (дата звернення 01.10.2022).

36. Бабенко О.О., Мокляк А.С. Теоретичний аналіз дослідження психологічного портрета кіберзлочинця. *Теорія і практика сучасної психології*. 2018. № 2. С. 89-93.

37. Баранов О.А. Інтернет речей (IoT): робот зі штучним інтелектом у правовідносинах. *Юридична Україна*. 2018. № 5-6. С. 75-95.

38. Батурин Ю. Проблемы компьютерного права. М.: Юридическая литература, 1991. 272 с.

39. Батурин Ю.М. Право и политика в компьютерном круге. Буржуазная демократия и "электронная диктатура" / Отв. ред. Шахназаров Г.Х. М.: Наука, 1987. 111 с.

40. Батурин Ю.М., Жодзишский А.М. Компьютерная преступность и компьютерная безопасность. М.: Юридическая литература, 1991. 160 с.

41. Бишевець О.В., Романенко Т.В. Особа злочинця як елемент криміналістичної характеристики шахрайств, що вчиняються в мережі Інтернет. *Вісник кримінального судочинства*. 2016. № 1. С. 81-87.

42. Біленчук П. Комп'ютерна психофізіологічна діагностика людини: правнича освіта, юридична наука і практика українського правосуддя. *Юридичний Вісник України*. 2018. № 9 (1182). С. 14-15.

43. Біленчук П., Малій М., Харитоненко І. Хакери, фрікери, кіберкрекери… Портрет сучасного професійного електронного кіберзловмисника. Ч. 2. *Юридичний Вісник України*. 2022. № 12-15. С. 16-17.

44. Біленчук П.Д. Електронна цивілізація: інноваційне майбутнє України: монографія / П.Д. Біленчук, М.М. Близнюк, О.Л. Кобилянський,

М.І. Малій, Ю.О. Пілюков, О.В. Соболєв; за заг. ред. П.Д. Біленчука. – К.: УкрДГРІ, 2018. 284 с.

45. Біленчук П.Д. Е-суспільство: цифрове майбутнє України. монографія / П.Д. Біленчук, О.Л. Кобилянський, М.І. Малій, та ін.; за заг ред. П.Д. Біленчука. 2-ге вид. переробл. Київ: УкрДГРІ, 2019. 292 с.

46. Біленчук П.Д. Конвергенція квантового майбутнього: правове, освітнє, наукове і ресурсне забезпечення. *Юридичний Вісник України*. 2018. № 42-43. С. 16-17.

47. Біленчук П.Д. Криміналістика нового тисячоліття. *Юридичний Вісник України*. 2017. № 46 (1167). С. 14-15.

48. Біленчук П.Д. Криміналістична характеристика портрета комп'ютерного злочинця. *Проблеми юридичної науки та правоохоронної практики*: збірник наукових праць. Київ: Українська академія внутрішніх справ, 1994. С. 260-262.

49. Біленчук П.Д. Криміналістична характеристика способів вчинення комп'ютерних злочинів. *Наукові розробки академії – удосконалення практичної діяльності та підготовки кадрів органів внутрішніх справ*. Київ, 1994. С. 216-218.

50. Біленчук П.Д. Криміналістичне дослідження обвинуваченого. К.: УАВС, 1995. 128 с.

51. Біленчук П.Д. Процесуальні та криміналістичні проблеми дослідження обвинуваченого (проблеми комплексного вивчення особи обвинуваченого в стадії попереднього слідства): монографія. Київ: Атіка, 1999. 352 с.

52. Біленчук П.Д. Стратегія інформаційної безпеки України: правові основи захисту інформації: монографія / П.Д. Біленчук, Л.В. Борисова, О.Л. Кобилянський, В.О. Собина. К.: Укр ДГРІ, 2018. 288 с.

53. Біленчук П.Д., Береський Я.О., Кобилянський О.Л., Малій М.І., Перелигіна Р.В. Конвергенція сонячного суспільства знань: креативна освіта і

цивілізаційний розвиток: монографія / за заг. ред. П.Д. Біленчука. К.: УкрДГРІ, 2019. 416 с.

54. Біленчук П.Д., Борисова Л.В., Кобилянський О.Л., Собина В.О. Стратегія інформаційної безпеки України: правові засади захисту інформації: монографія. К.: УкрДГРІ, 2018. 288 с.

55. Біленчук П.Д., Зубань М.А. Комп'ютерні злочини. Київ, 1994. 72 с.

56. Біленчук П.Д., Котляревський О.І. Портрет комп'ютерного злочинця: навчальний посібник. К.: В&В, 1997. 48 с.

57. Біленчук П.Д., Лихова С.Я., Малій М.І. Космічні й наземні кіберзагрози в сучасному електронному світі: системний асиметричний аналіз новітніх ноозасобів пізнання, доказування та розслідування. Ч. 1. *Юридичний Вісник України*. 2022. № 20-23. С. 18-19.

58. Біленчук П.Д., Лихова С.Я., Малій М.І. Космічні й наземні кіберзагрози в сучасному електронному світі: системний асиметричний аналіз новітніх ноозасобів пізнання, доказування та розслідування. Ч. 2. *Юридичний Вісник України*. 2022. № 20-23. С. 18-19.

59. Біленчук П.Д., Лихова С.Я., Малій М.І. Космічні кіберзагрози в третьому тисячолітті: наукове і правове пізнання. *50 років академічної науки на Закарпатті:* матеріали міжнародної конференції (м. Ужгород, 24-25 травня 2021 р.). / укладач: А.М. Завілопуло. Ужгород: Видавництво «ФОП Сабов А.М.», 2021. С. 283-286.

60. Біленчук П.Д., Лихова С.Я., Малій М.І. Шляхи реформування кримінальної кіберполіції на сучасному етапі цивілізаційного розвитку. *Шляхи реформування кримінальної поліції: вітчизняний та зарубіжний досвід*: матеріали Міжнар. наук.-практ. круглого столу (Київ, 18 лютого 2022 р.) / редкол.: В.В. Чернєй, С.Д. Гусарєв, С.С. Чернявський та ін. Київ: НАВС, 2022. С. 25-29.

61. Біленчук П.Д., Малій М.І. Карне електронне право Європи й України: порівняльний аналіз. Ч. 1. *Юридичний Вісник України*. 2021. № 8. С. 12-13.

62. Біленчук П.Д., Малій М.І. Карне електронне право Європи й України: порівняльний аналіз Ч. 2. *Юридичний Вісник України*. 2021. № 9. С. 11.

63. Біленчук П.Д., Малій М.І. Карне електронне право Європи й України: порівняльний аналіз Ч. 3. *Юридичний Вісник України*. 2021. № 10. С. 14-15.

64. Біленчук П.Д., Малій М.І. Кіберсвіт у новому тисячолітті. Хто вони: кіберзлочинці, кібершахраї, кібертерористи? *Юридичний Вісник України*. 2019. № 39. С. 14-15.

65. Біленчук П.Д., Малій М.І. Космічна і електронна кіберзлочинність третього тисячоліття: новітні виклики та загрози для людини, держави, цивілізації. *Бизнес и безопасность.* 2019. № 5. С. 18-21.

66. Біленчук П.Д., Малій М.І. Космічна й електронна кіберзлочинність: загрози і виклики нового тисячоліття. *Юридичний вісник України*. 2019. № 40. С. 14-15.

67. Біленчук П.Д., Малій М.І. Криміналістичне та судово-експертне забезпечення розвитку квантового майбутнього в третьому тисячолітті. *Актуальні проблеми криміналістики та судової експертології*: матеріали міжвідомчої науково-практичної конференції (м. Київ, 22 листопада 2018р.) / редкол.: В.В. Чернєй, С.Д. Гусарєв, С.С. Чернявський та ін. Київ: НАВС, 2018. С. 57-62.

68. Біленчук П.Д., Малій М.І. Міжнародно-правові і конституційні засади реалізації прав і свобод людини в Україні як контекст для розвитку кримінальної юстиції. *Проблеми підвищення ефективності кримінальної юстиції України:* колективна монографія / Інститут держави і права імені В.М. Корецького НАН України, Київський університет права НАН України; за заг. ред. Ю.С. Шемшученка, Ю.Л. Бошицького. Київ: Видавництво Ліра-К, 2021. С. 509-524.

69. Біленчук П.Д., Малій М.І. Планетарна електронна кіберзлочинність на шляху до сингулярності. *Злочинність і протидія їй в умовах сингулярності:*

тенденції та інновації: зб. тез доп. наук.-практ. конф., присвяч. пам'яті члена Правління Кримінологічної асоціації України, професора Тетяни Андріївни Денисової (м. Харків, 16 квітня 2021 р.). Харків, ХНУВС, 2021. С. 432-434.

70. Біленчук П.Д., Малій М.І. Портрет електронного зловмисника. *ООН – гарантування світового миропорядкування*: матеріали науково-практичної конференції ВНЗ «Київський університет ринкових відносин» (м. Київ, 20 жовтня 2020 р.). Київ: «Хай-Тек-Прес», 2021. С. 9-12.

71. Біленчук П.Д., Малій М.І. Пріоритетні напрями досліджень психологічного портрету електронного зловмисника. *Актуальні проблеми психологічного забезпечення службової діяльності працівників правоохоронних органів*: зб. тез Міжнар. наук.-практ. конф. (м. Київ, 30 жовтня 2020 р.). Київ: ДНДІ МВС України, 2020. С. 9-12.

72. Біленчук П.Д., Малій М.І. Сучасні комп'ютерні злочинці та кібертерористи: новітні технології на службі організованого злочинного світу. *Бизнес и безопасность*, 2019. № 4. С. 2-4.

73. Біленчук П.Д., Малій М.І., Колонюк В.П. Інноваційне науково-технологічне забезпечення правосуддя в еру асиметричної електронної трансформації. *Криміналістика і судова експертиза: Міжвідомчий науково-методичний збірник.КНДІСЕ Міністерства юстиції України*. Київ, 2021. Вип. 66. С. 70-80.

74. Біленчук П.Д., Малій М.І., Сватюк Н.І. Правове і наукове забезпечення міжзоряних польотів: електронний космічний всесвіт. *Юридичний Вісник України*. 2022. № 4. С. 12-13.

75. Біленчук П.Д., Малій М.І., Сватюк Н.І., Симканич О.І. Кібербезпека радіаційних випробувань космічних апаратів: правові засади, регламентні вимоги та стан їх інноваційного забезпечення. *Наукові праці Національного авіаційного університету. Серія: юридичний вісник «Повітряне і космічне право»*. 2020. № 4 (57). С. 156–162.

76. Біленчук П.Д., Перелигіна Р.В., Малій М.І. Кримінологічна характеристика особи комп'ютерного злочинця. *Кримінологічна теорія і*

практика: досвід, проблеми сьогодення та шляхи їх вирішення: матеріали міжвузів. наук.-практ. круглого столу (м. Київ, 22 березня 2019 р.) / редкол. В.В. Чернєй, С.Д. Гусарєв, С.С. Чернявський та ін. Київ, НАВС, 2019. С. 144–147.

77. Бірюк І. Кримінологічна характеристика особи кіберзлочинця. *Juvenia studia: Збірник студентських наукових праць*. Випуск 7. Чернігів: Видавець Лозовий В.М., 2017. С. 175-177.

78. Борисова Л.В. Суб'єкт (особа) транснаціонального комп'ютерного злочину: криміналістичні й психофізіологічні аспекти. *Актуальні проблеми держави і права.* 2008. Вип. 44. С. 76-81.

79. Борисова Л.В., Біленчук П.Д., Малій М.І., Виноградова В.С. Експертиза як засіб установлення фактів і обставин вчинення транснаціональних комп'ютерних злочинів. *Криміналістика і судова експертиза: Міжвідомчий науково-методичний збірник КНДІСЕ Міністерства юстиції України.* 2020. Вип. 65. С. 230-239.

80. Будник С. Ваша защита от вирусов в электронной почте. *Бизнес и безопасность*. 2003. № 1. С. 73.

81. Вехов В.Б. Компьютерные преступления: способы совершения и раскрытия. М., 1996. 182 с.

82. Виговський Д.Л. Використання термінів «особа злочинця» та «особистість злочинця» в кримінології. *Університетські наукові записки*. 2021. № 2 (80). С. 138-147.

83. Виговський Д.Л. До питання визначення суспільної небезпечності поширення норм кримінальної субкультури. *Теоретико-прикладні проблеми юридичної науки на сучасному етапі реформування кримінальної юстиції* (пам'яті В.П. Колгана): збірник тез Міжнародної науково-практичної конференції (м. Хмельницький, 27 травня 2022 року). Хмельницький: ХУУП імені Леоніда Юзькова, 2022. С. 48-49.

84. Виговський Д.Л., Нікіфорова Т.І. Окремі питання кримінологічного визначення поняття «жертва злочину». *Університетські наукові записки*. 2020. № 1 (73). С. 175-183.

85. Виговський Л.А, Виговська Т.В., Виговський Д.Л. Громадянське суспільство як чинник формування екологічної свідомості та культури людей. *Modern engineering and innovative technologies*. 2022. Issue 22. Part 2. С. 99-116.

86. Виговський Л.А. Постмодернізм як світоглядний чинник трансформації функціональності релігійного комплексу. *Релігія та Соціум*. 2015. № 3 (19). С. 40-49.

87. Власова О.В., Біленчук П.Д. Кримінологічна характеристика суб'єкта злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж. URL: https://www.crime-research.ru/articles/Vlasova0104/3 (дата звернення 25.04.2021).

88. Вопросы защиты информации. *Проблемы преступности в капиталистических странах*. М.: ВИНИТИ, 1987. № 10. С. 9-11.

89. Гавловський В.Д. Аналіз стану кіберзлочинності в Україні. *Інформація і право*. 2019. № 1. С. 108-117.

90. Гаврилишин Б. До ефективних суспільств. Дороговкази в майбутнє. К.: Пульсари, 2013. 248 с.

91. Головкін Б.М., Лисодєд О.В. Співвідношення понять «особа злочинця» та «особистість злочинця». *Кримінологічна теорія і практика: досвід, проблеми сьогодення та шляхи їх вирішення*. Ч. 1. С. 38-43. URL: http://elar.naiau.kiev.ua/jspui/handle/123456789/17717 (дата звернення 01.10.2022).

92. Гудков П.Б. Компьютерные преступления в сфере экономики. *Актуальные проблемы борьбы с коррупцией и организованной преступностью в сфере экономики*. М., 1995. С. 136-145.

93. Гузеева О.С. Предупреждение размещения информации, способствующей распространению наркотических средств, в российском

сегменте сети Интернет (криминологические и уголовно-правовые проблемы): автореф. дис. … канд. юрид. наук: 12.00.08. М., 2008. 25 с.

94. Давид Т. Мур. Критичне мислення та аналіз інформації / вступ О. Кучерак; пер. з англ. О. Кучерак. Івано-Франківськ: Місто НВ, 2022. 132 с.

95. Демура М.І. Міжнародний досвід використання алгоритмів штучного інтелекту у кримінальномупровадженні. *Використання технологій штучного інтелекту у протидії злочинності*: матеріали наук.-практ. онлайн-семінару (м. Харків, 5 листопада 2020 р.). Харків: Право, 2020. С. 24-28.

96. Денисов С.Ф. Особа злочинця у кримінологічній теорії України. *Вісник Кримінологічної асоціації України.* 2020. № 1 (22). С. 152-159.

97. Денисов С.Ф., Павлов В.Г. Штучний інтелект: теоретичні аспекти кримінальної відповідальності. *Злочинність і протидія їй в умовах сингулярності: тенденції та інновації*. 2021. С. 194–197. URL: http://dspace.univd.edu.ua/xmlui/bitstream/handle/123456789/10428/Shtuchnyi%20intelekt_Denysov_Pavlov_2021.pdf?sequence=1&isAllowed=y (дата звернення 01.10.2022).

98. Дзюндзюк В.Б., Дзюндзюк Б.В. Поява і розвиток кіберзлочинності. *Державне будівництво*. 2013. № 1. С. 1-12. URL: http://www.kbuapa.kharkov.ua/e-book/db/2013-1/doc/1/01.pdf (дата звернення 01.10.2022).

99. Доклад Генерального секретаря о работе Организации за 2021 год. (A/76/1, семдесят шестая сессия). Издание *Организация Обьединенных Наций*. URL: https://www.un.org/annualreport/2021/files/2021/09/2109745-R-ARWO21-WEB.pdf (дата звернення 01.10.2022).

100. Електронна цивілізація: інноваційне майбутнє України: монографія / П.Д. Біленчук, М.М. Близнюк, О.Л. Кобилянський, М.І. Малій, Ю.О. Пілюков, О.В. Соболєв; за заг. ред. П.Д. Біленчука. К.: УкрДГРІ, 2018. 284 с.

101. Електронне суспільство, електронне право, кібербезпека: стратегія розвитку інноваційної ери: монографія / П.Д. Біленчук, О.Л. Кобилянський,

М.І. Малій, Р.В. Перелигіна, Т.Ю. Тарасевич та ін.; за заг. ред. П.Д. Біленчука і Т.Ю. Тарасевич. Київ: УкрДГРІ, 2020. 388 с.

102. Європейська конвенція з прав людини. URL: https://www.echr.coe.int/documents/convention_ukr.pdf.

103. Єдиний звіт про кримінальні правопорушення по державі за 2016-2022 р.р. URL: https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogo-rozsliduvannya-2 (дата звернення 01.10.2022).

104. Загальна декларація прав людини прийнята і проголошена резолюцією 217 А (III) Генеральної Асамблеї ООН від 10 грудня 1948 р. URL: https://zakon.rada.gov.ua/laws/show/995_015#Text (дата звернення 01.10.2022).

105. Закалюк А.П. Курс сучасної української кримінології: теорія і практика: у 3 кн. Кн. 1: Теоретичні засади та історія української кримінологічної науки. К.: Видавничий дім «Ін Юре», 2007. 424 с.

106. Закон України «Про внесення змін до деяких законодавчих актів України щодо спрощення досудового розслідування окремих категорій кримінальних правопорушень» від 22 листопада 2018 р. URL: https://zakon.rada.gov.ua/laws/show/2617-19#Text (дата звернення 01.10.2022).

107. Закон України «Про електронні довірчі послуги» від 05 жовтня 2017 р. URL: https://zakon.rada.gov.ua/laws/show/2155-19#Text (дата звернення 01.10.2022).

108. Закон України «Про національну безпеку України» від 21 червня 2018 р. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text (дата звернення 01.10.2022).

109. Закон України «Про основні засади забезпечення кібербезпеки» від 05 жовтня 2017 р. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення 01.10.2022).

110. Закон України «Про ратифікацію Конвенції про кіберзлочинність» від 07 вересня 2005 р. URL: https://zakon.rada.gov.ua/laws/show/2824-15#Text (дата звернення 01.10.2022).

111. Звіт «Про склад засуджених за 2021 рік» (форма № 7). URL: https://court.gov.ua/inshe/sudova_statystyka/zvitnist_21 (дата звернення 01.10.2022).

112. Звіт Національної поліції України про результати роботи у 2021 р. URL: https://www.kmu.gov.ua/storage/app/sites/1/17-civik-2018/zvit2021/Zvit_NPU_2021_.pdf (дата звернення 01.10.2022).

113. Звіт роботи системи виявлення вразливостей і реагування на кіберінциденти та кібератаки, 2021. Оперативний центр реагування на кіберінциденти Державного центру кіберзахисту Державної служби спеціального зв'язку та захисту інформації. URL: https://cert.gov.ua/files/pdf/SOC_Annual_Report_2022.pdf (дата звернення 01.10.2022).

114. Зелинский А.Ф. Криминология: курс лекций. Харьков: Прапор, 1996. 260 с.

115. Зелинський А.Ф. Криминология: учебное пособие. Харьков: Рубикон, 2000. 238 с.

116. Зернецька О.В. Глобальна комунікація: монографія. К.: Наукова думка, 2017. 349 с.

117. Інтерв'ю з директором Інституту проблем штучного інтелекту. URL: https://bintel.org.ua/analytics/anatolii-shevchenko-intervyu-z-dyrektorom-instytutu-problem-shtuchnoho-intelektu (дата звернення 01.10.2022).

118. Інформаційні технології в державному управлінні. Ініціативи Президента України. *Інформаційно–бібліографічний бюлетень*. Випуск 08 (94). (огляд матеріалів ЗМІ за 1–31 серпня 2021 р.) URL: http://www.nbuviap.gov.ua/images/informaciyni_texnologii/2021/8.pdf (дата звернення 01.10.2022).

119. IT-право – це просто: посібник / за ред. д.ю.н., проф. Є.О. Харитонова. Одеса: Фенікс, 2017. 106 с.

120. IT-сфера в Україні. Законодавство. Судова практика. Коментар / за заг. ред. Т.В. Бачинського, Р.І. Радейко Київ: Юрінком Інтер, 2018. 360 с.

121. Калюга К. Історія походження криміналістичного поняття особи злочинця. *Підприємство, господарство та право*. 2016. № 12. С. 249-253.

122. Калюга К.В. Особи злочинця як обєкт криміналістичного дослідження: сучасний стан та перспективи розвитку: автореф. дис. … докт. юрид. наук: 12.00.09. Дніпро, 2021. 32 с.

123. Каткова Т.Г. Штучний інтелект в Україні: правові аспекти. *Право і суспільство*. 2020. № 6. С. 46–55.

124. Кіберполіція, СБУ та Держспецзв‘язку встановлюють причетних до кібератак на сайти державних структур URL: https://cyberpolice.gov.ua/news/kiberpolicziya-sbu-ta-derzhspeczzvyazku-vstanovlyuyut-prychetnyx-do-kiberatak-na-sajty-derzhavnyx-struktur-1630/ (дата звернення 01.10.2022).

125. Коваль О.Є. Психологічний портрет кіберзлочинця. *Україна в умовах реформування правової системи: сучасні реалії та міжнародний досвід*: матеріали ІІ Міжнар. наук.-практ. конф. (м. Тернопіль, 21-22 квітня 2017 р.). Тернопіль: Економічна думка, 2017. С. 189-192.

126. Комаров В.Г., Гусынин В.П., Гусынин А.В. Оптимизация управления выведением на орбиту многорежимной авиацыонно-космической системы с применением дифференциальных преобразований. *До 100-річчя від дня народження Генерального конструктора О.К. Антонова*: міжнародна науково-практична конференція (м. Київ, 06 лютого 2006 р.). К.: Видавн. центр «Холтех», 2008. С. 106–110.

127. Комп’ютерна вірусологія. *Комп’ютерний тероризм*: монографія / за ред. П.Д. Біленчука. К.: Наука і життя, 2008. 290 с.

128. Комп’ютерний тероризм: суперхакери, кібер-терористи, кібер-криміналісти: монографія / за заг. ред. П.Д. Біленчука. К.: Наука і життя, 2008. 292 с.

129. Компьютерные преступления в Великобритании. *Проблемы преступности в капиталистических странах*. М.: ВИНИТИ, 1988. № 3. С. 18-20.

130. Компьютерные преступления и обеспечение безопасности ЭВМ. *Проблемы преступности в капиталистических странах*. М., ВИНИТИ, 1983. № 6. С. 3-6.

131. Конвенція Ради Європи про кіберзлочинність. URL: http://zakon.rada.gov.ua/laws/show/994_575 (дата звернення 01.10.2022).

132. Конвергенція сонячного суспільства знань: креативна освіта і цивілізаційний розвиток: монографія / П.Д. Біленчук, Я.О. Береський, О.Л. Кобилянський, М.І. Малій, Р.В. Перелигіна; за заг. ред. П.Д. Біленчука. К.: УкрДГРІ, 2019. 416 с.

133. Кондратюк Л.В. Антропология преступления (микрокриминология). М.: Норма. 2001. 344 с.

134. Конституція України від 28 червня 1996 р. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text (дата звернення 01.10.2022).

135. Косік Ю. «Інтернет»-поліція - ваш захисник. *Столична міліція*. 2004. № 7. С. 36-37.

136. Костенко О.М., Перелигіна Р.В. Методологія і доктрина сучасної кримінології. К: КУП НАН України, 2016. 115 с.

137. Кравцова М. О., Литвинов О. М. Запобігання кіберзлочинності в Україні: монографія. Харків: Панов, 2016. 212 с.

138. Кравцова М.О. Сучасний стан і напрями протидії кіберзлочинності в Україні. *Вісник кримінологічної асоціації України*. 2018. № 2 (19). С. 155-166.

139. Краснопьоров П. Феномен Інтернет-субкультур: філософсько-антропологічний аналіз. *Схід*. 2016. № 2. С. 74-78.

140. Кримінальний кодекс України від 05 квітня 2001 року. URL: https://zakon.rada.gov.ua/laws/show/2341-14#n2491 (дата звернення 01.10.2022).

141. Кримінологія. Академічний курс / за заг. ред. О.М. Литвинова. Київ: Кондор, 2018. 588 с.

142. Кримінологія. Особлива частина: навчальний посібник для студентів юридичних спеціальностей вищих закладів освіти / І.М. Даньшин,

В.В. Голіна, О.Г. Кальман; за редакцією І.М. Даньшина. Харків: Право, 1999. 232с.

143. Кримінологія: Загальна та Особлива частини: підручник / І.М. Даньшин, В. В. Голіна, М. Ю. Валуйська та ін.; за заг. ред. В.В. Голіни. 2-ге вид. перероб. і доп. Х.: Право, 2009. 288 с.

144. Кримінологія: Загальна та Особлива частини: підручник / В.В. Голіна, Б.М. Головкін, М.Ю. Валуйська, О.В. Лисодєд та ін..; за ред. В.В. Голіни і Б.М. Головкіна. Х.: Право, 2014. 513 с.

145. Кримінологія: підручник / В.В. Голіна, Б.М. Головкін, М.Ю. Валуйська та ін.; за ред. В.В. Голіни, Б.М. Головкіна. Х.: Право, 2014. 440 с.

146. Кримінологія: підручник / за заг. ред. Л.С. Сміяна, Ю.В. Нікітіна. К.: Національна академія управління, 2010. 496 с.

147. Кримінологія: підручник / заг. ред. І.Г. Богатирьова, В.В. Топчія. Київ: В.Д. Дакор, 2018. 352 с.

148. Кримінологія: підручник / О.М. Джужа, В.В. Василевич, В.В. Чернєй, С.С. Чернявський та ін.; за заг. ред. д-ра юрид. наук, проф. В.В. Чернєя; за наук. ред. д-ра юрид. наук, проф. О.М. Джужі. Київ: Нац. акад. внутр. справ, 2020. 612 с.

149. Кримінологія: підручник. Практикум / Ю.В. Александров, П.Д. Біленчук, В.О. Валлє, А.П. Гель, В.С. Ковальський, О.М. Костенко, Р.В. Перелигіна, Г.С. Семаков. Київ: Юрінком Інтер, 2017. 344 с.

150. Крушинський С.А., Налуцишин В.В. Кримінологічна характеристика осіб, які вчиняють кримінальні правопорушення, пов’язані з рейдерством. *Європейські перспективи*. № 3. 2022. С. 48-55.

151. Куц В. Поняття злочинності. *Науковий часопис Національної академії прокуратури України*. 2016. № 2. С. 34-39.

152. Лихова С.Я., Біленчук П.Д. Космічні і наземні кіберзагрози третього тисячоліття: засоби пізнання, доказування, розслідування. *Наукові праці*

Національного авіаційного університету. Серія: Юридичний вісник «Повітряне і космічне право». 2021. Т. 2. № 59. С. 9-17.

153. Лукашевич В.Г., Калюга К.В. Щодо особи злочинця в нових умовах вчинення та розслідування злочинів із застосуванням інформаційних технологій. *Концептуальні проблеми розвитку сучасної гуманітарної та прикладної науки:* матеріали IV Всеукраїнського науково-практичного симпозіуму (м. Івано-Франківськ, 15 травня 2020 р.). Івано-Франківськ: Редакційно-видавничий відділ Університету Короля Данила, 2020. С. 202-206.

154. Малій М.І. Електронна кіберзлочинність як об'єкт кримінологічного дослідження. *Сучасне право в епоху соціальних змін*: матеріали XI Міжнародної науково-практичної конференції. (м. Київ, 26 лютого 2021 р.) Том. 1. Тернопіль: Вектор, 2021. С. 323-325.

155. Малій М.І. Інноваційні концепції застосування grid- і blockchain-технологій в юриспруденції. *Актуальні проблеми права України та Польщі:* монографія / Київський університет права НАН України; за заг. ред. проф. Ю.Л. Бошицького та проф. А. Шміта. Київ: Талком, 2020. С. 48-62.

156. Малій М.І. Міжнародний досвід запобігання і протидії корупції: системний аналіз діяльності Лі Куан Ю. *Реалізація державної антикорупційної політики в міжнародному вимірі*: матеріали V Міжнар. наук.-практ. конф. (м. Київ, 9–10 грудня 2020 р.): у 2 ч. Ч. 2. / редкол.: В.В. Чернєй, С.Д. Гусарєв, С.С. Чернявський та ін. Київ: Нац. акад. внутр. справ, 2020. С. 150-152.

157. Малій М.І. Правова відповідальність електронного інтелекту в новому тисячолітті. *Актуальні проблеми сучасної юридичної науки та практики*: матеріали круглого столу. Випуск 2 (м. Київ, 7 жовтня 2021 року). Київ: Видавництво Ліра-К, 2021. С. 40-54.

158. Малій М.І. Правовий статус саббота та відповідальність перед людством. *Економіка. Фінанси. Право.* 2022. № 8. С. 27-35.

159. Малій М.І. Міжнародні організації з протидії космічній кіберзлочинності. *AEPO-2019. Повітряне і космічне право:* матеріали

всеукраїнської конференції молодих учених і студентів (м. Київ, 21 листопада 2019 р.). Том.1. Тернопіль, Вектор. С. 216-218.

160. Меморандум про співробітництво між Національним авіаційними університетом та правничою компанією ТОВ «АЮР-КОНСАЛТИНГ» від 23 жовтня 2019 р.

161. Наказ Міністерства внутрішніх справ України «Про організацію діяльності Департаменту боротьби з кіберзлочинністю і торгівлею людьми МВС України та підрозділів боротьби з кіберзлочинністю і торгівлею людьми ГУМВС, УМВС» від 24 листопада 2010 р. № 581. URL: https://zakon.rada.gov.ua/rada/show/v0581320-10#Text (дата звернення 01.10.2022).

162. Наказ Національної поліції України «Про затвердження Положення про Департамент стратегічних розслідувань Національної поліції України» від 23 жовтня 2019 р. № 1077. URL: http://tranzit.ltd.ua/nakaz/files/%D0%9D%D0%B0%D0%BA%D0%B0%D0%B7%20%D0%9D%D0%9F%201077%20-%2023102019%20%D0%BF%D0%BE%D0%BB%D0%BE%D0%B6%D0%B5%D0%BD%D0%BD%D1%8F%20%D0%94%D0%A1%D0%A0.pdf (дата звернення 01.10.2022).

163. Наказ Міністерства внутрішніх справ України «Про затвердження Положення про підрозділи поліції особливого призначення «Корпус оперативно-раптової дії» від 26 листопада 2018 р. № 958. URL: https://zakon.rada.gov.ua/laws/show/z1436-18#Text (дата звернення 01.10.2022).

164. Налуцишин В.В., Крушинський С.А. Комп'ютерна злочинність: кримінально-правовий та кримінологічний аспект (досвід держав Європейського Союзу). *Юридичний науковий електронний журнал*. 2022. № 8. С. 445-449.

165. Некоторые аспекты компьютерной преступности. *Проблемы преступности в капиталистических странах*. М.: ВИНИТИ, 1990. № 6. С. 12-13.

166. Паламарчук Л.П. Криміналістичне забезпечення розслідування незаконного втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж: дис. канд. юрид. наук: 12.00.09. Київ, 2004. 215 с.

167. Перший щорічний звіт за результатами роботи системи виявлення вразливостей і реагування на кіберінциденти та кібератаки. URL: https://cert.gov.ua/article/17696 (дата звернення 01.10.2022).

168. Піцик Ю.М. Аналіз особистості кіберзлочинця, який вчиняє злочини проти власності у кіберпросторі. *Науковий вісник Міжнародного гуманітарного університету. Серія «Юриспруденція».* 2017. № 26. С. 105-107.

169. Плахотнік О.В. Практичне застосування штучного інтелекту у кримінальному провадженні. *Вісник кримінального судочинства*. 2019. № 4. С. 46-57.

170. Подгаєцький О. Еволюція розробок у галузі штучного інтелекту в Україні та світі. *Дослідження з історії техніки: збірник наукових праць*. 2012. Вип. 16. С. 48–54.

171. Подольный Н.А. Криминалистическая характеристика личности мошенника, совершающего преступную деятельность на рынке ценных бумаг. *Следователь*. 2002. № 5. С. 31–34.

172. Політті А. Злочинність у сфері інформатики і відмивання грошей. Нові трансформаційні ризики і європейська безпека. К., 1997. С. 22-23.

173. Правова соціалізація особистості в сучасному світі: людина, суспільство, цивілізація: монографія / за заг. ред. П.Д. Біленчука. К.: УкрДГРІ, 2020. 204 с.

174. Правовая информатика и кибернетика: учебник / Атанесян Г.А., Гаврилов О.А., Дери П., Каблуков А.Г., и др.; под ред. Полевой Н.С. М.: Юрид. лит., 1993. 528 с.

175. Радутний О.Е. Artificial Intelligence (штучний інтелект) та інші загрози (кримінально-правовий вимір). *ІТ-право: проблеми і перспективи розвитку в Україні*: матеріали ІІ Міжнародної науково-практичної кнференції

(м. Львів. 17 листопада 2017 р.). URL: https://www.academia.edu/34972216/Artificial_Intelligence_штучний_інтелект_та_інші_загрози_кримінально_правовий_вимір (дата звернення 01.10.2022).

176. Радутний О.Е. Кримінальна відповідальність штучного інтелекту. *Інформація і право*. 2017. № 2 (21). С. 124-132.

177. Различные аспекты компьютерной преступности. *Проблемы преступности в капиталистических странах*. М.: ВИНИТИ, 1987. №3. С. 16-19.

178. Расширение масштабов компьютерной преступности. *Проблемы преступности в капиталистических странах*. М.: ВИНИТИ, 1986. № 10. С. 9-11.

179. Резолюция Генеральной Асамблеи ООН «Противодействие использованию информационно-комуникационных технологий в преступных целях» принятая 17 декабря 2018 г. URL: https://documents-dds-ny.un.org/doc/UNDOC/GEN/N18/450/56/PDF/N1845056.pdf?OpenElement (дата звернення 01.10.2022).

180. Риков В.В. Штучний інтелект на допомогу правосуддю: дотримання прав людини. *Вища школа адвокатури НААУ*. URL: https://www.hsa.org.ua/blog/shtuchnyj-intelekt-na-dopomogu-pravosuddyu-dotrymannya-prav-lyudyny (дата звернення 01.10.2022).

181. Розпорядження Кабінету Міністрів України «Про схвалення Концепції розвитку штучного інтелекту в Україні» від 02 грудня 2020 р. № 1556-р. URL: https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text (дата звернення 01.10.2022).

182. Салтевский М.В. Следы человека и приемы их использования для получения информации о преступнике и обстоятельствах преступления: лекция. Киев: НИиРИО КВШ МВД СССР, 1983. 44 с.

183. Салтевський М.В. Основи методики розслідування злочинів, скоєних з використанням ЕОМ: навч. посібник. Харків: Нац. юрид акад. України. 2000. 35 с.

184. Совершено первое преступление в космосе? URL: https://cripo.com.ua/scandals/soversheno-pervoe-prestuplenie-v-kosmose (дата звернення 01.10.2022).

185. Сопілко І.М., Лихова С.Я., Біленчук П.Д. Космічний кіберзлочин як загроза національній безпеці України: матеріали XV міжнародної науково-технічної конференції «АВІА-2021». К.: НАУ, 2021. С. 14–31.

186. Соснін О. Ідеологія «суспільства знань»: нові завдання освіти і науки. *Юридичний Вісник України*. 2017. № 17. С. 12-13.

187. Старіш О.Г. Системологія: підручник. Київ, ЦУЛ, 2005. 232 с.

188. Титаренко А.В. Особа кіберзлочинця як елемент криміналістичної характеристики. *Журнал східноєвропейського права*. 2019. № 62. С. 159-168.

189. Ткачова О.В., Науменко К.В. Кримінологічна характеристика кіберзлочинця. *Юридичний науковий електронний журнал.* 2018. № 2. С. 200-204 (дата звернення 02.03.2021).

190. Туз Т.В. Перспективи встановлення кримінальної відповідальності внаслідок використання штучного інтелекту. URL: http://dspace.onua.edu.ua/bitstream/handle/11300/10461/15_%D0%A2%D1%83%D0%B7_140-142.pdf?sequence=1&isAllowed=y (дата звернення 01.10.2022).

191. У Китаї створили квантові комп'ютери в 10 млн разів потужніші за будь-який суперкомп'ютер. URL: https://focus.ua/uk/digital/496363-v-kitae-sozdali-kvantovye-kompyutery-v-10-mln-raz-moshchnee-lyubogo-superkompyutera-video (дата звернення 01.10.2022).

192. У ФРН запустили найпотужніший квантовий комп'ютер у Європі. URL: https://www.dw.com/uk/u-nimechchyni-zapustyly-naipotuzhnishyi-kvantovyi-kompiuter-u-yevropi/a-57908012 (дата звернення 01.10.2022).

193. Угода про асоціацію України з Європейським Союзом від 27 червня 2014 р. URL: https://www.kmu.gov.ua/diyalnist/yevropejska-integraciya/ugoda-pro-asociacyu (дата звернення 01.10.2022).

194. Указ Президента України «Про заходи щодо розвитку національної складової глобальної інформаційної мережі інтернет та забезпечення

широкого доступу до цієї мережі в Україні» від 31 липня 2000 р. URL: https://zakon.rada.gov.ua/laws/show/928/2000#Text (дата звернення 01.10.2022).

195. Указ Президента України «Про рішення Ради національної безпеки і оборони України» від 06 травня 2015 року «Про Стратегію національної безпеки України» від 26 травня 2015 р. № 287/2015. URL: https://zakon.rada.gov.ua/laws/show/287/2015#Text (дата звернення 01.10.2022).

196. Українська делегація вперше взяла участь у засіданні Керівного комітету Об'єднаного центру передових технологій з кібероборони НАТО (CCDCOE). *Рада національної безпеки і оборони України*. URL: https://www.rnbo.gov.ua/ua/Diialnist/5502.html (дата звернення 01.10.2022).

197. Фигурнов В.Э. IBM PC для пользователя. М: Финансы и статистика, 1997. 283 с.

198. Хананашвили М.М. Информационные неврозы. М.: Медицина, 1986. 310 с.

199. Харарі Ю.Н. Homo Deus. За лаштунками майбутнього / пер. з англ. О. Дем'янчука. К.: Форс Україна, 2018. 512 с.

200. Харарі Ю.Н. Людина розумна. Історія людства від минулого до майбутнього. Харків: Клуб сімейного дозвілля, 2016. 544 с.

201. Харитоненко І.О., Біленчук П.Д. Проблематика забезпечення кіберзахисту в сучасних умовах. *Збірник наукових праць «Права людини: історія та сучасність»*: матеріали V науково-практичної конференції. Київ: Університет «Україна», 2021. С. 236–240.

202. Харитонов Є.О., Харитонова О.І. До проблеми цивільної правосуб'єктності роботів. *Інтернет речей: проблеми правового регулювання та впровадження*: матеріали наук.-практ. конф. (м. Київ, 29 листопада 2018 р.) / упоряд. В.М. Фурашев, С.О. Дорогих. Київ: Вид-во "Політехніка", 2018. С. 42-46.

203. Чаплинська Ю.А. Особа злочинця як елемент криміналістичної характеристики злочинів. *Актуальні проблеми вітчизняної юриспруденції*. 2019. № 6. С. 181-184.

204. Чванкін С. Поширення порнографії може обійтись порушникам лише у 850 грн. штрафу. URL: https://zib.com.ua/ua/119942-poshirennya_pornografii_mozhe_obiytis_porushnikam_lishe_u_85.html (дата звернення: 19.11.2020).

205. Черкасов В.Н. Теория и практика решения организационно-методических проблем борьбы с экономической преступностью в условиях применения компьютерных технологий. М., 2004. 113 с.

206. Шавалюк Л. Давос, глобальний контекст. Про головні ідеї щорічної зустрічі світового економічного форуму. Український тиждень. 2018. № 5 (533). С. 8.

207. Шваб К. Четверта промислова революція. Формуючи четверту промислову революцію. Харків. Клуб сімейного дозвілля, 2019. 416 с.

208. Шваб К. Четвертая промышленная революция. М.: Эксмо, 2016. 136 с.

209. Шмідт Е., Коен Дж. Новий цифровий світ / переклад з англ. Г. Лелів. Львів: Літопис, 2015. 368 с.

210. Щодо проєкту Стратегії розвитку штучного інтелекту в Україні на 2022–2030 рр. *Artificial Intelligence.* 2022. № 1. С. 75-155. URL: https://www.slyusar.kiev.ua/AI_2022-1-1_ua.pdf (дата звернення: 19.11.2020).

211. Ярошовець В.І. Історія філософії: від структуролізму до постмодернізму: підручник. К.: Знання України, 2004. 214 с.

212. Яценко Я.С., Ісмайлов К.Ю. Деякі сучасні тенденції кіберзлочинності. *Актуальні задачі та досягнення у галузі кібербезпеки*: матеріали Всеукр. наук.-практ. конф. (м. Кропивницький, 23–25 листопада 2016 р.) / відп. за вип.: О.П. Доренський. Кропивницький: КНТУ, 2016. С. 54-55.

ДОДАТКИ

Додаток А

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

в яких опубліковані основні наукові результати дисертації:

1. Малій М.І. Інноваційні концепції застосування grid- і blockchain-технологій в юриспруденції. *Актуальні проблеми права України та Польщі:* монографія / Київський університет права НАН України; за заг. ред. проф. Ю.Л. Бошицького та проф. А. Шміта. Київ: Талком, 2020. С. 48-62. URL: http://kul.kiev.ua/images/A/25/Monografia/Polska_monografia_2020.pdf.

2. Малій М.І. Правовий статус саббота та відповідальність перед людством. *Економіка. Фінанси. Право.* 2022. № 8. С. 27-35. http://efp.in.ua/uk/journal-item/335 (DOI: https://doi.org/10.37634/efp.2022.8.6).

3. Борисова Л.В., Біленчук П.Д., Малій М.І., Виноградова В.С. Експертиза як засіб установлення фактів і обставин вчинення транснаціональних комп'ютерних злочинів. *Криміналістика і судова експертиза*. 2020. Вип. 65. С. 230-239. https://digest.kndise.gov.ua/wp-content/uploads/2020/06/Криміналістика_65_друк_новий-230-239.pdf (DOI: https://doi.org/10.33994/kndise.2020.65.22).

4. Біленчук П.Д., Малій М.І., Сватюк Н.І., Симканич О.І. Кібербезпека радіаційних випробувань космічних апаратів: правові засади, регламентні вимоги та стан їх інноваційного забезпечення. *Наукові праці Національного авіаційного університету. Серія: Юридичний вісник* «*Повітряне і космічне право*». 2020. № 4 (57). С. 156-162. http://www.law.nau.edu.ua/images/Nauka/Naukovij_jurnal/2020/4-57/24.pdf (DOI: 10.18372/2307-9061.57.15079).

5. Біленчук П.Д., Малій М.І., Колонюк В.П. Інноваційне науково-технологічне забезпечення правосуддя в еру асиметричної електронної

трансформації. *Криміналістика і судова експертиза.* 2021. Вип. 66. С. 70-80. https://digest.kndise.gov.ua/wp-content/uploads/2021/04/Bilenchuk.pdf (DOI: https://doi.org/10.33994/kndise.2021.66.08).

які засвідчують апробацію матеріалів дисертації:

6. Малій М.І. Міжнародні організації з протидії космічній кіберзлочинності. *АЕРО-2019. Повітряне і космічне право:* матеріали всеукраїнської конференції молодих учених і студентів (м. Київ, Національний авіаційний університет, 21 листопада 2019 р.). Том. 1. Тернопіль: Вектор, 2019. С. 216-218.

7. Малій М.І. Особливості кримінолого-криміналістичної характеристики особи електронного зловмисника. *Актуальні проблеми сучасної юридичної науки та практики:* матеріали круглого столу (м. Київ, 1 жовтня 2020 року). Київський університет права НАН України. Київ, Видавництво Ліра-К, 2020. С. 40-45.

8. Малій М.І. Міжнародний досвід запобігання і протидії корупції: системний аналіз діяльності ЛІ КУАН Ю. *Реалізація державної антикорупційної політики в міжнародному вимірі*: матеріали V Міжнар. наук.-практ. конф. (Київ, 9–10 грудня 2020 р.): у 2 ч. / [редкол.: В. В. Чернєй, С. Д. Гусарєв, С. С. Чернявський та ін.]. Київ, Нац. акад. внутр. справ, 2020. Ч. 2. С. 150-152.

9. Малій М.І. Електронна кіберзлочинність як об’єкт кримінологічного дослідження. *Сучасне право в епоху соціальних змін*: матеріали XI Міжнародної науково-практичної конференції. (м. Київ, Національний авіаційний університет, 26 лютого 2021 р.) Том. 1. Тернопіль: Вектор, 2021. С. 323-325.

10. Малій М.І. Правова відповідальність електронного інтелекту в новому тисячолітті. *Актуальні проблеми сучасної юридичної науки та практики.* Випуск 2: матеріали круглого столу (Київ, 7 жовтня 2021 р.). Київ: Видавництво Ліра-К, 2021. С. 40-54.

11. Біленчук П.Д., Лихова С.Я., Малій М.І. Космічні кіберзагрози в третьому тисячолітті: наукове і правове пізнання. *50 років академічної науки на Закарпатті*: матеріали міжнародної конференції (м. Ужгород, 24-25 травня 2021 року). Укладач: А.М. Завілопуло, д.ф.-м.н. Інститут електронної фізики НАН України. Ужгород, Видавництво «ФОП Сабов А.М.», 2021. С. 283-286.

12. Біленчук П.Д., Близнюк М.М., Кобилянський О.Л., Малій М.І., Пілюков Ю.О., Соболєв О.В. Електронна цивілізація: інноваційне майбутнє України: монографія / за заг. ред. П.Д. Біленчука. Київ: УкрДГРІ, 2018. 284 с.

13. Біленчук П.Д., Кобилянський О.Л., Ковальчук Ю.І., Копчук І.В., Малій М.І., Моргунов С.А., Соболєв О.В., Тимощук С.В. та ін. Е-СУСПІЛЬСТВО: цифрове майбутнє України: монографія / за заг. ред. П.Д. Біленчука. 2-е вид., допов. і переробл. Київ: УкрДГРІ, 2019. 292 с.

14. Біленчук П.Д., Береський Я.О., Кобилянський О.Л., Малій М.І., Перелигіна Р.В. Конвергенція сонячного суспільства знань: креативна освіта і цивілізаційний розвиток: монографія / за заг. ред. П.Д. Біленчука. Київ: УкрДГРІ, 2019. 416 с.

15. Біленчук П.Д., Кобилянський О.Л., Малій М.І. та ін. Правова соціалізація особистості в сучасному світі: людина, суспільство, цивілізація: монографія / за заг. ред. П.Д. Біленчука. Київ: УкрДГРІ, 2020. 204 с.

16. Біленчук П.Д., Кобилянський О.Л., Малій М.І., Перелигіна Р.В., Тарасевич Т.Ю. та ін. Електронне суспільство, електронне право, кібербезпека: стратегія розвитку інноваційної ери: монографія / за заг. ред. П.Д. Біленчука і Т.Ю. Тарасевич. Київ: УкрДГРІ, 2020. 388 с.

17. Біленчук П.Д., Перелигіна Р.В., Малій М.І. Кримінологічна характеристика особи комп'ютерного злочинця. *Кримінологічна теорія і практика: досвід, проблеми сьогодення та шляхи їх вирішення*: матеріали міжвузів. наук.-практ. круглого столу (м. Київ, 22 березня 2019 р.) [редкол. В.В. Чернєй, С.Д. Гусарєв, С.С. Чернявський та ін.]. Київ, Нац.акад.внутр.справ, 2019. С. 144-147.

18. Біленчук П.Д., Малій М.І. Сучасні комп'ютерні злочинці та кібертерористи: новітні технології на службі організованого злочинного світу. *Бизнес и безопасность*. 2019. № 4. С. 2-4.

19. Біленчук П.Д., Малій М.І. Космічна і електронна кіберзлочинність третього тисячоліття: новітні виклики та загрози для людини, держави, цивілізації. *Бизнес и безопасность*. 2019. № 5. С. 18-21.

20. Біленчук П.Д., Малій М.І. Портрет електронного зловмисника. *ООН – гарантування світового мировпорядкування:* матеріали Всеукраїнської науково-практичної конференції ВНЗ «Київський університет ринкових відносин» (м. Київ, 28 жовтня 2020 р.). Київ, «Хай-Тек Прес», 2021. С. 9-12.

21. Біленчук П.Д., Малій М.І. Пріоритетні напрями досліджень психологічного портрету електронного зловмисника. *Актуальні проблеми психологічного забезпечення службової діяльності працівників правоохоронних органів:* зб. тез Міжнар. наук.-практ. конф. (м. Київ, 30 жовтня 2020 р.). Київ, ДНДІ МВС України, 2020. С. 79-81.

22. Біленчук П.Д., Малій М.І. Космічна кіберзлочинність електронної ери асиметричної трансформації. *Актуальні проблеми кримінального права, процесу, криміналістики та оперативно-розшукової діяльності:* тези IV Всеукраїнської науково-практичної конференції (Хмельницький, 26 лютого 2021 р.). Хмельницький, Вид-во НАДПСУ, 2021. С. 337-340.

23. Біленчук П.Д., Малій М.І. Планетарна електронна кіберзлочинність на шляху до сингулярності. *Злочинність і протидія їй в умовах сингулярності: тенденції та інновації*: зб. тез доп. наук.-практ. конф., присвяч. пам'яті члена Правління Кримінологічної асоціації України, професора Тетяни Андріївни Денисової (м. Харків, 16 квіт. 2021 р.) / МВС України, Харків. нац. ун-т внутр. справ, Кримінол. асоц. України. Харків, ХНУВС, 2021. С. 432-434.

які додатково відображають результати дисертації:

24. Malii M. Prevention of computer crimes electronic intelligence against human, society, state. *Visegrad Journal on Human Rights*. 2021. № 4. С. 143-150.

25. Біленчук П.Д., Малій М.І. Міжнародно-правові і конституційні засади реалізації прав і свобод людини в Україні як контекст для розвитку кримінальної юстиції. *Проблеми підвищення ефективності кримінальної юстиції України:* колективна монографія / Інститут держави і права імені В.М. Корецького НАН України, Київський університет права НАН України; за заг. ред. Ю.С. Шемшученка, Ю.Л. Бошицького. Київ: Видавництво Ліра-К, 2021. С. 509-523.

Додаток Б

НАЦІОНАЛЬНА ПОЛІЦІЯ УКРАЇНИ
ДЕПАРТАМЕНТ КІБЕРПОЛІЦІЇ
ВІДДІЛ ПРОТИДІЇ КІБРЗЛОЧИНАМ В ХМЕЛЬНИЦЬКІЙ ОБЛАСТІ

вул. Зарічанська 7, м. Хмельницький, 29000, hm@cyberpolice.gov.ua

14.10.2022 №2475/38/121 – 2022

АКТ

про впровадження результатів дисертаційного дослідження Малія Миколи Івановича на тему: «Особа комп'ютерного злочинця як об'єкт кримінологічного дослідження» у практичну діяльність

Комісія у складі: начальника відділу протидії кіберзлочинам в Хмельницькій області Департаменту кіберполіції Національної поліції України Олега ДЯДИКА, заступника начальника відділу протидії кіберзлочинам в Хмельницькій області Департаменту кіберполіції Національної поліції України Артура ДЕРЕНОВСЬКОГО

склала цей акт про те, що матеріали дисертації Малія Миколи Івановича «Особа комп'ютерного злочинця як об'єкт кримінологічного дослідження» за різними напрямами правоохоронної діяльності можуть бути використані при участі у слідчих (розшукових) діях з метою підвищення ефективності залучення працівників як спеціалістів для участі в проведенні, а також під час проведення занять у системі службової підготовки.

Окрім цього результати дисертації М.І. Малія можуть бути використані при проведенні наукової діяльності працівниками, підготовки навчальних та практичних видань та

Результати дисертаційного дослідження знайшли своє відображення в багатьох навчально-практичних, довідкових та інших матеріалах для практичних працівників, серед яких рекомендованими є такі публікації та розробки:

1. Малій М.І. Інноваційні концепції застосування grid- і blockchain-технологій в юриспруденції. *Актуальні проблеми права України та Польщі:* монографія / Київський університет права НАН України; за заг. ред. проф. Ю.Л. Бошицького та проф. А. Шміта. Київ: Талком, 2020. С.48-62.
2. Малій М.І. Правовий статус саббота та відповідальність перед людством. *Економіка. Фінанси. Право.* 2022. №8. С.27-35.
3. Борисова Л.В., Біленчук П.Д., Малій М.І., Виноградова В.С. Експертиза як засіб установлення фактів і обставин вчинення транснаціональних комп'ютерних злочинів. *Криміналістика і судова експертиза: Міжвідомчий науково-методичний збірник. КНДІСЕ*

Міністерства юстиції України. Київ, 2020. Вип. 65. С.230-239. (DOI: https://doi.org/10.33994/kndise.2020.65.22)

4. Біленчук П.Д., Малій М.І., Сватюк Н.І., Симканич О.І. Кібербезпека радіаційних випробувань космічних апаратів: правові засади, регламентні вимоги та стан їх інноваційного забезпечення. *Наукові праці Національного авіаційного університету. Серія: Юридичний вісник «Повітряне і космічне право».* Київ: НАУ, 2020. №4(57). 204с. С. 156–162. (DOI: 10.18372/2307-9061.57.15079)

5. Біленчук П.Д., Малій М.І., Колонюк В.П. Інноваційне науково-технологічне забезпечення правосуддя в еру асиметричної електронної трансформації. *Криміналістика і судова експертиза: Міжвідомчий науково-методичний збірник. КНДІСЕ Міністерства юстиції України.* Київ, 2021. Вип. 66. С.70-80. (DOI: https://doi.org/10.33994/kndise.2021.66.08)

6. Малій М.І. Міжнародні організації з протидії космічній кіберзлочинності. *АЕРО-2019. Повітряне і космічне право:* матеріали всеукраїнської конференції молодих учених і студентів (м. Київ, Національний авіаційний університет, 21 листопада 2019 р.). Том.1.Тернопіль, Вектор. С.216-218.

7. Малій М.І. Особливості кримінолого-криміналістичної характеристики особи електронного зловмисника. *Актуальні проблеми сучасної юридичної науки та практики:* матеріали круглого столу (м. Київ, 1 жовтня 2020 року). Київський університет права НАН України. Київ, Видавництво Ліра-К, 2020.172с. С.40-45.

8. Малій М.І. Міжнародний досвід запобігання і протидії корупції: системний аналіз діяльності ЛІ КУАН Ю. *Реалізація державної антикорупційної політики в міжнародному вимірі:* матеріали V Міжнар. наук.- практ. конф. (Київ, 9–10 груд. 2020 р.): у 2 ч. / [редкол.: В. В. Чернєй, С. Д. Гусарєв, С. С. Чернявський та ін.]. Київ, Нац. акад. внутр. справ, 2020. Ч. 2. 395 с. С.150-152.

9. Малій М.І. Електронна кіберзлочинність як об'єкт кримінологічного дослідження. *Сучасне право в епоху соціальних змін:* матеріали XI Міжнародної науково-практичної конференції. (м. Київ, Національний авіаційний університет, 26 лютого 2021 р.) Том.1. Тернопіль, Вектор, 2021. 368с. С.323-325.

10. Малій М.І. Правова відповідальність електронного інтелекту в новому тисячолітті. *Актуальні проблеми сучасної юридичної науки та практики.* Випуск 2: матеріали круглого столу (Київ, 7 жовт. 2021 р.). Київ: Видавництво Ліра-К, 2021. С.40-54.

11. Біленчук П.Д., Лихова С.Я., Малій М.І. Космічні кіберзагрози в третьому тисячолітті: наукове і правове пізнання. *50 років академічної науки на Закарпатті:* матеріали міжнародної конференції (м. Ужгород, 24-25 травня 2021 року). Укладач: А.М. Завілопуло, д.ф.-м.н. Інститут електронної фізики НАН України. Ужгород, Видавництво «ФОП Сабов А.М.», 2021. 288с. С.283-286.

12. Біленчук П.Д., Близнюк М.М., Кобилянський О.Л., Малій М.І., Пілюков Ю.О., Соболєв О.В. Електронна цивілізація: інноваційне майбутнє України: монографія / за заг. ред. П.Д. Біленчука. Київ: УкрДГРІ, 2018. 284 с.

13. Біленчук П.Д., Кобилянський О.Л., Ковальчук Ю.І., Копчук І.В., Малій М.І., Моргунов С.А., Соболєв О.В., Тимощук С.В. та ін. Е-СУСПІЛЬСТВО: цифрове майбутнє України: монографія / за заг. ред. П.Д. Біленчука. 2-е вид., допов. і переробл. Київ: УкрДГРІ, 2019. 292 с.

14. Біленчук П.Д., Береський Я.О., Кобилянський О.Л., Малій М.І., Перелигіна Р.В. Конвергенція сонячного суспільства знань: креативна освіта і цивілізаційний розвиток: монографія / за заг. ред. П.Д. Біленчука. Київ: УкрДГРІ, 2019. 416с.

15. Біленчук П.Д., Кобилянський О.Л., Малій М.І. та ін. Правова соціалізація особистості в сучасному світі: людина, суспільство, цивілізація: монографія / за заг. ред. П.Д. Біленчука. Київ: УкрДГРІ, 2020. 204 с.

16. Біленчук П.Д., Кобилянський О.Л., Малій М.І., Перелигіна Р.В., Тарасевич Т.Ю. та ін. ЕЛЕКТРОННЕ СУСПІЛЬСТВО, ЕЛЕКТРОННЕ ПРАВО, КІБЕРБЕЗПЕКА: стратегія розвитку інноваційної ери: монографія / за заг. ред. П.Д. Біленчука і Т.Ю. Тарасевич. Київ: УкрДГРІ, 2020. 388 с.

17. П.Д. Біленчук, Р.В. Перелигіна, М.І. Малій Криміногічна характеристика особи комп'ютерного злочинця. *Криміногічна теорія і практика: досвід, проблеми сьогодення та шляхи їх вирішення:* матеріали міжвузів. наук.-практ. Круглого столу (Київ, 22 березня 2019 р.) [редкол. В.В. Чернєй, С.Д. Гусарєв, С.С. Чернявський та ін.]. Київ, Нац.акад.внутр.справ, 2019. С.144-147.

18. Біленчук П.Д., Малій М.І. Сучасні комп'ютерні злочинці та кібертерористи: новітні технології на службі організованого злочинного світу / *«Бизнес и безопасность»*, 2019. №4. С.2-4.

19. Біленчук П.Д., Малій М.І. Космічна і електронна кіберзлочинність третього тисячоліття: новітні виклики та загрози для людини, держави, цивілізації / *«Бизнес и безопасность»*, 2019. №5. С.18-21.

20. Біленчук П.Д., Малій М.І. Портрет електронного зловмисника. *ООН – гарантування світового мировпорядкування:* матеріали Всеукраїнської науково-практичної конференції ВНЗ «Київський університет ринкових відносин» (м. Київ, 28 жовтня 2020 року). Київ, «Хай-Тек Прес», 2021. 96 с. С.9-12.

21. Біленчук П.Д., Малій М.І. Пріоритетні напрями досліджень психологічного портрету електронного зловмисника. *Актуальні проблеми психологічного забезпечення службової діяльності працівників правоохоронних органів:* зб.тез Міжнар. наук.-практ. конф. (м. Київ, 30 жовтня 2020 р.). Київ, ДНДІ МВС України, 2020. 267 с. С.79-81.

22. Біленчук П.Д., Малій М.І. Космічна кіберзлочинність електронної ери асиметричної трансформації. *Актуальні проблеми кримінального права, процесу, криміналістики та оперативно-розшукової діяльності:* тези IV Всеукраїнської науково-практичної конференції (Хмельницький, 26 лютого 2021 року). Хмельницький, Вид-во НАДПСУ, 2021. 756 с. С.337-340.

23. Біленчук П.Д., Малій М.І. Планетарна електронна кіберзлочинність на шляху до сингулярності. *Злочинність і протидія їй в умовах сингулярності: тенденції та інновації:* зб. тез доп. наук.-практ. конф., присвяч. пам'яті члена Правління Кримінологічної асоціації України, професора Тетяни Андріївни Денисової (м. Харків, 16 квіт. 2021 р.) / МВС України, Харків. нац. ун-т внутр. Справ, Кримінол. асоц. України. Харків, ХНУВС, 2021. 464 с. С.432-434.

24. Malii Mykola Prevention of computer crimes electronic intelligence against human, society, state // Visegrad Journal on Human Rights. Bratislava, № 4. 2021. С.143-150.

25. Біленчук П.Д., Малій М.І. Міжнародно-правові і конституційні засади реалізації прав і свобод людини в Україні як контекст для розвитку кримінальної юстиції. *Проблеми підвищення ефективності кримінальної юстиції України:* колективна монографія / Інститут держави і права імені В.М. Корецького НАН України, Київський університет права НАН України; за заг. ред. Ю.С. Шемшученка, Ю.Л. Бошицького. Київ: Видавництво Ліра-К, 2021. 692 с. С.509-523.

Члени комісії:

Заступник начальника відділу **Артур ДЕРЕНОВСЬКИЙ**
14 . жовтня 2022 року

Начальника відділу **Олега ДЯДИК**
14 . жовтня 2022 року

Вадим НИЧИК
69-25-32

Додаток В

НАЦІОНАЛЬНА АКАДЕМІЯ НАУК УКРАЇНИ
КИЇВСЬКИЙ УНІВЕРСИТЕТ ПРАВА
Україна, м. Київ - 03142, вул. Ак. Доброхотова, 7-а, Тел.: (044) 409-26-43, факс: (044) 423-90-87
ЄДРПОУ - 25745915, e-mail: kul@kul.kiev.ua, www.kul.kiev.ua

№ 196/1/1 від 23.08.2022
на № _____ від _____

«ЗАТВЕРДЖУЮ»
Ректор Київського університету права
НАН України
професор
Юрій Бошицький
2022 року

АКТ

про впровадження наукових розробок дисертаційного дослідження Малія Миколи Івановича «Особа комп'ютерного злочинця як об'єкт кримінологічного дослідження» в освітній процес кафедри кримінального права та процесу Київського університету права НАН України

Комісія у складі: в.о. завідувача кафедри Савки О.І., доцента кафедри, к.ю.н., Перелигіної Р.В. та к.ю.н., доцента кафедри Сахнюка С.В. склала акт про те, що результати дисертаційного дослідження Малія Миколи Івановича «Особа комп'ютерного злочинця як об'єкт кримінологічного дослідження» використовуються під час проведення лекцій та практичних занять з навчальних дисциплін «Кримінологія», «Кримінальне право. Загальна частина», «Кримінальне право. Особлива частина», «Порівняльне кримінальне право». У списку літератури у робочих програмах та навчально-методичних комплексах рекомендовано опрацювання таких наукових праць Малія М.І.:

1. Малій М.І. Інноваційні концепції застосування grid- і blockchain-технологій в юриспруденції. Актуальні проблеми права України та Польщі: монографія / Київський університет права НАН України; за заг. ред. проф. Ю.Л. Бошицького та проф. А. Шміта. Київ: Таском, 2020. С.48-62.
2. Малій М.І. Правовий статус саббота та відповідальність перед людством. Економіка. Фінанси. Право. 2022. №8. С.27-35.
3. Борисова Л.В., Біленчук П.Д., Малій М.І., Виноградова В.С. Експертиза як засіб установлення фактів і обставин вчинення транснаціональних комп'ютерних злочинів. Криміналістика і судова експертиза: Міжвідомчий науково-методичний збірник. КНДІСЕ Міністерства юстиції України. Київ, 2020. Вип. 65. С.230-239. (DOI: https://doi.org/10.33994/kndise.2020.65.22)
4. Малій М.І. Особливості кримінолого-криміналістичної характеристики особи електронного зловмисника. Актуальні проблеми сучасної юридичної науки та практики: матеріали круглого столу (м. Київ, 1 жовтня 2020 року). Київський університет права НАН України. Київ, Видавництво Ліра-К, 2020.172с. С.40-45.

5. Малій М.І. Правова відповідальність електронного інтелекту в новому тисячолітті. Актуальні проблеми сучасної юридичної науки та практики. Випуск 2: матеріали круглого столу (Київ, 7 жовт. 2021 р.). Київ: Видавництво Ліра-К, 2021. С.40-54.
6. Біленчук П.Д., Близнюк М.М., Кобилянський О.Л., Малій М.І., Пілюков Ю.О., Соболєв О.В. Електронна цивілізація: інноваційне майбутнє України: монографія / за заг. ред. П.Д. Біленчука. Київ: УкрДГРІ, 2018. 284 с.
7. Біленчук П.Д., Кобилянський О.Л., Ковальчук Ю.І., Копчук І.В., Малій М.І., Моргунов С.А., Соболєв О.В., Тимощук С.В. та ін. Е-СУСПІЛЬСТВО: цифрове майбутнє України: монографія / за заг. ред. П.Д. Біленчука. 2-е вид., допов. і перероб. Київ: УкрДГРІ, 2019. 292 с.
8. Біленчук П.Д., Береський Я.О., Кобилянський О.Л., Малій М.І., Перелигіна Р.В. Конвергенція сонячного суспільства знань: креативна освіта і цивілізаційний розвиток: монографія / за заг. ред. П.Д. Біленчука. Київ: УкрДГРІ, 2019. 416с.
9. Біленчук П.Д., Кобилянський О.Л., Малій М.І. та ін. Правова соціалізація особистості в сучасному світі: людина, суспільство, цивілізація: монографія / за заг. ред. П.Д. Біленчука. Київ: УкрДГРІ, 2020. 204 с.
10. Біленчук П.Д., Кобилянський О.Л., Малій М.І., Перелигіна Р.В., Тарасевич Т.Ю. та ін. ЕЛЕКТРОННЕ СУСПІЛЬСТВО, ЕЛЕКТРОННЕ ПРАВО, КІБЕРБЕЗПЕКА: стратегія розвитку інноваційної ери: монографія / за заг. ред. П.Д. Біленчука і Т.Ю. Тарасевич. Київ: УкрДГРІ, 2020. 388 с.

В.о. завідувача кафедри кримінального права та процесу, к.ю.н. **Олександр САВКА**

Доцент кафедри кримінального права та процесу, к.ю.н. **Раїса ПЕРЕЛИГІНА**

Доцент кафедри кримінального права та процесу, к.ю.н. **Сергій САХНЮК**

КИЇВСЬКИЙ УНІВЕРСИТЕТ ПРАВА НАЦІОНАЛЬНОЇ АКАДЕМІЇ НАУК УКРАЇНИ
ЗАВІРЯЮ
ЗАВ.ВК
200 р.

ВІДДІЛ ОРГАНІЗАЦІЙНО-КАДРОВОЇ РОБОТИ ТА ДІЛОВОДСТВА

Додаток Г

Меморандум про співробітництво
між НАЦІОНАЛЬНИМ АВІАЦІЙНИМ УНІВЕРСИТЕТОМ
та правничою компанією ТОВ «АЮР-КОНСАЛТИНГ»

«05» листопада 2019 р. м. Київ

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ, в особі ректора Ісаєнка Володимира Миколайовича, який діє на підставі Статуту, з однієї сторони, та правнича компанія **ТОВАРИСТВО З ОБМЕЖЕНОЮ ВІДПОВІДАЛЬНІСТЮ «АЮР-КОНСАЛТИНГ»**, в особі директора Малія Миколи Івановича, який діє на підставі Статуту, з іншої сторони, у подальшому окремо іменовані як «Сторона», а разом – «Сторони», домовились про таке:

1. Мета і предмет Меморандуму

1.1. Метою цього Меморандуму є співпраця з реалізації спільного Проекту «Електронне судочинство і кібербезпека», у т.ч. обмін інформацією і досвідом в межах відповідних функцій і повноважень Сторін, здійснення практичної діяльності у сфері забезпечення верховенства права, захисту конституційних прав, свобод та обов'язків людини і громадянина інше на підставі чинного законодавства України.

1.2. Предметом цього Меморандуму є діяльність Сторін для досягнення мети Меморандуму, що здійснюється у форматі підготовки та реалізації спільного Проекту «Електронне судочинство і кібербезпека», інших узгоджених заходів, проектів і програм.

2. Напрями співпраці

Задля досягнення мети цього Меморандуму Сторони домовляються про співпрацю у таких напрямах:

2.1. Обмін інформацією про плани діяльності, проекти і програми, що розроблені та (або) реалізуються;

2.2. Спільна реалізація Проекту «Електронне судочинство і кібербезпека» – проведення наукового дослідження: 1) «Електронне кримінальне провадження» і 2) «Особа комп'ютерного злочинця як об'єкт кримінологічного дослідження»: правове, наукове і ресурсне забезпечення» та публікація результатів наукового дослідження з обраної тематики.

2.3. Проведення спільних заходів: круглі столи, семінари, конференції тощо за напрямами, що становлять взаємний інтерес;

2.4. Правнича компанія ТОВ «АЮР-КОНСАЛТИНГ» долучається до проведення Конкурсу по відбору кращих студентів Університету з метою проведення їх стажування та подальшого працевлаштування у Проекті «Електронне судочинство і кібербезпека»;

2.5. Взаємні візити представників Сторін з метою ознайомлення та вивчення досвіду роботи;

2.6. Інші узгоджені напрями співпраці.

3. Організація співпраці

З метою реалізації цього Меморандуму Сторони в межах наявних ресурсів:

3.1. Визначають контактних осіб для проведення консультацій і підготовки пропозицій щодо спільної реалізації напрямів, визначених цим Меморандумом;

3.2. Розробляють та підписують текст Договору про співробітництво, що відповідає меті Меморандуму;

3.3. Залучають, в разі необхідності, до спільної діяльності представників органів державної влади, громадських організацій у межах встановлених нормативно-правовими актами та домовленостями з ними;

3.4 Сторони беруть на себе зобов'язання зберігати конфіденційну інформацію, отриману в ході реалізації Меморандуму;

3.5. Сторони зобов'язуються утримуватися від дій, які можуть заподіяти матеріальну або моральну шкоду іншій Стороні;

3.6. Узгоджують інші спільні заходи в рамках Меморандуму.

4. Строк дії Меморандуму

4.1. Меморандум набирає чинності з дня його підписання.

4.2. Меморандум укладається строком на десять років. Дія цього Меморандуму автоматично продовжується на десять років, якщо жодна зі Сторін письмово не повідомить іншу про свій намір припинити його дію не пізніш як за один місяць.

4.3. Сторони можуть достроково припинити дію цього Меморандуму в будь-який час, письмово повідомивши про це іншу Сторону не пізніше ніж за один місяць.

4.4. У разі припинення дії цього Меморандуму заходи, які було розпочато на підставі Меморандуму й не завершено протягом строку його

дії, продовжуються і завершуються згідно з умовами, що були раніше узгоджені Сторонами, за винятком випадків, коли завершити ці заходи неможливо.

5. Заключні положення

5.1. Будь-які зміни та доповнення до цього Меморандуму вносяться тільки за письмовою згодою Сторін і стають його невід'ємною частиною.

5.2. Будь-які спірні питання щодо тлумачення або застосування положень цього Меморандуму вирішуватимуться Сторонами шляхом консультацій та досягнення взаємної згоди.

5.3. Цей Меморандум укладено українською мовою у двох автентичних примірниках, по одному примірнику для кожної зі Сторін.

6. Реквізити сторін

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
ЄДРПОУ 01132330
03058, м.Київ,
проспект Космонавта Комарова, б. 1
Р/р

МФО

Ректор _____ В.М. Ісаєнко
МП (підпис)
Тел.: +38 (044) 497-51-51
E-mail: post@nau.edu.ua

ТОВ «АЮР-КОНСАЛТИНГ»
ЄДРПОУ 38576321
03191, м. Київ,
вул. Лятошинського, буд. 18-А, к. 53
Р/р 26006053129381 в ПАТ "ПРИВАТБАНК", м. Київ,
МФО 321842
UA603218420000026006053129381

Директор _____ М. І. Малій
МП (підпис)
Тел.: +38 (067) 407-35-25
E-mail: aur.consalt@gmail.com

Додаток Д

ЗВІТ
Національної поліції України
про результати роботи у 2021 році

2021 рік був для Національної поліції роком, насиченим подіями, загрозами та викликами різних масштабів.

При цьому ряд чинників, серед яких фінансові, соціально-економічні, епідеміологічні, соціально-психологічні, демографічні, мали вплив на криміногенні процеси в державі та потребували від Національної поліції відповідного та оперативного реагування на них.

Зокрема, негативний вплив на криміногенну ситуацію в Україні мали такі фактори:

продовження збройної агресії Росії проти України на частині території Донецької та Луганської областей, що вимагає витрат значних людських та матеріальних ресурсів, гальмує економічний розвиток Донбасу та держави загалом, сприяє незаконному обігу зброї;

наявність серйозних загроз локального або масштабного вторгнення на територію держави;

міграційна криза на кордоні Білорусі з Литвою, Польщею і Латвією;

низькі темпи економічного розвитку держави, збереження значного тіньового сектору економіки, що його гальмує;

загроза зростання рівня безробіття;

зниження рівня ВВП, загроза зростання рівня інфляції;

збереження значного рівня внутрішньої та зовнішньої трудової міграції українського молодого, працездатного та кваліфікованого населення;

протестні настрої громадян у зв'язку з підвищенням вартості комунальних послуг, розбіжності у поглядах значних груп населення, політичних сил щодо політичної та соціально-економічної ситуації в державі, фіскалізацію малого бізнесу та скасуванням спрощеної системи оподаткування, «локдауном» та карантинними обмеженнями тощо.

Водночас сприяли зменшенню криміногенного потенціалу суспільства:

поширення пандемії COVID-19 в Україні та інших країнах світу, яке негативно вплинуло на всі сторони життєдіяльності суспільства, але внаслідок тимчасового обмеження соціальної активності та мобільності населення об'єктивно зменшило можливості для вчинення кримінальних правопорушень;

стабілізація і укріплення національної валюти;

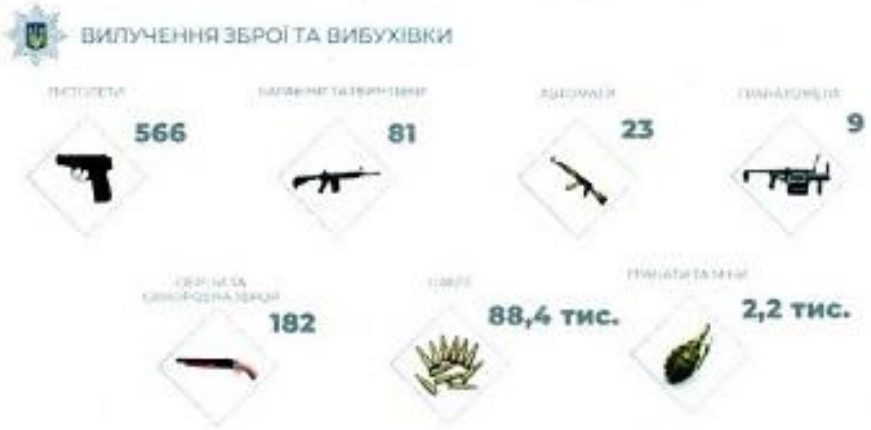
активна протидія Національної поліції організованій злочинності, так званим «злодіям у законі», зменшенням їх злочинного впливу на кримінальну ситуацію.

Оцінюючи роботу Національної поліції у 2021 році, першочергово слід брати до уваги рівень довіри населення до поліції як основний критерій оцінки ефективності діяльності органів та підрозділів поліції, визначений Законом України «Про Національну поліцію».

Послідовна реалізація заходів сприяла документуванню у 2021 році значної кількості кримінальних правопорушень, пов'язаних з використанням зброї.

Так, минулого року Національною поліцією викрито понад 3,9 тис. кримінальних правопорушень, пов'язаних з незаконним поводженням зі зброєю, бойовими припасами або вибуховими речовинами, незаконним виготовленням, переробкою чи ремонтом вогнепальної зброї або незаконним виготовленням бойових припасів, вибухових речовин, вибухових пристроїв. За результатами вжитих заходів розкрито 3,5 тис. таких кримінальних правопорушень.

З незаконного обігу вилучено майже 1,2 тис. одиниць вогнепальної зброї, 88,4 тис. набоїв, а також 2,2 тис. гранат, мін та боєприпасів.



Одним із негативних наслідків перебування в незаконному обігу значної кількості вогнепальної зброї є вчинення у 2021 році 288 кримінальних правопорушень з її використанням, з них 257 – розкрито.

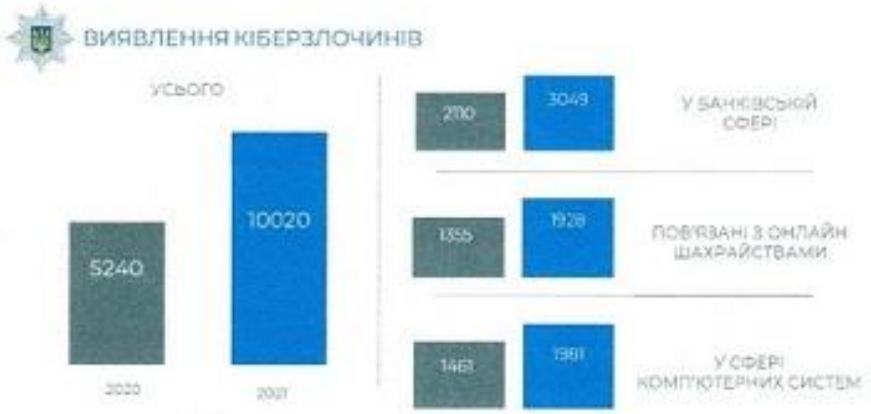
Зокрема, з початку 2021 року в органах та підрозділах поліції зареєстровано 40 умисних вбивств та замахів, вчинених з використанням вогнепальної зброї та вибухових речовин. Завдяки скоординованим заходам поліція розкрила 35 таких правопорушень.

Дієвим засобом боротьби з незаконним обігом зброї, що допомагає найбільш якісно задокументувати протиправну діяльність та отримати необхідну доказову базу, є контроль за вчиненням кримінального правопорушення у вигляді оперативної закупки та контрольованого постачання. Так, у 2021 році проведено майже 200 оперативних закупок вогнепальної зброї, боєприпасів та вибухівки.

Новітні можливості інформаційних технологій та їх стрімкий ріст у всьому світі дедалі активніше використовується людством у різних сферах діяльності. Кіберпростір створює неймовірні можливості, розширює свободу, стимулює

розвиток інновацій та збагачує суспільство. Однак, паралельно з позитивними тенденціями, набуває розвитку і кіберзлочинність, що, зрозуміло, завдає значної шкоди інтересам наших громадян та держави в цілому. З метою протидії такій кримінальній протиправності в Національній поліції функціонує підрозділ кіберполіції.

У 2021 році задокументовано майже вдвічі більше злочинів, учинених з використанням високих інформаційних технологій. Зокрема, у майже півтора рази зросла динаміка реєстрації злочинів у банківській сфері та на третину – у сфері комп'ютерних систем. При цьому кількість розкритих кіберзлочинів збільшилася вдвічі.



Періодичне обмеження соціальної активності громадян у зв'язку з посиленням карантину спровокувало збільшення на 42% шахрайств, пов'язаних з використанням електронно-обчислювальної техніки (ч. 3, 4 ст. 190 КК України). Завдяки оперативному реагуванню поліції на таку ситуацію розкрито понад 80% таких шахрайств.

Кіберполіцейські у 2021 році ініціювали проведення 9 міжнародних поліцейських операцій та взяли участь у 8 таких заходах на запрошення іноземних колег.

Як приклад, минулого року встановлено трьох громадян України, підозрюваних у створенні вірусу «EMOTET». Через незаконні дії цих громадян потерпілим завдано збитків на суму близько 2 млрд. доларів США. Крім того, встановлено шістьох громадян України, які за допомогою шкідливого програмного забезпечення «Ransomware» завдали компаніям Республіки Корея та США збитків на загальну суму 500 млн. доларів США.

Водночас кіберполіцейські продовжують тримати прямий зв'язок з громадянами. Так, у 2021 році по допомогу до кіберполіції звернулося понад 190 тис. громадян. Переважна більшість телефонувала до call-центру, водночас громадяни активно подавали звернення і через форми електронного запиту.