

**МІНІСТЕРСТВО ФІНАНСІВ УКРАЇНИ
ДЕРЖАВНИЙ ПОДАТКОВИЙ УНІВЕРСИТЕТ**

*Кваліфікаційна наукова
праця на правах рукопису*

БЕНЕСКУЛ АРТУР ВАСИЛЬОВИЧ

УДК 343.9:004-049.5(477)

ДИСЕРТАЦІЯ

**ЗАБЕЗПЕЧЕННЯ КРИМІНОЛОГІЧНОЇ БЕЗПЕКИ ТА ЗАПОБІГАННЯ
ЗЛОЧИННОСТІ У СФЕРІ ВИКОРИСТАННЯ ЦИФРОВИХ
ТЕХНОЛОГІЙ В УКРАЇНІ**

Подається на здобуття наукового ступеня доктора філософії

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

_____ **А. В. Бенескул**

.

Науковий керівник: **Грицюк Ігор Васильович**, кандидат юридичних наук,
доцент

Ірпінь – 2024

АНОТАЦІЯ

Бенескул А. В. Забезпечення кримінологічної безпеки та запобігання злочинності у сфері використання цифрових технологій в Україні. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття ступеня доктора філософії з галузі знань 08 «Право» за спеціальністю 081 «Право». – Державний податковий університет, Міністерство фінансів України. – Ірпінь, 2024.

Дисертація присвячена комплексному дослідженню кримінологічної безпеки у сфері використання цифрових технологій в Україні, а також аналізу напрямів запобігання злочинності у сфері використання цифрових технологій і на основі цього, розробці пропозицій щодо вдосконалення законодавства у досліджуваній сфері.

З появою цифрового банкінгу та цифрових технологій відкрилися й нові шляхи до кримінальної та незаконної діяльності, адже цифрові технології запровадили нові види вчинення протиправної діяльності у цій сфері; розширили можливості дій злочинців, надаючи їм майже необмежений глобальний доступ; зобов'язали потенційних жертв (громадян, компаній, держав тощо) шукати та розробляти нові способи захисту від протиправного впливу і навіть запровадили нові види кримінальних правопорушень з використанням цифрових технологій.

У роботі встановлено, що дотримання та забезпечення кримінологічної безпеки у сфері цифрових технологій є вагомим пріоритетом у системі державної, економічної, національної безпеки України загалом та кібербезпеки зокрема. Щоб належним чином реалізовувати зазначений пріоритет, потрібно в першу чергу посилювати спроможності національної системи кібербезпеки з метою протидії кіберзагрозам, кібератакам та кібершахрайствам у сучасному безпековому середовищі. Зазначено, що потрібно розробити дієву систему щодо ефективної профілактики правопорушень у сфері цифрових технологій на основі чітко встановлених законодавчих вимог, які повинні регулювати цей процес.

Автором сформульовані пропозиції щодо розробки та прийняття на законодавчому рівні Стратегії запобігання злочинності з використанням цифрових технологій. Запропонована Стратегія повинна містити конкретні напрями та заходи, спрямовані на використання цифрових технологій щодо запобігання різним видам злочинності на загальносоціальному, спеціально-кримінологічному та індивідуальному рівнях. Також вона повинна базуватися на основі вивченого та дослідженого позитивного зарубіжного досвіду, щодо використання цифрових технологій з метою запобігання злочинності, який можна імплементувати у національне законодавство і на основі цього напрями, щодо вдосконалення діяльності правоохоронних органів та навчання фахівців належної кваліфікації відповідно до розвитку цифровізації.

Запропоновано виокремити склади кримінальних правопорушень, що пов'язані із сферою цифрових технологій в окрему категорію злочинних діянь в інформаційно-цифровій сфері (цифровому середовищі), що матиме практичний зміст для кримінально-правової, так і кримінологічної науки, з погляду запобігання злочинності у сфері обігу цифрової інформації «злочинності у сфері цифрових технологій».

Визначено пріоритетні заходи щодо зміцнення системи цифрової безпеки, а саме: підвищення рівня підготовки фахівців у сфері цифрових технологій; оновлення та впровадження якісного програмного забезпечення правоохоронних структур для своєчасного виявлення та протидії цифровій злочинності і загалом запобігання правопорушенням у цифровому середовищі; формування дієвої системи автоматизованого обміну інформацією на випадок будь-якого виду загроз у цифровому просторі, адже сучасні цифрові технології можуть виступати способом чи засобом вчинення багатьох видів кримінальних правопорушень; вдосконалення системи управління інформаційною безпекою, що використовують інформацію з усіх сховищ даних та дотримання конфіденційності її забезпечення.

Детально проаналізовано поняття «цифрове кримінальне правопорушення або правопорушення у сфері цифрових технологій» та

наведено порівняння з поняттями: «кіберзлочинність» або комп'ютерна злочинність. Досліджено кримінальні правопорушення, що вчиняються із використанням цифрових технологій та цифрової валюти та відмічено необхідність встановлення конкретної міри кримінальної відповідальності за правопорушення у сфері обігу віртуальних активів, цифрової та електронної валюти та запропоновано прирівняти цифрову інформацію до майна, адже що хоч цифрову інформацію не можна доторкнутися і відчути, як носій інформації, виступає речовий предмет, що містить цифрову інформацію та представляє матеріальну цінність. На основі цього, наведено доцільність встановлення кримінальної відповідальності за придбання або збут цифрової інформації, яка свідомо одержана кримінально протиправним шляхом та внесення змін до КК України.

Охарактеризовано стан міжнародно-правового регулювання забезпечення кримінологічної безпеки у сфері використання цифрових технологій та акцентовано увагу на напрямках вдосконалення онлайн-дослідницької мережі, за підтримки міжнародних агентств і приватного сектору, що надасть можливості для більшого обміну інформацією, спілкування між експертами в усьому світі з питань комп'ютерної та цифрової злочинності, порівняльного аналізу і передачі знань про запобігання та боротьбу з комп'ютерними та цифровими кримінальними правопорушеннями, а також розвиток відповідних інструментів навчання, які мають бути доступними на міжнародному рівні, щоб ділитися знаннями та інформацією щодо способів і засобів виявлення, запобігання та боротьби з новими видами кіберзлочинності та злочинності у сфері цифрових технологій.

Ключові слова: злочинність, злочинність у сфері цифрових технологій, кримінальне правопорушення у сфері використання цифрових технологій, цифровізація, цифрові технології, цифрове кримінальне правопорушення, запобігання цифровій злочинності, цифрова інформація, цифрова злочинність, кримінологічна безпека, забезпечення кримінологічної безпеки у сфері цифрових технологій.

SUMMARY

Beneskul A. V. Ensuring criminological security and crime prevention in the field of digital technology use in Ukraine. – Qualifying scientific work on the rights of the manuscript.

The thesis for the degree of Doctor of Philosophy in the field of knowledge 08 «Law» in the specialty 081 «Law». – State Tax University, Ministry of Finance of Ukraine. – Irpin, 2024.

The dissertation is devoted to a comprehensive study of criminological security in the field of digital technology use in Ukraine, as well as an analysis of crime prevention in the field of digital technology use and, based on this, the development of proposals for improving legislation in the researched field.

With the advent of digital banking and digital technologies, new avenues for criminal and illegal activities have opened up, because digital technologies have introduced new types of illegal activities in this area; expanded the capabilities of criminals, giving them almost unlimited global access; obliged potential victims (citizens, companies, states, etc.) to seek and develop new ways of protection against illegal influence and even introduced new types of criminal offenses using digital technologies.

The work established that the observance and provision of criminological security in the field of digital technologies is a significant priority in the system of state, economic, national security of Ukraine in general and cyber security in particular. In order to properly implement the specified priority, it is necessary, first of all, to strengthen the capabilities of the national cyber security system in order to counter cyber threats, cyber attacks and cyber fraud in the modern security environment. It is noted that it is necessary to develop an effective system for the effective prevention of offenses in the field of digital technologies based on clearly established legal requirements that should regulate this process. The author formulated proposals for the development and adoption at the legislative level of the Strategy for the prevention of crime using digital technologies. The proposed Strategy should contain specific directions and measures aimed at the use of digital

technologies to prevent various types of crime at the general social, special criminological and individual levels. It should also be based on the studied and researched positive foreign experience regarding the use of digital technologies for the purpose of crime prevention, which can be implemented into national legislation and, based on this, directions for improving the activities of law enforcement agencies and training properly qualified specialists in accordance with the development of digitalization.

It is proposed to single out the composition of criminal offenses related to the sphere of digital technologies into a separate category of criminal acts in the information and digital sphere (digital environment), which will have practical meaning for both criminal law and criminological science, from the point of view of crime prevention in the sphere of circulation digital information "crime in the field of digital technologies".

Priority measures for strengthening the digital security system have been determined, namely: increasing the level of training of specialists in the field of digital technologies; update and implementation of high-quality software of law enforcement structures for timely detection and counteraction of digital crime and generally prevention of offenses in the digital environment; formation of an effective system of automated information exchange in case of any type of threats in the digital space, because modern digital technologies can act as a method or means of committing many types of criminal offenses; improvement of the information security management system, using information from all data repositories and maintaining the confidentiality of its provision. The concept of "digital criminal offense or offense in the field of digital technologies" is analyzed in detail and a comparison with the concepts of "cybercrime" or computer crime is given. Criminal offenses committed with the use of digital technologies and digital currency were investigated and the need to establish a specific measure of criminal liability for offenses in the field of circulation of virtual assets, digital and electronic currency was noted, and it was proposed to equate digital information with property, because even though digital information cannot be touched and to feel how a material object

containing digital information and representing material value acts as a carrier of information. Based on this, the expediency of establishing criminal liability for the purchase or sale of digital information knowingly obtained by criminally illegal means and making changes to the Criminal Code of Ukraine is indicated.

The state of international legal regulation of ensuring criminological security in the field of digital technologies is characterized and attention is focused on the areas of improvement of the online research network, with the support of international agencies and the private sector, which will provide opportunities for greater exchange of information, communication between experts around the world on computer issues computer and digital crime, benchmarking and transfer of knowledge on preventing and combating computer and digital criminal offenses, as well as the development of appropriate training tools that should be available internationally to share knowledge and information on methods and means of detection, prevention and fight against new types of cybercrime and crime in the field of digital technologies.

Key words: crime, crime in the field of digital technologies, criminal offense in the field of use of digital technologies, digitalization, digital technologies, digital criminal offense, prevention of digital crime, digital information, digital crime, criminological security, ensuring criminological security in the field of digital technologies.

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

в яких опубліковані основні наукові результати дисертації:

1. Бенескул А. В. Характеристика кримінальних правопорушень у сфері використання цифрових технологій. *Юридичний науковий електронний журнал*. 2021. № 12. С. 511-514. URL: http://www.lsej.org.ua/12_2021/132.pdf
2. Бенескул А. В. Забезпечення кримінологічної безпеки у сфері використання цифрових технологій: міжнародно-правовий аспект. *Держава та регіони. Серія: Право*. 2022. № 3 (77). С. 132-137. URL: http://law.stateandregions.zp.ua/archive/3_2022/17.pdf
3. Бенескул А. В. Кримінологічна безпека в умовах цифрової трансформації: поняття, сутність і значення. *Ірпінський юридичний часопис: науковий журнал*. 2023. Вип. 3 (12). С. 309-317. URL: <https://ojs.dpu.edu.ua/index.php/irplegchr/article/view/125/124>
4. Бенескул А. В. Нормативно-правове закріплення застосування цифрових технологій для забезпечення кримінологічної безпеки суспільства. *Науковий вісник Ужгородського національного університету*, 2023. Серія Право. Випуск 78: частина 2. С. 145-151. URL: <http://visnyk-pravo.uzhnu.edu.ua/article/view/285996/280061>

які засвідчують апробацію матеріалів дисертації:

5. Бенескул А. В. Досвід США щодо використання цифрових технологій та штучного інтелекту при запобіганні злочинності. *Науково-практичні засади розвитку наукової думки на сучасному етапі державотворення: матеріали міжнародної науково-практичної конференції, (м. Київ, 22–23 вересня 2021 р.)*. Київ: Науково-дослідний інститут публічного права, 2021. С. 132–135.
6. Бенескул А. В. Новітні напрями вдосконалення запобігання злочинності при використанні цифрових технологій. *Взаємодія публічного та приватного права: сучасні проблеми та виклики: матеріали міжнародної*

науково-практичної конференції (м. Київ, 21–22 лютого 2022 р.). Київ: Науково-дослідний інститут публічного права, 2022. С. 39–41.

7. Бенескул А. В. Використання цифрових технологій при запобіганні злочинності та впровадження цифрової кримінології. *Актуальні проблеми імплементації наукових досягнень у практичну діяльність: матеріали міжнародної науково-практичної конференції* (м. Київ, 19–20 січня 2022 р.). Київ: Науково-дослідний інститут публічного права, 2022. С. 22–24.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ.....	4
ВСТУП.....	7
РОЗДІЛ 1. ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ОСНОВИ ДОСЛІДЖЕННЯ ЗАБЕЗПЕЧЕННЯ КРИМІНОЛОГІЧНОЇ БЕЗПЕКИ В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ.....	20
1.1. Поняття, сутність та роль кримінологічної безпеки в умовах цифрової трансформації	20
1.2. Нормативно-правове регулювання використання цифрових технологій для забезпечення кримінологічної безпеки суспільства.....	29
1.3. Зарубіжний досвід використання цифрових технологій та штучного інтелекту при запобіганні злочинності.....	45
Висновки до Розділу 1.....	70
РОЗДІЛ 2. СУЧАСНИЙ СТАН ТА ТЕНДЕНЦІЇ КРИМІНОЛОГІЧНОЇ БЕЗПЕКИ У СФЕРІ ЦИФРОВИХ ТЕХНОЛОГІЙ.....	73
2.1. Сучасний стан забезпечення кримінологічної безпеки у сфері цифрових технологій	73
2.2. Кримінальні правопорушення, що вчиняються із використанням цифрових технологій та цифрової валюти	85
2.3. Міжнародно-правове регулювання забезпечення кримінологічної безпеки у сфері використання цифрових технологій	105
Висновки до Розділу 2.....	115
РОЗДІЛ 3. ЗАПОБІГАННЯ ЗЛОЧИННОСТІ У СФЕРІ ВИКОРИСТАННЯ ЦИФРОВИХ ТЕХНОЛОГІЙ В УКРАЇНІ	118
3.1. Заходи запобігання злочинності у сфері використання цифрових технологій в Україні.....	118
3.2. Сучасні пріоритетні напрями застосування цифрових технологій для забезпечення кримінологічної безпеки суспільства та запобігання злочинності.....	134

Висновки до Розділу 3.....	148
ВИСНОВКИ.....	151
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ.....	157
ДОДАТКИ.....	178

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

BBC – British Broadcasting Corporation (Британська телерадіомовна корпорація)

CCTV – Closed-circuit television (системи закритої трансляції телебачення, що часто застосовують для відеоспостереження)

CDEP – Committee on digital economy policy (Комітет з політики цифрової економіки)

CEPEJ – The European Commission for the Efficiency of Justice (Європейська комісія з питань ефективності правосуддя)

CERT-UA – Урядова команда реагування на комп'ютерні надзвичайні події України, яка функціонує в складі Державної служби спеціального зв'язку та захисту інформації України

DarkNet – «чорна, темна» мережа

DDoS – DoS attack, DDoS attack, (distributed) denial-of-service attack (Розподілена атака на відмову в обслуговуванні)

DEI PRO – Digital Evidence Investigator PRO (Програмне забезпечення для криміналістики цифрових доказів)

EC3 – European Cybercrime Centre (Європейський центр боротьби з кіберзлочинністю)

ENISA – European Union Agency for Network and Information Security (Агентство Європейського Союзу з кібербезпеки)

GCA – Global Cybersecurity Agenda (Глобальна програма кібербезпеки)

GPS – Global Positioning System (система глобального позиціювання, сукупність радіоелектронних засобів, що дозволяє визначати положення та швидкість руху об'єкта на поверхні Землі або в атмосфері)

ICS – Industrial control systems (Промислові системи управління)

IMPACT – International Multilateral Partnership Against Cyber Threats (Міжнародне багатостороннє партнерство проти кіберзагроз)

INTERPOL – International Criminal Police Organization (Міжнародна організація кримінальної поліції (**Інтерпол**))

ISA – International Society of Automation (Міжнародне товариство автоматизації (**МТА**))

ICSPA – International Cyber Security Protection Alliance (Міжнародний альянс захисту кібербезпеки)

ISAGCA – ISA Global Cybersecurity Alliance (Глобальний альянс ISA з кібербезпеки)

ІТ –сфера – сфера інформаційних технологій

ITU – International Telecommunication Union (Міжнародний союз електрозв'язку (**МСЕ**))

KYC – Know Your Client (Знай свого клієнта)

NDAS – National Data Analytics Solution (Національне рішення для аналізу даних)

NIS2 - нове законодавство Європейського Союзу в галузі кібербезпеки

OECD – Organisation for Economic Cooperation and Development (Організація економічного співробітництва та розвитку (**ОЕСР**))

PredPol – Predictive Policing (Прев'юдиційна (попереджувальна) поліція)

RAT – Remote Access Trojan (Троян віддаленого адміністрування або Троян віддаленого управління)

RFID – Radio Frequency ID entification (радіочастотна ідентифікація – спосіб автоматичної ідентифікації об'єктів, в якому за допомогою радіосигналів зчитуються або записуються дані).

RICAS – Real-time intelligence crime analytics system (Система криміналістичної розвідки в реальному часі)

WI-FI – Wireless Fidelity (бездротова правдивість відтворення)

Адміністрація Держспецзв'язку – Адміністрація Державної служби спеціального зв'язку та захисту інформації України

ВРУ – Верховна рада України

ДСЗІ – Державна служба спеціального зв'язку та захисту інформації України

ДЦКЗ – Державний центр кіберзахисту

ЄВРОПОЛ – Європейське поліцейське управління

ЄКПЛ – Європейська конвенція про права людини

ЄС – Європейський Союз

ЄСІТС – Єдина судова інформаційно-телекомунікаційна система

ЗМІ – засоби масової інформації

ЗУ – Закон України

ІБ – інформаційна безпека

ІКТ – інформаційно-комп'ютерні технології

ККУ – Кримінальний Кодекс України

КМДА – Київська міська державна адміністрація

КМУ – Кабінет Міністрів України

НАТО – North Atlantic Treaty Organization (Організація Північноатлантичного договору, Північноатлантичний альянс)

ОТ – Операційні технології; Оперативні технології

ПЗ – програмне забезпечення

РЄ – Рада Європи

США – Сполучені Штати Америки

СШІ – Система штучного інтелекту

ЦКУ – Цивільний Кодекс України

ШІ – штучний інтелект

ВСТУП

Обґрунтування вибору теми дослідження. Формування цифрового суспільства в Україні породжує досить значні зміни економічного, правового, культурного, політичного та соціального характеру. Так, зокрема відбувається трансформація цифрової економіки, вдосконалення і створення соціально спрямованої сучасної інфраструктури та загалом підвищується якість життя, враховуючи впровадження у суспільство процесів цифрової трансформації.

Проте, враховуючи повномасштабне вторгнення росії в Україну та реалії сьогодення, зростає необхідність проведення та закріплення належного і дієвого захисту інформації в цифровому середовищі, що й породжує важливість забезпечення кримінологічної безпеки загалом та кримінологічної безпеки у сфері цифрових технологій зокрема.

Оскільки, з появою цифрового банкінгу та цифрових технологій відкрилися й нові шляхи до кримінальної та незаконної діяльності, адже цифрові технології запровадили нові види вчинення протиправної діяльності у цій сфері; розширили можливості дій злочинців, надаючи їм майже необмежений глобальний доступ; зобов'язали потенційних жертв (громадян, компаній, держав тощо) шукати та розробляти нові способи захисту від протиправного впливу і навіть запровадили нові види кримінальних правопорушень з використанням цифрових технологій.

Враховуючи вказані загрози у цифровому середовищі та в мережі Інтернет, що можуть впливати на усіх користувачів, діяльність правоохоронних органів повинна бути спрямована в першу чергу на захист особи, суспільства і держави від таких посягань злочинного характеру.

Адже цифрові технології швидко поширюються у всі сфери життєдіяльності суспільства і саме тому, як держава так і громадянське суспільство повинно бути готовим як до позитивних так і до негативних факторів, які приносять впровадження будь-яких інноваційних технологій.

Окрім цього, необхідно зважати і на стан кримінологічної обстановки, який формується під впливом цифрових технологій.

Цифровий світ і сучасні цифрові технології, які поширені як у громадянському суспільстві так і в державі загалом, приносять не тільки величезні переваги, але й досить великі ризики. Цифрова злочинність є однією з тих, яка досить швидко поширює різноманітні злочинні прояви, а також особливістю її є те, що у зв'язку з розвитком цифрових технологій, змінюється загалом зміст злочинності; адже більшість із цих кримінальних правопорушень здійснюється у віртуальному середовищі. Міжнародне співтовариство та держави намагаються протистояти вчиненню правопорушень з використанням цифрових технологій, приймаючи низку нормативно-правових актів у цій сфері, але вони не повною мірою впливають на зростання цифрової злочинності.

Не менше уваги приділяється проблемам, викликаним використанням сучасних технологій у науковій літературі. Проте немає єдності у підходах до термінології у цій сфері і в основному використовується термінологія: «комп'ютерна злочинність», «кіберзлочинність» тощо. Проте, аналіз стану злочинності у цій сфері, а також міжнародного законодавства та наукової літератури свідчить про те, що є необхідність уточнення існуючого поняття комп'ютерної злочинності, розширення його до поняття «кримінальне правопорушення у сфері використання цифрових технологій».

У період з листопада 2021 року по жовтень 2022 року в усьому світі було виявлено майже 16 тисяч кіберзлочинів. З цієї загальної кількості майже 700 випадків стосувалися невеликих компаній. Організації в секторі державного управління найбільше постраждали серед досліджуваних галузей, де було зареєстровано 3270 випадків кіберзлочинності. Інформаційний сектор посів друге місце, а виробництво – з приблизно 1800 інцидентами в кожній галузі [113].

На сучасному етапі розвитку суспільства, крім зростання вчинених кримінальних правопорушень у цій сфері, відбувається їх модернізація, спостерігається впровадження нових предметів, знарядь, засобів та способів вчинення злочинних посягань. Більшість названих кримінальних правопорушень відбувається у віртуальному просторі, що значно ускладнює їх виявлення та запобігання. Яке б визначення ми не взяли, безсумнівно, нові технології підштовхнули традиційну злочинну діяльність до еволюції та адаптації до нового цифрового середовища, де зростає економічна та соціальна взаємодія. Інтернет-шахрайство, обман, крадіжка особистих даних, «відмивання грошей», несанкціоновані витoki інформації, витoki даних, пов'язані з інтернет-атаками, вимагання та купівля незаконних товарів або продуктів є традиційними кримінальними правопорушеннями, яким сприяють цифрові технології.

Оскільки світ розвивається у цифрову епоху, корпорації та уряди держав все більше покладаються на технології збору, аналізу та зберігання особистих даних. Це, у свою чергу, призвело до зростання кількості кіберправопорушень, починаючи від незначних проступків і закінчуючи глобальними, серйозними атаками, що вражають мільярди користувачів.

Саме тому, враховуючи, що в Україні теж досить стрімко розвиваються та впроваджуються цифрові технології, досить важливим напрямом діяльності є вдосконалення системи забезпечення кримінологічної безпеки в процесі застосування і використання цифрових технологій. І як результат цього, повинна бути прийнята чітка та дієва правова база, метою якої має виступати в першу чергу ефективне регулювання суспільних відносин щодо порядку, напрямів, механізмів, способів застосування цифрових технологій у різних сферах державного та суспільного життя. А також вказана нормативна база регулювання сфери кримінологічної безпеки щодо порядку застосування цифрових технологій, окрім цього, повинна містити напрями реагування

органів державної влади на ті кримінологічні загрози, які можуть виникати в процесі використання мережі Інтернет і різних цифрових технологій.

Таким чином, звертаючи увагу на виклики сьогодення, необхідно чітко визначити напрями державної політики щодо порядку виявлення, розгляду та вивчення можливих кримінологічних ризиків в умовах трансформації сучасного цифрового суспільства та вчасно реагувати на них з метою мінімізації та усунення.

Окремі аспекти дослідження, аналізу та вивчення кримінологічної безпеки загалом та безпеки у кіберпросторі зокрема, а також дослідження злочинності у сфері цифрових технологій були предметом досліджень у працях багатьох вчених, таких як: К. А. Автухова, О. М. Бабенка, О. М. Бандурки, О. О. Берназюка, Р. І. Благути, О. М. Бодунової, О. І. Бугери, В. М. Бутузова, В. Д. Гавловського, О. Ф. Гіда, М. Ю. Загрійчука, О. В. Косолап, О. М. Литвинова, Т. В. Мельничук, А. В. Мовчана, С. А. Мозоля, Є. В. Орлова, В. А. Пересадька, Г. В. Подзігун, В. В. Топчія, В. П. Шеломенцева, Н. С. Юзікової, О. Ю. Юроченко та інших вчених, проте поряд з основними характеристиками кримінологічної безпеки та злочинності у сфері цифрових технологій, враховуючи необхідність постійного моніторингу та наукового обґрунтування аналізу сфери цифрових технологій щодо їх використання з точки зору кримінологічної науки, досить важливим є дослідження стану забезпечення кримінологічної безпеки саме у сфері використання сучасних інформаційних та цифрових технологій.

Проаналізувавши дослідження вказаних науковців можна зазначити, що в основному вони спрямовані на кримінологічному аналізі дотримання та забезпечення окремих видів безпеки, зокрема: економічної, національної, громадської тощо або ж загалом кримінологічної безпеки, а також дослідженні окремих аспектів правопорушень в інформаційному просторі. Тому, враховуючи євроінтеграційні та глобалізаційні процеси, розширення сфери інформатизації, діджиталізації, потребує окремої уваги саме тема щодо

дослідження забезпечення кримінологічної безпеки саме у сфері використання цифрових технологій.

За останні декілька років у сучасній юридичній науці також захищено кандидатські та докторські дисертації, присвячені окремим питанням забезпечення кримінологічної безпеки та використання цифрових технологій, запобігання кіберправопорушенням, кримінальним правопорушенням у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку в праві загалом та при запобіганні злочинності зокрема. Так, до таких можна віднести дисертації: О. О. Берназюка («Цифрові технології у праві: тенденції та перспективи розвитку», м. Ужгород, 2021 р.), О. М. Бодунової («Кримінологічні засади запобігання злочинності у сфері інформаційних технологій», м. Ірпінь, 2023 р.), О. І. Бугери («Кримінологічні засади використання мережі інтернет для запобігання злочинності», м. Київ, 2020 р.), М. Ю. Загрійчука («Адміністративно-правові засади цифрової трансформації регіону», м. Харків, 2021 р.), С. А. Мозоля («Кримінологічна безпека в Україні: феномен та наукові засади забезпечення», м. Харків, 2018 р.), Г. В. Подзігун («Публічне адміністрування у сфері цифрової трансформації», м. Запоріжжя, 2021 р.), Б. Б. Теплицького («Техніко-криміналістичне забезпечення розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку», м. Київ, 2021 р.) та інших.

Втім, у проаналізованих наукових працях, питання щодо використання цифрових технологій при запобіганні злочинності та для забезпечення кримінологічної безпеки суспільства не були безпосереднім предметом їх дослідження, що й зумовлює актуальність обраної теми дослідження.

Таким чином, є дійсно необхідність поглибленого, всебічного та комплексного дослідження забезпечення кримінологічної безпеки та запобігання злочинності у сфері використання цифрових технологій в Україні, що в результаті і зумовило вибір теми цього дисертаційного дослідження.

Тому, враховуючи, що сучасна наука кримінального права та кримінології потребує комплексного монографічного дослідження з вказаної проблематики та розроблення сучасних дієвих напрямів запобігання кримінальним правопорушенням з використанням цифрових технологій, це й обумовило вибір предмета, мети і задач наукового дослідження.

Зв'язок роботи з науковими програмами, планами, темами, грантами. Дисертацію виконано відповідно до Концепції розвитку електронного урядування в Україні, схваленої розпорядженням Кабінету Міністрів України від 20 вересня 2017 р. № 649-р.; Концепції розвитку цифрових компетентностей, схваленої розпорядженням Кабінету Міністрів України від 3 березня 2021 р. № 167-р.; Концепція розвитку штучного інтелекту в Україні, схваленої розпорядженням Кабінету Міністрів України від 2 грудня 2020 р. № 1556-р.; Національної програми інформатизації, прийнятої Законом України від 1 грудня 2022 року. № 2807-IX; Національної стратегії сприяння розвитку громадянського суспільства в Україні на 2021-2026 роки, затвердженої Указом Президента України від 27 вересня 2021 року № 487/2021; Плану заходів з реалізації Концепції розвитку цифрових компетентностей, затвердженого розпорядженням Кабінету Міністрів України від 3 березня 2021 р. № 167-р.; Плану заходів з реалізації Стратегії інформаційної безпеки на період до 2025 року, затвердженого розпорядженням Кабінету Міністрів України від 30 березня 2023 р. № 272-р; Стратегії забезпечення державної безпеки, введеної в дію Указом Президента України від 16 лютого 2022 року № 56/2022; Стратегії інформаційної безпеки, затвердженої Указом Президента України від 28 грудня 2021 року № 685/2021; Стратегія кібербезпеки ЄС на цифрове десятиліття. Спільне повідомлення до Європейського парламенту та Ради. Документ 52020JC0018. Брюссель, 16.12.2020. (The EU's Cybersecurity Strategy for the Digital Decade. Joint communication to the European parliament and the council. Brussels, 16.12.2020 JOIN (2020) 18 final); Стратегії кібербезпеки України, введеної в дію Указом Президента України від 26 серпня 2021 року

№ 447/2021; Стратегії розвитку інформаційного суспільства в Україні, схваленої розпорядженням Кабінету Міністрів України від 15 травня 2013 р. № 386-р.

Тему дисертації затверджено Вченою радою Університету державної фіскальної служби України (протокол №13 від 26 листопада 2020 року).

Мета і завдання дослідження. *Метою* дисертаційного дослідження є комплексне дослідження кримінологічної безпеки у сфері використання цифрових технологій в Україні, а також аналіз напрямів запобігання злочинності у сфері використання цифрових технологій і на основі цього, розробка пропозицій щодо вдосконалення законодавства у досліджуваній сфері.

Досягнення цієї мети вимагає вирішення таких *завдань*:

- дослідити поняття, сутність та роль кримінологічної безпеки в умовах цифрової трансформації;
- проаналізувати нормативно-правове регулювання використання цифрових технологій для забезпечення кримінологічної безпеки суспільства;
- вивчити зарубіжний досвід використання цифрових технологій та штучного інтелекту при запобіганні злочинності;
- охарактеризувати сучасний стан забезпечення кримінологічної безпеки у сфері цифрових технологій;
- дослідити кримінальні правопорушення, що вчиняються із використанням цифрових технологій та цифрової валюти;
- охарактеризувати міжнародно-правове регулювання забезпечення кримінологічної безпеки у сфері використання цифрових технологій;
- запропонувати заходи запобігання злочинності у сфері використання цифрових технологій в Україні;
- визначити сучасні пріоритетні напрями застосування цифрових технологій для забезпечення кримінологічної безпеки суспільства та запобігання злочинності.

Об'єктом дослідження є суспільні відносини, які виникають у зв'язку із забезпеченням кримінологічної безпеки та запобіганням злочинності у сфері використання цифрових технологій в Україні.

Предметом дослідження є забезпечення кримінологічної безпеки та запобігання злочинності у сфері використання цифрових технологій в Україні.

Методологічна та теоретична основа дослідження. Методологічну основу дослідження обрано, виходячи з поставлених у дисертаційному дослідженні мети і задач, з урахуванням об'єкта і предмета дослідження. *Діалектичний метод* забезпечив комплексне дослідження правового регулювання кримінологічної безпеки та напрямів запобігання злочинності у сфері використання цифрових технологій в Україні. *Порівняльно-правовий метод* дав змогу виявити властиві нормам вітчизняного законодавства недоліки у сфері забезпечення кримінологічної безпеки та запобігання злочинності у сфері використання цифрових технологій в Україні, порівняно з відповідними нормами у законодавстві окремих зарубіжних країн та міжнародно-правових документах а також дозволив провести порівняльне дослідження кримінальних правопорушень у сфері цифрових технологій та відмежувати їх від інших кримінальних правопорушень. *Статистичний метод* сприяв опрацюванню статистичних даних щодо найбільш значних випадків витоку даних у всьому світі станом на серпень 2023 року (у мільйонах), за кількістю зламаних записів даних і постраждалих осіб; загальної кількості інцидентів кіберзлочинності з листопада 2021 року по жовтень 2022 року за галузями та розмірами організацій; глобальних секторів промисловості, які найбільше зазнали атак базових веб-додатків з листопада 2021 року по жовтень 2022 року; кількості запитів на дані користувачів, надісланих до Facebook в усьому світі станом на другу половину 2022 року та інших статистичних даних, що стосуються вчинених кримінальних правопорушень у сфері цифрових технологій, як джерела надходження відомостей про предмет дослідження. *Соціологічні методи* використані під час аналізу соціально-правового впливу на Інтернет-

середовище, а також стану захищеності громадян під час користування новітніми цифровими та інформаційними технологіями з метою мінімізації ризиків кібератак, кібершахрайств та інших правопорушень, що стосуються застосування чи використання сфери цифрових технологій.

Нормативну основу дослідження склали: Конституція України, закони і підзаконні нормативно-правові акти України, Кримінальний кодекс України, міжнародні нормативно-правові акти та міжнародні договори, стороною яких є держава Україна.

Емпіричною базою дослідження була правозастосовна практика, судова практика України, Європейського Союзу та статичні дані з міжнародних джерел щодо злочинності у сфері цифрових технологій.

Наукова новизна одержаних результатів полягає в тому, що дисертація є одним із перших у вітчизняній юридичній науці комплексним дослідженням забезпечення кримінологічної безпеки та запобігання злочинності у сфері використання цифрових технологій в Україні, на підставі якого сформульовано нові наукові положення, висновки та пропозиції, зокрема:

уперше:

- наведено доцільність встановлення кримінальної відповідальності за придбання або збут цифрової інформації, яка свідомо одержана кримінально протиправним шляхом та внесення змін до КК України, шляхом доповнення його статтею 198-1 «Придбання, отримання, зберігання чи збут цифрової інформації, одержаної кримінально протиправним шляхом»;

- наведено авторське визначення «кримінальних правопорушень у сфері цифрових технологій», під якими розуміється передбачене кримінальним законом винне, протиправне, суспільно небезпечне діяння, спрямоване на порушення конфіденційності, цілісності, достовірності та доступності цифрової інформації, що охороняється законом або вчинене з використанням цифрових технологій або щодо них;

– сформульовано визначення «злочинності у сфері використання цифрових технологій», а саме як сукупність кримінальних правопорушень, що вчиняються із використанням систематизованих правових, науково-технічних, організаційних рішень, спрямованих на застосування комп'ютерної та іншої електронно-обчислювальної техніки, програмного забезпечення та інших засобів для зменшення участі користувача інформаційно-комунікаційних систем і засобів інформатизації під час збирання, приймання, обробки, передавання інформації чи трудомісткості виконуваних операцій

– запропоновано прийняти на рівні держави Стратегію кримінологічної безпеки України на 2024-2028 роки, на основі проведеного наукового дослідження поняття, сутності та ролі кримінологічної безпеки в умовах цифрової трансформації, з метою належного рівня захисту прав та свобод людини і громадянина від негативних посягань в кіберпросторі, з яким певним чином пов'язаний кожен громадянин нашої держави;

– визначені сучасні пріоритетні напрями застосування цифрових технологій для забезпечення кримінологічної безпеки суспільства та запобігання злочинності;

удосконалено:

– аргументацію щодо пропозиції виокремити в окрему галузь віктимології – кібервіктимологію або цифрову віктимологію, оскільки віктимізація кіберправопорушень останнім часом набуває все більшого поширення, тому доцільним, на нашу думку є дослідження кіберзлочинності не лише щодо форм та способів їх вчинення та заходів запобігання, а ще й з точки зору жертви даних видів правопорушень, тобто з погляду кібервіктимізації;

– пропозицію внесення змін до Кримінального Кодексу України зміни, а саме: змінити назву Розділу XVI «Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» на «Кримінальні

правопорушення у сфері використанням цифрових технологій» та розширити його;

- виокремлення складів кримінальних правопорушень, що пов'язані із сферою цифрових технологій в окрему категорію злочинних діянь в інформаційно-цифровій сфері (цифровому середовищі), що матиме практичний зміст для кримінально-правової, так і кримінологічної науки, з погляду запобігання злочинності у сфері обігу цифрової інформації «злочинності у сфері цифрових технологій»;

- пріоритетні заходи щодо зміцнення системи цифрової безпеки та заходи інформування громадян щодо забезпечення та дотримання безпеки в кіберпросторі;

- способи попередження та запобігання злочинності, щодо їх використання не тільки шляхом застосування штучного інтелекту і цифрових технологій, а й запровадженням нових інститутів та обґрунтування розробки магістерської програми для здобувачів вищої освіти, яка б саме і стосувалася застосування та використання цифрових технологій під час запобігання злочинності;

дістали подальшого розвитку:

- напрям кримінологічної науки – цифрова кримінологія та доцільність в Особливій частині Кримінології розглядати такий вид злочинності, як «Злочинність у сфері цифрових технологій» або «Цифрова злочинність»;

- способи забезпечення кримінологічної безпеки у сфері цифрових технологій та вагомі напрями діяльності щодо побудови дієвої системи кібербезпеки в суспільстві;

- аналіз складів кримінальних правопорушень, що вчиняються із використанням цифрових технологій та цифрової валюти;

- заходи національного характеру та міжнародного співробітництва у кримінальних провадженнях, зокрема щодо посилення заходів виявлення кримінальних правопорушень у сфері цифрових технологій;
- пропозиції щодо запобігання злочинності у сфері цифрових технологій.

Практичне значення одержаних результатів полягає в тому, що теоретичні положення, висновки та пропозиції, викладені в дисертації, становлять науково-теоретичний та практичний інтерес і можуть бути використані у:

- *законотворчості* – з метою розроблення нових нормативно-правових актів й удосконалення чинних, що встановлюють кримінальну відповідальність за кримінальні правопорушення у сфері цифрових технологій;
- *правозастосуванні* – для вдосконалення практичної діяльності правоохоронних органів, кіберполіції при виявленні та запобіганні кримінальним правопорушенням у сфері цифрових технологій;
- *науково-дослідній сфері* – подальшого поглиблення досліджень проведення розробки проблем запобігання та попередження кримінальним правопорушенням у сфері використання цифрових технологій в Україні та практики застосування кримінального закону;
- *освітньому процесі* – при викладанні курсу «Кримінальне право», «Кримінологія» та у процесі підготовки лекцій, підручників, методичних рекомендацій і навчальних посібників з питань попередження та кваліфікації кримінальних правопорушень.

Апробація результатів дослідження. Основні наукові положення та висновки дисертаційної роботи, а також практичні рекомендації щодо вдосконалення кримінального законодавства України обговорювалися на кафедрі кримінального права та процесу Державного податкового університету і були представлені у доповідях науково-практичних конференцій, зокрема на таких: «Науково-практичні засади розвитку наукової думки на сучасному етапі державотворення» (м. Київ, 22-23 вересня 2021 р.); «Взаємодія публічного та

приватного права: сучасні проблеми та виклики» (м. Київ, 21-22 лютого 2022 р.); «Актуальні проблеми імплементації наукових досягнень у практичну діяльність» (м. Київ, 19–20 січня 2022 р.).

Публікації. Основні наукові положення та результати дисертаційного дослідження висвітлено у 7 публікаціях, серед яких: 4 статті у наукових виданнях, включених до переліку наукових фахових видань України та 3 тез доповідей на науково-практичних конференціях.

Структура та обсяг дисертації визначена метою та завданнями дослідження. Робота складається з анотації, вступу, трьох розділів, логічно об'єднаних у вісім підрозділів, висновків, списку використаних джерел. Загальний обсяг дисертації становить 183 сторінки, із яких основного тексту – 156 сторінок. Список використаних джерел міститься на 21 сторінці і налічує 156 найменувань та 5 додатків на 6 сторінках.

РОЗДІЛ 1

ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ ОСНОВИ ДОСЛІДЖЕННЯ ЗАБЕЗПЕЧЕННЯ КРИМІНОЛОГІЧНОЇ БЕЗПЕКИ В УМОВАХ ЦИФРОВОЇ ТРАНСФОРМАЦІЇ

1.1. Поняття, сутність та роль кримінологічної безпеки в умовах цифрової трансформації

Цифровізація у сучасному суспільстві полягає в першу чергу в інтеграції цифрових технологій у повсякденне життя. Застосування цифрових технологій, використання передових технологій та динаміки цифрових мереж, гігантського потоку інформації, реалізовується в першу чергу у формі оновлення різноманітних процесів, шляхом оцифрування. Саме тому, цифровізація може бути застосована в багатьох галузях наук, включаючи, зокрема, гуманітарні та соціальні науки. Тим часом кримінально-правова наука серед гуманітарних і соціальних наук теж піддається впливу цифрової трансформації, адже кримінальне правосуддя, останнім часом досить потужно зазнає впливу цифровізації та розвитку технологій.

Подзігун Г. В. до основних проявів цифрової трансформації відносить: а) цифровізацію; б) розвиток цифрової економіки, цифрових інновацій та технологій; в) впровадження електронного урядування та електронної демократії; г) впровадження електронного документообігу та вироблення національних електронних інформаційних ресурсів, використання принципу інтероперабельності тощо [52, с. 10].

Проблема забезпечення належного рівня безпеки громадянського суспільства, в яких би формах вона не виражалася (національна, суспільна, економічна, екологічна тощо) завжди залишається пріоритетною, оскільки від її вирішення залежить доля усієї цивілізації. В період повномасштабного вторгнення росії в Україну, питання безпеки загострилося найбільше, адже

саме від її дотримання та забезпечення залежить життя громадян. Саме тому, сучасні виклики все більше спонукають держави будувати безпечне майбутнє і дійсно розробляти ефективні заходи запобігання та нейтралізації численних загроз і забезпечення безпеки на різних її рівнях.

Серед таких загроз одне з перших місць у сьогоденній реальності займає злочинність, яка суттєво гальмує цивілізоване реформування нашого суспільства. Загалом, злочинність за своїми статистичними показниками становить не лише внутрішню небезпеку, але, що страшніше, загрожує інтересам міжнародної безпеки. Тому, забезпечення відповідного контролю з боку державних органів, громадських організацій і громадян зокрема, за злочинністю не може бути ефективним без вирішення проблеми безпеки особи, суспільства та загалом держави від злочинних посягань. От саме, комплексність та повнота вказаного процесу і зумовлює значення дослідження кримінологічної безпеки, особливо в сучасний стан цифрових технологій та використання різноманітних цифрових ресурсів [6, с. 310-311].

Окремі аспекти дослідження, аналізу та вивчення кримінологічної безпеки загалом та безпеки у кіберпросторі зокрема були предметом досліджень у працях багатьох українських та закордонних вчених, таких як: О. М. Бандурки [2], В. Д. Гавловського [21], О. М. Литвинова [40], Т. В. Мельничук [42], С. А. Мозоля [46], В. П. Шеломенцева [74;75] та інших, проте поряд з основними характеристиками кримінологічної безпеки, досить важливим є дослідження стану забезпечення кримінологічної безпеки саме у сфері використання сучасних інформаційних та цифрових технологій, що й потребує ґрунтового вивчення та дослідження.

В період переходу до інформаційного суспільства особливої актуальності набуває саме питання дослідження забезпечення безпеки людини, громадянського суспільства, держави загалом від різноманітних потужних можливостей сучасних цифрових та комп'ютерних технологій. Адже, як показує практика реального життя, вони можуть використовуватися не лише

для підвищення і покращення якості життя людей, але й, нажаль, для порушення прав, свобод чи інтересів особи, а в окремих випадках, ще й нанесення шкоди суспільству, громадянам чи державі, залежно від ситуації.

Тому, все більшої підтримки серед науковців викликає необхідність застосування до цієї сфери концепції кримінологічної безпеки, що в останні часи набуває особливої актуальності [21;74;75].

Мозолем С.А. наведено формулювання визначення системи забезпечення кримінологічної безпеки, яку він визначає як організовану на державному рівні сукупність суб'єктів (до яких він відносить посадових осіб та окремих громадян, громадських організацій, державних органів), які об'єднані спільними завданнями та цілями, що здійснюють узгоджену діяльність, відповідно до законодавства України з метою захисту важливих інтересів особи, суспільства та держави від кримінального впливу злочинності та для підтримання соціально допустимого рівня забезпечення кримінологічної безпеки. Також, ним наводиться система аргументів, які покладені в обґрунтування концепції багатовимірного комплексу основних об'єктів кримінологічної безпеки, до яких відносяться: особа – її права, обов'язки та свободи; суспільство – його духовні, морально-етичні, культурні, історичні, інтелектуальні та матеріальні цінності; держава – її конституційний устрій, суверенітет і територіальна цілісність та недоторканість; цивілізація – сукупність духовних сфер, культурних і матеріальних цінностей та форм організації управління суспільством [47, с. 5].

Також, на основі дослідження існуючих підходів до формулювання поняття «безпека» Мозолем С.А. було визначено кримінологічну безпеку у широкому та вузькому розумінні. У широкому сенсі, як зазначає автор, вона є порядком та умовою життєдіяльності соціальної системи, що відзначається доброякісністю здійснення її саморегулятивних функцій. Водночас це і спроможність цієї системи за наявності зовнішніх і внутрішніх кримінальних впливів підтримувати константний, стійкий стан і вирішувати питання безпеки

життєвих процесів у суспільстві. У вузькому ж сенсі, на погляд Мозоля С.А. кримінологічна безпека характеризує такий стан, за якого надійно захищено всі життєво важливі інтереси країни (нації), до мінімуму знижено реальні та потенційні кримінальні загрози й найкращим чином забезпечуються можливості прогресивного розвитку особи, суспільства та держави. Вона має всі необхідні властивості, що дозволяють зарахувати її до класу складних соціальних систем із конкретно-історичним (динамічним) характером, елементи якого інтегровано з усіма формами та напрямками взаємодії в системі «природа-людина-суспільство» [47, с. 9].

Значення та необхідність Стратегії кримінологічної безпеки обґрунтовує також і О. М. Литвинов: «Кримінологічна стратегія надає функціонуванню механізму протидії злочинності плановірності, стабільності, спрямованості, також забезпечує послідовність і безпосередність розробки завдань діяльності та їх диференціацію за рівнями та сферами застосування. Вона вбирає в себе фундаментальні надбання науки та новітні форми організації практичної сторони справи, виступає певною платформою для довгострокових і перспективних планів діяльності окремих суб'єктів, чітко визначає засоби, у тому числі обумовлені специфікою дії механізмів реалізації довгострокової кримінологічної політики» [40, с. 138].

Поряд з цим, Мозоль С.А. відмічає, що Стратегія забезпечення кримінологічної безпеки є складовою частиною більш глобальних стратегій; її мета полягає в недопущенні прояву криміногенних (стимулюючих злочинність) і власне кримінальних (проявів злочинності в конкретних кримінально караних діяннях) загроз національному та міжнародному спокою. А забезпечення кримінологічної безпеки є діяльністю держави, суспільства в цілому та їх інститутів, що ґрунтується на принципах комплексного програмування та планування, мета якої полягає у досягненні та підтримці соціально прийнятного рівня захищеності основних прав і свобод особи та суспільства, законних інтересів держави від злочинних посягань. Окрім цього, автор Мозоль С. А.

пропонує розглядати кримінологічну безпеку у широкому та вузькому розумінні. У широкому сенсі вона є порядком та умовою життєдіяльності соціальної системи, що відзначається доброякісністю здійснення її саморегулятивних функцій. Водночас це і спроможність цієї системи за наявності зовнішніх і внутрішніх кримінальних впливів підтримувати константний, стійкий стан і вирішувати питання безпеки життєвих процесів у суспільстві. У вузькому сенсі кримінологічна безпека характеризує такий стан, за якого надійно захищено всі життєво важливі інтереси країни (нації), до мінімуму знижено реальні та потенційні кримінальні загрози й найкращим чином забезпечуються можливості прогресивного розвитку особи, суспільства та держави. Вона має всі необхідні властивості, що дозволяють зарахувати її до класу складних соціальних систем із конкретно-історичним (динамічним) характером [47, с. 24].

Враховуючи зазначені вище положення, необхідно вказати, що перш за все, досліджуючи та вивчаючи стан захищеності кримінологічної безпеки в Україні, потрібно вчасно виявляти та реагувати на можливі загрози у кіберпросторі, тобто ефективно проводити попереджувальну діяльність, з метою недопущення настання негативних наслідків. Тобто, забезпечення кримінологічної безпеки повинно відбуватися у спосіб, що передбачає не просто визначення потенційного джерела кримінологічної загрози та впливу на нього, а має на меті – уже передбачений та можливий захист користувача від реального вказаного криміногенного джерела небезпеки, при використанні цифрових технологій. Саме тому, одним із перспективних та необхідних напрямів запобігання сучасній злочинності в Україні має стати ефективна програма забезпечення кримінологічної безпеки у різних сферах суспільного життя.

Проте, не потрібно ототожнювати поняття державної безпеки з поняттям «кримінологічна безпека», адже перше поняття є набагато ширшим та закріпленим на законодавчому рівні.

Так, відповідно до Стратегії забезпечення державної безпеки забезпечення державної безпеки – це створення умов для забезпечення захищеності державного суверенітету, територіальної цілісності та демократичного конституційного ладу й інших життєво важливих національних інтересів від реальних і потенційних загроз Україні. Державна політика у сфері державної безпеки спрямовується на попередження, своєчасне виявлення і запобігання зовнішнім та внутрішнім загрозам державній безпеці України, припинення розвідувальних, терористичних, диверсійних та інших протиправних посягань спеціальних служб іноземних держав, а також організацій, окремих груп та осіб на державну безпеку України, усунення умов, що призводять до цих загроз та причин їх виникнення [67].

Поряд із забезпеченням кримінологічної безпеки загалом, варто її розглядати і з погляду окремих сфер. Так особливо принципового значення має дотримання належного її рівня забезпечення у сфері цифрових технологій, адже розвиток інформатизації та комп'ютеризації постійно розвивається, удосконалюється, що ставить і нові виклики перед державними та громадськими органами для оперативного реагування на прояви її порушення.

Кіберзлочинність – це загальний термін для незаконної діяльності, яка відбувається в Інтернеті, або коли цифрові технології виступають способом чи засобом вчинення таких кримінальних правопорушень. На сьогодні це один із найшвидше зростаючих кримінальних правопорушень у світі, який впливає на більшість підприємств. За даними Risk IQ, кіберзлочинність коштує світовій економіці 2,3 мільйона фунтів стерлінгів за хвилину [145]. Якщо говорити точніше, то сектор фінансових послуг незмінно є однією з найбільш поширених галузей, на які полюють кібершахраї [114]. У Великій Британії майже половина підприємств (46%) і чверть благодійних організацій (26%) повідомили про порушення кібербезпеки або атаки за 2020 рік. Характер кібератак також змінився з 2017 року. За цей період було зафіксовано зростання кількості

компаній, які стикаються з фішинговими атаками (з 72% до 86%), а також загрози поширення вірусів або інших шкідливих програм (з 33% до 16%) [93].

У період з листопада 2021 року по жовтень 2022 року фінансова індустрія була найбільшою мішенню для атак на базові веб-додатки в усьому світі. Установи в цьому секторі бачили 173 такі інциденти за вимірний період. Другим за кількістю нападів був інформаційний сектор із 173 атаками, тоді як професійний сектор посів третє місце, зазнавши 113 випадків атак на базові веб-додатки. Глобальні сектори промисловості, які найбільше зазнали атак базових веб-додатків з листопада 2021 року по жовтень 2022 року наведені у Додатку [112]. (Додаток Г)

Тож постійна загроза кіберзлочинності є дуже сучасною та дуже реальною. Широке використання цифрових технологій та Інтернету в сучасному суспільстві привертає увагу кримінологів все частіше, зокрема розширюється такий напрям у кримінології як кіберкримінологія. Кіберкримінологія є майже новою міждисциплінарною галуззю дослідження кримінологічної науки, яка направлена на дослідження проблеми комп'ютерної злочинності. Із розвитком технологій і науки, злочинність і кримінальна поведінка, як наслідок цьому теж змінюються, тому необхідно вчасно реагувати та протидіяти проявам кримінальних правопорушень у цій сфері.

Кіберзлочинність включає у себе злочинну діяльність з використанням технологій і цифровізації, які складаються з протиправних дій щодо доступу до інформації, її перехоплення чи пошкодження даних, втручання в роботу комп'ютерної системи чи пристрою тощо.

Кіберпростір все частіше стає новим місцем для вчинення кримінальних правопорушень, тому забезпечення належного рівня кримінологічної безпеки в умовах цифрової трансформації є одним із першочергових завдань правоохоронних органів.

Як стверджує Джайшанкар, засновник кіберкримінології, «кримінологія раніше не надавала важливого значення феномену

кіберзлочинності та важливості дослідження кіберпростору, проте зі зміною природи, масштабів та загалом віктимізації у галузі цифрових технологій, кіберзлочинність стала міждисциплінарною галуззю і включає в себе дослідження причинно-наслідкового зв'язку кримінальних правопорушень, що вчиняються в кіберпросторі, та його впливу на фізичний простір особи [121]. Окрім цього, генеральний директор ITRS Group Гай Уоррен, зазначив: «Перехід до «цифрового бізнесу» збільшує кількість точок входу в IT-системи та даних різних компаній. Злочинці знайдуть точку найменшого захисту, зокрема через мобільні додатки, щоб отримати все більше точок входу на різні портали» [115].

Підприємства, установи, організації і просто фізичні особи прагнуть стимулювати свій розвиток, ефективність і головне фінансову віддачу і все частіше роблять це з використанням цифрових технологій. Але з цим виникає безліч ризиків, на які необхідно вчасно реагувати та запобігати. Адже, нові технології та цифрова еволюція також створюють нові можливості для кримінальних правопорушень, оскільки світ цифрових технологій надає різноманітні можливості злочинцям щодо удосконалення злочинних способів доступу до цінної інформації, отримання несанкціонованого доступу до інформації про різноманітні компанії та клієнтів, витоку персональних даних, комерційної таємниці тощо.

Отже, на сучасному етапі розвитку цифрових технологій, коли світ постійно удосконалюється та стає все більш цифровим, продовжує зростати потреба в застосуванні і нових технологій, щоб зуміти забезпечити себе належним рівнем у цьому цифровому середовищі. Саме тому питання кримінологічної безпеки в сучасному світі цифрових трансформацій набуває все більш актуального характеру, тому дослідження вказаної проблематики є вкрай важливим, а головне необхідним.

Адже, навички та знання, які необхідні сьогодні дуже швидко розвиваються. Тому вкрай важливо, щоб підприємства, установи та організації

забезпечували свій персонал необхідним практичним навчанням, щоб допомогти їм бути в безпеці у кіберпросторі. Тому, відмінне розуміння нових технологій і кібербезпеки потрібне не лише ІТ-відділам, а загалом кожен користувач мережею Інтернет повинен бути захищеним від кібершахрайств. Потрібно, щоб інші розуміли наслідки та можливості роботи в цифровому світі, задля зменшення загальних ризиків та ефективного використання цифрових технологій, щоб не потрапити на кібершахраїв.

Таким чином, щоб протистояти негативним проявам в мережі Інтернет та використовувати нові можливості, необхідно розуміти суть та значення кібербезпеки, кіберзлочинності і загалом напрямів нових інформаційних технологій. Окрім цього, важливе значення має дослідження та вплив на такі напрями, як: середовище загроз кібербезпеки; потенційна вартість кібератаки для бізнесу для інших структур; оцінки ступеня безпеки підприємства, установи чи організації; аналіз можливостей вчасно реагувати на негативні інциденти та способи використання нових цифрових технологій.

Саме тому, враховуючи вказані положення, віктимізація кіберправопорушень останнім часом набуває все більшого поширення, тому доцільним, на нашу думку є дослідження кіберзлочинності не лише щодо форм та способів їх вчинення та заходів запобігання, а ще й з точки зору жертви даних видів правопорушень, тобто з погляду кібервіктимізації та виокремлення окремої галузі віктимології – кібервіктимології.

На нашу думку, дослідження та вивчення теорії кримінологічної безпеки покликані сприяти визначенню основної її суті, тобто захисту особи, суспільства та держави від такого негативного, антисоціального явища, як злочинність, тобто виокремлення тих головних цінностей, яким і гарантується на відповідному рівні кримінологічна безпека. Саме тому, важливим та необхідним на рівні держави, ми вважаємо, є прийняття Стратегії кримінологічної безпеки України на 2024-2028 роки, адже це саме те завдання, яке повинно бути виконаним, щоб належним чином захистити права та свободи

людини і громадянина від негативних посягань в кіберпросторі, з яким певним чином пов'язаний кожен громадянин нашої держави. Тому, розробка, прийняття та затвердження вказаної Стратегії кримінологічної безпеки України на державному рівні надасть законодавчого дотримання належного рівня кримінологічної безпеки.

1.2. Нормативно-правове регулювання використання цифрових технологій для забезпечення кримінологічної безпеки суспільства

Сучасні існуючі ризики, які стосуються сфери застосування цифрових технологій та впливають на кримінологічну безпеку можуть виступати злочинною загрозою і потенційно впливати на різні об'єкти, внаслідок чого завдавати державі, суспільству та кожному індивіду різних видів шкоди, як матеріального так і нематеріального характеру. Такі ризики, про які ми уже зазначали у попередньому підрозділі, необхідно аналізувати і оцінювати системно, тобто передбачати напрям боротьби із злочинністю у сфері цифрових технологій, як окреме та обов'язкове завдання державної політики у боротьбі зі злочинністю загалом. Щоб відповідним чином реагувати на загрози кримінологічній безпеці у сфері цифрових технологій, перш за все потрібно правильно та вчасно оцінити можливі загрози, які спричиняють відповідні ризики, але усі вказані дії щодо реагування та запобігання повинні бути чітко до встановлених нормативних вимог. Тобто, належний рівень нормативно-правового забезпечення та регулювання сфери застосування цифрових технологій має забезпечувати реалізацію найефективніших механізмів протидії усім можливим загрозам, що можуть впливати на стан кримінологічної безпеки в державі.

На думку Берназюка О. О. основними проблемами у сфері застосування в Україні цифрових технологій у праві є: 1) непослідовність державної політики у сфері запровадження цифрових технологій у сферу публічного управління,

яка зумовлена відсутністю єдиної та комплексної державної стратегії в цій сфері, яка б була розроблена з урахуванням рекомендації інституцій ЄС, інших міжнародних організацій, експертів та фахівців у сфері права, інформаційних технологій та ін.; 2) цифрова нерівність, яка виражається в недоступності Інтернет-технологій та якісного програмного забезпечення для окремих верств населення, що ускладнює, а подекуди унеможлиблює користування електронними державними та регіональними онлайн-сервісами, а також у відсутності належного оснащення місцевих органів державної влади та органів місцевого самоврядування окремих регіонів необхідними для надання якісних електронних послуг технологіями; 3) невідповідність законодавства, неузгодженість з міжнародними стандартами, що зумовлено прийняттям у різні періоди нормативних актів, що регулюють різні види суспільноуправлінських правовідносин в інформаційній сфері, у сфері використання цифрових технологій у публічному управлінні за відсутності узгодженості та єдиного підходу [10, с. 19].

На сучасному етапі розвитку суспільства, цифрові технології використовуються абсолютно в різних сферах суспільного життя, адже сюди можна віднести оплату рахунків громадянами, сферу охорони здоров'я, політику, безпеку учасників дорожнього руху, які для прикладу використовують Інтернет-навігацію, сферу освіти, управління, фінансів, економіки тощо. І цей список можна продовжувати і продовжувати, проте в першу чергу, слід відмітити, що, на жаль, застосування цифрових технологій, як показує практика їх використання, не лише допомагає в оптимізації окремих сфер діяльності людини, суспільства і держави, але й на жаль породжує вчинення різних правопорушень, як у самій сфері цифрових технологій, так і з їх використанням, що й свідчить про актуальність тематики дослідження та необхідність виокремлення дієвих способів захисту інформації в кіберпросторі.

Дослідження та належний рівень забезпечення і реалізації кримінологічної політики, враховуючи також повномасштабне вторгнення

російської федерації на територію України полягає в першу чергу у нейтралізації чинників, які детермінують та породжують злочинність у цифровій сфері. Оскільки, негативний вплив, який можуть завдавати правопорушення у цифровій сфері стосуються кожного громадянина, кожного члена громадянського суспільства та й загалом держави. Саме тому, необхідно саме вчасно виявляти ті негативні чинники, які з використанням певних елементів цифровізації можуть здійснювати шкідливий вплив на економіку, соціально-культурну сферу, правосвідомість громадян, телекомунікаційну, комп'ютерну та загалом інформаційну сфери.

Як вдало відмічає Бугера О. І. «сучасною тенденцією розвитку кримінологічної науки є пошук шляхів використання можливостей мережі Інтернет для запобігання злочинності, як на спеціально-кримінологічному, так і на загальносоціальному рівні. Особливо актуальним є забезпечення розвитку Інтернет-освіти, зокрема правової освіти» [16, с. 57]. Проте, поява нових кримінальних загроз, що пов'язані з використанням високих технологій зі злочинною метою, потребують удосконалення методичних підходів щодо проведення кримінологічних досліджень, і зокрема, шляхом їх цифровізації » [14, с. 46].

Тобто, як бачимо сфера цифровізації з одного боку може слугувати як допомога при розслідуванні окремих видів правопорушень, а з іншого містити нові загрози, які знову ж таки стосуватимуться сфери застосування цифрових технологій. Тому, напрями їх досліджень містять системний характер і з одного боку ця системність і комплексність полягає у їх широкому застосуванні при виявленні, розслідуванні чи аналізі кримінальних правопорушень, а з іншого – необхідно вчасно реагувати на можливі ризики у сфері цифровізації, що можуть завдати значно більшої шкоди та нанести збитків.

Розслідування майже всіх видів кримінальних правопорушень має цифрову складову. У 2019 році кількість інцидентів, зростає втричі. За оцінками, існує близько 700 мільйонів нових зразків злочинного програмного

забезпечення – найчастішого засобів сприяння кібератакам. Річні витрати світової економіки від кіберзлочинності в 2020 році оцінюються в 5,5 трильйона євро, що вдвічі більше, ніж у 2015 році. В результаті одного великого злочинного інциденту, кібератаки програм-вимагачів WannaCry у 2017 році, світова економіка втратила понад 6,5 мільярдів євро [151].

Останнім часом, все більше уваги приділяється питанням, що стосуються правопорушень, вчинених з використанням цифрових технологій, а також цифрових активів, виробляються різноманітні форми, засоби боротьби з цим явищем. Інтеграція цифрових технологій у кожен із сфер юридичної діяльності: правотворчу, правозастосовну, правоохоронну, окрім цього у діяльність щодо тлумачення права однозначно має свої переваги, адже відкриває широкі можливості. Проте, з швидким розвитком інформаційних технологій в Україні, який активно відбувається останнім часом, набуває динаміки і злочинність у цій сфері, що свідчить про те, що кожен прогрес чи розвиток, який несе для суспільства певні новітні можливості, цивілізаційні блага, досить часто супроводжується і протиправними, негативними явищами. Так само, це стосується і стрімкого розвитку цифрових технологій, масової комп'ютеризації, цифровізації, які однозначно спростили життя, адже полегшили досить велику кількість процесів, які раніше відбувалися з використанням робочої сили, але й понесли за собою виникнення протиправних діянь та зловживань. Враховуючи особливість та складність сфери цифрових технологій, діяльність правоохоронних органів вимагає особливої уваги та підходу до виконання завдань із захисту прав та свобод особи, суспільства і держави від посягань у цифровій сфері, зокрема від кримінальних правопорушень, які вчиняються з використанням цифрових технологій [8, с. 147].

Цифрові технології та їх застосування і використання в громадянському суспільстві і державі набувають широкого розповсюдження, зокрема й ту правозастосовній практиці, що обумовлює актуальність досліджуваної теми та

проблематики, особливо з погляду забезпечення належного рівня кримінологічної безпеки у суспільстві. Так, зокрема, необхідно дослідити дефініції понять «кримінальні правопорушення у сфері цифрових технологій», «злочинність у сфері цифрових технологій» та загалом поняття «кіберзлочинність» і «цифрова злочинність». Всі вказані поняття досить тісно стосуються сучасного стану розвитку громадянського суспільства, проте на практиці, при кваліфікації вчинених протиправних діянь виникають суперечності.

Дослідивши та проаналізувавши окремі національні нормативно-правові акти, необхідно зазначити, що в основному у нас використовують наступні поняття: «інформаційні технології», «інформаційно-комунікаційні технології», «інформаційно-комп'ютерні технології», «електронно-обчислювальні машини» (комп'ютери), «інформаційні системи та комп'ютерні мережі», проте зміст термінів потребує чіткого розмежування для їх правильного використання та застосування.

Окрім цього, Загрійчук М. Ю., відмічає також, що ряд законодавчих та підзаконних нормативно-правових актів (зокрема: загальнодержавних стратегій, концепцій та програм), в яких визначаються напрямки розвитку державної політики у сфері цифрової трансформації регіону є досить застарілою та потребує комплексного перегляду [24, с. 14].

Берназюк О. О. відносить до системи національного законодавства у сфері регулювання цифрових технологій у праві становлять такі групи актів: 1) акти, які визначають поняття та види цифрових технологій, фундаментальні принципи їх використання у праві; 2) акти, у яких закріплено основні права громадян, інших фізичних і юридичних осіб; 3) акти, у яких визначено законодавчі засади забезпечення інформаційної безпеки у сфері використання цифрових технологій; 4) акти, що регламентують порядок використання цифрових технологій у зовнішньоуправлінській діяльності суб'єктів владних повноважень; 5) акти, що визначають порядок використання цифрових

технологій у внутрішньоорганізаційній діяльності суб'єктів владних повноважень. А до основних недоліків сучасного стану правового регулювання цифрових технологій у праві відносить: 1) неузгодженість основних понять та категорій між собою та з нормами ЄС, їх розрізненість у значній кількості нормативно-правових актів; 2) недостатній рівень гарантування захисту персональних даних та неврегульованість прав громадян, інших фізичних та юридичних осіб у мережі Інтернет; 3) розрізненість нормативно-правових актів та відсутність уніфікованого підходу до визначення процедур застосування тих чи інших видів цифрових технологій у публічному управлінні та інших видах юридичної діяльності [10, с. 13].

Так, поняття «цифрова технологія» має нормативно закріплене визначення на законодавчому рівні. Відповідно до п. 24 і п. 25 ч. 1 ст. 1 Національної програми інформатизації, «цифрова технологія – це сукупність систематизованих правових, науково-технічних, організаційних рішень, спрямованих на застосування комп'ютерної та іншої електронно-обчислювальної техніки, програмного забезпечення та інших засобів для зменшення участі користувача інформаційно-комунікаційних систем і засобів інформатизації під час збирання, приймання, обробки, передавання інформації чи трудомісткості виконуваних операцій», а «цифровізація – процес впровадження цифрових технологій у всі сфери суспільного життя». Також закріплений термін «інформатизація – сукупність взаємопов'язаних організаційних, правових, політичних, соціально-економічних, науково-технічних, технологічних та виробничих процесів, спрямованих на створення умов для забезпечення розвитку інформаційного суспільства та впровадження інформаційно-комунікаційних і цифрових технологій» [61].

Як бачимо, цифрові технології є широким збірним поняттям, які в свою чергу включають і комп'ютерні, і електронні, і інформаційно-комунікаційні та інші засоби та технології. Тому, доцільно, цей термін використовувати і

кримінально-правових і кримінальних процесуальних нормативних актах, адже сфера його застосування доволі широка.

Так, Закон України «Про авторське право і суміжні права» фактично ототожнює поняття «цифрової» та «електронної» інформації і надає наступне визначення: цифровий контент (електронна (цифрова) інформація) – будь-які відомості чи дані в електронній (цифровій) формі, що містять об'єкти авторського права та/або суміжних прав і можуть зберігатися та/або поширюватися у вигляді одного або декількох файлів (частин файлів), записів у базі даних на зберігаючих пристроях комп'ютерів, серверів тощо у мережі Інтернет [57].

Тобто, можна визначити, що під «цифровою технологією» мається на увазі електронний спосіб передачі, зберігання, обробки та здійснення інших дій з інформацією.

Окрім цього, Національна стратегія сприяння розвитку громадянського суспільства в Україні на 2021-2026 роки, метою якої є формування та діяльності інститутів громадянського суспільства, створення сприятливих умов для розвитку громадської ініціативи та самоорганізації, налагодження взаємодії між громадянами, згаданими інститутами та органами державної влади, органами місцевого самоврядування, передбачає теж використання цифрових технологій. Зокрема: підтримку процесів цифрової трансформації діяльності інститутів громадянського суспільства з метою сприяння підвищенню ефективності їх діяльності; навчання та надання консультаційної підтримки інститутам громадянського суспільства щодо впровадження та використання в їх діяльності цифрових технологій та інструментів електронної демократії; реалізація проектів, спрямованих на розвиток інфраструктури, у тому числі цифрової, яка створює умови для ефективного функціонування інститутів громадянського суспільства, сприяє поліпшенню доступу таких інститутів до навчання, комунікації, мережування, обміну ресурсами [48].

Стратегія кібербезпеки України конкретно вказує на необхідності того, що країна повинна мати змогу забезпечити свій соціально-економічний розвиток у цифровому світі, і це в свою чергу вимагає досягнення кіберстійкості на всіх рівнях та взаємодії всіх суб'єктів забезпечення кібербезпеки, яка ґрунтується на довірі і набуття спроможності ефективно стримувати деструктивні дії в кіберпросторі [64].

Проаналізувавши норми Концепції розвитку електронного урядування в Україні, слід відмітити, що вона теж містить положення про цифрові технології та їх застосування. Так вона відмічає, що повсякденне життя громадян стає дедалі все більш «цифровим», містить положення щодо розвитку сучасних електронних форм взаємодії, прозорості та відкритості діяльності, залучення громадян до прийняття управлінських рішень. Окрім цього, відмічається, що реалізація вказаної Концепції здійснюється за одним із основних принципів, який має назву «цифровий за замовчуванням» і передбачає забезпечення будь-якої діяльності органів влади через електронну форму реалізації як пріоритетну, а планування та реалізацію будь-якої реформи, проекту чи завдання – із застосуванням інформаційно-комунікаційних технологій [36].

У Стратегії розвитку інформаційного суспільства в Україні від 15 травня 2013 р. № 386-р. було зазначено, що цифрові технології давно стали потужною рушійною силою соціального та економічного розвитку, вони впливають на визначення основ сталого розвитку в майбутньому і відновлення економіки багатьох держав світу. Окрім цього, Стратегія передбачала, що для прискореного впровадження інформаційних і комунікаційних технологій, створення на їх основі нових методів, ресурсів, інструментів, технологій необхідно прискорити розвиток національної системи цифрової науково-технічної інформації, забезпечивши при цьому створення цифрових ресурсів та електронних баз даних наукової та науково-технічної інформації та забезпечити доступ до іноземних цифрових ресурсів і електронних світових баз даних наукової та науково-технічної інформації [69].

Стратегія інформаційної безпеки від 28 грудня 2021 року № 685/2021 визначає стратегічні цілі та завдання, спрямовані на протидію загрозам національній безпеці України в інформаційній сфері, захист прав осіб на інформацію та захист персональних даних, а також передбачає, що в умовах стрімкого розвитку цифрових технологій, але недостатнього рівня медіаграмотності (медіакультури), відбувається значне розширення джерел доступу до інформації, проте воно супроводжується зменшенням критичності сприйняття інформації, що сприяє зростанню впливу дезінформації та деструктивної пропаганди та створює підґрунтя для можливих маніпуляцій громадською думкою. Саме тому, Стратегія й вказує основні напрями, стратегічні цілі і завдання для забезпечення інформаційної безпеки України, серед яких в першу чергу відмічені стійкість та взаємодія [68].

Для їх втілення та реалізації був затверджений План заходів з реалізації Стратегії інформаційної безпеки на період до 2025 року, відповідно до якого передбачені стратегічні цілі, завдання і строки їх виконання. Так, зокрема однією із стратегічних цілей, поряд з іншими, є саме розвиток інформаційного суспільства та запобігання інформаційних загрозам в цифровому полі. План заходів передбачає і відповідальних за виконання, так, наприклад, для виконання стратегічної цілі щодо протидії дезінформації та інформаційним операціям, насамперед держави-агресора, передбачені конкретні напрями: створення системи раннього виявлення, прогнозування та запобігання гібридним загрозам, зокрема створення системи протидії дезінформації та інформаційним операціям, спрямованої на запобігання, максимально швидке виявлення та реагування держави і суспільства на інформаційні загрози; розвиток спроможностей складових сил оборони щодо протидії загрозам в інформаційному просторі; посилення відповідальності за поширення недостовірної інформації (дезінформації), тощо [51].

Таким чином, як бачимо досить широке законодавче застосування сфери цифрових технологій у сучасному громадянському суспільстві, але конкретного

визначення «цифрової технології» немає. Проте, якщо проаналізувати окремі міжнародні правові акти, то можна дослідити дефініцію цього поняття. Так, ЄС також приділяє увагу навчанню своїх громадян щодо використання цифрових технологій.

План дій із цифрової освіти (2021-2027) – це оновлена політична ініціатива ЄС, спрямована на підтримку стійкої та ефективної адаптації освітніх і навчальних систем держав-членів ЄС до епохи цифрових технологій. Для досягнення цих цілей план дій визначає два пріоритетні напрямки: сприяння розвитку високоефективної екосистеми цифрової освіти та підвищення цифрових навичок і компетенцій для цифрової трансформації [98]. Як бачимо, сфера цифрових технологій досить активно поширюється та трансформується в громадянське суспільство, тому однозначно необхідно на це звертати увагу та своєчасно реагувати в нормативно-правовому та законодавчому полі.

Тобто, цифрові технології – це електронні інструменти, пристрої та ресурси, які обробляють генерують або зберігають дані. Відомі приклади: соціальні мережі, ігри, мультимедіа, планшети та мобільні телефони тощо [31].

Таким чином, до кримінальних правопорушень, вчинених з використанням цифрових технологій, можна віднести, протиправні дії, що здійснюються в цифровій сфері за допомогою різноманітних технічних засобів, телефонних пристроїв (смартфонів, цифрових телевізорів, планшетів та іншої гаджетоподібної техніки). У зв'язку з цим очевидно, що роль цифрових технологій зростає, а механізм їх проникнення у всі галузі життєдіяльності громадян, суспільства, держави загалом продовжує удосконалюватись та видозмінюватись.

Саме тому, якщо говорити про кримінальні правопорушення у сфері цифрових технологій то необхідно розглядати склади конкретних кримінальних правопорушень, які можуть вчинятися або ж вчиняються із використанням цифрових технологій.

Проаналізувавши, норми КК України, жодна із статей не містить саме поняття цифрових технологій, хоча в реальності вони вчиняються з їх використанням, що однозначно потребує внесення змін до КК України. КК України містить розділ XVI «Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» [39].

Проте, з метою визначення загальних ознак кіберзлочину, можна звернутися до окремих законодавчих актів, які надають визначення, що стосуються сфери кіберінформації та кібербезпеки. Так Закон України «Про основні засади забезпечення кібербезпеки України» визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки. Саме вказаний нормативний документ вказує, що кіберзлочин (комп'ютерний злочин) – це суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України, а кіберзлочинність є сукупністю кіберзлочинів. Таким чином, як бачимо, однією із ознак кіберзлочину є вчинення діяння у кіберпросторі, що вказаний Закон України визначає, як середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних. Тобто, аналізуючи та порівнюючи вказане твердження із визначенням «цифрових технологій», що ми наводили раніше, можна дійти висновку, що злочинність у сфері цифрових технологій є

ширшим поняттям, ніж кіберзлочинність, оскільки містить у собі використання інших технічних, цифрових засобів, поряд із електронно-обчислювальною та комп'ютерною технікою [62].

Таким чином, враховуючи реалії сьогодення, повномасштабне вторгнення РФ в Україну та загалом значний рівень активності користувачів різними Інтернет-ресурсами в глобальній мережі, зростає постійно і кількість різних операцій, що вчиняються із застосуванням цифрових технологій. Але поряд з цим вказані технології не залишаються, нажаль, і поза увагою злочинної сфери, яка також використовує їх у різноманітних злочинних цілях, що і породжує необхідність своєчасного виявлення та попередження. Особливої небезпеки такі правопорушення набувають поряд з їх великою кількістю вчинення також і через об'єкт на який вони посягають, адже досить часто із використанням різних цифрових технологій у телекомунікаційних мережах вони здійснюють злочинний вплив на важливі об'єкти державного значення, зокрема шляхом викрадення інформації щодо стану економіки, безпеки, оборони тощо.

Але, навіть враховуючи шкоду, яку вказані правопорушення у цифровій сфері наносять суспільству та державі, у нас на законодавчому рівні немає чіткого визначення, розмежування чи чіткого аналізу таких понять, як: «злочинність у сфері цифрових технологій», «кримінальні правопорушення, що вчиняються із використанням цифрових технологій» чи взагалі поняття «цифрової злочинності».

Так, КК України, оперує поняттям інформації, яка міститься в інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних системах, електронних комунікаційних мережах, електронно-обчислювальних машинах (комп'ютерах), комп'ютерних мережах або на носіях такої інформації [36]. Проте самого визначення, що належить до цієї інформації він не надає, тобто виходить, що дані норми є бланкетними. Таким чином, щоб

конкретизувати вказані визначення необхідно в першу чергу надати чіткі дефініції досліджуваним поняттям.

Так, для прикладу чинним кримінальним та цивільним законодавством України не надано конкретного визначення поняття комп'ютерної інформації.

Але ЦКУ містить дефініцію поняття інформації, що наведена у статті 200 та вказує наступне твердження: «Інформацією є будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді» [73].

Тобто, якщо застосувати аналогію права та аналогію закону, то можна до комп'ютерної інформації віднести будь-який вид інформації, що виготовляється за допомогою комп'ютерних технологій. Зокрема можна віднести сюди різноманітні комп'ютерні програми, комп'ютерні ігри, комп'ютерні (автоматизовані) бази даних, абсолютно всі веб-сторінки в мережі Інтернет тощо. Можна відмітити, що в принципі все, що людина може сприймати за допомогою комп'ютера (комп'ютерних технологій), різноманітних цифрових засобів (смартфонів, планшетів, телефонів, ноутбуків тощо) і є комп'ютерною інформацією.

Але тут, необхідно ще відмітити такий факт, що «цифрові технології» та загалом «цифрове середовище» не стоять на місці, а постійно динамічно розвиваються та вдосконалюються, що породжує в свою чергу нові види інформації, що може бути віднесена до комп'ютерної, або ж до інформації у сфері цифрових технологій, чи нових цифрових засобів. Наприклад сучасні розробки та виробництво робототехніки, використання штучного інтелекту, сучасних інформаційних мереж, телекомунікаційних систем, оптоволоконних кабелів, які дозволяють працювати в мережі Інтернет, навіть при відсутньому електропостачанні.

Вдосконалюючись та трансформуючись в нові види технологій, інформаційні та телекомунікаційні системи все частіше стають засобом чи способом вчинення правопорушень, використання їх у злочинній діяльності,

наприклад з метою порушити безпеку захисту певного виду інформації, незаконно отримати особисті чи конфіденційні дані певних осіб чи вплинути незаконно на окремі фінансові операції. Усе вказане свідчить про те, що застосування цифрових технологій у злочинних цілях значно перешкоджає вчасному та ефективному їх виявленню правоохоронними органами, що породжує збільшення їх кількості у загальній статистиці вчинення.

Тобто усе це свідчить про динамічність та постійний розвиток цифрових технологій, і в свою чергу також про зміни у видах порушень, які можуть бути вчинені у цій сфері та з їх застосуванням.

Адже, соціально-економічні зміни, що впливають на сферу цифрових технологій працюють таким чином, що активний розвиток цифрових технологій працює на випередження, чим часто і користуються у своїй злочинній діяльності правопорушники, які намагаються їх застосувати на випередження правоохоронним органам. І вказане, нажаль негативно відображається на загальній кримінальній ситуації у цій сфері.

Отже, як показує практика, цифрові технології і є складними у їх застосуванні у правоохоронній сфері через те, що вони з однієї сторони використовуються злочинцями при вчиненні кримінальних правопорушень, а з іншої – ними користуються органи правоохоронної системи з метою своєчасного виявлення, попередження за запобігання вчиненню злочинності у цифровій сфері.

Оскільки, за своєю сутністю і природою, кримінальні правопорушення, які вчиняються із застосуванням різних цифрових технологій є складними через їх віртуальну ознаку, тобто вчинення у віртуальному просторі. Саме цей факт, надає можливість особам злочинців вчиняти злочинні дії на відстані, а правоохоронним органам ускладнює можливість вчасного їх попередження, встановлення винних осіб та притягнення їх до кримінальної відповідальності.

Проте, навіть враховуючи значний рівень криміналізації сфери цифрових технологій, значного поширення використання цифровізації у

різноманітних злочинних цілях, застосування новітніх цифрових засобів злочинцями, що мають спеціальні знання у сфері цифровізації, комп'ютеризації, діджиталізації тощо, у нас на законодавчому рівні відсутнє чітке визначення видів кримінальних правопорушень, що вчиняються із використанням цифрових технологій. Також, не надані конкретні дефініції ознакам складу кримінальних правопорушень цієї категорії, немає визначень багатьох термінів, які стосуються кримінальних правопорушень у сфері цифрових технологій та й в принципі цифрової злочинності загалом, що ускладнює процес кваліфікації порушень у цій сфері. Вказане свідчить про необхідність внесення змін до Кримінального кодексу України з метою чіткої диференціації досліджуваних кримінальних правопорушень та визначення їх дефініції.

Стратегія кібербезпеки Європейського Союзу на цифрове десятиліття передбачає, що Європейська Комісія продовжить працювати над забезпеченням відповідних каналів і роз'ясненням правил отримання транскордонного доступу до електронних доказів для кримінальних розслідувань (потрібно у 85% розслідувань, при цьому 65% загальних запитів надходять до постачальників, що знаходяться в іншій юрисдикції), шляхом сприяння прийняттю та подальшій реалізації «пакету електронних доказів» і практичних заходів. Швидке прийняття Європейським парламентом і Радою пропозицій щодо електронних доказів є ключовим моментом, щоб забезпечити практиків ефективним інструментом. Електронні докази повинні мати чітке зчитування, тому Комісія й надалі працюватиме над підтримкою потенціалу правоохоронних органів у сфері цифрових розслідувань, зокрема щодо шифрування під час кримінальних розслідувань, повністю зберігаючи свою функцію захисту основних прав і забезпечення кібербезпеки [151].

Саме тому, дотримання та забезпечення кримінологічної безпеки у сфері цифрових технологій є вагомим пріоритетом у системі державної, економічної, національної безпеки України загалом та кібербезпеки зокрема. Щоб належним

чином реалізовувати зазначений пріоритет, потрібно в першу чергу посилювати спроможності національної системи кібербезпеки з метою протидії кіберзагрозам, кібератакам та кібершахрайствам у сучасному безпековому середовищі.

Проаналізувавши зазначені вище нормативно-правові акти, можна сформулювати визначення «злочинності у сфері використання цифрових технологій», а саме як сукупність кримінальних правопорушень, що вчиняються із використанням систематизованих правових, науково-технічних, організаційних рішень, спрямованих на застосування комп'ютерної та іншої електронно-обчислювальної техніки, програмного забезпечення та інших засобів для зменшення участі користувача інформаційно-комунікаційних систем і засобів інформатизації під час збирання, приймання, обробки, передавання інформації чи трудомісткості виконуваних операцій.

Окрім цього, для вдосконалення нормативно-правового регулювання у сфері телекомунікаційних та цифрових технологій в умовах сучасності їх розвитку, необхідно сформулювати та закріпити чіткі норми, що визначають ознаки злочинності у цифровій сфері. Для боротьби зі злочинними діями, що вчиняються з використанням цифрових технологій, пропонуємо внести до КК України зміни, а саме: змінити назву Розділу XVI «Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» на «Кримінальні правопорушення у сфері використанням цифрових технологій» та розширити його, шляхом перенесення статей, склади яких передбачають застосування чи використання будь-яких цифрових технологій, що дозволить систематизувати ці види кримінальних правопорушень, враховуючи їх значне поширення на сучасному етапі розвитку громадянського суспільства та його цифровізації.

1.3. Зарубіжний досвід використання цифрових технологій та штучного інтелекту при запобіганні злочинності

Цифрові технології є невід’ємною частиною життя сучасної людини. Розвиток нових технологій позитивно впливає не тільки безпосередньо на ІТ-сферу, але і на всі сфери людського життя, такі як освіта, наука, медицина, сільське господарство (цей список можна продовжувати до безкінечності). Також людство оцінило значущість цифрових технологій під час пандемії, особливо в період самоізоляції, коли люди могли підтримувати зв’язок зі світом лише за допомогою технологій.

Людство за останнє століття здійснило значний стрибок у технологічному розвитку, який є більшим за усі попередні досягнення. З цим важко не погодитись, адже вказаній тезі є чимало наочних прикладів, які застосовуються у різних сферах. Сучасне життя важко уявити без великоформатного і яскравого Smart телевізора, ноутбука, кавомашини чи мікрохвильової печі. Останнім технологічним трендом можна вважати смартфони. Рівень їх поширення серед українців протягом 2011–2019 рр. збільшився з 7 % до 55 % відповідно. За результатами опитувань, 57 % користувачів смартфонами взагалі не уявляють своє життя без них. Смартфон за останні роки перетворився на найпоширеніший девайс. За його допомогою можна не лише безкоштовно спілкуватися з абонентом, який знаходиться у будь-якому куточку світу, а й здійснювати широкий набір операцій, у тому числі фінансових. Вже не кажучи про можливості сучасних екологічних електричних або водневих автомобілів, «розумних» будинків, які замість свого господаря виключають світло, доведуть температуру приміщення до оптимальної, викличуть сервісну службу і навіть поліцію у разі потреби. Цей список можна продовжувати і надалі [34, с. 179-180].

Охоплення життєдіяльності людей сучасними технологіями виглядає вражаюче. До переліку пристроїв і послуг, що підтримуються можливостями цифрової фіксації, можна віднести використання:

- різноманітних мобільних пристроїв, що забезпечують доступ до мережевих локальних та інтернет-ресурсів;
- послуг стільникового зв'язку
- пристроїв віртуальної реальності для безперервного доступу осіб до мобільного телекомунікаційного середовища, що дають людині можливість оперативного прийняття рішень (наприклад, окуляри «Google» полегшують орієнтування в незнайомому місці, допомагають у пошуку об'єктів і побудов, допомагають у режимі «online» отримувати інформацію про характеристики окремих пристроїв тощо);
- систем геопозиціонування, які забезпечують прив'язку фізичних об'єктів до конкретних географічних координат на місцевості;
- технології розпізнання фізичних і цифрових зображень (обличчя людей, місцевості, номерів автомобілів, різних аудіо звуків тощо);
- «розумних речей», оснащених мікропроцесорами з функціями здійснення обміну даними з телекомунікаційними мережами (наприклад, система «розумного дому», побутові прилади, оргтехніка, навігаційні системи автотранспорту, інформаційні датчики в місцях громадського користування тощо);
- концепції «інтернету речей», що дає можливість людині задовольнити запити користувачів за рахунок розширення їх мережевої взаємодії з оточуючими об'єктами [49, с. 83].

В даний час складно знайти людину, яка не була б залучена до віртуальної реальності. Люди, які проживають у розвинених країнах та країнах, що розвиваються, з удосконаленням технологій отримали можливість взаємодії через глобальну мережу – Інтернет. Саме собою функціонування «всесвітньої павутини» спричинило чимало позитивних досягнень, що використовуються в

тому числі і для боротьби зі злочинністю. Тим не менш, сам простір Інтернету є середовищем, сприятливим для розвитку злочинності. Для сучасної дійсності характерна модернізація способів та засобів вчинення кримінальних правопорушень саме за рахунок використання нових цифрових технологій. Якщо говорити про сучасну цифровізацію кримінологічних досліджень то необхідно в першу чергу, звернути увагу на важливості використання цифрових технологій для вивчення процесів криміналізації особи [3, с. 22].

Питання запобігання злочинності в умовах розвитку мережі Інтернет та цифрових технологій вивчені та досліджені недостатньо. Проте окремі аспекти використання цифрових технологій для запобігання злочинності розглядали такі автори, як В. О. Біляєв [11], О. І. Бугера [15], В. В. Ключ [11], О. І. Кузнєцов [78], П. М. Маланчук [41], Ю. А. Невмержицька [41], С. В. Пеньков [49], В. В. Шедрик [49], І. А. Юрій [78] та інші.

Проте, досить актуальним та важливим питанням діяльності правоохоронних органів на сучасному етапі є саме напрями та особливості використання цифрових технологій загалом та штучного інтелекту зокрема. Адже, необхідно досліджувати не лише переваги, але й недоліки їх застосування, оскільки їх впровадження завжди тягне за собою певні ризики. Саме тому, слід повно і всебічно вивчати напрями впровадження цифрових технологій у правоохоронну сферу, вивчати їх місце та роль при запобіганні чи попередженні злочинності, прогнозувати негативні наслідки та мінімізувати їх, визначати межі та критерії їх застосування і найголовніше визначати сферу правового регулювання їх використання.

Реалії сьогодення вказують на той факт, що досить змінилася структура мікросоціального середовища, оскільки крім негативного впливу зовнішніх чинників додався ще й криміногенний шкідливий вплив тих Інтернет ресурсів, які з метою отримання контролю над особою, цілеспрямовано використовують технології впливу на її свідомість і підсвідомість. Результатом всебічного проникнення в повсякденне життя різноманітних цифрових технологій стало

те, що віртуальна реальність отримала можливість впливати на саму особу та її свідомість [33, с. 163-164].

Множинність змінних параметрів дуже ускладнює аналіз досліджуваного феномена. Однак стан справ у даній сфері кримінологічних досліджень може бути істотно поліпшено в разі створення державної програми з дослідження особи злочинця (в тому числі і її криміналізації) з використанням сучасних можливостей цифрових технологій для збору і обробки інформації [33, с. 164; 19, с. 38].

Цифрове суспільство — це таке суспільство, яке продуктивно та інтенсивно використовує цифрові технології для власних потреб (самореалізація, робота, відпочинок, навчання, дозвілля кожного), а також для досягнення та реалізації спільних економічних, суспільних та громадських цілей. До цифрових технологій можна віднести: Інтернет речей, роботизація та кіберсистеми, штучний інтелект, великі дані, безпаперові технології, адитивні технології (3D-друк), хмарні та туманні обчислення, безпілотні та мобільні технології, біометричні, квантові технології, технології ідентифікації, блокчейн тощо. Споживачами цифрових технологій виступають усі — держава, бізнес, громадяни [72]. В Україні розроблено інноваційний комплекс аналітичної обробки інформації різноманітних банків даних з відображенням на детальній інтерактивній карті міста, як самих об'єктів, так і результатів їх аналізу. Система дозволяє відшукати логічні відкриті та приховані зв'язки між заданими об'єктами та відобразити знайдені зв'язки як у вигляді геоінформації, так і з використанням часового ряду [33, с. 164; 55]. Мова йде про інтелектуальну систему кримінального аналізу даних — RICAS (Real-time intelligence crime analytics system), яка поєднує в собі єдиний простір відображення основних і найбільш передових методів і методики кримінального аналізу та аналітичного пошуку в реальному часі, що дозволяє значно підвищити ефективність і результативність розкриття кримінальних правопорушень по гарячих слідах, а також нерозкритих раніше. RICAS

дозволяє виконувати наступні види аналізу: аналіз кримінального стану (crime pattern analysis); аналіз загального профілю (general profile analysis); аналіз конкретного розслідування (case analysis); порівняльний аналіз (comparativ analysis); аналіз групової злочинності (offender group analysis); аналіз особливостей профілю (specific profile analysis); аналіз розслідувань (investigation analysis). Призначення вказаної інтелектуальної системи кримінального аналізу даних полягає в наступному: підвищення в оперативно-розшуковій діяльності співробітників правоохоронних органів, досудовому розслідуванні, діяльності з охорони громадського порядку ефективності використання різних інформаційних обліків; зменшення часу реакції на вхідну інформацію про кримінальні правопорушення, і, як наслідок, більш ефективне їх розкриття по гарячих слідах; профілактика і попередження кримінальних правопорушень та підвищення якості та своєчасності управлінських рішень керівників усіх рівнів відповідальності [33, с. 165; 144].

Концепція розвитку цифрових компетентностей передбачає прискорення процесів цифрової трансформації в Україні; підвищення рівня цифрових навичок та цифрових компетентностей в суспільстві; підвищення конкурентоспроможності працівників шляхом оволодіння новими цифровими навичками та цифровими компетентностями; суттєве зменшення ризиків виникнення небезпек під час користування Інтернетом; запровадження правового регулювання з питань формування державної політики у сфері розвитку цифрових навичок та цифрових компетентностей громадян; розробку комплексних змін до законодавства, щодо забезпечення визначення цифрової освіти, цифрових навичок та цифрових компетентностей у сферах суспільного життя; забезпечення координації дій на рівні органів виконавчої влади з питань розвитку цифрових навичок та цифрових компетентностей; створення індикаторів для моніторингу стану розвитку цифрових навичок та цифрових компетентностей [37].

А План заходів з реалізації Концепції розвитку цифрових компетентностей містить конкретні заходи, які передбачають втілення в життя вказаних вище напрямів впровадження цифровізації. Так, зокрема, щодо: запровадження правового регулювання з питань формування державної політики у сфері розвитку цифрових навичок та цифрових компетентностей громадян з урахуванням досвіду країн ЄС; проведення інформаційних кампаній, спрямованих на популяризацію цифрових технологій в цілому та цифрових навичок та цифрових компетентностей, зокрема серед населення, на національному, регіональному та місцевому рівні тощо [50].

Незважаючи на такий позитивний вплив нових технологій на життя людини, вони впроваджуються, нажалі і в злочинність, що й виступає поштовхом до виникнення злочинності у сфері цифрових технологій. Перш за все, це пов'язано з відкритістю та доступністю інформації про нові дослідження у сфері цифрових технологій. По-друге, злочинний світ має значні матеріальні ресурси, що дозволяє їм набувати нових розробок і залучити на свою сторону передових ІТ-фахівців.

Вразливість людей у віртуальному середовищі та загрози, які воно створює зростають, тому все частіше постає питання щодо безпеки користувачів на просторах мережі Інтернет. Злочинність у сфері цифрових технологій є особливо шкідливою, адже вона проявляється в різних сферах життєдіяльності суспільства і має досить негативні наслідки, які проявляються у різних формах. Цифрова злочинність, як правова, практична та політична проблема є прямою загрозою правам людини, економіці, держави і глобального світу в цілому. Адже злочинці, навіть, у віртуальному середовищі можуть порушити або дестабілізувати стан громадянського суспільства, завдати шкоди і навіть атакувати державні інфраструктури (електромережі тощо).

Зараз кримінальні правопорушення із використанням різних технологій цифрового, інформаційного спрямування, досить зростають в структурі злочинності загалом. Окрім цього, ситуацію ускладнює посилення

транснаціонального характеру даного виду злочинності [125]. Дані Global Cyber «Дослідження сприйняття ризиків 2018» показало, що майже дві третини респондентів оцінили кіберризик як один із п'яти найвищих ризиків у своїй організації [111]. Дані звіту Євробарометр щодо кібербезпеки показують, що більшість респондентів у Латвії та серед громадян Європи стурбовані правопорушеннями в Інтернеті. Основні страхи громадян пов'язані з онлайн-транзакціями і використанням онлайн-банкінгу. Наприклад, у Латвії це визнали 65% респондентів, вони зазвичай відчують себе погано поінформованими про ризики кіберзлочинності, хоча в країнах, де більшість користувачів Інтернету відчують себе добре поінформованими, впевнені в незахищеності в Інтернеті та в тому, що зростає нездатність користувачів Інтернет захистити себе [149].

Проблема злочинності у сфері цифрових технологій визначається стрімкими розробленнями, впровадженням та використанням інформаційних технологій, а також використанням цих технологій у злочинних цілях. Кримінологічний аспект сучасних цифрових технологій різноманітний. Цифрова злочинність – це специфічна, складна сукупність кримінальних правопорушень, які можна оцінювати не тільки за їх видом, способами їх вчинення, шкідливістю, ступенем суспільної небезпеки, шкідливими наслідками, а й характеристикою особи злочинця.

Виникнення нових, сучасних кримінальних загроз, які пов'язані з використанням новітніх цифрових технологій досить часто відбувається із злочинною метою, що в свою чергу викликає необхідність вдосконалення існуючих методів кримінологічних досліджень, в тому числі і засобами цифровізації.

Як вдало відмічають Топчій В. В. та Маркушин О. Г. «визначається практична необхідність і доцільність прийняття відповідних нормативних актів у нашій державі, які передбачатимуть заходи та механізм запобігання цього виду злочинності» [71, с. с. 206].

Нині, розробляється досить багато різних програм, спрямованих на запобігання зростанню злочинності у сфері цифрових технологій, так, наприклад, в окремих зарубіжних країнах, з'являється новий напрямок у кримінології – цифрова кримінологія.

Що стосується кримінологічної науки України, то на думку О. Бугери: «для вирішення складних завдань сьогодення щодо запобігання злочинності, вона також потребує відповідного рівня фахівців, що володіють цифровими технологіями. Загалом в Україні процес цифровізації починає активно розвиватися у сфері суспільних відносин, що стосуються юриспруденції» [14, с. 47].

Саме тому, ми вважаємо, доцільно в Особливій частині Кримінології розглядати такий вид злочинності, як «Злочинність у сфері цифрових технологій» або «Цифрова злочинність», а також виокремити окремий вид Кримінології, а саме – «Цифрову кримінологію».

Сучасна кримінологічна наука потребує використання цифрових технологій при проведенні різних кримінологічних досліджень, що й обґрунтовує необхідність формування та розвитку цифрової кримінології (Digital Criminology). В межах вивчення цифрової кримінології необхідно досліджувати та вивчати сучасні напрями запобігання злочинності в умовах цифровізації; залучати громадськість до запобігання злочинності в умовах розвитку цифрових технологій; забезпечувати права громадян в цифровому суспільстві тощо.

На нашу думку, в межах цифрової кримінології можна виокремити такі основні напрями її розвитку: протидія злочинності; формування та використання баз даних кримінологічної інформації, її аналізу на основі цифрових технологій для прогнозування злочинності та запобігання і попередження злочинності; кримінологічне профілювання; використання штучного інтелекту; геномна реєстрація.

За допомогою сучасних цифрових технологій можуть створюватися обґрунтовані прогнози щодо темпоральних, територіальних і якісних показників злочинності. Ці прогнози покликані сприяти правоохоронним органам в оптимізації використання наявних ресурсів та виконання поліцейських функцій [79, с. 101].

Досліджуючи питання зарубіжного досвіду використання цифрових технологій та штучного інтелекту при запобіганні злочинності, можна проаналізувати окремі аспекти досвіду США щодо протидії злочинності у сфері цифрових технологій.

Так, можна навести приклад розпізнавання обличчя, що стало звичним інструментом для співробітників правоохоронних органів як на федеральному, так і на муніципальному рівнях. З приблизно 42 федеральних агенцій, у яких працюють співробітники правоохоронних органів, у 2021 році Управління звітності уряду виявило, що приблизно 20, або половина, використовували систему розпізнавання обличчя. У 2016 році дослідники Georgetown Law підрахували, що приблизно кожен четвертий державний і місцевий правоохоронний орган мав доступ до технології. Федеральні, державні та місцеві правоохоронні органи США часто покладаються на інструменти, розроблені в приватному секторі, і в деяких випадках можуть отримати доступ до величезних обсягів даних, які зберігаються на приватних хмарних серверах або обладнанні (наприклад, смартфони чи жорсткі диски), або доступні в громадські місця, такі як соціальні мережі чи онлайн-форуми. Зокрема, кілька державних установ придбали доступ до точної історії геолокації в агрегаторів даних, які збирають інформацію з додатків для смартфонів або інших пристроїв. Через загальну відсутність більш надійного захисту конфіденційності на федеральному рівні чи рівні штату для врахування таких досягнень у технологіях, посилені форми спостереження, які використовують поліцейські, створюють значні ризики для цивільних осіб, які вже стали

мішенню в системі кримінального правосуддя, і сприяють історичним упередженням, що впливають на громади [130].

Окремо необхідно проаналізувати цифрові технології, що застосовуються в зарубіжних країнах з метою ефективного прогнозування та планування боротьби зі злочинністю та запобігання і попередження злочинності загалом та цифрової зокрема. Проте тут необхідно пам'ятати, що цифрові системи прогнозування постійно вдосконалюються і безсумнівно допомагають правоохоронним органам, проте ті, хто їх використовує або пропонує використовувати, повинні пам'ятати і про нові проблеми, які вони можуть спричинити, в першу чергу щодо конфіденційності тих осіб, на кого вона потенційно може впливати.

Так, для прикладу ще в 2017 році Privacy News Online писав про створення в Китаї масивної поліцейської системи, яка дозволить «прогнозувати діяльність правоохоронній системі», тобто здатність виявляти осіб злочинців ще до того, як вони вчинять кримінальне правопорушення. Вказана прогностична функція поліції з використанням підходів на основі штучного інтелекту починає набувати популярності в США та Великобританії. Поліція США в містах і муніципалітетах, де проживає понад 1 мільйон людей, використовують систему від компанії PredPol. «PredPol використовує алгоритм машинного навчання для розрахунку прогнозів. Три точки даних – тип злочину, місце злочину та дата/час злочину – використовуються для розрахунку прогнозу». У результаті, місцева поліція може «передбачити, де і коли найімовірніше відбуватимуться конкретні злочини» та «проактивно патрулювати, щоб допомогти зменшити рівень злочинності та віктимізацію». У Великій Британії правозахисна група Liberty виявила, що 14 поліцейських підрозділів використовують, раніше використовували або планують використовувати алгоритми, які відображають майбутні злочини або передбачають, хто вчинить або стане жертвою злочину, спираючись на наявні поліцейські дані. PredPol використовує алгоритм машинного навчання для

обчислення своїх прогнозів. Інформація надходить із системи управління записами агентства (RMS). Жодна особиста інформація ніколи не використовується. Ніколи не використовується демографічна, етнічна чи соціально-економічна інформація. Це виключає ймовірність порушення конфіденційності чи громадянських прав, які спостерігаються в інших моделях поліцейської діяльності на основі розвідувальних даних. Прогнози відображаються у вигляді червоних прямокутників у веб-інтерфейсі Google Maps. Кожна інформація являє собою квадрат 150×150 метрів. Комірки представляють зони найвищого ризику для кожного дня та для відповідної зміни [138].

Також позитивним з точки зору зарубіжного досвіду є дослідження та вивчення проекту ЄС e-POOLICE.

Організована злочинність стає все більш різноманітною у своїй діяльності та методах, включаючи «вищий рівень співпраці між злочинними групами, більшу мобільність в ЄС та навколо нього, диверсифікацію незаконної діяльності та зростаючу залежність від динамічної інфраструктури, закріпленої в ключових місцях і сприяючої широким використанням Інтернету». Важливим засобом для правоохоронних органів у боротьбі з такою злочинністю є стратегічне раннє попередження, яке значною мірою залежить від ефективного та дієвого сканування середовища. Для цього проект e-POOLICE – у тісній співпраці з партнерами з правоохоронних органів, а також експертами з кримінології та права — розробить прототип системи сканування навколишнього середовища, яка реалізує рішення із застосуванням найперспективніших технологічних досягнень і проривів, наданих партнерами. Рішення будуть перевірені та оцінені за допомогою реалістичних сценаріїв використання, розроблених нашими партнерами-користувачами. Центральним у цьому рішенні є розробка сховища екологічних знань, що містить всю відповідну інформацію та знання, включаючи відскановану інформацію та отримані чи гіпотетичні знання, а також метадані, необхідні для оцінки

достовірності та довіри, відстеження та захисту конфіденційності. Для ефективного та дієвого використання, а також для взаємодії репозиторій застосовуватиме стандартну форму представлення всієї інформації та знань. Система вивчає електронне листування, сторінки сайтів, поліцейську інформацію тощо для пошуку даних щодо діяльності організованої злочинності та для оцінки ризику появи кримінальної активності. Для ефективного та результативного сканування джерел необробленої інформації в рамках проекту буде розроблено інтелектуальний екологічний радар, який використовуватиме сховище знань для фокусування сканування. Ключовою частиною цього процесу є семантична фільтрація для ідентифікації елементів даних, які становлять слабкі сигнали про нові загрози організованої злочинності, повністю використовуючи концепцію центрів злочинності, індикаторів злочинності та факторів сприяння [102].

Враховуючи сучасний стан злочинності та поширення вчинення легалізації доходів одержаних злочинним шляхом, а також їх транснаціональний аспект, досить важливим є застосування новітніх цифрових технологій в цілях попередження та боротьби з відмиванням коштів і загалом при запобіганні фінансовій злочинності.

Для прикладу можна дослідити та проаналізувати програмне забезпечення Palantir, якому довіряють світові банки та інші міжнародні інституції. Спочатку розроблений для використання державними розвідувальними службами та оборонними агентствами, з урахуванням проблем конфіденційності та громадянських свобод, Palantir Foundry включає неперевершені детальні засоби контролю безпеки. Усі дані шифруються як під час передачі, так і в стані спокою, і Palantir пропонує високу можливість аудиту та рольові структури контролю доступу, щоб усі команди могли отримувати доступ до необхідних даних і ділитися ними без шкоди для безпеки. Завдяки цілісному розумінню ризиків транзакцій, відносин, контрагентів, KYC і санкцій аналітики можуть швидко сортувати сповіщення та задавати додаткові

запитання, щоб усунути повну мережу пов'язаних організацій. Вбудоване керування робочим процесом забезпечує своєчасну та належну ескалацію, сортування та перегляд – із повною співпрацею та прозорістю для всіх відповідних команд. Після завершення розслідування Palantir генерує необхідну звітну інформацію з повною лінією даних до вихідних систем, динамічно оновлює звіти в міру зміни інформації та попереджає аналітиків про нові ризики [81].

Також досить активно застосовується у зарубіжній практиці запобігання злочинності метод кримінологічного профілювання. На відміну від методу криміналістичного профілювання особи злочинця, цей метод дозволяє проаналізувати окремі характеристики особи, що вчинила кіберправопорушення за результатами індукції та дедукції кримінального правопорушення.

Для прикладу в США, на основі вивчення та дослідження інтернет-файлів, що користувалася особа, історії електронних сторінок, за якими здійснювала пошук інформації ця особа виявляють певні звички особи кіберправопорушника, встановлюють певні технологічні особливості його діяльності, що дозволяє швидше ідентифікувати особу. Так, профіль кіберзлочинця поєднує в собі особисті риси, моделі поведінки та демографічні дані на основі характеристики кіберзлочинності. У кримінологічному профілюванні злочинців у сфері цифрових технологій визначаються специфічні спільні ознаки та риси [126].

Доцільно зазначити, що профілювання злочинців у сфері цифрових технологій має міждисциплінарний характер. Адже, різні типи профілювання правопорушників можна поділити на два типи: географічне профілювання та профілювання характеристики особи правопорушника [140]. Мета географічного профілювання – це використання місцезнаходження правопорушника або його відправної точки, географічний профайлер

намагається передбачити територію, в якій правопорушник живе або з якої здійснюється вчинення кримінального правопорушення [95].

Кримінальні провадження у справах про вчинення правопорушень із використанням цифрових технологій зазвичай можуть містити досить велику кількість доказів в електронній або цифровій формі. Адже, навіть саме місце вчинення кримінального правопорушення містить комп'ютерні системи або комп'ютерні мережі.

Кримінологічний профіль невідомого кіберзлочинця складається з трьох етапів: перший – це офіцер правоохоронних органів збирає дані, отримані з місця злочину, і передає їх профайлеру; по-друге, профайлер аналізує дані, а по-третє, профайлер надає можливі характеристики цього правопорушника. Процеси, які профайлери виконують для аналізу отриманих даних з місця злочину, класифікуються за природою на: «клінічні» або «статистичні» [83, с. 449].

На основі досвіду США, де досить широко використовується процес профілювання кіберзлочинців, можна проаналізувати, що він складається з чотирьох взаємопов'язаних та послідовних етапів: 1) Віктимологічний аспект. Сучасною процедурою кримінального профілювання є вивчення віктимологічних аспектів – ролі і поведінки жертви кіберзлочину, під час і після нього. Вони відкривають нову інформацію; дозволяють детально вивчити причини і наслідки та оцінити вагу ризику дій потенційної жертви. Віртуальний простір створює багато шансів зіткнутися з соціально небезпечною людиною. Контент, введений в Інтернеті, є вічним, що забезпечує довготривалий зміст інформації, саме тому, повторна віктимізація жертви, може тривати багато років і жертва навіть не здогадується про це [4, с. 132-133].

Дослідження показують, що більшості користувачам Інтернету бракує досвіду, навичок щодо визначення оцінки ризику та виявлення і запобігання шкідливим наслідкам. Наприклад, досить часто, необдумано у кіберпросторі користувачі розголошують дані особистої інформації, що є досить високим

ризиком. Кіберзлочин може завдати шкоди будь-кому: особі, підприємству чи організації.

Кібератаки на промислові системи управління (ICS) різко зросли у 2022 році, згідно зі звітом компанії-вимагача. Кількість атак програм-вимагачів на промислові організації зросла на 87%, а кількість груп програм-вимагачів, націлених на системи промислового контролю та операційних технологій (OT), зросла на 35%. Dragos Security, фірма з кібербезпеки, яка спеціалізується на захисті систем ICS. Огляд Dragos ICS/OT Cybersecurity Year in Review за 2022 рік знайшов привід для занепокоєння, оскільки у 2022 році більше кіберзлочинців і державних груп націлилися на промислові компанії. Минулого року також з'явилася нова група загроз ICS, Chernovite і Pipedream, хакерська платформа наступного покоління ICS, розроблена групою, яка здатна націлюватися на технології систем багатьох постачальників. Pipedream знаменує собою перший випадок, коли дослідники виявили зловмисне програмне забезпечення, яке може бути руйнівним або руйнівним у промислових системах управління в різних галузях, сказав Лі. Раніше зловмисне програмне забезпечення, орієнтоване на ICS, було специфічним для певних платформ, які використовувалися в об'єктах певного типу. Наприклад, Crashoverride та Industroyer 2 працювали лише на об'єктах електричних підстанцій. Шкідлива програма Trisis працювала лише на хімічних підприємствах, які використовували платформу Triconex. Pipedream не має таких обмежень, і зловмисники можуть використовувати його для націлювання на будь-яку кількість платформ і типів об'єктів [136].

Віктимологічні аспекти кіберзлочинності можна описати за допомогою Routine теорія діяльності (RAT) і Загальної теорії злочинності та віктимізації. Згідно з рекомендаціями RAT, злочин відбувається, коли три елементи взаємодіють у часі та просторі: мотивований кіберзлочинець, відповідна жертва (відповідна ціль) і відсутність активного та належного (дієвого) захисту. Таким чином, кіберзлочинність вчиняється, коли є мотивований кіберзлочинець, є

відповідна жертва і немає нікого, хто міг би запобігти кіберзлочину [150, с. 542].

Наприклад, за даними дослідження американських спеціалістів, низький рівень самоконтролю в мережі Інтернет був суттєво пов'язаний з ймовірністю відчувати три з п'яти форм віктимізації кіберзлочинців – несанкціонований доступ до власного комп'ютера, додавання, видалення чи зміна інформації на власному комп'ютері без відома чи дозволу та переслідування в Інтернеті [109].

2) З'ясування мотивів злочинця. У межах цифрової кримінології можна виділити декілька мотивів кіберзлочинності.

Так, наприклад, у Великобританії було проведено опитуванням у якому 67% хакерів визнали, що головним стимулом є гроші за злочинну діяльність у сфері цифрових технологій. Підраховано, що одному кіберзлочинцю вдається отримати більше 20 тис фунтів на рік в середньому, в середньому 8600 фунтів за кожен атаку [146].

Емоційний мотив: часто в основі кіберзлочинів лежать емоції – гнів, ненависть, помста, любов чи відчай, безвихідь. Спектр мотивацій для шахрайства широкий – жадібність, вияв влади, мстивість, авантюризм, бажання скуштувати «заборонений плід», здобути вигоду задоволення, самоствердження, здобути повагу, завдати шкоди тощо. Також це може бути помста незадоволеного працівника, приєднавшись до комп'ютерної системи роботодавця.

Мотив «Просто так» зазвичай характерний для підлітків або дітей [96]. Дані, отримані з опитування «Звички користування мобільним телефоном та Інтернетом серед дітей та молоді» показують, що лише 4% батьків знають, що їхню дитину емоційно принизили, образили через мобільний телефон, а 3% – знають, що дитина погрожувала комусь за допомогою за допомогою мобільного телефону. У свою чергу, 12% дітей зізналися, що це вчиняли. Батьки не знають про такі заняття своїх дітей: 23% батьків – не знають про

емоційне приниження, 18% – про погрози за допомогою мобільного телефону [82].

Досить потужний та швидкий розвиток інформаційних і цифрових технологій надав поштовх щодо цифровізації громадянського суспільства та використання систем штучного інтелекту (СШІ) в різноманітних сферах життєдіяльності.

Впровадження та розвиток технологій СШІ у судові системи провідних країн світу сприяли виникненню необхідності виробити єдині правила і принципи їх використання. Європейська комісія з питань ефективності правосуддя (СЕРЕJ) Ради Європи прийняла в грудні 2018 року перший європейський документ, що встановлює етичні принципи, пов'язані з використанням штучного інтелекту (ШІ) у судових системах.. Це стало першим кроком Європейської комісії з питань ефективності правосуддя до сприяння відповідальному використанню СШІ в Європейській судовій системі відповідно до цінностей РЄ.

Хартія містить положення щодо принципів діяльності політиків, законодавців та фахівців в галузі правосуддя, коли вони стикаються зі швидким розвитком ШІ в національних судових процесах . Погляд СЕРЕJ, викладений у Хартії, полягає в тому, що застосування ШІ у сфері правосуддя може сприяти підвищенню ефективності та якості і має впроваджуватися у відповідальний спосіб, який відповідає основним правам, гарантованим, зокрема, Європейською конвенцією про права людини (ЄКПЛ) і Конвенцією Ради Європи про захист персональних даних. СЕРЕJ визначила наступні основні принципи, яких слід дотримуватися у сфері ШІ та правосуддя: принцип поваги основних прав: забезпечення сумісності розробки та впровадження інструментів і послуг штучного інтелекту з основними правами; принцип недискримінації: спеціальне запобігання розвитку чи посиленню будь-якої дискримінації між окремими особами чи групами осіб; принцип якості та безпеки: щодо обробки судових рішень і даних, використовуючи сертифіковані

джерела та нематеріальні дані з моделями, розробленими на міждисциплінарній основі, у безпечному технологічному середовищі; принцип прозорості, неупередженості та справедливості: зробити методи обробки даних доступними та зрозумілими, дозволити зовнішній аудит; принцип «під контролем користувача»: виключає директивний підхід і гарантує, що користувачі є поінформованими учасниками та контролюють свій вибір. Хартія СЕРЕJ супроводжується поглибленим дослідженням використання штучного інтелекту в судових системах, зокрема додатків ШІ для обробки судових рішень і даних [108; 86].

Теплицький Б.Б. відмічає, що «перспективними напрямками використання зарубіжного досвіду боротьби з кіберзлочинами у вітчизняній науці є: удосконалення правового регулювання протидії кіберзлочинам; залучення цивільних фахівців у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку до вирішення завдань техніко-криміналістичного забезпечення розслідування кіберзлочинів (досвід Німеччини); запровадження інституту консультантів, які вивчають обставини конкретного кримінального провадження, аналізують наявну доказову базу і надають рекомендації слідчим щодо доцільності дослідження конкретних речових доказів, визначення виду експертиз та послідовності їх призначення (досвід Великої Британії); налагодження взаємодії правоохоронних та інших державних інституцій у сфері протидії кіберзлочинності (досвід Франції); залучення міжнародної технічної допомоги (зокрема, для проведення транскордонного обшуку в комп'ютерних мережах), пов'язаної з техніко-криміналістичним забезпеченням протидії кіберзлочинам в Україні. Також перспективним і доцільним є запровадження в діяльність судово-експертних установ України «Глобальних керівних принципів лабораторій цифрової криміналістики», підготовлених й опублікованих Інтерполом (INTERPOL Global guidelines for digital forensics laboratories), які схвалені та рекомендовані до впровадження Європейською

мережею криміналістичних установ (European Network of Forensic Science Institutes)» [70, с. 14-15].

Впровадження інформаційних та цифрових технологій, до системи яких належать і технології штучного інтелекту, обов'язково повинні застосовуватися задля розвитку правової, економічної, соціальної, наукової, технічної, оборонної та іншої діяльності, тобто загалом у сферах загальнодержавного значення. Саме тому, для розвитку конкурентоспроможного середовища в зазначених сферах діяльності, системи штучного інтелекту мають бути впроваджені і застосовуватися в межах концептуальних засад державної політики.

Так, освіта і професійне навчання, наука, економіка, кібербезпека, інформаційна безпека, оборона, публічне управління, правове регулювання та етика, правосуддя є пріоритетними сферами, в яких реалізуються завдання державної політики розвитку галузі штучного інтелекту, відповідно до норм Концепції розвитку штучного інтелекту в Україні. Також, вона вказує, які завдання необхідно виконати, щоб забезпечити належний рівень кібербезпеки, сфери публічного управління, правосуддя в Україні, а саме: удосконалити норми законодавства і створити сучасну нормативно-правову базу для впровадження кращих світових практик США у сфері кібербезпеки і кіберзахисту; розробити інноваційні системи кібербезпеки, які широко застосовують технології США для автоматичного аналізу та класифікації загроз і автоматичного вибору стратегії їх стримування і запобігання; вивчити питання ліцензування іноземних розробок США у сфері кібербезпеки, особливо у державному секторі; створити національні інформаційні системи, платформи і продукти у сфері кібербезпеки, що використовується органами державного управління; оновити державні стандарті щодо інформаційної безпеки, а також розробити нові національні стандарти у сфері кібербезпеки і кіберзахисту, зокрема організаційних і технічних вимог, що стосуються безпеки додатків, мобільних пристроїв, робочих станцій, серверів і мереж, моделей хмарних

обчислень; застосувати технологій США з метою виявлення випадків неправомірного втручання у діяльність електронної системи державних публічних закупівель та інших державних електронних систем; визначити необхідні заходи ресоціалізації засуджених шляхом проведення аналізу наявних даних за допомогою технологій штучного інтелекту [38].

Поліція Великобританії хоче передбачити серйозні насильницькі злочини за допомогою штучного інтелекту. Ідея полягає в тому, що особам, позначеним системою, будуть запропоновані заходи, такі як консультування, щоб запобігти потенційній злочинній поведінці. Система під назвою NDAS використовує комбінацію штучного інтелекту та статистичних даних, щоб спробувати оцінити ризик того, що хтось вчинить або стане жертвою злочину з використанням зброї чи ножа, а також ймовірність того, що хтось стане жертвою сучасного рабства [88].

Передовими користувачами ШІ в правосудді залишаються США, які використовують цифрові технології переважно в цивільних і кримінальних справах. Дослідники зі Стенфордського університету (Stanford Computational Policy Lab) розробили алгоритм, який асистує судді під час обрання запобіжного заходу для підсудного: тримання під вартою або застава. Розглянувши близько 100 тисяч процесуальних документів, пов'язаних з обранням запобіжних заходів, розробники виявили, що одні судді в 90% випадків дозволяють громадянам виходити під заставу, тоді як інші – тільки в 50%. Програма дає змогу справедливо оцінити ризики й тримати під вартою значно меншу кількість осіб, не наражаючи на небезпеку громадськість. Передумовою впровадження ШІ в Україні є запуск ЄСІТС. Проте повноцінне впровадження ЄСІТС — питання не одного року. Наразі лише у деяких судах працюють певні модулі, а електронні позови доводиться дублювати в паперовій формі. Це спричинено низкою проблем, проте у час активної політики уряду щодо цифрової трансформації можна очікувати стрімкого розвитку цієї сфери та подальшої ефективної й прозорої роботи українських судів [76].

Взагалі питання взаємовідношення використання штучного інтелекту у діяльності правоохоронних органів є доволі дискусійним. Адже, виникають питання конфіденційності даних щодо особи, як засади демократичної, соціальної держави. Адже з однієї сторони застосування умов штучного інтелекту, наприклад при виявленні особи правопорушника, може значно зекономити час, спростити та допомогти у діяльності правоохоронних органів провести певні процесуальні чи слідчі дії, оскільки основи ШІ можуть досить швидко опрацьовувати та аналізувати великі обсяги різноманітної інформації, проте з іншого боку виникає питання щодо етичної складової формування таких даних. Тому з метою ефективного застосування засобів цифрових технологій у правоохоронній діяльності необхідна чітка правова база та нормативне врегулювання такого питання, щоб дані, які отримували в результаті їх застосування були отримані законним шляхом.

Як відомо, наразі технології ШІ активно впроваджують у систему відеоспостереження з метою виявлення та припинення правопорушень, виявлення осіб, які готуються до вчинення правопорушень або їх вже вчинили. Для прикладу, ефективна робота камер відеоспостереження може допомогти попереджати кримінальні правопорушення, тим самим зменшуючи їх кількість, що надає можливість перейти на новий рівень запобігання злочинності у столиці.

Так, в межах виконання Стратегії розвитку міста Києва до 2025 року, станом на початок 2022 року комплексна система відеоспостереження Києва налічувала 7848 камер, зокрема на дорожньо-транспортних мережах з інтелектуальною аналітикою, на перехідних, завантажених станціях метрополітену, у столичних закладах освіти. Також, станції метро мають камери відеоспостереження, які мають функцію розпізнавання обличчя особи. Дані з камер надходять до поліції, муніципальної варти, державної служби з надзвичайних ситуацій, а також є джерелом статистичної інформації для департаменту охорони здоров'я КМДА [45; 1].

Отже, проведений аналіз видів цифрових технологій та порядку їх застосування при запобіганні злочинності свідчить загалом про позитивний їх вплив щодо ефективної діяльності в роботі правоохоронних органів, що однозначно свідчить про необхідність розширення напрямів і можливостей їх використання практичними працівниками. Але, однозначно, необхідно, щоб цей процес ґрунтувався і базувався на чіткій нормативно-правовій базі, а працівники правоохоронної сфери, що ними користуються мали необхідний рівень знань щодо ефективності їх застосування при попередженні та запобіганні кримінальним правопорушенням.

Під час запобігання та попередження злочинності завжди вагоме та першочергове завдання посідає ідентифікація особи. Найбільш перспективним різновидом цього є геномна реєстрація, тобто ідентифікація особи по ДНК.

В Україні прийнятий окремий ЗУ «Про державну реєстрацію геномної інформації людини», який визначає правові засади обробки геномної інформації людини з метою її державної реєстрації в Україні. Відповідно до ч. 1 ст. 4 вказаного ЗУ, державна реєстрація геномної інформації проводиться з метою: 1) ідентифікації осіб, які вчинили кримінальне правопорушення; 2) розшуку осіб, зниклих безвісти; 3) ідентифікації невідомих трупів людей, їх останків та частин тіла людини; 4) ідентифікації осіб, які не здатні через стан здоров'я, вік або інші обставини повідомити інформацію про себе. Законом передбачено проведення в Україні обов'язкової та добровільної державної реєстрації геномної інформації. Обов'язковій державній реєстрації підлягає геномна інформація: 1) осіб, яким повідомлено про підозру у вчиненні умисних тяжких чи особливо тяжких злочинів проти основ національної безпеки України, життя, здоров'я, волі, честі, гідності, статевої свободи та статевої недоторканості особи, власності, громадської безпеки, у сфері обігу наркотичних засобів, психотропних речовин, їх аналогів або прекурсорів, проти миру, безпеки людства та міжнародного правопорядку, або стосовно яких обвинувальний акт у кримінальних провадженнях зазначеної категорії злочинів

передано до суду; 2) осіб, які вчинили суспільно небезпечні діяння або злочини проти основ національної безпеки України, життя, здоров'я, волі, честі, гідності, статевої свободи та статевої недоторканості особи, власності, громадської безпеки, у сфері обігу наркотичних засобів, психотропних речовин, їх аналогів або прекурсорів, проти миру, безпеки людства та міжнародного правопорядку, та до яких за рішенням суду застосовані примусові заходи медичного характеру; 3) осіб, засуджених за вчинення умисних злочинів проти основ національної безпеки України, життя, здоров'я, волі, честі, гідності, статевої свободи та статевої недоторканості особи, власності, громадської безпеки, у сфері обігу наркотичних засобів, психотропних речовин, їх аналогів або прекурсорів, проти миру, безпеки людства та міжнародного правопорядку; 4) установлена з біологічного матеріалу, отриманого під час проведення слідчих (розшукових) дій відповідно до Кримінального процесуального кодексу України, та неідентифікована; 5) невпізнаних трупів людей, їх останків та частин тіла людини, відомості про виявлення яких унесено до Єдиного реєстру досудових розслідувань або відображено у постанові про початок досудового розслідування, винесеній у порядку, передбаченому статтею 615 Кримінального процесуального кодексу України; 6) встановлена з раніше відібраних біологічних зразків осіб, зниклих безвісти, або біологічного матеріалу з особистих речей осіб, зниклих безвісти, відомості щодо яких внесено до Єдиного реєстру досудових розслідувань або відображено у постанові про початок досудового розслідування, винесеній у порядку, передбаченому статтею 615 Кримінального процесуального кодексу України; 7) осіб, які не здатні через стан здоров'я, вік або інші обставини повідомити інформацію про себе [59].

Прийняття вказаного Закону є безумовно позитивним кроком задля забезпечення ефективного розслідування кримінальних правопорушень та пошуку осіб, зниклих безвісти чи ідентифікації загиблих. Втім, як і в мирний час, в період воєнного стану залишаються ризики і загрози витоку інформації,

які варто попереджувати вживаючи відповідних заходів та запроваджуючи на практиці належні гарантії захисту від надмірного втручання в права особи. Тобто, хоч прийняття Закону й сприятиме профілактиці та боротьбі зі злочинністю, особливо у разі вчинення особою злочину повторно, а також ефективному виконанню правоохоронними органами їхніх функцій щодо розшуку безвісти зниклих осіб і ідентифікації невпізнаних осіб, втім залишаються певні ризики, пов'язані з обробкою геномної інформації. Так, в Законі відсутні чіткі гарантії та запобіжники щодо попередження ризику втрати геномної інформації чи її витоку, а також не закріплений обов'язок володільця (контролера) повідомити особу про такі порушення безпеки персональних даних. Фактично питання запобігання ризику розкриття інформації для інших цілей чи її розголошення, у тому числі шляхом несанкціонованого доступу, в Законі чітко врегульовано лише щодо обміну геномною інформацією з іншими країнами чи міжнародними організаціями під час кримінального провадження [32].

Захищати персональні дані різних користувачів в мережі Інтернет є важливим завданням кібербезпеки та кібергігієни. Досить важливим напрямом є розробка та впровадження ефективних систем безпеки користувачів в мережі Інтернет, а також захист конфіденційної інформації і персональних даних. Враховуючи, що кібербезпека користувачів є широким поняттям, адже стосується як просто осіб-користувачів глобальної мережі Інтернет, так і підприємств, установ, організацій, органів державної влади, місцевого самоврядування, то й захист користувачів повинен бути комплексним.

Отже, сучасним напрямом розвитку кримінологічної науки є саме цифрова кримінологія, тобто використання різноманітних цифрових технологій з метою запобігання злочинності. Для підвищення рівня ефективного попередження та запобігання злочинності вказані цифрові технології необхідно застосовувати під час збору, зберігання чи аналізу кримінологічно значимої інформації. Проте задля належного та головне ефективного практичного

застосування сучасних цифрових технологій при запобіганні злочинності необхідна достатня освітня та професійна складова, тобто потрібна підготовка таких фахівців в структурі правоохоронних органів, які б могли як розробляти відповідне програмне забезпечення так і його належним чином використовувати на практиці під час попередження, запобігання, виявлення, розкриття чи загалом процесу розслідування кримінальних правопорушень.

Окрім цього, ми зазначали, щодо необхідності вдосконалення тих цифрових технологій, які застосовуються в процесі запобігання, попередження та профілактики кримінальних правопорушень, але поряд з цим необхідно також звертати увагу на професійне навчання у цій сфері працівників правоохоронної сфери. Тому, доцільною рекомендацією тут буде запровадження такої посади, як цифровий кримінолог, які чітко володітимуть крім професійної юридичної освіти, ще й знаннями у сфері програмування, програмного забезпечення, цифрових, комп'ютерних, інформаційних технологій, враховуючи перспективність такого напрямку, як цифрова кримінологія, про що ми зазначали вище.

Саме тому, на нашу думку, цілком логічною є пропозиція, щодо розробки магістерської програми для здобувачів вищої освіти, яка б саме і стосувалася застосування та використання цифрових технологій під час запобігання злочинності.

Таким чином, проаналізувавши зазначену вище інформацію, можна дійти висновку, що з метою законодавчого врегулювання питання щодо запобігання злочинності в умовах стрімкого та досить потужного розвитку мережі Інтернет та різноманітних інформаційних технологій, пропонуємо розробити та прийняти на законодавчому рівні Стратегію запобігання злочинності з використанням цифрових технологій. Запропонована Стратегія повинна містити конкретні напрями та заходи, спрямовані на використання цифрових технологій щодо запобігання різним видам злочинності на загальносоціальному, спеціально-кримінологічному та індивідуальному рівнях.

Також вона повинна базуватися на основі вивченого та дослідженого позитивного зарубіжного досвіду, щодо використання цифрових технологій з метою запобігання злочинності, який можна імплементувати у національне законодавство і на основі цього напрями, щодо вдосконалення діяльності правоохоронних органів та навчання фахівців належної кваліфікації відповідно до розвитку цифровізації.

Висновки до Розділу 1

1. Обґрунтовано положення, що для того, щоб протистояти негативним проявам в мережі Інтернет та використовувати нові можливості, необхідно розуміти суть та значення кібербезпеки, кіберзлочинності і загалом напрямів нових інформаційних технологій. Окрім цього, важливе значення має дослідження та вплив на такі напрями, як: середовище загроз кібербезпеки; потенційна вартість кібератаки для бізнесу для інших структур; оцінки ступеня безпеки підприємства, установи чи організації; аналіз можливостей вчасно реагувати на негативні інциденти та способи використання нових цифрових технологій. Запропоновано виокремити в окрему галузь віктимології – кібервіктимологію або цифрову віктимологію, оскільки віктимізація кіберправопорушень останнім часом набуває все більшого поширення, тому доцільним, на нашу думку є дослідження кіберзлочинності не лише щодо форм та способів їх вчинення та заходів запобігання, а ще й з точки зору жертви даних видів правопорушень, тобто з погляду кібервіктимізації.

2. Визначено, що, дослідження та вивчення теорії кримінологічної безпеки покликані сприяти визначенню основної її суті, тобто захисту особи, суспільства та держави від такого негативного, антисоціального явища, як злочинність, тобто виокремлення тих головних цінностей, яким і гарантується на відповідному рівні кримінологічна безпека.

3. Відмічено, що кримінальними правопорушеннями у сфері цифрових технологій є суспільно-небезпечні, протиправні, винні діяння (дія або бездіяльність), які вчиняються суб'єктами кримінальних правопорушень або у сфері цифрових технологій, або із використанням/застосуванням цифрових технологій та інших цифрових/технічних засобів, телефонних та комп'ютерних засобів та інших інформаційних та автоматизованих систем.

4. Відмічено, що дотримання та забезпечення кримінологічної безпеки у сфері цифрових технологій є вагомим пріоритетом у системі державної, економічної, національної безпеки України загалом та кібербезпеки зокрема. Щоб належним чином реалізовувати зазначений пріоритет, потрібно в першу чергу посилювати спроможності національної системи кібербезпеки з метою протидії кіберзагрозам, кібератакам та кібершахрайствам у сучасному безпековому середовищі. Зазначено, що потрібно розробити дієву систему щодо ефективної профілактики правопорушень у сфері цифрових технологій на основі чітко встановлених законодавчих вимог, які повинні регулювати цей процес.

5. Детально вивчено та проаналізовано норми Національної програми інформатизації, Закону України «Про авторське право і суміжні права», Національної стратегії сприяння розвитку громадянського суспільства в Україні на 2021-2026 роки, Стратегії кібербезпеки України, Концепції розвитку електронного урядування в Україні, Стратегії розвитку інформаційного суспільства в Україні, Стратегії інформаційної безпеки, Плану заходів з реалізації Стратегії інформаційної безпеки на період до 2025 року, Плану дій ЄС із цифрової освіти (на 2021-2027), Закону України «Про основні засади забезпечення кібербезпеки України», Стратегії кібербезпеки Європейського Союзу на цифрове десятиліття і на основі чого встановлено, що потрібно нейтралізувати чинники, які детермінують та породжують злочинність у цифровій сфері, а також необхідно своєчасно виявляти ті негативні чинники, які з використанням певних елементів цифровізації можуть здійснювати

шкідливий вплив на економіку, соціально-культурну сферу, правосвідомість громадян, телекомунікаційну, комп'ютерну та загалом інформаційну сфери.

6. Сформульовані пропозиції щодо розробки та прийняття на законодавчому рівні Стратегії запобігання злочинності з використанням цифрових технологій. Запропонована Стратегія повинна містити конкретні напрями та заходи, спрямовані на використання цифрових технологій щодо запобігання різним видам злочинності на загальносоціальному, спеціально-кримінологічному та індивідуальному рівнях. Також вона повинна базуватися на основі вивченого та дослідженого позитивного зарубіжного досвіду, щодо використання цифрових технологій з метою запобігання злочинності, який можна імплементувати у національне законодавство і на основі цього напрями, щодо вдосконалення діяльності правоохоронних органів та навчання фахівців належної кваліфікації відповідно до розвитку цифровізації.

7. Запропоновано вдосконалити способи попередження та запобігання злочинності не тільки шляхом застосування штучного інтелекту і цифрових технологій, а й запровадженням нових інститутів. Також наведено обґрунтування розробки магістерської програми для здобувачів вищої освіти, яка б саме і стосувалася застосування та використання цифрових технологій під час запобігання злочинності. Окрім цього досліджено та проаналізовано зарубіжний досвід використання цифрових технологій при запобіганні злочинності та наведено шляхи імплементції позитивних змін до законодавства України, з урахуванням практики окремих держав.

РОЗДІЛ 2

СУЧАСНИЙ СТАН ТА ТЕНДЕНЦІЇ КРИМІНОЛОГІЧНОЇ БЕЗПЕКИ У СФЕРІ ЦИФРОВИХ ТЕХНОЛОГІЙ

2.1. Сучасний стан забезпечення кримінологічної безпеки у сфері цифрових технологій

З розвитком інформатизації суспільства, забезпечення безпеки цифрових технологій стало одним із найважливіших аспектів дотримання безпеки держави. На законодавчому рівні правові засади забезпечення кримінологічної безпеки створено, але належний рівень забезпечення безпеки цифрових технологій може бути реалізовано завдяки правовим, організаційно-технічним та іншим заходам щодо прогнозування, виявлення та запобігання можливим загрозам у цій сфері, яка в даний час набула розвитку на всіх рівнях як держави, так і громадянського суспільства.

Сучасна цивілізація є свідком справді визначних змін в технологічній сфері, які модифікують курс геополітичних і геоекономічних процесів сучасного світового порядку.

Діджиталізація — вже не просто тренд, а обов'язковий етап розвитку сучасного бізнесу. Аналітики прогнозують, що інвестиції в діджиталізацію піднімуться до 16,5% на рік у 2022-2024 роках порівняно з 15,4% у 2019-2021, і до кінця 2024-го вони становитимуть 55% від усіх інвестицій в ІКТ (інформаційно-комунікаційні технології) [20].

Цифровий світ і його потенціал поширюються на всі сфери діяльності сучасного суспільства, стрімко витісняючи старий спосіб життя, старе мислення та застарілі технології. Розвиток і досить широке розповсюдження цифрових технологій створюють також можливість настання кримінологічних ризиків, які в сучасному суспільстві і визначають окремі напрями кримінальної політики країни.

Оскільки світ продовжує свою подорож у цифрову епоху, корпорації та уряди по всьому світу все більше покладаються на технології збору, аналізу та зберігання особистих даних. Це, у свою чергу, призвело до зростання кількості кіберзлочинів, починаючи від незначних порушень і закінчуючи глобальними атаками, що вражають мільярди користувачів.

Напрями запобігання злочинним проявам у цифровій сфері повинні бути зосередженими на аналізі та розумінні злочинної діяльності, неправомірної поведінки та антисоціальної поведінки, які відбуваються в Інтернеті або стосуються мережі Інтернет чи цифрових систем та середовища з метою забезпечення належного рівня кібербезпеки. Важливе значення у цьому має саме предмет дослідження цифрової кримінології, яка є актуальною та перспективною галуззю кримінології, адже впровадження цифрових технологій у сучасне суспільство має значні наслідки для повсякденного життя та стосується і сфери запобігання вчинення кримінальних правопорушень із застосуванням цифрових технологій.

Цифрова кримінологія, об'єднуючи концептуальні межі, досліджує основоположні, правові, політичні та культурні причини та умови виникнення злочинності у сфері цифрових технологій, а також загальну кримінологічну характеристику злочинності у сфері цифрових технологій та напрями її запобігання. Тобто, загалом цифрова кримінологія допоможе надати відповіді на такі питання, як: які наслідки розширення та трансформації цифрового суспільства для розвитку і виникнення злочинності? Як нові технології впливають на злочинність та яким чином сприяють вчиненню окремих видів кримінальних правопорушень? Якими будуть фундаментальні зміни в кримінологічних дослідженнях і межах для розуміння злочинності та запобігання в цьому технологічно опосередкованому контексті? Що означає бути «просто» цифровим громадянином? Як цифрові комунікації та соціальні мережі впливають на розвиток злочинності?

Пріоритетними напрямками забезпечення кримінологічної безпеки та розвитку цифрової кримінології, цифрових напрямів запобігання злочинності є:

- вивчення прихованих крипторинків, криптовалют та тіньових інфраструктур для цифрового зв'язку, а також нових технологій та нових видів злочинності, з метою вчасного її попередження;
- дослідження кібер-шахрайства, незаконних фінансових потоків і відмивання грошей, а також ринки спортивних ставок і шахрайств із використанням цифрових технологій;
- дослідження шкоди від кіберзлочинності та цифрової неправомірної поведінки, онлайн-дезінформації, сексуального насильства в Інтернеті, тощо;
- вивчення цифрових взаємодій регулятора та регулюючого органу, та дослідження поведінки жертв цифрових неправомірних дій, а також вчасного повідомлення правоохоронним органам про вчинені кримінальні правопорушення у цифровій сфері.

Значне поширення застосування цифрових технологій значно впливає на сферу та стан забезпечення кримінологічної безпеки, адже досить часто різні інформаційні та цифрові технології застосовуються під час кібератак та вчинення кібертероризму.

Так, відповідно до Закону України «Про основні засади забезпечення кібербезпеки України» кібертероризм є терористичною діяльністю, що здійснюється у кіберпросторі або з його використанням [62].

У минулому кібертероризм здебільшого був спрямований на державні установи. Але тепер підприємства та інші організації також стають цілями, тому вони повинні впроваджувати масштабні заходи кібербезпеки та пильності для протидії кібертероризму. По-перше, вони повинні переконатися, що всі пристрої Інтернету речей захищені та недоступні через загальнодоступні мережі. Для захисту від програм-вимагачів і подібних типів атак вони повинні регулярно створювати резервні копії систем і застосовувати методи постійного моніторингу. Вони також повинні використовувати брандмауери, антивірусне

програмне забезпечення та засоби захисту від шкідливих програм , щоб захистити свої системи від цих векторів атак. Компанії також повинні запровадити засоби контролю та політики ІТ-безпеки для захисту бізнес-даних. Це включає обмеження доступу до конфіденційних даних і застосування суворих паролів і процедур автентифікації, як-от двофакторна автентифікація або багатфакторна автентифікація.

Як приклад, можна навести статистичні дані найбільш значних випадків витоку даних у всьому світі станом на листопад 2023 року, за кількістю зламаних записів даних і постраждалих осіб. Найбільшим виток даних станом на листопад 2023 року став витік даних Sam4 у березні 2020 року, коли виявилось понад 10 мільярдів записів даних. Другий за величиною витік даних в історії на сьогоднішній день, витік даних Yahoo, стався в 2013 році. Спочатку компанія повідомила про один мільярд відкритих записів даних, але після розслідування компанія оновила цифру, виявивши, що постраждали три мільярди облікових записів. Наступним значним виток даних став в березні 2018 року злам безпеки національної бази даних ідентифікаторів Індії Aadhaar, коли виявлено понад 1,1 мільярда записів. Це включало біометричну інформацію, таку як ідентифікаційні номери та сканування відбитків пальців, які могли використовуватися для відкриття банківських рахунків та отримання фінансової допомоги, серед інших державних послуг. Станом на 2022 рік середня вартість одного витоку даних у всіх галузях у всьому світі становила близько 4,35 мільйона доларів США. Це виявилось найдорожчим у секторі охорони здоров'я : кожен витік, як повідомляється, коштував постраждалій стороні чималих 10,1 мільйона доларів США. Фінансовий сегмент йшов слідом за ним. Тут кожне порушення призвело до збитків приблизно в 6 мільйонів доларів США – на 1,5 мільйона більше, ніж у середньому по світу [129] (Додаток Б).

Інформаційний обмін, координація та спільні дії суб'єктів забезпечення кібербезпеки під час реагування на кіберінциденти/кібератаки здійснюються

відповідно до Порядку взаємодії суб'єктів забезпечення кібербезпеки під час реагування на кіберінциденти/кібератаки, затвердженого 22 вересня 2022 року протоколом № 20 засідання Національного координаційного центру кібербезпеки при Раді національної безпеки і оборони України. Під час обміну інформацією про кіберінциденти/кібератаки суб'єкти забезпечення кібербезпеки керуються загальними правилами обміну інформацією про кіберінциденти та переліком категорій і типів кіберінцидентів. Заходи з реагування на кіберінцидент/кібератаку проводяться суб'єктами забезпечення кібербезпеки таким чином, щоб забезпечити: швидке виявлення кіберінциденту/кібератаки; належне інформування про їх виникнення уповноважених органів та залучених сторін; запобігання, мінімізацію та усунення негативних наслідків; виявлення вразливостей; відновлення надання суб'єктами забезпечення кібербезпеки послуг; сталість і надійність систем та інших об'єктів кіберзахисту, що належать суб'єктам забезпечення кібербезпеки; унеможливлення повторної реалізації виявленого кіберінциденту, а щодо кібератак – збереження можливих електронних доказів. Окремі заходи є повторюваними і можуть виконуватися та змінюватися безперервно, доки підозріла поведінка не буде усунена, наслідки кіберінциденту/кібератаки не будуть ліквідовані, електронні докази, необхідні для проведення розслідування та аналізу процесу реагування на кіберінциденти/кібератаки, не будуть зібрані. Користувачі мають володіти якомога більшою кількістю інформації про виявлення підозрілої поведінки, знати порядок повідомлення про неї відповідним уповноваженим підрозділам (посадовим особам) суб'єкта забезпечення кібербезпеки та порядку реагування (подальші дії) на них. Для цього мають бути передбачені такі процедури: ознайомлення з політикою використання систем, мереж і застосунків (із засвідченням (фіксацією) такого ознайомлення); поширення рекомендацій, інструкцій та інших наочних матеріалів щодо виявлення підозрілої поведінки, дій та елементів, що можуть бути ознаками події безпеки, в паперовому (пам'ятки, брошури, бюлетені,

плакати тощо) чи електронному вигляді (сповіщення на комп'ютер, кінцеве (термінальне) обладнання, розсилка на електронні пошти користувачів); поширення зазначених вище матеріалів на офіційних платформах суб'єкта забезпечення кібербезпеки (вебсайти, соціальні мережі, інші платформи); навчання користувачів навичкам кібергігієни та реагуванню на підозрілу поведінку шляхом проведення онлайн- та офлайн-заходів (навчальні курси, воркшопи, вебінари, семінари, лекції тощо); підвищення обізнаності користувачів щодо порядку та способів звітування та звернення до посадових осіб (спеціалістів), що відповідають за підтримку інформаційних ресурсів та платформ суб'єкта забезпечення кібербезпеки та реагування на події інформаційної та кібербезпеки суб'єкта забезпечення кібербезпеки (проведення регулярних опитувань); забезпечення зворотного зв'язку щодо виявлення підозрілої поведінки, дій та елементів користувачем (створюються канали інформування, в тому числі анонімні та альтернативні) [43].

Урядова команда реагування на комп'ютерні надзвичайні події CERT-UA, яка діє при Держспецзв'язку, зареєструвала та дослідила протягом 2022 року 2 100 кіберінцидентів та кібератак. А від початку повномасштабного воєнного вторгнення росії в Україну – понад 1 500. За даними CERT-UA, найчастіше ворожі хакери атакують державний сектор: на нього припадає близько чверті всіх досліджених випадків. Тому захист державної інформаційної інфраструктури є надзвичайно важливим. Під особливою увагою російських хакерів залишається енергетичний сектор. Кібератаки на підприємства енергетики відрізняються складністю проведення та підготовки, їх важче виявляти. Також під постійним прицілом – компанії, що є постачальниками послуг, апаратного і програмного забезпечення для енергокомпаній. Таким чином, атаки через ланцюжок постачання залишаються джерелом загроз, яке зростає. Так, у грудні цього року фахівці зафіксували спробу атаки на один із українських об'єктів енергетики. Цю атаку намагалися здійснити саме через злам компанії-постачальника і розробника ПЗ. Окрім того,

ворожі хакери активно атакували логістичний, телеком-, комерційний, оборонний сектори тощо [87].

Система виявлення вразливостей і реагування на кіберінциденти та кібератаки – це сукупність програмних та програмно-апаратних засобів, які забезпечують проведення цілодобового моніторингу, аналізу та передачі телеметричної інформації про кіберінциденти та кібератаки, які відбулися або відбуваються на об'єктах кіберзахисту і можуть мати негативний вплив на їх стає функціонування. Загалом протягом I кварталу 2023 року за допомогою засобів Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки було детектовано 7 мільйонів підозрілих подій інформаційної безпеки (при первинному аналізі); опрацьовано 34 тисячі критичних подій інформаційної безпеки (потенційні кіберінциденти, виявлені шляхом фільтрації підозрілих подій ІБ та вторинного аналізу); зафіксовано та оброблено безпосередньо аналітиками безпеки 202 кіберінциденти [66; 27].

Протягом II кварталу 2023 року за допомогою засобів Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки було детектовано 122 мільйони підозрілих подій інформаційної безпеки (при первинному аналізі) та опрацьовано 55 тисяч критичних подій інформаційної безпеки (потенційні кіберінциденти, виявлені шляхом фільтрації підозрілих подій ІБ та вторинного аналізу). При цьому зафіксовано та оброблено безпосередньо аналітиками безпеки 191 кіберінцидент. Порівняно з I кварталом 2023 року кількість подій інформаційної безпеки у категорії «Шкідливий програмний код» зросла на 95,8%, а в категорії «Збір інформації зловмисником» – на 35,8%. Загальна кількість критичних подій інформаційної безпеки зросла на 38,1%. Загалом протягом II кварталу 2023 року фахівці ДЦКЗ продовжували фіксувати тренд до зменшення загальної кількості кібератак, націлених на українські організації різних форм власності та галузей, що спостерігається від початку 2023 року. При цьому найбільша кількість атак

була націлена на фінансовий, урядовий, медійний, енергетичний та телекомунікаційний сектори [28].

У період з листопада 2021 року по жовтень 2022 року в усьому світі було виявлено майже 16 тисяч кіберзлочинів. З цієї загальної кількості майже 700 випадків стосувалися невеликих компаній. Організації в секторі державного управління найбільше постраждали серед досліджуваних галузей, де було зареєстровано 3270 випадків кіберзлочинності. Інформаційний сектор посів друге місце, а виробництво – з приблизно 1800 інцидентами в кожній галузі. Загальна кількість інцидентів кіберзлочинності з листопада 2021 року по жовтень 2022 року за галузями та розмірами організацій наведена у Додатку [113] (Додаток В).

Реагування на кіберінциденти/кібератаки здійснюється суб'єктами забезпечення кібербезпеки шляхом вжиття заходів до кіберзахисту, спрямованих на швидке виявлення та захист від кіберінцидентів/кібератак, належне інформування про них, запобігання негативним наслідкам, їх мінімізації та усунення, виправлення вразливостей, а також відновлення сталості і надійності функціонування інформаційних, електронних комунікаційних, інформаційно-комунікаційних систем, технологічних систем та інших об'єктів кіберзахисту. Реагування на кіберінциденти/кібератаки здійснюється суб'єктами забезпечення кібербезпеки послідовно такими етапами, як підготовка, виявлення та аналіз, стримування, усунення, відновлення, аналіз ефективності заходів з реагування на кіберінциденти/кібератаки. На етапі виявлення та аналізу суб'єкти забезпечення кібербезпеки здійснюють виявлення кіберінциденту/кібератаки та визначають їх критичність для забезпечення пропорційності та/або співрозмірності подальших заходів з кіберзахисту реальним та потенційним ризикам. Суб'єкти забезпечення кібербезпеки визначають критичність кіберінциденту/кібератаки відповідно до методичних рекомендацій щодо реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі, затверджених

Адміністрацією Держспецзв'язку, за такими категоріями (рівнями): рівень 0, некритичний (білий); рівень 1, низький (зелений); рівень 2, середній (жовтий); рівень 3, високий (помаранчевий); рівень 4, критичний (червоний); рівень 5, надзвичайний (чорний) [54].

Особливу роль у запобіганні кібератакам та кіберінцидентам займає створення ефективної системи правового регулювання цифрової економіки, в тому числі і системи протидії кримінальним правопорушенням у зазначеній сфері.

Так ЗУ «Про стимулювання розвитку цифрової економіки в Україні» «визначає організаційні, правові та фінансові засади функціонування правового режиму Дія Сіті, що запроваджується з метою стимулювання розвитку цифрової економіки в Україні шляхом створення сприятливих умов для ведення інноваційного бізнесу, розбудови цифрової інфраструктури, залучення інвестицій, а також талановитих спеціалістів» [65].

Саме тому, в межах кримінально-правових та кримінологічних досліджень, вагоме значення має чітке розмежування та класифікація окремих складів кримінальних правопорушень, які вчиняються в цифровому середовищі та інформаційно-комп'ютерних сферах, як визначення їх окремої типології, а також надання чіткого визначення цифрової злочинності, що включає в себе ті суспільно-небезпечні, винні, протиправні діяння, які вчиняються у цифровому середовищі загалом або з використанням цифрових технологій.

Діяльність із забезпечення кібербезпеки спрямована на зниження ризиків кібербезпеки, носить безперервний циклічний характер та формує цикл управління кібербезпекою, який складається з п'яти функцій кібербезпеки: ідентифікація ризиків; кіберзахист; виявлення кіберінцидентів; реагування; відновлення поточного стану кібербезпеки. Аналіз інцидентів кібербезпеки проводиться для забезпечення ефективного реагування та заходів з відновлення відповідно до процесу виявлення та плану реагування. Аналіз передбачає перегляд повідомлень і визначення необхідності подальшого розслідування,

розуміння потенційного впливу, проведення криміналістичних заходів, класифікацію інциденту відповідно до плану реагування та аналіз виявлених вразливостей [60].

Функціонування організаційно-технічної моделі кіберзахисту забезпечується шляхом: формування та реалізації державної політики у сфері кібербезпеки, зокрема з урахуванням досвіду держав – членів ЄС та НАТО; координації суб'єктів кіберзахисту під час здійснення заходів щодо забезпечення кібербезпеки об'єктів критичної інформаційної інфраструктури та національних електронних інформаційних ресурсів; кіберзахисту інформаційно-телекомунікаційних систем, що обробляють національні електронні інформаційні ресурси, комунікаційних систем та об'єктів критичної інформаційної інфраструктури, їх кіберстійкості, здійснення постійного контролю за станом їх кіберзахисту; розвитку системи реагування на кіберзагрози; розвитку сил кіберзахисту та системи їх координації; створення систем управління ризиками інформаційної безпеки на об'єктах критичної інфраструктури; формування та розвитку спроможностей суб'єктів забезпечення кібербезпеки; створення умов для безпечного функціонування інформаційної інфраструктури державних органів, органів місцевого самоврядування, військових формувань, утворених відповідно до закону, підприємств, установ та організацій незалежно від форми власності; створення умов для розвитку державно-приватної взаємодії в сфері кібербезпеки; розвитку системи кадрового, матеріально-технічного та експертно-аналітичного забезпечення сил кіберзахисту; розвитку та постійного вдосконалення систем кіберзахисту об'єктів критичної інфраструктури з урахуванням результатів оцінки повноти, адекватності, результативності та ефективності процесів, що виконуються в рамках впровадження системи інформаційної безпеки на об'єктах критичної інфраструктури [53].

Кібертерористичні акти можуть здійснюватися з використанням комп'ютерних серверів, інших пристроїв і мереж, видимих у публічному

Інтернеті. Захищені державні мережі та інші обмежені мережі теж можуть ставати цілями таких дій. Інші цілі можуть включати банківську індустрію, військові об'єкти, електростанції, центри управління повітряним рухом і системи водопостачання.

У межах міжнародної технічної допомоги, завдяки підтримці проєкту USAID «Кібербезпека критично важливої інфраструктури України», Державний центр кіберзахисту Держспецзв'язку отримав можливість розширити ключові компоненти основних складових Системи виявлення вразливостей і реагування на кіберінциденти та кібератаки, Системи захищеного доступу державних органів до мережі Інтернет та Національного центру резервування державних інформаційних ресурсів. Серед переданого, телекомунікаційне і мережеве обладнання, яке необхідне для безперебійного та резервного забезпечення функціонування зазначених вище систем, а також інше технічне та програмне устаткування. Завдяки цьому Державний центр кіберзахисту Держспецзв'язку посилить захист критичних інформаційних ресурсів державних органів та установ, що в свою чергу надасть можливість збільшити стійкість критичної інфраструктури країни до кібератак з боку російської федерації, а також дозволить суттєво зменшити витрати коштів державного бюджету [23].

Саме тому досить важливим напрямом діяльності на рівні держави є саме визначення пріоритетних заходів щодо зміцнення системи цифрової безпеки. В першу чергу, вважаємо, що завжди важливо звертати увагу на якість фахівців в тій чи іншій галузі, тому доцільно постійно підвищувати рівень підготовки фахівців у сфері цифрових технологій, а також оновлювати та впроваджувати якісне програмне забезпечення правоохоронних структур для своєчасного виявлення та протидії цифровій злочинності і загалом запобігання правопорушенням у цифровому середовищі. Окрім цього, має бути сформована дієва система автоматизованого обміну інформацією на випадок будь-якого виду загроз у цифровому просторі, адже сучасні цифрові технології можуть

виступати способом чи засобом вчинення багатьох видів кримінальних правопорушень. Необхідно розгортати системи управління інформаційною безпекою, що використовують інформацію з усіх сховищ даних і велике значення у цьому відіграє питання конфіденційності її забезпечення.

Враховуючи той факт, що зростає кількість кримінальних правопорушень, що вчиняються з використанням цифрових технологій, змінюються і вдосконалюються способи їх вчинення, що однозначно впливає на стан протидії і виявлення вказаних правопорушень. Саме тому, вагомим напрямом діяльності щодо побудови дієвої системи кібербезпеки є в першу чергу вдосконалення нормативно-правової бази, яка регулює вказану сферу діяльності та вдосконалення системи управління щодо регулювання цифровізації суспільства. Окрім цього, вважаємо за доцільне, проведення різних курсів підвищення кваліфікації, тренінгів з питань кібербезпеки не лише для працівників Кіберполіції України, а й для усіх співробітників правоохоронних органів і також проводити інформування громадян щодо забезпечення та дотримання безпеки в кіберпросторі, шляхом, наприклад проведення лекцій у навчальних закладах, на підприємствах, установах, організаціях, розміщення інформації щодо безпечного користування всесвітньою мережею Інтернет тощо, з метою забезпечення належного рівня кримінологічної безпеки в нашій державі.

Останнім часом, все частіше стає популярним використання віртуальних сховищ пам'яті для зберігання інформації, що свідчить про необхідність створення системи безпеки таких серверів. Також вимагає окремої уваги і використання штучного інтелекту. Такі технології вимагають експертних знань у галузі безпеки для вирішення трьох ключових завдань: захист цифрових бізнес-систем, що працюють на базі штучного інтелекту, використання штучного інтелекту в продуктах та сервісах для посилення захисту та запобігання його використанню в злочинних цілях.

Під час проведення заходів із дотримання та забезпечення кримінологічної безпеки у сфері цифрових технологій, доцільним у діяльності правоохоронних органів забезпечувати співробітництво і взаємодію із різними підприємствами, установами і організаціями, які мають досвід щодо протидії правопорушенням у цифровій сфері та застосовують відповідні заходи захисту даних та інформації в процесі своєї діяльності.

За рахунок масового впровадження нових інформаційних технологій не лише прискорюється розвиток цивілізації, а й виникають різні негативні наслідки. Відповідно, для боротьби з такими наслідками має бути своєчасно розроблена відповідна державна політика у цій сфері, особливо це важливо у вирішенні питань, пов'язаних із забезпеченням безпеки цифрової інформації та протидією злочинним посяганням у сфері цифрових технологій. Саме тому, проблему забезпечення кримінологічної безпеки в цілому та кримінально-правового захисту цифрової інформації, зокрема, необхідно вважати пріоритетними напрямками діяльності, оскільки перехід до цифрової економіки пов'язаний із необхідністю вирішення цілої низки політичних, економічних та соціальних завдань з метою мінімізації можливих негативних наслідків для суспільства.

2.2. Кримінальні правопорушення, що вчиняються із використанням цифрових технологій та цифрової валюти

Кіберпростір є цифровою платформою, віртуальним, штучним, онлайн-світом, який створений комп'ютерами або пристроями чи компонентами з підтримкою Інтернету для спілкування та іншими цифровими технологіями. На цій онлайн-платформі користувачі взаємодіють і спілкуються один з одним за допомогою Інтернету, проте, нажаль цей простір стає також можливістю для злочинних проявів. Правопорушення у віртуальному світі становлять серйозну загрозу для людей, оскільки злочинці у сфері цифрових технологій

використовують абсолютно різні сучасні комп'ютерні технології для доступу до особистої, конфіденційної чи іншої інформації, документів особи чи організації за певних зазвичай матеріальних цілей.

Загальна цифровізація, діджиталізація та інформатизація суспільства значно загострила зазначену проблематику та потребує правового врегулювання також актуальним є питання щодо змісту, характеристики та поняття злочинності у сфері цифрової інформації та цифрових технологій, а також визначення кримінальних правопорушень, що вчиняються із використанням цифрових технологій та цифрової валюти.

Цифрова злочинність продовжує створювати економічні, безпекові та технологічні проблеми для розвинутих і менш розвинених країн. Суспільство та держави все більше залежать від цифровізації та інформаційних комунікацій, цифрових технологій, що в свою чергу підвищує і ймовірність кіберзлочинності.

Так, цифрова валюта все частіше використовується організованими злочинними групами для здійснення незаконної їх злочинної діяльності, наприклад з метою легалізації доходів, одержаних злочинним шляхом, або вчинення інших кримінальних правопорушень, що пов'язані з корупцією. Злочинці можуть використовувати цифрові технології та цифрову валюту замість офіційної банківської системи з метою переміщення коштів у великих чи особливо великих розмірах. Вказані злочинні дії набагато складніше стає виявити правоохоронним органам або певним фінансовим установам, які зобов'язані подавати звіти про підозрілі операції. Тому, дослідження вказаної проблематики є важливим як з теоретичної так і практичної сторони, що повинно включати координацію розробки та впровадження нормативної та законодавчої бази, інформування громадськості про ризики використання цифрових ресурсів та зміцнення потенціалу правоохоронних органів для ліквідації злочинних мереж.

Цифрова ера персональних комп'ютерів та інших пов'язаних технологій використовується для обміну інформацією з іншими за допомогою різних підходів. Однак є багато злочинних організацій, які використовують комп'ютерні і цифрові технології для вчинення кримінальних правопорушень, які варіюються від викрадення особистої інформації з комп'ютера до викрадення іншої конфіденційної інформації з метою отримання конкурентної переваги. Цифрові кримінальні правопорушення бувають багатьох видів, і інколи їх важко своєчасно виявити.

Хакери можуть використовувати персональний комп'ютер, анонімний пристрій або портативний пристрій для вчинення різних видів кримінальних правопорушень. Програмне забезпечення можуть використовувати для копіювання імен користувачів і паролів для доступу до секретних або захищених даних. Тому, із зростанням злочинності у сфері цифрових технологій, комп'ютерних систем, все більше коштів витрачається і на запобігання вказаним правопорушенням та боротьбу з ними.

Теплицький Б. Б. зауважує, що аналіз криміногенної ситуації в Україні та практики органів досудового розслідування підтверджує тенденцію до збільшення кількості випадків кримінальних правопорушень, пов'язаних з обігом комп'ютерної інформації, а також діянь, у яких комп'ютерні інформаційні системи є засобами та знаряддями їх учинення або ж використовуються для приховування факту і слідів злочинної діяльності, а також спрямування зусиль правоохоронців на хибні об'єкти. Процеси глобальної інформатизації безпосередньо впливають на криміногенну ситуацію, обумовлюють нові способи і технології злочинних посягань в інформаційному просторі й середовищі комп'ютерних мереж. Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем і комп'ютерних мереж, а також мереж електрозв'язку здебільшого високолатентні. Злочинній діяльності відповідного спрямування притаманні переважно системний, професійний і груповий характер, наявність

у правопорушників спеціальних знань, умінь і навичок у різних галузях науки і техніки (електроніка, електротехніка, програмування, телекомунікації, зв'язок тощо) [70, с. 1].

Вивчення та дослідження злочинності у сфері цифрових технологій є важливим з кількох причин: по-перше, цей вид злочинності стає все більш поширеною загрозою в епоху цифрових технологій і досить велика кількість користувачів мережі Інтернет стають жертвами кібератак, тому необхідно розробляти ефективніші стратегії попередження та боротьби зі злочинністю у сфері цифрових технологій; по-друге, потрібно вдосконалювати нормативно-правову базу, спрямовану на мінімізацію впливу злочинності у сфері цифрових технологій на окремих осіб, суспільство та державу загалом.

Технічні інновації можна використовувати для суспільного блага, проте досить часто вони стають елементом також злочинного світу. Це більше стосується кіберзлочинності, ніж, можливо, будь-якої іншої сфери злочинності. Крім того, кіберзлочинці стають більш агресивними. Сучасні реалії такі, що цифрові технології кардинально змінили наше повсякденне життя і, водночас, створили нові види загроз безпеці інформації та всього глобального інформаційного простору.

Так, зокрема Бодунова О. М. відмічає, що сьогодні суспільство переживає стрімкий прогрес автоматизації, інформатизації та комп'ютеризації у всіх сферах. Ці процеси відкривають нові перспективи для розвитку культури, освіти, науки й економіки кожної країни, а також сприяють швидкій взаємодії з іншими країнами та міжнародними організаціями. Однак розповсюдження інформаційних технологій має й негативні наслідки, оскільки воно відкриває можливості для кримінально протиправної поведінки. Комп'ютерні системи надають нові, дуже вдосконалені можливості для вчинення раніше невідомих порушень та традиційних кримінальних правопорушень, але за допомогою нетрадиційних засобів. У цьому контексті терміни «кіберзлочинність», «кібершахрайство», «хакери», «комп'ютерний злом» та «крадіжка машинного

часу» вже не є невідомими поняттями. Сьогодні злочинність у сфері інформаційних технологій є однією з найдинамічніших категорій суспільно небезпечних порушень. Неможливо заперечити, що швидке зростання поширення такої злочинності та постійне збільшення її суспільної небезпеки стали негативним результатом такого важливого суспільного процесу, як інформатизація [12, с. 285].

Зважаючи на те, що кіберзлочинність вчиняється у всьому світі, контекст кіберзлочинності залишається спірним. Так, деякі зарубіжні дослідники стверджують, що відсутність визначень, стандартизації та класифікації кіберзлочинності перешкоджають зусиллям у прогнозуванні та оцінці такої незаконної діяльності [137, с. 381].

Для визначення та класифікації кіберзлочинності використовувалися такі терміни: кіберзлочинність, комп'ютерна злочинність, електронна злочинність, інтернет-злочинність, цифрова злочинність, онлайн-злочинність, віртуальна злочинність, техно-злочинність та чиста злочинність [128, с. 8].

З розвитком цифрових технологій розвивається і кіберзлочинність, змінюються та вдосконалюються правопорушення, які вчиняються у цій сфері, так, для прикладу до них можна віднести: фішинг, несанкціонований доступ до різноманітних комп'ютерних систем і сайтів; поширення дитячої порнографії через мережу інтернет, кібергрумінг (онлайн-грумінг – це новий вид сексуального насильства дітей та підлітків в інтернеті), порушення авторських прав, продаж нелегальних речей через мережу інтернет, різні фінансові шахрайства у віртуальному середовищі, кіберсталкінг (анонімне, приховане вистежування потерпілих задля організації злочинних дій на кшталт спроб домагання, зґвалтування, фізичного насильства, побиття. Відстежуючи через Інтернет користувачів, злочинець може отримувати інформацію про час, місце та всі необхідні умови здійснення майбутнього нападу) [84, с. 44].

Подібні кримінальні правопорушення часто називають «комп'ютерними», проте кримінальні правопорушення у сфері цифрових

технологій необхідно відмежовувати від кримінальних правопорушень у сфері інформаційно-телекомунікаційних технологій. Оскільки це є правопорушення, предметом яких виступає цифрова інформація і як спосіб вчинення виступають цифрові технології.

Поняття цифрової злочинності досить часто замінюють такими термінами як кіберзлочинність, електронна злочинність, комп'ютерна злочинність, тощо. Незважаючи на те, що, на відміну від інших кримінальних правопорушень, правопорушення у сфері цифрових технологій мають свої особливості. Так, вони не мають чітких географічних меж, адже можуть бути вчиненими в одній державі, а наслідки наступати абсолютно в іншій. Місцем вчинення цифрового кримінального правопорушення є віртуальне середовище; комп'ютерні дані, цифрові системи або соціальні мережі, які використовуються для його вчинення.

Діапазон можливостей, якими намагалися скористатися кіберзлочинці, вражає, адже ці кримінальні правопорушення включають: використання ботнетів – мереж пристроїв, заражених зловмисним програмним забезпеченням без відома користувачів — для передачі вірусів, які отримують незаконне дистанційне керування пристроями, крадуть паролі та відключають антивірусний захист; створення «чорних дверей» на скомпрометованих пристроях, щоб дозволити крадіжку грошей і даних, або віддалений доступ до пристроїв для створення ботнетів; створення онлайн-форумів для торгівлі хакерським досвідом; непробивний хостинг і створення контр-антивірусних сервісів; відмивання традиційних і віртуальних валют; вчинення онлайн-шахрайства, наприклад через системи онлайн-платежів, карток і соціальної інженерії ; різні форми сексуальної експлуатації дітей в Інтернеті, включаючи розповсюдження в Інтернеті матеріалів про сексуальне насильство над дітьми та пряму трансляцію сексуального насильства над дітьми; онлайн-хостинг операцій, пов'язаних з продажем зброї, фальшивих паспортів, підроблених і клонованих кредитних карток, наркотиків і хакерських послуг. Зловмисне або

шкідливе програмне забезпечення проникає в комп'ютерну систему або мобільний пристрій і отримує контроль над ними, щоб викрасти цінну інформацію або пошкодити дані. Технічні та цифрові інновації використовуються як для суспільного блага, так нажаль і в злочинних цілях, про що ми неодноразово відмічали. Це більше стосується кіберзлочинності, ніж, можливо, будь-якої іншої сфери злочинності. Крім того, кіберзлочинці стають більш агресивними. Тому Європол та його партнерські організації ведуть боротьбу з ними на всіх фронтах. Кіберзлочинність є зростаючою проблемою для таких країн, як країни-члени ЄС, у більшості з яких інфраструктура Інтернету добре розвинена, а платіжні системи онлайн. Але ключовою мішенню для кіберзлочинців є не лише фінансові дані, а дані в цілому. Кількість і частота витоку даних зростає, а це, у свою чергу, призводить до збільшення випадків кібершахрайства та кібервимагання [94].

З огляду на такий спектр заходів, які здійснюються з такою винахідливістю, реакція Європолу та його партнерів сама по собі повинна бути комплексною, динамічною та невинно інноваційною. Таким чином, Європол створив Європейський центр боротьби з кіберзлочинністю (EC3), щоб посилити реагування правоохоронних органів на кіберзлочинність у ЄС і допомогти захистити європейських громадян, підприємства та уряди. EC3 був створений за ініціативою Європейської комісії та після схвалення Ради ЄС, з мандатом служити європейським інформаційним центром з кіберзлочинності. Він був створений як частина структури Європолу, щоб полегшити взаємодію з іншими сферами злочинності. Робота EC3 зосереджена на таких напрямках: кіберзлочини, вчинені організованими групами, зокрема тими, які отримують великі кримінальні прибутки, як-от онлайн-шахрайство; кіберзлочини, які завдають серйозної шкоди жертві, наприклад, сексуальна експлуатація дітей в Інтернеті; кіберзлочини (включаючи кібератаки), що впливають на критичну інфраструктуру та інформаційні системи в Європейському Союзі. Однією з функцій Центру є звітування про відповідну кіберзлочинність, сексуальну

експлуатацію дітей в Інтернеті, шахрайство з платежами та пов'язані з ними онлайн-загрози, а також надання спеціалізованих тематичних стратегічних оцінок щодо нових тенденцій, злочинних методів і посередників злочинності. У зв'язку з цим щорічна оцінка загрози організованої злочинності в Інтернеті є головним стратегічним продуктом ЕСЗ. ЕСЗ також бере участь у навчанні та діяльності з розвитку потенціалу; вони в основному адресовані правоохоронним органам держав-членів ЄС і охоплюють такі сфери, як: шахрайство з платіжними картками, боротьба з сексуальною експлуатацією дітей в Інтернеті та ІТ-криміналістика з відкритим кодом. Однією з головних цілей ЕСЗ є підвищення його превентивних можливостей у боротьбі з кіберзлочинністю, водночас допомагаючи правоохоронним органам бути на крок попереду кіберзлочинців. Важливою частиною цих зусиль є спеціалізація на ранньому попередженні, оцінці загроз кіберзлочинності та методах підвищення обізнаності. ЕСЗ сприяє узгодженню взаємодії правоохоронних органів у державах-членах ЄС, працюючи над колективним оглядом, який матиме важливе значення для політики, зокрема щодо визначення IP-адрес, злочинного зловживання системою доменних імен, питань акредитації конфіденційності проксі, реєстрації точних даних та потужний механізм відповідності для акредитованих реєстраторів і реєстрів доменних імен. Досліджуючи та вдосконалюючи знання правоохоронних органів про архітектуру та структуру управління Інтернетом, ЕСЗ може отримати краще розуміння ландшафту управління Інтернетом, що стане в нагоді для розслідувань усіх держав-членів і третіх сторін [107].

Під кримінальними правопорушеннями у сфері цифрових технологій розуміється передбачене кримінальним законом винне, протиправне, суспільно небезпечне діяння, спрямоване на порушення конфіденційності, цілісності, достовірності та доступності цифрової інформації, що охороняється законом або вчинене з використанням цифрових технологій або щодо них.

До них зокрема, можна віднести шахрайства з використанням інтернет-технологій, продаж і поширення конфіденційної інформації, шахрайські схеми в геймерській індустрії, обіг товарів та послуг, які не є легальними в правовому обігу, зростання кіберекстремізму, і особливо його найбільш небезпечної форми – кібертероризму.

Проаналізувавши кримінально-правові норми КК України, можна визначити перелік кримінальних правопорушень, які можуть вчинятися у цифровій сфері. Так, можна зазначити правопорушення, які пов'язані з використанням цифрових технологій, застосуванням засобів чи способів цифрової сфери та передбачені в КК України, а саме:

- ч.3 ст. 190 КК України «Шахрайство, вчинене шляхом незаконних операцій з використанням електронно-обчислювальної техніки»;
- ст. 163 КК України «Порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв'язку або через комп'ютер»;
- ст. 111-1 КК України «Колабораційна діяльність», примітка до якої зазначає, що «публічним вважається поширення закликів або висловлення заперечення до невизначеного кола осіб, зокрема у мережі Інтернет або за допомогою засобів масової інформації»;
- ст. 176 КК України «Порушення авторського права і суміжних прав», яка передбачає «Незаконне відтворення, використання та розповсюдження творів науки, літератури і мистецтва, комп'ютерних програм і баз даних, інших творів, а так само незаконне відтворення, використання та розповсюдження виконань, фонограм, відеогам і програм мовлення, їх незаконне тиражування та розповсюдження на аудіо- та відеокасетах, дискетах, інших носіях інформації, камкординг, кардшейрінг або інше умисне порушення авторського права і суміжних прав, а також фінансування таких дій, якщо це завдало матеріальної шкоди у значному розмірі»;

– ст. 200 КК України «Незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, електронними грошима, обладнанням для їх виготовлення», яка передбачає підробку документів на переказ, платіжних карток чи інших засобів доступу до банківських рахунків, електронних грошей, а так само придбання, зберігання, перевезення, пересилання з метою збуту підроблених документів на переказ, платіжних карток або їх використання чи збут, а також неправомірний випуск або використання електронних грошей;

– ст. 156-1 КК України «Домагання дитини для сексуальних цілей», яка у ч.1 передбачає, пропозицію зустрічі, зроблену повнолітньою особою, у тому числі з використанням інформаційно-телекомунікаційних систем або технологій, особі, яка не досягла шістнадцятирічного віку, з метою вчинення стосовно неї будь-яких дій сексуального характеру або розпусних дій, у разі якщо після такої пропозиції було вчинено хоча б одну дію, спрямовану на те, щоб така зустріч відбулася;

– ч.2 ст. 156-1 КК України «Пропозиція зустрічі, зроблена повнолітньою особою, у тому числі з використанням інформаційно-телекомунікаційних систем або технологій, неповнолітній особі з метою втягнення її у виготовлення дитячої порнографії, якщо після такої пропозиції було вчинено хоча б одну дію, спрямовану на те, щоб така зустріч відбулася»;

– ст. 203-2 КК України «Незаконна діяльність з організації або проведення азартних ігор, лотерей», яка передбачає «організацію або проведення азартних ігор без ліцензії на провадження відповідного виду діяльності з організації та проведення азартних ігор, що видається відповідно до закону або випуск чи проведення лотерей особою, яка не має статусу оператора лотерей, або організація чи функціонування закладів з метою надання доступу до азартних ігор чи лотерей, які проводяться в мережі Інтернет»;

– ч. 2 ст. 289 КК України «Незаконне заволодіння транспортним засобом», яка передбачає «Незаконне заволодіння транспортним засобом, вчинене з використанням електронних пристроїв для втручання в роботу технічних засобів охорони»;

– ч. 2 ст. 301 КК України «Ввезення, виготовлення, збут і розповсюдження порнографічних предметів», яка передбачає «Ввезення в Україну творів, зображень або інших предметів порнографічного характеру з метою збуту чи розповсюдження або їх виготовлення, зберігання, перевезення чи інше переміщення з тією самою метою, або їх збут чи розповсюдження, а також примушування до участі в їх створенні, вчинені щодо кіно- та відеопродукції, комп'ютерних програм порнографічного характеру, а також збут неповнолітнім чи розповсюдження серед них творів, зображень або інших предметів порнографічного характеру»

– ст. 301-1 КК України «Одержання доступу до дитячої порнографії, її придбання, зберігання, ввезення, перевезення чи інше переміщення, виготовлення, збут і розповсюдження», яка у ч.1 передбачає «умисне одержання доступу до дитячої порнографії з використанням інформаційно-телекомунікаційних систем чи технологій або умисне її придбання, або умисне зберігання, ввезення в Україну, перевезення чи інше переміщення дитячої порнографії без мети збуту чи розповсюдження»;

– ст. 301-2 КК України «Проведення видовищного заходу сексуального характеру за участю неповнолітньої особи», яка у ч.1 передбачає «проведення видовищного заходу сексуального характеру, у тому числі з використанням інформаційно-телекомунікаційних систем або технологій, у якому задіяно неповнолітню особу»;

– ч. 2 ст. 301-2 КК України «Відвідування видовищного заходу сексуального характеру з метою його перегляду, у тому числі з використанням інформаційно-телекомунікаційних систем або технологій, у якому завідомо для відвідувача задіяно малолітню чи неповнолітню особу»;

– ч. 3 ст. 301-2 КК України «Втягнення неповнолітньої особи до участі у видовищному заході сексуального характеру, що проходить, у тому числі з використанням інформаційно-телекомунікаційних систем або технологій»;

– ст. 321-1 КК України «Фальсифікація лікарських засобів або обіг фальсифікованих лікарських засобів», яка у ч. 2 передбачає «виготовлення, придбання, перевезення, пересилання, зберігання з метою збуту або збут завідомо фальсифікованих лікарських засобів за допомогою інформаційних систем, у тому числі Інтернету»;

– ст. 361 КК України «Несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж»;

– ст. 361-1 КК України «Створення з метою протиправного використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут»;

– ст. 361-2 КК України «Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації»;

– ст. 362 КК України «Несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї»;

– ст. 363 КК України «Порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється»;

– ст. 363-1 КК України «Перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних

мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку;

– ст. 368-5 КК України «Набуття особою, уповноваженою на виконання функцій держави або місцевого самоврядування, активів, вартість яких більше ніж на шість тисяч п'ятсот неоподатковуваних мінімумів доходів громадян перевищує її законні доходи», де під активами розуміється також і криптовалюта [39].

Таким чином, кримінальні правопорушення, що пов'язані із використанням цифрових технологій, можна поділити на дві категорії:

– кримінальні правопорушення, що посягають безпосередньо на саму цифрову інформацію, роботу інформаційних систем та банків даних цифрову інфраструктуру тощо, тобто коли цифрові технології виступають загальними або окремими характеристиками предмету злочинного посягання. Загалом, такими кримінальними правопорушеннями можна охарактеризувати ті, що пов'язані із використанням шкідливого програмного забезпечення, так, для прикладу шкідливих вірусів, які можуть заражати комп'ютерні пристрої, або ж кримінальні правопорушення щодо несанкціонованого доступу до електронних систем, цифрових об'єктів, комп'ютерних мереж тощо. Що ж стосується суб'єктів вчинення таких кримінальних правопорушень, то зазвичай вони володіють спеціальними знаннями в галузі комп'ютерної безпеки, програмування, цифрових сервісів, комп'ютерних систем, тощо. Окрім цього, такі кримінальні правопорушення часто мають транснаціональний, латентний і анонімний характер (особливо, на початку розслідування). Також потрібно відмітити, що кримінальні правопорушення вказаного виду посягають не лише на суспільні відносини у сфері цифрових технологій і комп'ютерної інформації, а й на безпосередньо впливають на здоров'я населення, сферу економіки, конституційні права людини та громадянина;

– кримінальні правопорушення, при вчиненні яких цифрові технології виступають саме як способи вчинення. Так, можна навести приклад,

коли при вчиненні злочину у співучасті, співучасники з метою вчинення кримінального правопорушення, комунікують через різні мобільні додатки-месенджери, тобто використовують їх як спосіб комунікації або, наприклад, злочинці змінюють номери sim-карти з метою вчинення шахрайських дій, або ж створюють різні фішингові сайти для вчинення різного роду шахрайства. Тобто в таких випадках, використання цифрових технологій виступає частиною способу підготовки, вчинення або приховування самого кримінального правопорушення, а саме безпосередньо із використанням самих цифрових технологій або як способу вчинення. У таких випадках правоохоронними органами здійснюється аналіз інформації про саму комунікацію між абонентами та/або абонентськими пристроями. Також можуть вивчатися SMS-повідомлення або ж спілкування (переписки) у інших месенджерах чи соціальних мережах, що може свідчити прикладом підтвердження факту співучасті або з'ясування ролей самих співучасників.

Комп'ютерна інформація, будучи елементом, що відноситься до механізму цифрової сфери, одночасно виступає ємністю, що акумулює та наповнюється змістом постійних процесів виникнення, формування, видозміни різних баз даних, інформаційних банків та інших сховищ, у яких поряд з іншими відомостями даних концентрується необхідна інформація.

Особливістю досліджуваних кримінальних правопорушень є те, що в процесі їх вчинення, формується система цифрових слідів, які, аналогічно іншим типам слідової інформації, можуть бути виявлені, досліджені, зафіксовані, і в остаточному результаті отримати статус доказів у кримінальному провадженні. Але необхідно пам'ятати, що сам процес їх дослідження та виявлення має особливий характер, враховуючи специфіку самих цифрових технологій та цифрових доказів, що й потребує особливої уваги з боку правоохоронних органів. Також необхідно звернути увагу на той факт, що кожен окремий спосіб вчинення кримінальних правопорушень, пов'язаний з цифровими технологіями, має самостійний механізм

слідоутворення і, відповідно, різні типи об'єктів, що підлягають дослідженню, а також способи приховування даних злочинних дій.

Слід зазначити, що стрімкий розвиток сфери цифрових технологій постійно призводить не лише до появи нових видів послуг у фінансовій сфері, а й вдосконаленню способів та методів незаконного отримання коштів у кіберсередовищі. Значної шкоди завдають кримінальні правопорушення у цифровому середовищі бізнесу, тобто, юридичним особам, для яких вже стали критичними втрати від кібератак на фінанси. Практично неможливо оцінити справжні масштаби негативних наслідків від цифрової злочинності, оскільки не всі жертви завжди усвідомлюють та розуміють, що вони стали жертвами таких кримінальних правопорушень і неможливо точно визначити реальну кількість потерпілих від, наприклад фішингових чи хакерських атак тощо. Саме тому, існуюча правова база боротьби з цифровою злочинністю та інші антикримінальні інструменти впливу потребують вдосконалення.

Досить часто правопорушення, що вчиняються у цифровому середовищі важко ідентифікувати та виявити, зокрема: правопорушення, вчинені організованими групами, особливо ті, що генерують великі та особливо великі кримінальні прибутки, такі як онлайн-шахрайство; правопорушення, які завдають серйозної шкоди своїм жертвам, наприклад, сексуальна експлуатація дітей в Інтернеті; правопорушення (включаючи кібератаки), що впливають на критичну інфраструктуру та інформаційні системи; правопорушення, пов'язані із захистом та обігом цифрової інформації, тощо.

Така норма, яка б передбачала кримінальну відповідальність за придбання чи збут цифрової інформації, яка одержана кримінально протиправним шляхом, відсутня. Так, інформація зазвичай не визнається майном, і, відповідно, внаслідок маніпуляцій із нею не можна притягти особу до кримінальної відповідальності за ст. 198 КК України «Придбання, отримання, зберігання чи збут майна, одержаного кримінально протиправним шляхом». Оскільки, відповідно до ст. 190 ЦК України «Майном як особливим

об'єктом вважаються окрема річ, сукупність речей, а також майнові права та обов'язки. Майнові права є неспоживною річчю. Майнові права визнаються речовими правами» [39; 73].

Отже, на сьогодні цифрові технології використовуються абсолютно скрізь, адже комп'ютери, ноутбуки, планшети, смартфони, мобільні телефони тощо є атрибутами кожного суспільства. Головна мета цифрових технологій полягає в тому, щоб швидко встановити зв'язок між людьми, без зусиль і з мінімальними витратами. Люди пов'язані один з одним за допомогою величезного спектру цифрових послуг і ресурсів. Цифрова інформація дуже відрізняється від її фізичного аналогу, оскільки її можна швидко скопіювати, розподілити контрольованим чином і зберігати в різних місцях.

Потребує конкретизації і додаткового вивчення і правова природа криптовалют та необхідності захисту їх власників заходами чинного законодавства, у тому числі кримінального. Адже, швидко впроваджуються та розповсюджуються в суспільстві технологічні зміни у сфері криптовалют, яка пропонує окремі переваги перед традиційними валютами, включаючи нижчі комісії за транзакції та швидший переказ коштів за послуги. Проте, тут необхідно звернути окрему увагу на кримінологічні ризики торгівлі криптовалютою, проблему фальшивих криптовалют, фальшивих гаманців, фішингу, за допомогою якого злочинці намагаються змусити жертву надати ім'я користувача та пароль.

Американські вчені розглядають можливість застосування традиційних кримінологічних концепцій для пояснення причин злочинної діяльності у віртуальному просторі та виявлення факторів, що сприяють злочинам, пов'язаним з біткоїнами. Відповідно до закону, криптовалюта як продукт або власність визнається законодавством кількох країн. Так, податкове законодавство Австралії та законодавство США позиціонують криптовалюту як майно, яке враховується для розрахунку податку на прибуток. В Ізраїлі встановлений податок на прибуток при продажу криптовалют за

диференційованим курсом, і його розмір становить до 25% від загальної вартості реалізації [127].

Доцільно розмежувати поняття «електронні гроші» та «цифрові гроші». Відповідно до ЗУ «Про платіжні послуги» електронні гроші та цифрові гроші існують лише в безготівковій формі. Електронні гроші, номіновані в гривні, та цифрові гроші використовуються фізичними і юридичними особами для проведення платіжних операцій та розрахунків виключно у випадках, передбачених законами України та/або нормативно-правовими актами Національного банку України. Порядок випуску, зберігання та погашення цифрових грошей, а також особливості виконання платіжних операцій із застосуванням цифрових грошей визначаються нормативно-правовими актами Національного банку України. Вимоги щодо випуску електронних грошей та виконання платіжних операцій з електронними грошима не поширюються на емісію цифрових грошей та виконання платіжних операцій з цифровими грошима. Цифрові гроші Національного банку України (далі - цифрові гроші) – електронна форма грошової одиниці України, емітентом якої є Національний банк України. Електронні гроші – одиниці вартості, що зберігаються в електронному вигляді, випущені емітентом електронних грошей для виконання платіжних операцій (у тому числі з використанням наперед оплачених платіжних карток багатоцільового використання), які приймаються як засіб платежу іншими особами, ніж їх емітент, та є грошовим зобов'язанням такого емітента електронних грошей [63].

А відповідно до норм ЗУ «Про віртуальні активи», який набере чинності з дня набрання чинності законом України про внесення змін до Податкового кодексу України щодо особливостей оподаткування операцій з віртуальними активами, віртуальний актив – нематеріальне благо, що є об'єктом цивільних прав, має вартість та виражене сукупністю даних в електронній формі. Існування та оборотоздатність віртуального активу забезпечується системою забезпечення обороту віртуальних активів. Віртуальний актив може

посвідчувати майнові права, зокрема права вимоги на інші об'єкти цивільних прав [58].

Криптовалюта може бути засобом вчинення кримінальних правопорушень. У свою чергу, криптовалюта, яка відображає предмет кримінального посягання, є цифровим активом, який має матеріальну цінність, у зв'язку з яким або з приводу якого вчинено кримінальне правопорушення.

Так, відповідно примітки до ст. 368-5 КК України «Незаконне збагачення», криптовалюта передбачена, як можливий актив, що є предметом складу кримінального правопорушення, яке передбачає кримінальну відповідальність за «набуття особою, уповноваженою на виконання функцій держави або місцевого самоврядування, активів, вартість яких більше ніж на шість тисяч п'ятсот неоподатковуваних мінімумів доходів громадян перевищує її законні доходи» [39].

Що стосується вдосконалення чинного законодавства, спрямованого на розвиток механізму протидії кримінальним правопорушенням у сфері обігу криптовалют, в першу чергу, необхідно на законодавчому рівні визначити правовий статус криптовалюти, включно з її визначенням: «цифровий актив», «віртуальна валюта», «результати інтелектуальної діяльності». Окрім цього потрібно визначити права та обов'язки учасників – власників такого «товару», а також види відповідальності за протиправні посягання на цю групу суспільних правовідносин. Окрім цього, враховуючи досить значне поширення віртуальних активів на сучасному етапі, слід встановити конкретну міру кримінальної відповідальності за правопорушення у сфері обігу віртуальних активів, цифрової та електронної валюти. Так, в першу чергу, доцільно визначити в межах кримінально-правової доктрини, чим виступає криптовалюта в процесі вчинення кримінального правопорушення: предметом і (або) засобом вчинення. Це важливо для його теоретичного визначення в доктрині кримінального права та правоохоронної діяльності, оскільки це поняття залежить від: визначення суб'єкта повноважень щодо протидії правопорушенням у сфері обігу даного

виду актів та забезпечення координації протидії в інформаційному полі та кіберпросторі, що постійно змінюється та зростанні фактів використання криптовалют у злочинних цілях. Отже, цифрові можливості стають досить часто способами чи засобами вчинення кримінальних правопорушень, або ж полегшують їх вчинення. Особливість цих кримінальних правопорушень полягає в тому, що на сьогодні вони не обмежені кордонами однієї держави, вони можуть бути вчинені з будь-якого місця і проти будь-якого користувача, який знаходиться в будь-якій точці світу. На сьогодні цифрова злочинність вимагає від держав серйозних зусиль щодо боротьби з нею. Ефективність протидії їй, перш за все, залежить від міжнародної угоди про уніфікацію підходів до визначення цього негативного явища. Цифрова злочинність – це суспільне протиправне явище, яке включає сукупність кримінальних правопорушень, вчинених у сфері або з використання цифрових технологій, у тому числі нелегального отримання чи (та) поширення інформації в інформаційно-телекомунікаційних мережах, а також з використанням віртуального середовища [9, с. 513-514].

Пропонуємо прирівняти цифрову інформацію до майна, адже що хоч цифрову інформацію не можна доторкнутися і відчутти, як носій інформації виступає речовий предмет (наприклад, Flash-карта), що містить цифрову інформацію та представляє матеріальну цінність. Тому, вважаємо за необхідне встановити кримінальну відповідальність за придбання або збут цифрової інформації, яка свідомо одержана кримінально протиправним шляхом та внести зміни до КК України, шляхом доповнення його *статтею 198-1 «Придбання, отримання, зберігання чи збут цифрової інформації, одержаної кримінально протиправним шляхом» та викласти її у наступній редакції:*

«Заздалегідь не обіцяне придбання або отримання, зберігання чи збут цифрової інформації, одержаної кримінально протиправним шляхом

карається арештом на строк до шести місяців або обмеженням волі на строк до трьох років, або позбавленням волі на той самий строк».

Незважаючи на суспільну небезпеку вказаних злочинних дій, в теорії та практиці кримінального права відсутнє єдине їх визначення, що може бути відображено як «цифрова злочинність», «кримінальні правопорушення, вчинені з використанням цифрових технологій» або «кримінальні правопорушення, вчинені у цифровій сфері». Тому, враховуючи, що на законодавчому рівні поняття «цифрова злочинність» відсутня, є необхідність внесення змін до КК України.

Загалом, необхідно визнати, що Інтернет сьогодні набув досить значного поширення і розглядати лише комп'ютерні правопорушення не зовсім вірно, адже розвиток цифрового простору охоплює не тільки комп'ютерні технології, а й мережеві різні ресурси, інтернет-ресурси, використання гаджетів, електронно-обчислювальних машин, інформаційно-телекомунікаційних технологій тощо. Окрім цього, розвиток штучного інтелекту, блокчейну, великих даних, цифрових близнюків, хмарних програм та чат-ботів, інтегрованих в різні платформи, які також змінюють спосіб взаємодії людей з цифровим світом, свідчать про те, що цифрове життя значно розширює межі та можливості людей, а цифрове життя поступово виходить за межі комп'ютера, адже з'являється все більше і більше нових цифрових продуктів.

Усе це дозволяє стверджувати, що поняття «цифрове кримінальне правопорушення або правопорушення у сфері цифрових технологій» є значно ширшим за поняття «кіберзлочинність» або комп'ютерна злочинність. Цифрова злочинність включає ширший спектр протиправних дій, у тому числі вчинених як з використанням комп'ютерних систем і мереж, так і з використанням цифрових технологій, у тому числі віртуального середовища, яке доповнює нашу реальність.

2.3. Міжнародно-правове регулювання забезпечення кримінологічної безпеки у сфері використання цифрових технологій

Цифровий простір, який приносить багато значних переваг у повсякденне життя, нажаль передбачає і досить значну кількість прихованих загроз. Так, переважна більшість правопорушень в економічній сфері, вчиняються у міждержавному просторі та включає в себе використання мережі Інтернет, що характеризує злочинність у сфері цифрових технологій як довготривалий та складний транскордонний процес.

Стрімкий розвиток інформаційних технологій змінив те, як державні органи, підприємства, інші організації та індивідуальні користувачі, які розробляють ці інформаційні системи та мережі керують ними, обслуговують та використовують їх, адже в першу чергу, вони повинні реагувати на загрози та дотримуватися вимог кібербезпеки.

Враховуючи напрями міжнародного співробітництва щодо запобігання кіберзлочинності, вагоме значення має дослідження окремих міжнародних інституційних механізмів протидії злочинам у сфері злочинності у сфері цифрових технологій, адже кожна міжнародна інституція вносить свій вклад у формування засад протидії злочинності у досліджуваній сфері.

Незважаючи на великі позитиви, досягнуті у сфері цифрових та інформаційних технологій, їх значне поширення і розвиток призвели до досить негативних наслідків і в першу чергу слід відмітити появу цифрової злочинності, небезпека якої зростає й створює нові види злочинності, для прикладу такі як: транскордонна, трансконтинентальна злочинність, та транснаціональна злочинність. Адже їх небезпека та злочинний вплив не обмежуються певними країнами і створюють низку правових проблем для органів із запобігання злочинності.

У зв'язку з цим доцільним є розвиток та вдосконалення співробітництва у сфері протидії розширенню та впливу цифрової злочинності. У протидії

кіберзлочинності, міжнародний підхід передбачає консолідацію зусиль правоохоронних органів різних держав, формування спеціальних підрозділів, діяльність яких спрямована на боротьбу зі злочинністю в цифровому просторі. Окрім цього, специфічний характер кібершахрайства передбачає не ізольоване державне протистояння у вирішенні зростаючої проблеми цифрової злочинності, а в першу чергу ефективну протидію їй при активізації міжнародної співпраці і об'єднання зусиль різних організацій.

Загалом, вперше проблеми запобігання комп'ютерній злочинності розглядалися на Дев'ятому Конгресі ООН щодо запобігання злочинності та поводження з правопорушниками (28 квітня – 5 травня 1995 року), в межах проведення якого була обговорена Стратегія комп'ютеризації кримінального правосуддя. У 2000 році на Десятому Конгресі ООН щодо запобігання злочинності та поводження з правопорушниками, однією із тем Конгресу та семінарів-практикумів було питання щодо злочинів, пов'язані з комп'ютерними мережами. На Одинадцятому Конгресі ООН «Взаємодія та запобіжні заходи: стратегічні напрями взаємодії у сфері попередження злочинності та кримінального правосуддя» (18-25 квітня 2005 року) була обговорена тема «Заходи боротьби із злочинами, пов'язаними з використанням комп'ютерів». Дванадцятий Конгрес ООН «Комплексні стратегії для відповіді на глобальні виклики: системи попередження злочинності та кримінального правосуддя та їх розвиток у світі, що змінюється» (12-19 квітня 2010 року) прийняв декларацію, яка, серед іншого, відкрила можливості для обговорення нових національних та міжнародних заходів щодо протидії кіберзлочинності. А на Чотирнадцятому Конгресі ООН «Активізація заходів запобігання злочинності, кримінального правосуддя та забезпечення верховенства права: назустріч до здійснення, на період до 2030 року» (7–12 березня 2021 року) однією із тем семінару-практикуму була: «Сучасні тенденції у сфері злочинності, останні зміни та нові рішення, зокрема використання сучасних технологій як засобів вчинення злочинів та інструментів боротьби зі злочинністю» [153].

На 57 сесії Генеральної Асамблеї ООН було прийнято резолюцію A/RES/57/239 «Створення глобальної культури кібербезпеки», відповідно до якої Генеральна Асамблея, відзначаючи зростаючу залежність урядів, бізнесу та інших організацій і окремих користувачів щодо інформаційних технологій для ведення бізнесу та надання і обміну інформацією, визначила, що потреба в кібербезпеці зростає разом із участю країн в інформаційному суспільстві [142].

Ефективна кібербезпека – це не лише питання уряду чи закону на практиці правозастосування, але її необхідно вирішувати шляхом профілактики кіберзлочинності та підтримки всього суспільстві в інформаційному середовищі. Уряди країн, бізнес, інші організації, а також окремі власники та користувачі інформаційних технологій повинні знати про відповідні ризики кібербезпеки та профілактичні заходи і повинні брати на себе відповідальність щодо вжиття заходів для підвищення безпеки інформаційних та цифрових технологій. Визнаючи також наявність прогалин у доступі та використанні інформаційних технологій, держави мають ефективно налагоджувати міжнародне співробітництво в боротьбі із злочинністю, пов'язаною із інформаційними технологіями та створювати глобальну культуру кібербезпеки. Тому кожна держава має взяти до уваги потребу в глобальній культурі кібербезпеки; враховувати елементи дотримання кібербезпеки, зокрема, в рамках їхніх зусиль щодо розвитку у себе в суспільстві культури кібербезпеки при застосуванні та використанні інформаційних технологій; підкреслює необхідність сприяння передачі інформаційної технології країнам, що розвиваються, і створенню в них потенціалу з метою надання їм допомоги у вжитті заходів у сфері кібербезпеки.

Резолюція відобразила Керівні принципи і запропонувала «Державам-членам і всім відповідним міжнародним організаціям враховувати положення щодо кібербезпеки та захисту інформаційних систем [142].

Адже забезпечення кібербезпеки є одним із найважливіших елементів безпеки в розвинених країнах, оскільки вона базується на захисті досить

важливих об'єктів і постає необхідність інтегрувати кібербезпеку в захист, розвиток та інформаційну складову безпеки держав загалом. Електронна інформаційна та цифрові мережі стають невід'ємною частиною сучасного повсякденного життя і захист цифрової інформації стає більш життєво важливим і має ефективний вплив на національну безпеку та технічний прогрес.

Враховуючи, трансформаційні процеси та динамічність розвитку цифрових технологій, вказані Керівні принципи згодом були переглянуті та прийняті 25 липня 2002 р., як Рекомендації ОЕСР щодо безпеки інформаційних систем і мереж: до культури безпеки», а 1 жовтня 2015 р. вказану рекомендацію було замінено на «Рекомендацію Ради щодо управління ризиками цифрової безпеки для економічного та соціального процвітання». Прийняті в 2002 році Рекомендації, встановлюють межі принципів, які застосовуються до всіх учасників для підвищення безпеки інформаційних систем і мереж з метою сприяння економічному процвітання та соціальному розвитку суспільства. Після їх прийняття ОЕСР спостерігала за їх впровадженням і організовувала заходи для обміну досвідом і найкращими практиками між урядами, бізнес-спільнотою та громадянським суспільством [132; 133].

Таким чином, Рекомендація 2015 року, яка замінила Рекомендації ОЕСР 2002 року, вказує на переваги цифрового середовища та необхідність інтеграції управління ризиками цифрової безпеки в процес прийняття економічних і соціальних рішень. А при розробці державної політики, також необхідно враховувати складність ризику цифрової безпеки через його численні виміри від економічного та соціального процвітання до правоохоронної діяльності («кіберзлочинність»), в першу чергу для забезпечення національної та міжнародної безпеки [101].

А в грудні 2019 року, вказані Рекомендації були доповнені Рекомендацією ОЕСР щодо цифрової безпеки критично важливих видів діяльності. Рекомендація щодо цифрової безпеки критично важливих видів

діяльності була ухвалена Радою ОЕСР 11 грудня 2019 року за пропозицією Комітету з політики цифрової економіки (CDEP).

Ця Рекомендація, звертає увагу, що цифрова трансформація впливає на всю економічну та соціальну діяльність, стимулюючи інновації та створюючи значні вигоди, але також наражає цю діяльність на зростаючий ризик порушення цифрової безпеки, що є наслідком потенційних навмисних або ненавмисних загроз, які мають транскордонний характер, використовують вразливі місця та викликають інциденти, що впливають на доступність, цілісність і конфіденційність даних, апаратного забезпечення, програмного забезпечення та мереж, на які покладається ця діяльність. Враховуючи, вказані ризики, у досліджуваному міжнародно-правовому акті містяться чіткі рекомендації і стратегічні підходи, щодо забезпечення безпеки цифрового середовища у суспільстві, а саме:

- прийняття на найвищому урядовому рівні та в рамках національної стратегії цифрової безпеки чітких цілей для посилення цифрової безпеки та стійкості критично важливих дій, а також забезпечення узгодженості з національною оцінкою ризиків та іншими стратегіями ризиків і секторів;

- прийняття та публічне оприлюднення національного механізму управління, який розподіляє повноваження та відповідальність конкретних державних органів для розробки та впровадження політики разом із відповідними зацікавленими сторонами для підвищення цифрової безпеки критично важливих видів діяльності всередині та між секторами. Механізм національного управління також має визначати чітку міру відповідальності, органів державної влади, які відповідальні за національну безпеку та оборону;

- забезпечення внутрішньодержавної координації з метою: налагодження внутрішньодержавного співробітництва, яке має повною мірою враховувати важливість діалогу між цифровою безпекою та окремими галузевими експертами; сприяти транскордонному співробітництву у вказаній сфері;

– ефективне забезпечення дотримання цифрової безпеки для критично важливих функцій до рівня, прийнятного для суспільства, узгодженого з національною оцінкою ризику, заохочуючи або вимагаючи, де це доцільно, вжиття заходів щодо управління, захисту, виявлення та реагування, а також заходів стійкості.

Вказані заходи повинні включати такі заходи: управління – створення організаційної основи для циклічної оцінки та зменшення ризиків цифрової безпеки; захист – впровадження відповідних заходів безпеки для зменшення ризиків цифрової безпеки для критично важливих функцій; виявлення та реагування – впровадження процесів і заходів для захисту від інцидентів і реагування на них; стійкість – прийняття відповідних заходів готовності та відновлення для забезпечення безперервності критичних функцій [141].

Також необхідно звернути увагу на стратегічний документ, що прийнятий Європейським Союзом «Цифровий компас 2030», який містить напрями розвитку сучасного та більш вдосконаленого цифрового майбутнього. Проаналізувавши зазначений документ, можна виокремити такі основні конкретні цілі для кожного: кваліфіковане населення та висококваліфіковані фахівці у галузі цифрових технологій; безпечна та ефективна стала цифрова інфраструктура; цифрова трансформація бізнесу; оцифрування державних послуг [91].

Останнім часом досить розширюються цифрові навички у суспільстві та створюються нові цифрові продукти, проте необхідно, щоб і був значний рівень довіри у громадян до новітніх цифрових продуктів. Тому, сучасні онлайн-сервіси мають не лише створювати щось нове, але й виявляти дезінформацію та спроби шахрайства, захищатися від кібератак, шахрайства та шахрайства в Інтернеті, і в першу чергу звертати увагу на дітей, які вчаться розуміти та орієнтуватися у безлічі інформації, до якої вони мають доступ в Інтернеті. Це свідчить про зростання кількості інтернет-загроз для дітей, зокрема: грумінг в

цифровому середовищі, сексуальні зловживання і сексуальна експлуатація тощо, що потребує необхідності захисту їх у цифровому середовищі.

Так, Міжнародний союз електрозв'язку (МСЕ) є спеціалізованою агенцією Організації Об'єднаних Націй з інформаційно-комунікаційних технологій (ІКТ), покликаний здійснювати законодавчі, управлінські, виконавчі та консультативні функції, надавати технічну підтримку, розробляти стандарти і правила у сфері електрозв'язку та формулювати рекомендації, спрямовані на активізацію розвитку телекомунікацій та підвищення якості послуг [134].

Однією з його ініціатив є саме захист дітей в мережі Інтернет і на виконання цієї функції Союзом були розроблені Керівні настанови щодо захисту дитини в цифровому середовищі. Рекомендації спрямовані на захист дітей в усіх сферах і від усіх ризиків цифрового світу і, як такі, виділяють передовий досвід галузевих заінтересованих сторін, який можна враховувати в процесі проєктування, розробки та керування політиками захист дітей у цифровому середовищі на рівні компаній. Вони скеровують учасників індустрії не тільки в тому, як управляти і стримувати незаконну онлайн-діяльність, якій вони зобов'язані протидіяти за допомогою своїх послуг, але і в тому, як вирішувати інші питання, які можуть не вважатися злочинами в різних юрисдикціях. До них належать насильство між однолітками, кібербулінг і домагання в інтернеті, а також питання, пов'язані з конфіденційністю або загальним добробутом, шахрайством або іншими загрозами, які можуть лише нашкодити дітям у певному контексті. Так, вказані рекомендації передбачають створення більш безпечного онлайн-середовища, що відповідає віку; розроблення стандартних методів поведінки з матеріалами, пов'язаними із сексуальними зловживаннями щодо дітей; навчання дітей, батьків і педагогів правилам дитячої безпеки та відповідального використання ними ІКТ; сприяння просуванню цифрових технологій як засобу збільшення участі в житті громадянського суспільства [25].

Як бачимо, дослідження міжнародно-правових нормативних документів та рекомендацій щодо забезпечення належного рівня кібербезпеки вказує на необхідність формування національної політики з врахуванням дотримання кібербезпеки у кожному напрямі, як вагомого пріоритету. Це відображає ключові зміни в середовищі ризику, коли кіберзагрози розвиваються та набирають швидкий темп, що призводить до вчинення різних правопорушень у цій сфері. Джерела загроз розширюються разом з їх мотивацією та технікою, адже суб'єкти цих правопорушень теж часто мають спеціальну освіту в ІТ-сфері, що ускладнює виявлення та запобігання цим правопорушенням. Пріоритет, який тепер надається кібербезпеці, також відображається реальністю того, що Інтернет та ІКТ стали важливими для економічного та соціального розвитку і загалом для інфраструктури. Нове покоління стратегій кібербезпеки спрямоване на стимулювання економічного та соціального розвитку, напрямів захисту суспільства, що залежать від кіберпростору, від кіберзагроз, зберігаючи відкритість Інтернету як платформи для інновацій і нових джерел зростання. Проте, виклики кіберзагрозам теж досить великі та постійно трансформуються і видозмінюються, тому правоохоронні органи повинні мати сучасний фундаментальний підхід, який необхідний для боротьби з кіберзагрозами у відкритому доступі [5, с. 134-135].

Загалом, сама кіберзлочинність була визначена в 2000 році на Десятій сесії ООН «Конгрес із запобігання злочинності та кримінального правосуддя», де було визначено що комп'ютерна злочинність стосується будь-якого кримінального діяння, «які можуть бути вчинені з використанням комп'ютерної системи або мережі, в межах комп'ютерної системи чи мережі, або проти комп'ютерної системи або мережі», що в принципі, охоплювало будь-яке правопорушення, яке може бути вчинене в електронному навколишньому середовищі [143].

Проте, вже на одинадцятому Конгресі ООН «Запобігання злочинності та кримінальне правосуддя (2005)», було запропоновано «сформулювати

концептуальну модель запобігання комп'ютерним злочинам». Таким чином, розглядали комп'ютерні злочини як поведінку, яка заборонена законом та/або судовою практикою, що: а) є спрямованою власне на комп'ютерну сферу та комунікацію інформаційних цифрових технологій; б) включає використання цифрових технологій у вчиненні правопорушення; або с) включає використання комп'ютера як інструмента у процесі вчинення інших злочинів, і, відповідно, джерелом електронних процесуальних доказів виступає саме комп'ютер» [103].

14-й Конгрес ООН із запобігання злочинності та кримінального правосуддя проходив у березні 2021 року в Кіото, як найбільше та найрізноманітніше зібрання політиків, практиків, академічних кіл, міжурядових організацій та громадянського суспільства у сфері запобігання злочинності та кримінального правосуддя. Питання кіберзлочинності теж було розглянуто в межах Конгресу, зокрема більшість правопорушень, які підпадають під цей термін включають кіберзлочини, що вчиняються заради прибутку, який вони приносять і досить часто вчиняються організованими злочинними групами. Використання інформаційних технологій для кримінальних цілей та методи кіберзлочинців постійно розвиваються зі швидкістю технічних досягнень в ході розвитку національних і міжнародних стандартів та механізмів. В межах Конгресу була розглянута Програма з кіберзлочинності, що спрямована на підтримку держав-членів у формуванні спеціалізованого міжнародного слідчого співробітництва в галузі кіберзлочинності [80].

Отже, як бачимо, більшість як соціальних так і економічних видів діяльності у суспільстві все більше залежать від цифрових технологій. Окремі з цих видів діяльності є досить важливими, а інколи мають навіть критичний вплив на суспільство, оскільки їх порушення можуть суттєво вплинути на безпеку громадян, їх здоров'я безпеку суспільства загалом, на ефективне функціонування органів державної влади чи інших інституцій громадянського суспільства, необхідних для економічного та соціального процвітання в більш широкому сенсі.

Так, зокрема, цифрове перетворення таких критично важливих видів діяльності, таких як для прикладу: охорона здоров'я, водопостачання, енергопостачання, телекомунікації та банківські послуги, дедалі більше наражає їх на загрози кібербезпеці, які можуть вплинути на безпеку та функціонування основних послуг або економічного та соціального процвітання в більш широкому сенсі. Саме тому, залежність громадянського суспільства від цифрових технологій зростає щороку і постійно прискорюється завдяки цифровій трансформації та узагальненню таких технологій, як штучний інтелект та постійна комп'ютеризація та цифровізація. Проте, нажаль, паралельно зростає кількість і складність загроз цифровій безпеці, на які необхідно вчасно впливати та запобігати, щоб не допустити до вчинення правопорушень. Поєднання посилення цифрової залежності та загроз для критично важливих видів діяльності у суспільстві повинно в першу чергу зміцнювати цифровий захист критично важливих видів діяльності.

Враховуючи, викладене вище, а також досліджені міжнародно-правові документи, пропонуємо, в межах запобігання кіберзлочинності та забезпечення кримінологічної безпеки у сфері використання цифрових технологій наступні заходи:

- розвиток заходів національного характеру та міжнародне співробітництво у кримінальних провадженнях, зокрема щодо посилення заходів виявлення кіберзлочинності, відмивання коштів, одержаних злочинним шляхом та незаконної торгівлі культурними цінностями, а також щодо екстрадиції, взаємної правової допомоги та конфіскації, стягнення та повернення доходів, одержаних злочинним шляхом;
- посилення міжнародного правоохоронного співробітництва, шляхом підвищення потенціалу та кваліфікації існуючої системи правоохоронних органів, які зосереджені на запобіганні кіберзлочинності;
- необхідність покращення взаємної правової допомоги та співпраці на початкових стадіях транскордонних кримінальних проваджень, що

стосуються злочинності у сфері цифрових технологій та спрощення процедури взаємної правової допомоги і міжвідомчої слідчої співпраці;

- створення централізованих навчальних курсів по актуальним та сучасним напрямам запобігання кіберзлочинності для слідчих, враховуючи постійні трансформаційні процеси у сфері цифровізації суспільства, що будуть забезпечені експертами у сфері запобігання кіберзлочинності, а також наявність сучасного комп'ютерного обладнання;

- вдосконалення онлайн-дослідницької мережі, за підтримки міжнародних агентств і приватного сектору, що надасть можливості для більшого обміну інформацією, спілкування між експертами в усьому світі з питань комп'ютерної злочинності, порівняльного аналізу і передачі знань про запобігання та боротьбу з комп'ютерними злочинами та розвиток відповідних інструментів навчання, які мають бути доступними на міжнародному рівні, щоб ділитися знаннями та інформацією щодо способів і засобів виявлення, запобігання та боротьби з новими видами кіберзлочинності.

Висновки до Розділу 2

1. Запропоновано виокремити склади кримінальних правопорушень, що пов'язані із сферою цифрових технологій в окрему категорію злочинних діянь в інформаційно-цифровій сфері (цифровому середовищі), що матиме практичний зміст для кримінально-правової, так і кримінологічної науки, з погляду запобігання злочинності у сфері обігу цифрової інформації «злочинності у сфері цифрових технологій».

2. Визначено пріоритетні заходи щодо зміцнення системи цифрової безпеки, а саме: підвищення рівня підготовки фахівців у сфері цифрових технологій; оновлення та впровадження якісного програмного забезпечення правоохоронних структур для своєчасного виявлення та протидії цифровій злочинності і загалом запобігання правопорушенням у цифровому середовищі;

формування дієвої системи автоматизованого обміну інформацією на випадок будь-якого виду загроз у цифровому просторі, адже сучасні цифрові технології можуть виступати способом чи засобом вчинення багатьох видів кримінальних правопорушень; вдосконалення системи управління інформаційною безпекою, що використовують інформацію з усіх сховищ даних та дотримання конфіденційності її забезпечення.

3. Наведено заходи інформування громадян щодо забезпечення та дотримання безпеки в кіберпросторі, шляхом, наприклад проведення лекцій у навчальних закладах, на підприємствах, установах, організаціях, розміщення інформації щодо безпечного користування всесвітньою мережею Інтернет тощо, з метою забезпечення належного рівня кримінологічної безпеки в нашій державі та закріплено необхідність захисту цифрових бізнес-систем, що працюють на базі штучного інтелекту та досліджено використання штучного інтелекту в продуктах та сервісах для посилення захисту і запобігання його використанню в злочинних цілях.

4. Детально проаналізовано поняття «цифрове кримінальне правопорушення або правопорушення у сфері цифрових технологій» та наведено порівняння з поняттями: «кіберзлочинність» або комп'ютерна злочинність. І на основі детального аналізу, наведено авторське визначення «кримінальних правопорушень у сфері цифрових технологій», під якими розуміється передбачене кримінальним законом винне, протиправне, суспільно небезпечне діяння, спрямоване на порушення конфіденційності, цілісності, достовірності та доступності цифрової інформації, що охороняється законом або вчинене з використанням цифрових технологій або щодо них.

5. В межах запобігання кіберзлочинності та забезпечення кримінологічної безпеки у сфері використання цифрових технологій запропоновано розвивати заходи національного характеру та міжнародного співробітництва у кримінальних провадженнях, зокрема щодо посилення заходів виявлення кіберзлочинності, відмивання коштів, одержаних злочинним

шляхом та незаконної торгівлі культурними цінностями, а також щодо екстрадиції, взаємної правової допомоги та конфіскації, стягнення та повернення доходів, одержаних злочинним шляхом.

РОЗДІЛ 3

ЗАПОБІГАННЯ ЗЛОЧИННОСТІ У СФЕРІ ВИКОРИСТАННЯ ЦИФРОВИХ ТЕХНОЛОГІЙ В УКРАЇНІ

3.1. Заходи запобігання злочинності у сфері використання цифрових технологій в Україні

Відповідно до статті 17 Конституції України «Захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу» [35].

Як бачимо, інформаційна безпека виступає однією із конституційно закріплених найважливіших функцій держави, тому й захист її повинен відбуватися належним чином. Проте, в умовах розвитку цифрового суспільства та впровадження цифрових технологій суспільство зіткнулося з низкою нових негативних соціальних явищ, одним із яких є злочинність у сфері цифрових технологій та посягання на інформаційну безпеку держави, суспільства та громадян. Цей вид злочинності вимагає особливої уваги та особливого підходу в діяльності щодо її попередження та запобігання, оскільки ще не вироблено достатніх ефективних механізмів виявлення та припинення кримінальних правопорушень, вчинених у сфері цифрових технологій.

Буюджи С. А, відмічає, що стрімкий розвиток науково-технічного прогресу призвів до застосування електронно-обчислювальних машин (комп'ютерів), комп'ютерних мереж та різноманітних систем електронного зв'язку практично в усіх сферах суспільного життя. Разом з тим, внаслідок поширення названих технічних інновацій виникли й негативні соціальні явища, які пов'язані з діяльністю відповідного обладнання та техніки, зокрема інформаційні злочини. За таких умов перед Українською державою постала нагальна необхідність забезпечити ефективну боротьбу з кіберзлочинністю, що,

серед іншого, включає й механізм правового регулювання відповідних суспільних відносин. Зростання кількості інформаційних злочинів, тяжкість завданих ними наслідків, транскордонний характер та інші негативні чинники зумовлюють необхідність запровадження тісної міжнародної співпраці у даній галузі, яка передбачає дієве функціонування як національних, так і міжнародних заходів боротьби з кіберзлочинністю [18, с. 68].

Юзікова Н. С. вважає, що головною метою системи інформаційної безпеки є забезпечення механізму захисту від негативного впливу на фізичне, емоційне та психологічне благополуччя особи у цифровому середовищі. Ефективна практична реалізація такої мети має ґрунтуватись на залученні всіх суб'єктів інформаційних відносин. Комплексна та системна взаємодія держави з приватним секто-ром та громадою в інтересах ефективного розвитку інформаційної сфери є запорукою спільно-го захисту особи, держави, суспільства від загроз пов'язаних з інформаційними технологіями. Для запобігання злочинності у сфері інформаційних технологій необхідно сформулювати адресний цифровий кейс нормативно-правових, організаційно-управлінських та техніко-технологічних заходів спрямованих на захист різних сфер суспільної діяльності з урахуванням викликів, спричинених військовою агресією та іншими надзвичайними та кризовими станами [77].

В епоху цифрового світу, значно змінилася динамічність різних процесів, соціального, економічного, технічного, технологічного, управлінського та інших спрямувань, і в результаті цього відбулися кардинальні зміни і в самій інтенсивності життя та статистиці вчинених кримінальних правопорушень.

На думку Гребенюка М. та Черняка А., практичні здобутки та надбання цифрової економіки активно використовуються транснаціональними організованими злочинними угрупованнями з метою отримання надприбутків шляхом вчинення злочинів економічної спрямованості на території однієї або

декількох держав з використанням кіберпростору та його можливостей [22, с. 299].

Бодунова О.М. відмічає, що на сьогодні суспільство переживає стрімкий розвиток автоматизації, інформатизації та комп'ютеризації кожної зі сфер діяльності. Ці процеси надають нові можливості для розвитку культури, освіти, науки й економіки кожної держави, а також дають змогу оперативно взаємодіяти з іншими державами та міжнародними організаціями. Проте поширення інформаційних технологій має й негативні наслідки, адже відкриває шлях до злочинної поведінки. Комп'ютерні системи надають нові, дуже досконалі можливості для вчинення невідомих раніше правопорушень, а також для вчинення традиційних злочинів, але нетрадиційними засобами [13, с. 246].

Враховуючи сучасний стан розвитку цифровізації у суспільстві та цифрову трансформацію сучасної злочинності, особливої актуальності набувають питання запобігання злочинності у сфері цифрових технологій, а також кримінальним правопорушенням, вчинених з використанням різноманітних цифрових та інформаційно-телекомунікаційних технологій. Аналізуючи вплив цифрових технологій на злочинну діяльність, слід зазначити ще й такий фактор, як її поступальний розвиток, адже через появу нових способів вчинення кримінальних правопорушень та їх інтеграції, цифрові технології досить часто виступають способами вчинення таких правопорушень, що потребує особливої уваги з боку правоохоронних органів.

Як ми уже відзначали у підрозділі 2.2., кримінальні правопорушення, що пов'язані із використанням цифрових технологій, можна поділити на дві категорії: кримінальні правопорушення, що посягають на цифрову інформацію, цифрову інфраструктуру, роботу інформаційних систем та банків даних тощо, тобто коли цифрові технології визначають загальні або окремі характеристики предмету злочинного посягання та кримінальні правопорушення, при вчиненні яких цифрові технології визначають безпосередньо сам спосіб вчинення кримінального правопорушення. Враховуючи такий поділ, необхідно і

аналізувати безпосередньо самі заходи запобігання цим кримінальним правопорушенням.

Останнім часом значно розширюються можливості телекомунікаційного та комп'ютерного зв'язку через мережу «Інтернет», які спрямовані на забезпечення комунікаційного механізму різних форм взаємодії людей, організацій та установ, у тому числі з органами державної влади. Адже в межах інформаційного простору та загалом в мережі «Інтернет» відбувається отримання важливої, необхідної інформації, обмін нею між різними користувачами. На сучасному етапі життя громадян, суспільства та держави загалом неможливо уявити без комп'ютерної інформації, що забезпечує функціонування в галузі управління фінансами, медицини, освіти (дистанційне навчання), а також політики, безпеки держави тощо.

Так, напрям цифровізації проникає активно уже майже у всі сфери життєдіяльності, адже напевно уже не знайдеш того, хто взагалі не користується чи не використовує окремі інтернет та цифрові технології у повсякденному житті, зокрема: Інтернет-банкінг, придбання одягу чи будь-яких інших речей з використанням смартфона чи для прикладу отримують певну інформацію шляхом он-лайн консультації тощо.

Транспорт, енергетика та охорона здоров'я, телекомунікації, фінанси, безпека, демократичні процеси, космос і оборона значною мірою залежать від мережевих та інформаційних систем, які все більше взаємопов'язані. Міжгалузеві взаємозалежності є дуже сильними, оскільки функціонування мереж та інформаційних систем, у свою чергу, залежить від постійного постачання електроенергії. Підключених пристроїв уже більше, ніж людей на планеті, і, за прогнозами, їх кількість зросте до 25 мільярдів до 2025 року [106].

Криміналізація сфери цифрових технологій очевидна, і на сьогодні необхідно вживати заходів щодо запобігання глобалізації криміналізації даної сфери та протидіяти кримінальним правопорушенням, що вчиняються з використанням цифрових технологій. Важко виміряти точну кількість

цифрових кримінальних правопорушень, оскільки їх жертви не завжди повідомляють про вчинені щодо них злочинні діяння, а іноді вони навіть не знають, що вони стали жертвою такого кримінального правопорушення. Тобто інколи жертви таких кримінальних правопорушень навіть не усвідомлюють, що вони стали об'єктом цифрового кримінального правопорушення, або вважають, що завдана шкода недостатньо значна, щоб звертати на неї увагу. Вказане свідчить про необхідність підняття рівня цифрової обізнаності громадян.

Так, зокрема про це зазначають і такі науковці як Топчій В. В. та Маркушин О. Г., які на основі проаналізованого зарубіжного досвіду щодо діджиталізації та цифровізації окремих сфер суспільного життя, відмічають: «більшість зарубіжних країн досить активно впроваджують реформу діджиталізації економічних процесів, використовуючи при цьому різноманітні напрями реформування. Перевагами такої реформи є зниження рівня безробіття, боротьба з бідністю, деградація навколишнього середовища, пришвидшення надання адміністративних послуг. Цифровізація економіки за кордоном передбачає створення інноваційних підприємств, збільшення числа працюючих, підвищення цифрової компетентності населення тощо. У більшості зарубіжних держав реалізуються такі заходи щодо цифровізації економіки: стрімкий розвиток інфраструктурних об'єктів, залучення до цифровізації економіки більшої кількості людей різних професій, проведення повномасштабного навчання працівників щодо оволодіння цифровими технологіями, розвиток цифрового економічного сектору тощо» [71, с. 203-204].

Колодяжний М. Г. зазначає, що прогресивна світова практика запобігання злочинності йде шляхом постійної модернізації й технологізації правоохоронної діяльності. І на його думку, на теперішній час основною її формою можна вважати розгалужену мережу камер відеоспостереження у багатьох країнах світу, що дозволяє не лише підвищувати ефективність діяльності поліції, а й заощаджувати бюджетні кошти. А для технічної

модернізації правоохоронної діяльності в Україні Колодяжний М.Г. пропонує:

- а) розробити в кожному обласному і районному центрі України програми «Безпечне місто» і «Розумне місто»; б) місцевими органами влади виділяти кошти на монтаж камер відеоспостереження у громадських місцях; в) оснащати камери відеоспостереження системами штучного інтелекту; г) створювати умови для організації картографування злочинності з боку Управління кримінального аналізу Національної поліції України; д) формувати у державі сучасну базу даних ДНК злочинців; е) продовжувати реалізацію проекту країн ЄС «Підтримка реформи поліції України»; є) оснащувати охоронників портативними детекторами для виявлення холодної і вогнепальної зброї у відвідувачів установ й організацій тощо [34, с. 181, с. 189].

На думку ж Микитчика А. В. у запобіганні досліджуваного виду злочинності має місце організаційний та технічний підхід. Технічний підхід передбачає запобігання кіберзлочинам за рахунок реалізації заходів технічного характеру, що забезпечують безпеку в інформаційній сфері, а також формування матеріально-технічної бази підрозділів по боротьбі з кіберзлочинністю, виходячи з принципу «найсучасніша техніка». Організаційний підхід має на меті розробку і запровадження в практику, удосконалених організаційно профілактичних заходів. Перш за все слід відійти від вирішення проблеми запобігання кіберзлочинності шляхом подолання існуючих тенденцій, і перейти до активної розробки інформаційної безпеки на випередження. Необхідно об'єднання зусиль всіх учасників, зацікавлених у запобіганні кіберзагрозам: правоохоронних органів, підприємницького середовища, громадських організацій, науково-дослідних установ і громадян. Запобігання кіберзлочинності має включати в себе заходи віктимологічної профілактики – підвищення рівня цифрової грамотності населення і сприяння в просуванні індивідуальних засобів захисту особистої інформації. Актуальними є поглиблені віктимологічні кримінологічні дослідження кіберзлочинності, спрямовані на виявлення об'єктивних закономірностей, детермінант

кіберзлочинності, характеристик окремих типів особистості кіберзлочинців, а також різних аспектів забезпечення кібербезпеки [44, с. 138].

Бугера О. І. ж вважає, що дієвим заходом запобігання злочинності на загальносоціальному рівні є правова освіта в мережі Інтернет. А основними напрямками підвищення рівня правової освіти з використанням можливостей мережі Інтернет є: створення умов для вільного та якісного доступу громадян до освітніх послуг та джерел правової інформації в мережі Інтернет; розроблення Концепції системи правової інтернет-освіти населення з використанням цифрових технологій; розроблення механізмів надання первинної та вторинної правової допомоги в мережі Інтернет та інше [16, с. 59].

Разом з тим, основною перешкодою для використання онлайн-сервісів є саме занепокоєння щодо безпеки. Близько двох п'ятих користувачів ЄС стикалися з проблемами, пов'язаними з безпекою, а три п'ятих вважають, що не можуть захистити себе від кіберзлочинців [[148;99]. Одна третина отримувала шахрайські електронні листи або телефонні дзвінки з проханням надати особисті дані за останні три роки, але 83% ніколи не повідомляли про кіберзлочин. Кожен восьмий бізнес постраждав від кібератак [56]. Більше половини корпоративних і споживчих персональних комп'ютерів, які одного разу були інфіковані зловмисним програмним забезпеченням, заражаються повторно протягом того самого року. Вплив кібератаки часто неможливо ізолювати, і він може викликати ланцюгові реакції в економіці та суспільстві, негативно впливаючи на мільйони людей [26].

Можна констатувати, що залежність суспільства від онлайн-інструментів значно збільшила і траєкторію атак для кіберзлочинців і призвела до того, що майже кожне кримінальне правопорушення або кримінальне провадження включає в себе окремих цифровий компонент. Враховуючи це, слід наголосити, що запобігання кримінальним правопорушенням у цифровій сфері відіграє важливу роль для забезпечення кібербезпеки загалом. В цьому напрямі необхідно розширювати межі та форми співпраці, взаємодії та обміну

інформацією між різними суб'єктами забезпечення кібербезпеки та правоохоронними органами.

Таким чином, на рівні ЄС, Європол і ENISA вже налагодили тісну співпрацю, організовуючи спільні конференції та семінари та надаючи спільні звіти Комісії, державам-членам та іншим зацікавленим сторонам щодо загроз кібербезпеці та технологічних проблем. Комісія продовжує підтримувати цей інтегрований підхід, щоб забезпечити узгоджену та ефективну відповідь на основі комплексної інформаційної картини. Одним з важливих елементів цієї відповіді є те, що влада ЄС і національні органи влади повинні розширювати та вдосконалювати спроможність правоохоронних органів розслідувати кіберзлочини, повністю поважаючи основні права та дотримуючись необхідного балансу між різними правами та інтересами. ЄС повинен мати можливість боротися з кіберзлочинністю за допомогою повністю імplementованого законодавства, яке відповідає меті, з особливим акцентом на боротьбі з сексуальним насильством над дітьми в Інтернеті та на цифрових розслідуваннях. Правоохоронні органи мають бути повністю оснащені для цифрових розслідувань. Тому Комісія запропонує план дій для покращення цифрових можливостей правоохоронних органів, надавши їм необхідні навички та інструменти. Крім того, Європол і надалі розвиватиме свою роль як експертного центру для підтримки національних правоохоронних органів у боротьбі з кіберзлочинністю та кіберзалежною злочинністю, сприяючи визначенню загальних стандартів криміналістичної експертизи (через Інноваційну лабораторію та центр Європолу). Комісія також продовжує працювати над забезпеченням відповідних каналів і роз'ясненням правил отримання транскордонного доступу до електронних доказів для кримінальних розслідувань (потрібно у 85% розслідувань, при цьому 65% загальних запитів надходять до постачальників, що знаходяться в іншій юрисдикції), шляхом сприяння прийняттю та подальшій реалізації «пакету електронних доказів» і практичних заходів. Швидке прийняття пропозицій щодо електронних доказів є

ключовим моментом, щоб забезпечити практиків ефективним інструментом. Електронні докази мають бути інформативними та зчитуватися правоохоронними органами, тому Комісія й надалі працює над підтримкою потенціалу правоохоронних органів у сфері цифрових розслідувань, включаючи роботу з шифруванням, коли вони зустрічаються під час кримінальних розслідувань, повністю зберігаючи свою функцію щодо захисту основних прав та кібербезпеки [124].

Враховуючи ці положення, вважаємо за доцільне конкретизувати нормативні напрями вдосконалення правового регулювання у сфері цифрових технологій в умовах сучасності їх розвитку. Тому, в межах запобігання кримінальним правопорушенням, що вчиняються з використанням цифрових технологій, пропонуємо на нормативному рівні врегулювати родові та видові об'єкти кримінальних правопорушень, що вчиняються з використанням цифрових технологій. Це дозволить не тільки логічно правильно спланувати процес доведення і кваліфікувати злочинне діяння, а й скоригувати вектор розвитку правових засобів боротьби з кримінальними правопорушеннями у цифровій сфері, підвищити рівень цифрової безпеки та захисту громадян, суспільства та держави загалом.

Окрему увагу необхідно приділяти інформаційному забезпеченню правоохоронних органів з метою здійснення належного кримінологічного захисту населення від злочинних посягань у сфері цифрових технологій і в той же час такий самий напрямок діяльності має бути спрямований на навчання населення самостійним способам, методам, прийомам та формам самостійного захисту від злочинних посягань у сфері цифрових технологій.

Важливе значення має також правильний вибір напрямів і заходів запобігання злочинності у цифровій сфері, що мають забезпечувати комплексність такого підходу запобіжної діяльності, до котрих можна віднести:

– вплив суб'єктів попередження злочинності на негативні явища, що детермінують кримінальні правопорушення у сфері цифрових технологій, тобто

у сучасних умовах є важливою підготовка теоретично і практично обґрунтованої та фінансованої програми запобігання злочинності у сфері цифрових технологій, яка була б зорієнтована на усунення всього комплексу факторів, що призводять до зростання та зміцнення цифрової злочинності;

- чітка взаємодія та активізація органів державної влади і громадських організацій, пов'язаних із сферою цифрової діяльності;

- застосування форм і методів запобігання злочинності у сфері цифрових технологій, які ґрунтуються на результатах наукових досліджень, що впроваджені у практичну діяльність правоохоронних органів;

- підготовка та реалізація стратегій або програм запобігання злочинності у сфері цифрових технологій.

Враховуючи важливе значення форм міжнародної та європейської співпраці у боротьбі зі злочинністю у сфері використання цифрових технологій, Агентство Європейського Союзу з кібербезпеки (ENISA) оформило робочу домовленість з українськими партнерами, спрямовану на розбудову спроможності, обмін найкращими практиками та підвищення обізнаності про ситуацію. Російське повномасштабне та незаконне вторгнення в Україну стало переломним моментом для глобальної кіберсфери та підтвердило необхідність посиленого та ширшого міжнародного співробітництва. Робоча домовленість базується на дискусії, розпочатій минулого року у Варшаві під час Діалогу з кібербезпеки між Україною та ЄС, і стане ключовим пунктом наступного Діалогу. Угоду про партнерство підписали ENISA, Національний координаційний центр з кібербезпеки (НКЦК) та Адміністрація Державної служби спеціального зв'язку та захисту інформації України (ДСЗІ). Ця домовленість має широкий характер і охоплює короткострокові структуровані заходи співпраці, водночас відкриваючи шлях для довгострокового узгодження політики кібербезпеки та підходів до реалізації. Співпраця відбуватиметься в таких сферах:

- розвиток кіберобізнаності та потенціалу для підвищення кіберстійкості, включаючи сприяння участі в якості представників третіх країн у конкретних загальноєвропейських навчаннях або тренінгах з кібербезпеки, можливі домовленості про відрядження, а також обмін та просування інструментів і програм кіберобізнаності;

- обмін найкращими практиками для забезпечення узгодження законодавства та впровадження, в тому числі щодо впровадження ключового кіберзаконодавства, такого як NIS2 і таких секторів, як телекомунікації та енергетика;

- обмін знаннями та інформацією для підвищення загальної обізнаності про ситуацію, включаючи більш систематичний обмін знаннями та інформацією щодо ландшафту загроз кібербезпеці для підвищення загальної обізнаності про ситуацію серед зацікавлених сторін і спільнот [104].

Цінність зарубіжного досвіду у формуванні системи заходів запобігання кримінальним правопорушенням у сфері інформаційних технологій, на думку Юзікової Н. С., полягає у можливості координації та ефективної міжнародної співпраці між національними та зарубіжними спеціалізованими правоохоронними органами, неурядовими організаціями які здійснюють моніторинг ризиків і загроз у цифровому середовищі, формують систему протидії їм та здійснюють навчання громадян заходам захисту від небезпеки, яка виходить від ворожої дезінформації; укріплення критичного мислення кожного громадянина та громадянського суспільства в цілому. Крім того, важливо отримувати послуги міжнародних консультантів з питань інформованої безпеки та захисту й дотримання прав людини у цифровому середовищі, з урахуванням воєнного стану та перспективи післявоєнної розбудови України [77, с. 511].

Бугера О. І. відмічає, що ефективне запобігання злочинності в умовах активного розвитку інтернет-технологій можливе у разі постійної технологічної переваги правоохоронних органів над злочинцями, які використовують

технологічний прогрес зі злочинною метою. Тобто ідеться про високотехнологічний підхід до запобігання злочинності, що є сучасною тенденцією розвитку кримінологічної науки та забезпечує підвищення рівня ефективності запобіжної діяльності правоохоронних органів шляхом використання інформаційно-комунікаційних технологій для збору, обміну, аналізу, зберігання, картографування кримінологічної інформації, прогнозування злочинності, розроблення заходів щодо її запобігання на загальносоціальному, спеціально-кримінологічному, індивідуальному рівнях. Для законодавчого забезпечення цього процесу, на думку Бугери О.І., доцільним є розроблення та прийняття Стратегії запобігання злочинності з використанням інтернет-технологій та відповідного Плану заходів з її реалізації з відображенням шляхів вирішення проблем щодо технологічного переоснащення правоохоронних органів, підвищення професійного рівня їх працівників, створення баз даних кримінологічної інформації та забезпечення їх функціонування [17, с. 68].

Калайда Ю. П. звертає окрему увагу на запобіганні правопорушенням у сфері обігу криптовалют і на основі цього наголошує на тому, що важливим напрямом протидії такому явищу залишається використання сучасного програмного забезпечення у правоохоронній діяльності. З метою ефективності розкриття злочинів, що вчинюються з використанням криптовалют, доцільним вбачається: прискорити схвалення правових засад, які мають врегулювати криптовалюту та розробку методологічних основ щодо розкриття та розслідування цієї категорії кримінальних правопорушень. Також правоохоронним органам необхідно налагодити концептуальну взаємодію з криптовалютними компаніями з метою блокування незаконної та протиправної діяльності у блокчейн платформах. Вирішення цієї проблеми має комплексний характер та вимагає розробки стратегії, направленої на запобігання використанню злочинцями нових сучасних фінансових механізмів. Серед пріоритетних напрямків розвитку міжнародної кримінально-правової політики

у сфері попередження використання криптовалют у злочинній діяльності виділяється: визначення моделі податкового адміністрування криптовалюти та правового статусу криптовалют; обов'язкове ліцензування діяльності у сфері обігу криптовалют (біржових сервісів, обмінних площадок, компаній, які випускають токени); встановлення міжнародних стандартів протидії легалізації злочинних доходів та фінансуванню тероризму. Також на думку автора, доцільно створити міжнародну базу даних про осіб, які займаються незаконним обігом та застосуванням цифрових фінансових активів в контексті технологій, що використовуються у протиправній діяльності. В нашій країні в умовах інституційного становлення новоствореного у 2021 році правоохоронного органу – Бюро економічної безпеки України, гостро стоїть питання утворення в його складі спеціального підрозділу, до компетенції якого слід віднести проведення розслідування протиправної діяльності з криптовалютами [30, с. 177].

Тобто, запобігання злочинності у сфері цифрових технологій повинно відбуватися на основі чітко розробленої стратегії запобігання та відповідно тактики її проведення. Окрім цього, враховуючи зміни та постійну трансформацію цифрових та комп'ютерних технологій, має здійснюватися пошук та впровадження більш ефективних методів і форм проведення запобіжної чи попереджувальної діяльності в цифровій сфері. Така діяльність у сфері запобігання цифровій злочинності має визначати конкретні цілі та завдання, містити суб'єктів, котрі будуть їх виконувати, а також включати методичне, кадрове, аналітичне, інформаційне забезпечення, чітке планування профілактичних заходів і координацію роботи і обов'язково контроль за виконанням. І як результат, має бути розроблена та затверджена довгострокова державна комплексна цільова програма щодо запобігання злочинності у сфері цифрових технологій, а її основою має бути орієнтація на вплив та усунення всього комплексу детермінантів, які сприяють вчиненню кримінальних правопорушень у сфері цифрових технологій. Для того, щоб така програма була

дійсно дієвою та комплексною і мала результативність виконання необхідно проводити моніторинг стану захищеності населення від кіберзагроз в мережі Інтернет. Проведення таких моніторинрів має на меті отримати відомості щодо рівня торгівлі в мережі Інтернет, кількості Інтернет-магазинів, які ведуть активну торгівлю в мережі Інтернет, обсяги інвестицій у телекомунікаційну сферу тощо. Тобто, з метою кримінологічного прогнозування цифрової злочинності особливу увагу слід приділяти електронному маркетингу, електронному банкінгу, наданням електронних страхових послуг тощо.

Також для розробки вказаної програми потрібно: визначати ступінь кримінологічної безпеки загалом та кібербезпеки зокрема; вивчати та аналізувати кіберзагрози та кіберризики, а також вивчати зміни у злочинній поведінці осіб під впливом цифрових технологій; аналізувати, вивчати та впроваджувати позитивний зарубіжний досвід щодо запобігання правопорушенням у цифровій сфері.

Так, зокрема, слід відмітити, що Радою Європи було прийнято Конвенцію про злочинність у сфері комп'ютерної інформації, відповідну Резолюцію та Декларацію, спрямовані на побудову безпечного інформаційного суспільства [92;97]. Вони сьогодні визначають кримінально-правову політику у європейському вимірі, що спрямовується на захист суспільства від кримінальних правопорушень, що вчиняються у сфері цифрових технологій шляхом підготовки нормативно-правових актів та зміцнення співпраці міжнародного співтовариства у зазначеній сфері.

Інтерпол же у своїй діяльності надає великого значення в першу чергу інформаційному забезпеченню міжнародного співробітництва у сфері протидії окремим видам кримінальних правопорушень, а саме: легалізації (відмиванню) злочинних доходів, фінансуванню тероризму, організованій злочинній діяльності, злочинам, що посягають на економічні та соціальні засади життєдіяльності суспільства, у тому числі у фінансовій сфері, тощо. Інтерпол посилює боротьбу зі злочинами, пов'язаними з цифровими активами, та

допоможе у цьому напрямі іншим країнам. Ним застосовуються нові методи та способи роботи, оскільки злочинці використовують в даний час найновіші цифрові технології, стійку криптографію, що дозволяє їм уникнути кримінальної відповідальності. Ускладнюється робота ще й тим, що злочинці часто використовують тіньовий бізнес, у тому числі користуються такими цифровими майданчиками, як DarkNet. У зв'язку з цим Інтерпол оголосив про посилення діяльності щодо протидії злочинності з протиправним використанням криптовалюти в DarkNet, оскільки вона є майданчиком для хакерів усіх типів, шахраїв та осіб, які здійснюють незаконний обіг зброї, наркотиків тощо [29].

Тобто, вважаємо, що для запобігання злочинності у сфері цифрових технологій важливим є, по-перше, створення електронної платформи для протидії таким кримінальним правопорушенням, по-друге, співпраця та взаємодія з фахівцями ІТ-технологій, провайдерами відповідних послуг та всі ті компанії, які пов'язані з цифровими технологіями. Тобто, це розширить межі співпраці правоохоронних органів та загалом ІТ-сфери, що буде слугувати одним із напрямів покращення ефективності розслідування кримінальних правопорушень у сфері використання цифрових технологій. І по третє – запобігання злочинності у сфері цифрових технологій повинно мати комплексний підхід, що має включати також активізацію віктимологічної профілактики, яка спрямовується на збільшення захисного потенціалу громадян, що в даному випадку передбачає учасників «цифрових правовідносин» задля зменшення їх рівня віктимності.

Що стосується віктимологічної профілактики у глобальній мережі Інтернет, то вона повинна здійснюватися за такими основними напрямками: вдосконалення програмного забезпечення, що стосується захисту комп'ютерної інформації та підвищення рівня захисту інформаційної безпеки і кібербезпеки, що є складовими національної безпеки; здійснення автоматичного блокування спаму по електронній пошті та запобігання використанню Інтернету як

інформаційного ресурсу для запобігання кримінальним правопорушенням у сфері цифрових технологій; неможливість реєстрації анонімних інтернет-користувачів у місцях колективного доступу, власників електронних поштових скриньок, власників рахунків електронних платіжних систем; налагодження належного рівня взаємодії правоохоронних органів, інших органів державної влади, недержавних суб'єктів запобігання та громадян з метою забезпечення кібербезпеки в мережі Інтернет і швидкого реагування та можливі прояви кіберзагроз.

Таким чином, враховуючи трансформацію суспільства з погляду цифровізації, чинна нормативна база в державі повинна забезпечувати належний рівень протидії та запобігання кримінальним правопорушенням у сфері цифрових технологій. А враховуючи те, що злочинність у сфері цифрових технологій досить часто має транскордонний або ж транснаціональний характер, то заходи щодо протидії і запобігання такій злочинності повинні передбачати налагодження, перш за все, ефективного міжнародного співробітництва.

Саме тому, вважаємо, що до ефективних заходів запобігання злочинності у сфері цифрових технологій можна запропонувати наступні:

- оновлення та модернізація комп'ютерного забезпечення, комп'ютерної техніки та сучасних Інтернет-програм для правоохоронних органів в цілях ефективного виявлення, розслідування кримінальних правопорушень у сфері цифрових технологій та притягнення винних осіб до кримінальної відповідальності ;

- внесення змін до чинного законодавства, щодо регулювання напрямів запобігання сучасним кіберзагрозам, враховуючи реалії сьогодення та кількість загроз, яку несуть різноманітні правопорушення в мережі Інтернет з метою їх своєчасного виявлення та недопущення настання злочинних наслідків;

- здійснення належного захисту персональної інформації самими користувачами в мережі Інтернет та проведення інформаційно-просвітницької

діяльності правоохоронними органами серед населення щодо запобігання кримінальним правопорушенням у сфері цифрових технологій;

- оновлення Стратегії інформаційної безпеки з врахуванням сучасних та дієвих систем захисту інформації;
- налагодження ефективної співпраці між правоохоронними органами та криптовалютними організаціями в цілях запобігання та протидії злочинній діяльності, пов'язаній з незаконним обігом криптовалюти.

3.2. Сучасні пріоритетні напрями застосування цифрових технологій для забезпечення кримінологічної безпеки суспільства та запобігання злочинності

Злочинна діяльність є поширеною проблемою в сучасному суспільстві, і завданням кожної країни є пошук необхідних та достатніх заходів боротьби з нею. Історичний розвиток заходів із запобігання злочинності підкреслює важливість застосування цифрових технологій, різних технологічних інновацій, що виступали рушійною силою, яка призводила до реформування стратегій запобігання злочинності та боротьби зі злочинністю.

Так, технологічні інновації були однією з головних рушійних сил, що призвели до постійного вдосконалення стратегій боротьби зі злочинністю та запобігання їй (наприклад, GPS-відстеження, відеоспостереження тощо).

Відповідно до нещодавнього огляду поліцейських технологій, перша інноваційна революція в США, яка змінила спосіб організації та роботи поліції, зосереджена навколо трьох технологічних інновацій, які були використані поліцією: телефон, радіо та автомобіль: «З поширенням телефонів на початку двадцятого століття поліцейська діяльність змінилася. Громадяни викликали – і насправді їх закликали викликати – поліцію для вирішення багатьох проблем, і поліція відповідала на ці дзвінки з диспетчерської через двосторонню радіостанцію та швидко їхала до місця за допомогою патрульних автомобілів.

Ці технологічні досягнення разом із змінами в адміністративних процедурах поліції допомогли створити поліцію такою, якою ми її знаємо сьогодні» [116, с. 153].

Мобільні телефони, бездротові камери спостереження, системи GPS та Інтернет-мережі все частіше використовуються підрозділами боротьби зі злочинністю. В останні роки відеоспостереження замкнутого каналу (CCTV) використовується у всьому світі як основний спосіб запобігання злочинності [105].

Система відеоспостереження з відповідними камерами відеоспостереження здатна зафіксувати будь-яке правопорушення, яке може відбутися у полі її спостереження. Звичайні системи відеоспостереження чудово справляються із записуванням кримінальних правопорушень. Камери відеоспостереження зазвичай призначені для зменшення злочинності, адже, по-перше, це стримування правопорушників які бояться бути впізнаними у вчиненні кримінального правопорушення на камеру, а по-друге – це забезпечення правоохоронних органів можливістю виявляти кримінальні правопорушення, що вчиняються чи готуються до вчинення і вчасно їм запобігати. Якщо ж не спрацювали вчасно правоохоронні органи на випередження вчиненню кримінального правопорушення, то камери відеоспостереження можуть записати докази того, що вчинено кримінальне правопорушення, хто вчинив чи був причетним до його вчинення і загалом ті чи інші деталі вчиненого правопорушення, які можуть бути використані в кримінальному провадженні для встановлення істини у кримінальному процесі та притягненні винних осіб до кримінальної відповідальності [7].

Європейські правоохоронні органи все частіше використовують штучний інтелект для максимально ефективною та швидкої обробки цифрових даних. Для запобігання злочинам на вокзалах, торгових об'єктах і в містах встановлено багато камер спостереження. Однак зі збільшенням кількості камер значно збільшився і обсяг відеоданих. Це практично унеможлиблює для

правоохоронних органів відстежувати підозрілу поведінку та виявляти злочини вручну. Для вирішення цієї проблеми в боротьбі зі злочинністю використовується штучний інтелект. ШІ підтримує віддалений моніторинг цілодобово, 365 днів на рік, підвищуючи точність аналізу відеоданих, дозволяючи виявляти в режимі реального часу підозрілу активність і повідомляти про неї. Камери відеоспостереження, які в основному були встановлені для запису та діяли як стримуючий фактор злочинності, тепер можна використовувати для прогнозування, виявлення та запобігання злочинам [152, с. 39-40].

Саме тому, системи відеоспостереження повинні постійно вдосконалюватися, щоб включати новітні функції програмних технологій, адже якість реагування на ті чи інші правопорушення, які можуть зафіксувати камери полягає в можливостях самих систем відеоспостереження. І досить часто буває так, що камери ввімкнені, ведеться відеоспостереження, проте камера не веде фіксацію зйомки, а лише знімає в реальному часі. В такому разі багато чого залежить від персоналу, який закріплений за цими камерами для вчасного реагування на окремі підозрілі активності. До таких напрямів вдосконалення систем відеоспостереження можна віднести: розпізнавання обличчя, аналіз ходи, виявлення руху, виявлення відсутності об'єкта тощо.

Штучний інтелект у відеоспостереженні може виявляти потенційні загрози та запускати механізм реагування для запобігання кримінальному правопорушенню. Розумна відеоаналітика камери безпеки зі штучним інтелектом виявляє підозрілі рухи у приміщенні та вмикає гучний сигнал тривоги або попереджає, щоб налякати порушника. Камери безпеки також можуть активувати яскраве світло, коли спрацьовує рух або підозріла активність у темний час доби. Блискучі вогні, які спрацьовують в камері спостереження, можуть налякати порушника через страх бути спійманим. Камери відеоспостереження зі штучним інтелектом і мережеві відеореєстратори не тільки діють як стримуючий фактор, але й здатні

сповістити правоохоронні органи про вчинення правопорушення. Функція розпізнавання обличчя дозволяє камері визначити, чи є особа знайомим обличчям чи потенційною загрозою на основі її дій. Функція виявлення номерних знаків транспортних засобів може розпізнавати часті відвідування приміщень певними автомобілями. Інтелектуальна відеоаналітика також може виявляти моделі поведінки. Наприклад, камера відеоспостереження зафіксувала людину, яка неодноразово стояла поза межами огорожі без будь-якої причини. Камери відеоспостереження зі штучним інтелектом позначатимуть цю підозрілу поведінку для попереджувальних дій проти потенційної загрози. З додатковим навчанням системи відеоспостереження зможуть визначити, чи є особа, яка проходить через приміщення, загрозою чи ні, і, відповідно, система відеоспостереження вживатиме попереджувальних дій. Система відеоспостереження зі штучним інтелектом також надсилає сповіщення в режимі реального часу на мобільний телефон, коли виявляє підозрілий рух у приміщенні [117].

Таким чином, системи відеоспостереження можуть допомогти запобігти кримінальним правопорушенням, контролювати підозрілу діяльність, ідентифікувати номерні знаки та збирати докази, тощо.

Мітки бездротової радіочастотної ідентифікації (RFID) часто використовуються поліцією для спостереження за умовно-достроково звільненими та особами, які перебувають під домашнім арештом. Мітки передають сигнал, який контролює місцезнаходження суб'єкта, повідомляючи поліцію, якщо суб'єкт входить у зону, куди йому чи їй не слід [123].

Технологія Bluetooth все ширше використовується для молоді та груп ризику в містах, щоб зменшити злочинність або підвищити обізнаність. У деяких випадках він може використовуватися й використовувався для пошуку свідків серйозних злочинів у певних областях, оскільки Bluetooth може охоплювати широку кількість користувачів за короткий проміжок часу без необхідності збору номерів телефонів та ідентифікаційної інформації.

Незважаючи на те, що технологія, як і метод передачі повідомлень, не є новою, таке використання технології показує, що поліція в усьому світі визнає використання широко поширеної технології та користується тим фактом, що багато людей використовують Bluetooth, хоча й не покладаються на нього для інформування громадян про важливі повідомлення [156].

Прийомопередавачі бездротового зв'язку малого радіусу дії, такі як Bluetooth і WI-FI, широко використовуються в багатьох портативних та мобільних пристроях, включаючи ноутбуки, мобільні телефони та смарт-годинники. Їх можливості можна використовувати для запобігання або розслідування викрадення дітей. Систему можна використовувати для постійної реєстрації пристроїв Bluetooth поблизу дитини, тобто, наприклад, через мобільний додаток, батьки можуть контролювати місцеперебування чи соціальну активність дитини.

Однією з передових технологій є живі пристрої відбитків пальців. Ці пристрої електронно сканують відбитки пальців людини, передають інформацію до кримінальної бази даних і негайно надають будь-які збіги.

Напевно чи не щодня відбуваються завантаження мобільних додатків на смартфони користувачів, а також зростає екранний час проведений за гаджетами. З огляду на це, розвиток використання мобільних додатків, як засобу запобігання злочинності виглядає дуже корисним для просування та підвищення кримінологічної безпеки. В цьому контексті існує широкий спектр програм, які допомагають як у запобіганні кримінальним правопорушенням, так і щодо повідомлень про вже вчинені кримінальні правопорушення. Програми для запобігання кримінальним правопорушенням можна умовно розділити на дві категорії, а саме додатки, призначені для використання правоохоронними органами, і ті, які призначені для широкої громадськості в суспільстві.

Останніми роками було розроблено численні мобільні програми для полегшення повідомлення про надзвичайні та панічні ситуації близьким

родичам та поліцейським установам. Наприклад, Circle of 6 – це програма для iPhone, призначена для студентів та їхніх друзів, щоб залишатися поруч, бути в безпеці та запобігати насильству, поки воно не сталося. Це швидкий, простий у використанні та безпечний спосіб піклуватися один про одного. Щоб отримати допомогу, потрібно два дотики, тому не потрібно багато часу, щоб шукати якийсь мобільний номер. Програма використовує піктограми для позначення дій, щоб ніхто не міг зрозуміти, що особа задумала, побачивши її телефон. Конструкція забезпечує безпеку, швидкість і конфіденційність. GPS інтегрований (за допомогою карт Google), активується лише особою та надсилається до потрібних користувачів [89].

Подібним чином працює програма Noonlight, що забезпечує механізм сповіщення про надзвичайні ситуації установи, натиснувши й утримуючи кнопку, вбудовану в додаток. Коли кнопку відпустити, користувача запитується для її/його PIN-коду і користувачеві достатньо ввести PIN-код, щоб вказати, що він чи вона в безпеці. Якщо код не надається, ситуація негайно повідомляється до екстрених установ разом із геолокацією GPS у реальному часі користувача [154].

Принцип роботи, подібний до Circle of 6 і Noonlight, забезпечує Silent Beacon. Тут, поряд із додатком постачається портативний пристрій у формі тривожної кнопки. Після натискання кнопки, пристрій повідомляє про дію програмі для смартфона, яка потім автоматично викликає службу екстренної допомоги під час передачі надзвичайних ситуацій і місцезнаходження до визначеного користувачем списку контактів. Silent Beacon — це пристрій безпеки Bluetooth, який з'єднується з смартфоном користувача або планшетом і дозволяє миттєво зателефонувати в службу екстренної допомоги або на будь-який номер, який особа обирає, одночасно надсилаючи поточне GPS-місцезнаходження кільком людям одночасно [120].

Інші мобільні додатки, які також спрямовані на запобігання кримінальним правопорушенням різними способами, доступними для

громадськості. Одним з таких є мобільний додаток BrightSky, який спрямований на жертв або потенційних жертв домашнього насильства, будучи першим додатком для смартфонів у Великобританії. BrightSky дозволяє користувачам знайти найближчий центр підтримки за допомогою пошуку їхнього регіону, поштового індексу або поточного місцезнаходження. Інші функції включають інструмент для реєстрації випадків зловживань, візуальні та звукові форми [85].

Загалом, боротьбу з кіберзлочинністю в сучасних реаліях здійснюють такі структури:

1. Міжнародне багатостороннє партнерство проти кіберзагроз (ІМРАСТ) є органом виконавчої влади у сфері кібербезпеки спеціалізованого агентства ООН, що об'єднує зусилля багатьох держав, неурядових організацій, а також фахівців у сфері інформаційної безпеки. Це глобальне некомерційне партнерство між урядами, науковими колами, промисловістю та експертами з кібербезпеки, спрямоване на боротьбу з кіберзагрозами, що допомагає країнам-партнерам, особливо країнам, що розвиваються, прийняти методи підвищення кібербезпеки. Його штаб-квартира в Кіберджайї, Малайзія, також є «фізичним і оперативним центром Глобальної програми кібербезпеки (GCA)» міжнародної структури кібербезпеки, розробленої у співпраці з Міжнародним союзом електрозв'язку (ITU) [118];

2. ISA Global Cybersecurity Alliance (ISAGCA) – це глобальний консорціум, який працює над захистом критичної інфраструктури, який створений Міжнародним товариством автоматизації (ISA) і є форумом для співпраці з підвищення обізнаності, освіти, готовності, стандартизації та обміну знаннями щодо кібербезпеки ОТ та Міжнародний альянс кібербезпеки (ICSPA), який об'єднує правоохоронні органи, в тому числі Європол, міжнародний бізнес і уряди багатьох країн світу (Австралія, Велика Британія, Канада, Нова Зеландія, США та ін.). ICSPA був створений для наряду фінансування, експертних знань і допомоги для допомоги підрозділам правоохоронних

органів, які займаються кіберзлочинністю, як на внутрішньому, так і на міжнародному ринках. Тобто, це організація, що складається з великих національних і міжнародних компаній, які визнають необхідність надання додаткових ресурсів і підтримки співробітників правоохоронних органів у всьому світі в їхній боротьбі з кіберзлочинністю [135; 119];

3. Міжнародна організація кримінальної поліції (Інтерпол), що забезпечує швидкий та ефективний механізм для координації комунікацій між державами. Інтерпол об'єднує країни за допомогою системи зв'язку під назвою I-24/7. Країни використовують цю захищену мережу для зв'язку одна з одною та з Генеральним секретаріатом. Це також дозволяє їм отримувати доступ до баз даних і послуг у режимі реального часу як з центрального, так і з віддалених місць. Цей досвід підтримує національні зусилля у боротьбі зі злочинністю в чотирьох глобальних сферах, які є найбільш актуальними сьогодні: тероризм, кіберзлочинність та організована злочинність [155].

Міжнародний підхід означає вдосконалення та перевірку правових механізмів на національному та міжнародному рівнях щодо протидії злочинним проявам у сфері цифрових комунікацій. У зв'язку з цим необхідний в першу чергу комплекс міжурядових заходів, щоб мінімізувати кібератаки та злочинні прояви у сфері цифрових технологій, а саме: уніфікувати національне законодавство щодо кримінальних правопорушень в цифровій сфері; розвинути практику швидкого реагування на міжнародному та національному рівнях у відповідь на злочинні дії у сфері цифрових технологій; налагодити механізм перегляду та вирішення питань, пов'язаних з різними проявами порушень у сфері цифрових технологій.

Також, необхідно відмітити, що розвиток цифрових технологій в кримінальному провадженні, перш за все повинен набути належного процесуального закріплення, тобто процес використання цифрових технологій у роботі з доказовою інформацією при її збиранні та дослідженні має отримати нормативне закріплення, а також потрібно удосконалити професійну підготовку

суб'єктів застосування цифрових засобів та методів при їх використанні у розслідуванні кримінальних правопорушень.

Як, ми уже відмічали у попередньому підрозділі, запобігання злочинності у сфері цифрових технологій включає також і низку віктимологічних заходів в різних вікових групах і верствах населення. Так, зокрема необхідно зосередитися на виявленні віктимологічних закономірностей у вчиненні правопорушень, пов'язаних із різними цифровими технологіями, з метою виявлення об'єктивних тенденцій та характеристики вчинення протиправних дій зокрема щодо незахищених верств населення (наприклад неповнолітніх осіб, осіб похилого віку, які в силу різних обставин можуть бути більш вразливі до того, щоб стати жертвою такого правопорушення).

Варто також звернутися і до зарубіжного досвіду застосування цифрових технологій в методиці розслідування кримінальних правопорушень, їх виявлення та запобігання.

Інноваційні цифрові технології в системі кримінального правосуддя у США розділяють на дві широкі категорії: жорсткі технології (апаратне забезпечення або матеріали) та м'які технології (комп'ютерне програмне забезпечення, інформаційні системи тощо). Жорсткі технологічні інновації включають нові матеріали, пристрої та обладнання, які можна використовувати в процесі розслідування злочинів або запобігання та боротьбі зі злочинністю. Так, зокрема можна проаналізувати технологічні інновації, призначені для запобігання злочинам – поширеність камер відеоспостереження, металопрошукачі в школах, перевірка багажу в аеропортах, куленепробивні вікна кас у банках і системи безпеки в будинках і на підприємствах тощо. Окремо хочеться звернути увагу на використанні технологічних засобів індивідуального захисту: шокери, рятувальні мотузки, щодо механізмів виклику екстреної допомоги, системи блокування запалювання з пристроями датчика алкоголю для запобігання запуску автомобіля особою в нетверезому стані [122, с.19].

Також інформаційні цифрові технології використовуються для запобігання злочинності в соціальних мережах, так зокрема мова йде про використання розробленого комп'ютерного програмного забезпечення та створення пристроїв для моніторингу трансакцій і комунікацій особи по мобільному телефону, через Інтернет і на різних веб-сайтах соціальних мереж. Ця нова технологія змінила спосіб, у який поліція розслідує фінансові злочини, злочини, пов'язані з наркотиками, торгівлю людьми через Інтернет і сексуальні злочини. В огляді електронного спостереження поліцейськими службами у США, встановлені особливі вимоги до звітності що стосується проведення прослуховування телефонних розмов, наказів про перехоплення, ручні реєстри, пристрої для перехоплення й відстеження і екстрене добровільне розкриття інформації), запити на перегляд «збережених комунікацій та записи абонентів. Це включає збережені електронні листи, миттєві повідомлення, історію веб-перегляду, документів, що зберігаються в «Інтернет сховищі-хмарі» [147].

Так, для прикладу, у період з липня по грудень 2022 року Facebook отримав 239 000 запитів правоохоронних органів щодо інформації про користувачів. Загалом соціальна мережа видала дані користувачів для понад 76 відсотків запитів. Перше місце за кількістю запитів посідають США, на які припадає 111 тисяч запитів [131;139] (Додаток А).

Отже, незважаючи на те, що традиційні методи правоохоронних органів і пильність громади залишаються вирішальними, інтеграція цифрових технологій у стратегії запобігання злочинності зробила революцію в безпеці та розкритті кримінальних правопорушень. Правоохоронні органи використовують різноманітні методи запобігання злочинності, щоб забезпечити безпеку своїх громадян.

Цифрові технології стають потужним помічником у боротьбі зі злочинністю. Використання різноманітних аналітичних методів в прогностичній поліцейській діяльності можуть допомогти ідентифікувати потенційних правопорушників і жертв. Цифрове криміналістичне програмне

забезпечення має можливість отримувати та контролювати індивідуальні комунікації, які відбуваються через Інтернет, веб-сайти соціальних медіа та мобільні пристрої. Це може допомогти правоохоронним органам у розслідуванні кримінальних правопорушень у фінансовій сфері, правопорушень, пов'язаних з наркотиками, торгівлею людьми через Інтернет (зокрема, електронні листи, миттєві інтернет-повідомлення, історія веб-перегляду, записи пошуку та дані на інтернет-ресурсах можуть виступати доказами у кримінальних провадженнях).

Досить суперечливою на практиці використання виступає методика автоматичного розпізнавання обличчя особи із застосуванням ШІ. Алгоритми розпізнавання обличчя особи можуть аналізувати цифрові зображення або відео, щоб виявляти та ідентифікувати обличчя людей. Це допомагає ідентифікувати жертв або підозрюваних. Аналіз може також включати порівняння обличчя, зафіксованих на записах камер спостереження, або зображень, отриманих із профілів соціальних мереж, з відомими базами даних осіб для встановлення їх особи.

Так, зокрема Штучний інтелект Clearview використовувався поліцією США майже мільйон разів, за даними BBC. Clearview має 30 мільярдів зображень, зібраних із таких платформ, як Facebook, зроблених без дозволу користувачів. Компанію неодноразово штрафували на мільйони доларів у Європі та Австралії за порушення конфіденційності. Clearview — приватна компанія, яка робить відбитки обличчя людей на основі їхніх фотографій в Інтернеті без їхньої згоди, тому й виступає таке застосування цифрових технологій неоднозначним та з багатьма судовими спорами. Система Clearview дозволяє клієнту з правоохоронних органів завантажувати фотографію обличчя та знаходити збіги в базі даних із мільярдів зібраних зображень. Потім надає посилання на відповідні зображення в Інтернеті. Вважається однією з найпотужніших і найточніших компаній у світі розпізнавання обличчя. Використання розпізнавання обличчя поліцією часто подається громадськості

як таке, що використовується лише для серйозних або насильницьких злочинів. Враховуючи неоднозначність та суперечливість застосування такої методики, її досить часто коментують як можливість отримання підказки, певного алгоритму у пошуку осіб чи їх ідентифікації, задля ефективного розслідування кримінального правопорушення [90].

Впровадження таких технологій докорінно змінило те, як правоохоронні органи борються зі злочинною діяльністю. Штучний інтелект, цифрові, комп'ютерні, інформаційні технології, експертиза соціальних мереж і розпізнавання обличчя озброюють правоохоронні органи інструментами, необхідними для здійснення запобігання та боротьби зі злочинністю в епоху цифрових технологій. Поєднання різноманітних цифрових технологій не тільки посилює превентивні заходи, але й дозволяє правоохоронним органам краще розуміти, передбачати та реагувати на нові загрози.

Ми уже зазначали, у попередніх підрозділах щодо доцільності та необхідності впровадження у навчальний курс «Кримінологія», вивчення цифрової кримінології. Враховуючи розвиток та диференціацію різноманітних сучасних цифрових технологій, досить перспективним напрямом вивчення та дослідження виступає цифрова криміналістика та можливості цифрових криміналістичних технологій не тільки при розслідуванні кримінальних правопорушень у цифровій, комп'ютерній, інформаційній сфері зокрема та й інших правопорушень загалом, а й також при запобіганні злочинності.

Кожна дія користувача в соціальних мережах залишає цифрові сліди і такі відбитки, що містять метадані, часові позначки, дані про геолокацію та дії користувачів, можуть надати безцінне розуміння послідовності подій та осіб, які беруть участь. Правоохоронні органи можуть виявляти та ідентифікувати злочинців, аналізуючи цифрові докази, відновлюючи дані, досліджуючи онлайн сліди та перевіряючи онлайн докази. Оскільки технології продовжують розвиватися, тому розвиватиметься й цифрові технології все більше застосовуються в процесі запобігання, розслідування чи профілактики

кримінальних правопорушень, надаючи ще потужніші інструменти для боротьби зі злочинами в соціальних мережах і забезпечення кримінологічної безпеки людей у цифровому просторі [110].

Так, для прикладу можна навести технології цифрової криміналістики DEI PRO, яка плавно інтегрує апаратні та програмні технології, надаючи слідчим портативний інструмент із програмним забезпеченням для автоматизованої цифрової криміналістики. DEI PRO – це комплексне програмне забезпечення для криміналістики цифрових доказів, сортування та використання носіїв, створене для швидкості, масштабованості та простоти у використанні для слідчих, яким потрібні результати. Програмне забезпечення швидко обробляє та аналізує смартфони (iOS, Android і ChromeOS), комп'ютери, зовнішні диски, образи дисків та інші носії (флеш-накопичувачі USB, карти пам'яті тощо). DEI PRO збирає цифрові докази в кіберзлочинах і представляє їх у вигляді часової шкали, щоб прив'язати користувача до файлів і артефактів, створюючи колекцію цифрових доказів, щоб допомогти вам вирішити ваше розслідування та зменшити кількість судово-медичних досліджень. Також дозволяє швидко правоохоронним органам, слідчим, експертам перевіряти пристрої Mac, Windows, Linux, ChromeOS, iOS і Android, а також зовнішні накопичувачі на наявність заборонених матеріалів, таких як образа сексуального насильства, імена користувачів і контакти як у польових, так і в лабораторних умовах [100].

Загалом, різноманіття соціальних мереж стали для кожного члена суспільства невід'ємною частиною повсякденного життя, способом спілкування, отримання заробітку, розміщення реклами тощо. Тобто, від обміну особистими фото, відео до спілкування з друзями та колегами чи формою заробітку. Проте, враховуючи кількість користувачів соціальними мережами, способи їх використання та застосування, нажаль соціальні мережі також стали середовищем для вчинення різноманітних кримінальних правопорушень, незаконної діяльності, від кіберзалякування та онлайн-шахрайства до крадіжки

особистих даних і кібертероризму, про що ми зазначали у попередніх підрозділах.

Тобто, коли кримінальні правопорушення вчиняються з використанням соціальних мереж, чи частково пов'язані з ними, цифрова криміналістика та цифрова кримінологія відіграють досить вирішальну роль при вирішенні винуватості особи, пошуку прихованої інформації, відстеженні цифрових слідів особи та загалом вивченні та відтворенні видалених чи змінених дій в мережі Інтернет.

Таким чином, застосування різноманітних цифрових технологій під час запобігання злочинності, виявленні чи пошуку винних осіб, дослідженні слідів вчинення кримінальних правопорушень, вагоме значення необхідно приділяти аналізу доказів із платформ соціальних мереж. Це включає в себе вивчення і дослідження таких даних, як: дописи користувачів, повідомлення, коментарі, лайки та поширення, які можуть свідчити про встановлення певних зв'язків особи з іншими користувачами, ідентифікації підозрюваних, встановлення часових меж певних подій тощо.

Саме тому, в цьому аспекті, необхідно ще раз зазначити про необхідність залучення експертів у цих галузях і також проведення різних семінарів, практикумів, підвищення кваліфікації слідчих щодо дослідження цифрових доказів. Адже правопорушники досить часто намагаються приховати свої дії, шляхом видалення чи зміни певних цифрових даних з метою знищення своїх слідів чи своєї причетності до певного кримінального правопорушення. Тому, слідчим необхідно звертати увагу, при аналізі та вивченні кримінальних проваджень у сфері цифрових технологій на різноманітні онлайн-докази, такі як: знімки екрану, журналів чатів та їх мультимедійного змісту, що в майбутньому зможуть слугувати вагомими підтверджуючими доказами винуватості чи невинуватості особи.

Тобто застосування цифрових технологій в забезпеченні кримінологічної безпеки суспільства та запобіганні злочинності відіграє вагому

роль, оскільки аналізуючи закономірності, тенденції та онлайн-поведінку особи злочинця, можна визначати потенційні загрози, позначати підозрілі дії та втручатися, щоб запобігти кримінальним правопорушенням до того, як вони будуть вчинені або ж припинити на стадіях готування чи замаху. Цей цифровізаційний підхід використовує потужність цифрових технологій для забезпечення безпеки кримінологічної безпеки у цифровій сфері.

Висновки до Розділу 3

1. Запропоновано конкретизувати нормативні напрями вдосконалення правового регулювання у сфері цифрових технологій в умовах сучасності їх розвитку. А саме, в межах запобігання кримінальним правопорушенням, що вчиняються з використанням цифрових технологій, запропоновано на нормативному рівні врегулювати родові та видові об'єкти кримінальних правопорушень, що вчиняються з використанням цифрових технологій, що дозволить не тільки логічно правильно спланувати процес доведення і кваліфікувати злочинне діяння, а й скоригувати вектор розвитку правових засобів боротьби з кримінальними правопорушеннями у цифровій сфері та підвищити рівень цифрової безпеки і захисту громадян, суспільства та держави загалом.

2. Запропоновано необхідність визначення на державному та місцевому рівнях напрями і заходи запобігання злочинності у цифровій сфері, що мають забезпечувати комплексність такого підходу запобіжної діяльності, до яких мають належати: вплив суб'єктів попередження злочинності на негативні явища, що детермінують кримінальні правопорушення у сфері цифрових технологій, тобто у сучасних умовах є важливою підготовка теоретично і практично обґрунтованої та фінансованої програми запобігання злочинності у сфері цифрових технологій, яка була б зорієнтована на усунення всього комплексу факторів, що призводять до зростання та зміцнення цифрової

злочинності; чітка взаємодія та активізація органів державної влади і громадських організацій, пов'язаних із сферою цифрової діяльності; застосування форм і методів запобігання злочинності у сфері цифрових технологій, які ґрунтуються на результатах наукових досліджень, що впроваджені у практичну діяльність правоохоронних органів.

3. Запропоновано розробити та реалізувати для початку короткострокову або середньострокову стратегію чи програму запобігання злочинності у сфері цифрових технологій та передбачити тактику її проведення, яка має визначати конкретні цілі та завдання, містити суб'єктів, котрі будуть їх виконувати, а також включати методичне, кадрове, аналітичне, інформаційне забезпечення, чітке планування профілактичних заходів і координацію роботи і обов'язково контроль за виконанням. А як результат її впровадження, має бути розроблена та затверджена довгострокова державна комплексна цільова програма щодо запобігання злочинності у сфері цифрових технологій, а її основою має бути орієнтація на вплив та усунення всього комплексу детермінантів, які сприяють вчиненню кримінальних правопорушень у сфері цифрових технологій. Для того, щоб така програма була дійсно дієвою та комплексною і мала результативність виконання пропонується проводити моніторинг стану захищеності населення від кіберзагроз в мережі Інтернет.

4. Охарактеризовано доцільність визначення ступеня кримінологічної безпеки загалом та кібербезпеки з метою вивчення та аналізу кіберзагроз та кіберризиків, а також вивчення змін у злочинній поведінці осіб під впливом цифрових технологій; аналізу, вивчення та впровадження позитивного зарубіжного досвіду щодо запобігання правопорушенням у цифровій сфері.

5. З метою активізації сучасних напрямів забезпечення кримінологічної безпеки у сфері використання цифрових технологій, запропоновано такі напрями: оновлення та модернізація комп'ютерного забезпечення, комп'ютерної техніки та сучасних Інтернет-програм для

правоохоронних органів в цілях ефективного виявлення, розслідування кримінальних правопорушень у сфері цифрових технологій та притягнення винних осіб до кримінальної відповідальності; внесення змін до чинного законодавства, щодо регулювання напрямів запобігання сучасним кіберзагрозам, враховуючи реалії сьогодення та кількість загроз, яку несуть різноманітні правопорушення в мережі Інтернет з метою їх своєчасного виявлення та недопущення настання злочинних наслідків; здійснення належного захисту персональної інформації самими користувачами в мережі Інтернет та проведення інформаційно-просвітницької діяльності правоохоронними органами серед населення щодо запобігання кримінальним правопорушенням у сфері цифрових технологій; оновлення Стратегії інформаційної безпеки з врахуванням сучасних та дієвих систем захисту інформації.

6. Наведено обґрунтування необхідності налагодження ефективної співпраці між правоохоронними органами та криптовалютними організаціями в цілях запобігання та протидії злочинній діяльності, пов'язаної з незаконним обігом криптовалюти.

7. Конкретизовано цілі та завдання впровадження цифрових технологій в кримінальне провадження та відмічено, що перш за все воно має набути належного процесуального закріплення, тобто процес використання цифрових технологій у роботі з доказовою інформацією при її збиранні та дослідженні має отримати нормативне закріплення, а також потрібно удосконалити професійну підготовку суб'єктів застосування цифрових засобів та методів при їх використанні у розслідуванні кримінальних правопорушень.

ВИСНОВКИ

1. Запропоновано прийняти на рівні держави Стратегію кримінологічної безпеки України на 2024-2028 роки, на основі проведеного наукового дослідження поняття, сутності та ролі кримінологічної безпеки в умовах цифрової трансформації, з метою належного рівня захисту прав та свобод людини і громадянина від негативних посягань в кіберпросторі, з яким певним чином пов'язаний кожен громадянин нашої держави. Тому, розробка, прийняття та затвердження вказаної Стратегії кримінологічної безпеки України на державному рівні надасть законодавчого дотримання належного рівня кримінологічної безпеки.

2. В результаті детального аналізу стану нормативно-правового регулювання використання цифрових технологій для забезпечення кримінологічної безпеки суспільства, сформульовано визначення «злочинності у сфері використання цифрових технологій», а саме як сукупність кримінальних правопорушень, що вчиняються із використанням систематизованих правових, науково-технічних, організаційних рішень, спрямованих на застосування комп'ютерної та іншої електронно-обчислювальної техніки, програмного забезпечення та інших засобів для зменшення участі користувача інформаційно-комунікаційних систем і засобів інформатизації під час збирання, приймання, обробки, передавання інформації чи трудомісткості виконуваних операцій.

3. Запропоновано внести до Кримінального Кодексу України зміни, а саме: змінити назву Розділу XVI «Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» на «Кримінальні правопорушення у сфері використанням цифрових технологій» та розширити його, шляхом перенесення статей, склади яких передбачають застосування чи використання будь-яких цифрових технологій, що дозволить систематизувати

ці види кримінальних правопорушень, враховуючи їх значне поширення на сучасному етапі розвитку громадянського суспільства та його цифровізації. Вказані пропозиції вдосконалять нормативно-правове регулювання у сфері телекомунікаційних та цифрових технологій в умовах сучасності їх розвитку, а саме мають на меті обґрунтувати формулювання та закріплення чітких норм, що визначають ознаки злочинності у цифровій сфері.

4. На основі вивчення та аналізу зарубіжного досвіду використання цифрових технологій та штучного інтелекту при запобіганні злочинності визначено, що сучасним напрямом розвитку кримінологічної науки є саме цифрова кримінологія, тому обґрунтована доцільність в Особливій частині Кримінології розглядати такий вид злочинності, як «Злочинність у сфері цифрових технологій» або «Цифрова злочинність», а також виокремити окремий вид Кримінології – «Цифрову кримінологію». Проаналізовано можливість в межах цифрової кримінології виокремити такі основні напрями її розвитку: протидія злочинності; формування та використання баз даних кримінологічної інформації, її аналізу на основі цифрових технологій для прогнозування злочинності та запобігання і попередження злочинності; кримінологічне профілювання; використання штучного інтелекту; геномна реєстрація.

5. Охарактеризовано сучасний стан забезпечення кримінологічної безпеки у сфері цифрових технологій та визначено, що вагомим напрямом діяльності щодо побудови дієвої системи кібербезпеки є в першу чергу вдосконалення нормативно-правової бази, яка регулює вказану сферу діяльності та вдосконалення системи управління щодо регулювання цифровізації суспільства. Окрім цього, обґрунтовано важливість проведення різних курсів підвищення кваліфікації, тренінгів з питань кібербезпеки не лише для працівників Кіберполіції України, а й для усіх співробітників правоохоронних органів і також проведення інформування громадян щодо забезпечення та дотримання безпеки в кіберпросторі, шляхом, наприклад

проведення лекцій у навчальних закладах, на підприємствах, установах, організаціях, розміщення інформації щодо безпечного користування всесвітньою мережею Інтернет тощо, з метою забезпечення належного рівня кримінологічної безпеки в нашій державі.

6. Досліджено кримінальні правопорушення, що вчиняються із використанням цифрових технологій та цифрової валюти та відмічено необхідність встановлення конкретної міри кримінальної відповідальності за правопорушення у сфері обігу віртуальних активів, цифрової та електронної валюти та запропоновано прирівняти цифрову інформацію до майна, адже що хоч цифрову інформацію не можна доторкнутися і відчутти, як носій інформації виступає речовий предмет (наприклад, Flash-карта), що містить цифрову інформацію та представляє матеріальну цінність. На основі цього, наведено доцільність встановлення кримінальної відповідальності за придбання або збут цифрової інформації, яка свідомо одержана кримінально протиправним шляхом та внесення змін до КК України, шляхом доповнення його статтею 198-1 *«Придбання, отримання, зберігання чи збут цифрової інформації, одержаної кримінально протиправним шляхом» та викласти її у наступній редакції:*

«Заздалегідь не обіцяне придбання або отримання, зберігання чи збут цифрової інформації, одержаної кримінально протиправним шляхом

карається арештом на строк до шести місяців або обмеженням волі на строк до трьох років, або позбавленням волі на той самий строк».

7. Охарактеризовано стан міжнародно-правового регулювання забезпечення кримінологічної безпеки у сфері використання цифрових технологій та акцентовано увагу на напрямках вдосконалення онлайн-дослідницької мережі, за підтримки міжнародних агентств і приватного сектору, що надасть можливості для більшого обміну інформацією, спілкування між експертами в усьому світі з питань комп'ютерної та цифрової злочинності, порівняльного аналізу і передачі знань про запобігання та боротьбу з комп'ютерними та цифровими кримінальними правопорушеннями, а також

розвиток відповідних інструментів навчання, які мають бути доступними на міжнародному рівні, щоб ділитися знаннями та інформацією щодо способів і засобів виявлення, запобігання та боротьби з новими видами кіберзлочинності та злочинності у сфері цифрових технологій.

8. Обґрунтовано доцільність посилення міжнародного правоохоронного співробітництва, шляхом підвищення потенціалу та кваліфікації існуючої системи правоохоронних органів, які зосереджені на запобіганні кіберзлочинності; покращення взаємної правової допомоги та співпраці на початкових стадіях транскордонних кримінальних проваджень, що стосуються злочинності у сфері цифрових технологій та спрощення процедури взаємної правової допомоги і міжвідомчої слідчої співпраці; створення централізованих навчальних курсів по актуальним та сучасним напрямам запобігання кіберзлочинності для слідчих, враховуючи постійні трансформаційні процеси у сфері цифровізації суспільства, що будуть забезпечені експертами у сфері запобігання кіберзлочинності, а також наявність сучасного комп'ютерного обладнання.

9. Для запобігання злочинності у сфері цифрових технологій виокремлені наступні пропозиції: по-перше, створення електронної платформи для протидії таким кримінальним правопорушенням, по-друге, співпраця та взаємодія з фахівцями ІТ-технологій, провайдерами відповідних послуг та всі ті компанії, які пов'язані з цифровими технологіями, що допоможе розширити межі співпраці правоохоронних органів та загалом ІТ-сфери та буде слугувати одним із напрямів покращення ефективності розслідування і запобігання кримінальним правопорушенням у сфері використання цифрових технологій; по-третє активізувати віктимологічну профілактику, яка спрямовується на збільшення захисного потенціалу громадян, що в даному випадку передбачає учасників «цифрових правовідносин» задля зменшення їх рівня віктимності. А враховуючи трансформацію суспільства з погляду цифровізації, чинна нормативна база в державі повинна забезпечувати належний рівень протидії та

запобігання кримінальним правопорушенням у сфері цифрових технологій. А враховуючи те, що злочинність у сфері цифрових технологій досить часто має транскордонний або ж транснаціональний характер, то заходи щодо протидії і запобігання такій злочинності повинні передбачати налагодження, перш за все, ефективного міжнародного співробітництва.

10. Визначені сучасні пріоритетні напрями застосування цифрових технологій для забезпечення кримінологічної безпеки суспільства та запобігання злочинності. На основі аналізу зарубіжного досвіду, обґрунтовано та запропоновано важливість розвитку та впровадження в процес запобігання злочинності використання різних мобільних додатків, як засобів запобігання злочинності, що є дуже корисним для просування та підвищення кримінологічної безпеки. Запропоновано використання новітніх, сучасних цифрових технологій з метою забезпечення кримінологічної безпеки суспільства та для запобігання злочинності у сфері цифрових технологій, а саме: системи блокування запалювання з пристроями датчика алкоголю для запобігання запуску автомобіля особою в нетверезому стані; системи відеоспостереження для допомоги запобігання кримінальним правопорушенням, контролю підозрілої діяльності, ідентифікації номерних знаків автомобіля та збору доказів, тощо; прийомопередавачі бездротового зв'язку малого радіусу дії, такі як Bluetooth і WI-FI, можливості яких можна використовувати для запобігання або розслідування викрадення дітей; комплексного програмного забезпечення DEI PRO для дослідження цифрових доказів, сортування та використання електронних і цифрових носіїв, що створене для швидкості, масштабованості та простоти у використанні для слідчих в процесі їх діяльності.

11. Проаналізовано та обґрунтовано перспективність впровадження можливостей цифрових та інших комп'ютерних технологій при виявленні та запобіганні кримінальним правопорушенням у цифровій, комп'ютерній, інформаційній сфері зокрема та й інших правопорушень загалом та при

запобіганні злочинності. Відмічено необхідність врахування доказів із платформ соціальних мереж, зокрема вивчення і дослідження таких даних, як: дописи користувачів, повідомлення, коментарі, лайки та поширення, які можуть свідчити про встановлення певних зв'язків особи з іншими користувачами, ідентифікації підозрюваних, встановлення часових меж певних подій; знімки екрану мобільних чи комп'ютерних пристроїв, журналів чатів та їх мультимедійного змісту, що в майбутньому зможуть слугувати вагомими підтверджуючими доказами винуватості чи невинуватості особи.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Авдєєва Т. Чи легально встановлювати на міських вулицях камери із системою розпізнавання обличчя? Офіційний сайт Центру демократії та верховенства права. URL: <https://cedem.org.ua/analytics/kamery-rozpiznavannya-oblych/> (дата звернення: 10.07.2023)
2. Бандурка О.М., Литвинов О.М. Стратегія і тактика протидії злочинності. Монографія. Харків. Видавництво «Золота миля». 2012. 287 с.
3. Бенескул А.В. Використання цифрових технологій при запобіганні злочинності та впровадження цифрової кримінології. *Актуальні проблеми імплементації наукових досягнень у практичну діяльність*: матеріали міжнародної науково-практичної конференції, м. Київ, 19–20 січня 2022 р. – Київ: Науково-дослідний інститут публічного права, 2022. С. 22–24.
4. Бенескул А.В. Досвід США щодо використання цифрових технологій та штучного інтелекту при запобіганні злочинності. *Науково-практичні засади розвитку наукової думки на сучасному етапі державотворення*: матеріали міжнародної науково-практичної конференції, м. Київ, 22–23 вересня 2021 р. – Київ: Науково-дослідний інститут публічного права, 2021. С. 132–135.
5. Бенескул А.В. Забезпечення кримінологічної безпеки у сфері використання цифрових технологій: міжнародно-правовий аспект. *Держава та регіони. Серія: Право*. 2022. № 3 (77). С. 132-137. URL: http://law.stateandregions.zp.ua/archive/3_2022/17.pdf
6. Бенескул А.В. Кримінологічна безпека в умовах цифрової трансформації: поняття, сутність і значення. *Ірпінський юридичний часопис: науковий журнал*. 2023. Вип. 3 (12). С. 309-317. URL: <https://drive.google.com/file/d/1wJrT-86XsnozaO4W8ST8kYM8JOZFWMqK/view>
7. Бенескул А.В. Новітні напрями вдосконалення запобігання злочинності при використанні цифрових технологій. *Взаємодія публічного та приватного права: сучасні проблеми та виклики*: матеріали міжнародної

науково-практичної конференції, м. Київ, 21–22 лютого 2022 р. – Київ: Науково-дослідний інститут публічного права, 2022. С. 39–41.

8. Бенескул А.В. Нормативно-правове закріплення застосування цифрових технологій для забезпечення кримінологічної безпеки суспільства. *Науковий вісник Ужгородського національного Університету*, 2023. Серія Право. Випуск 78: частина 2. С. 145-151. URL: <http://visnyk-pravo.uzhnu.edu.ua/article/view/285996/280061>

9. Бенескул А.В. Характеристика кримінальних правопорушень у сфері використання цифрових технологій. *Юридичний науковий електронний журнал*. 2021. № 12. С. 511-514. URL: http://www.lsej.org.ua/12_2021/132.pdf

10. Берназюк О.О. Цифрові технології у праві: тенденції та перспективи розвитку: автореф. дис. ... д-ра юрид. наук : 12.00.07 Ужгород, 2021. 35 с.

11. Біляєв В. О., Ключ В. В. Перспективи використання Internet-технологій під час протидії екстремістським організаціям. *Використання інноваційних технологій у попередженні злочинів: матеріали наук.-практ. семінару* (м. Харків, 06 груд. 2012 р.) / МВС України, Харківський нац. ун-т внутрішніх справ. Харків: ХНУВС, 2012. С. 17–20

12. Бодунова О.М. Кримінологічні засади запобігання злочинності у сфері інформаційних технологій: : дис... д-ра. юрид. наук : 12.00.08, Ірпінь, 2023. 433с.

13. Бодунова О.М. Запобігання злочинності у сфері інформаційних технологій: міжнародно-правовий аспект. *Юридичний науковий електронний журнал*. № 4/2020. С. 246-248. URL: http://www.lsej.org.ua/4_2020/61.pdf (дата звернення: 10.11.2023)

14. Бугера О. Цифровізація кримінологічних досліджень: стан та перспективи. *Юридичний вісник*. 2022/2. С. 46-52. URL: http://yurvisnyk.in.ua/v2_2022/6.pdf (дата звернення: 01.07.2023)

15. Бугера О.І. Кримінологічні засади використання мережі інтернет для запобігання злочинності: дис... д-ра. юрид. наук : 12.00.08 / Інститут

держави і права імені В.М. Корецького. Національна академія наук України. Київ, 2020. 492 с.

16. Бугера О.І. Правова освіта в мережі Інтернет як захід запобігання злочинності на загальносоціальному рівні. *Науковий вісник Херсонського державного університету. Серія Юридичні науки*. Випуск 1. Том 2. 2018. С. 57-59. URL: <https://journals.indexcopernicus.com/api/file/viewByFileId/733798.pdf> (дата звернення: 10.11.2023)

17. Бугера О.І. Сучасний стан та проблеми використання новітніх інтернет-технологій для запобігання злочинності. *Вчені записки ТНУ імені В.І. Вернадського. Серія: юридичні науки*. Том 33 (72) № 1 2022. С. 65-69. URL: https://www.juris.vernadskeyjournals.in.ua/journals/2022/1_2022/12.pdf (дата звернення: 10.11.2023)

18. Буяджи С.А. Правове регулювання боротьби з кіберзлочинністю: теоретико-правовий аспект: : дис. ... канд. юрид.наук : 12.00.01. Київ, 2018. 203 с.

19. Валуйська М. Ю. Криміналізація особистості: сучасний стан вивчення та перспективи застосування цифрових технологій. *Журнал східноєвропейського права*. 2018. № 57. С. 34–39. URL: http://easternlaw.com.ua/wp-content/uploads/2018/11/valuiska_57.pdf (дата звернення: 04.07.2023)

20. Вернигора О. Як розвиватиметься цифрова економіка у найближчі роки. Чому цифровій економіці прогнозують стрімкий розвиток та як українським компаніям диджиталізувати свій бізнес зараз. *Українська правда*. URL: <https://www.epravda.com.ua/columns/2022/01/13/681412/> (дата звернення: 17.07.2023)

21. Гавловський В. Д., Бутузов В. М. Протидія організованим злочинності у сфері інформаційних технологій як окремий аспект кримінологічної безпеки. *Боротьба з організованою злочинністю і корупцією (теорія і практика)*. 2010. Вип. 22. С. 236–246.

22. Гребенюк М., Черняк А. Проблеми протидії організованих злочинності у сфері цифрової економіки. *Підприємництво, господарство і право*. №3, 2019. С. 297-303

23. Державний центр кіберзахисту збільшує технічні спроможності ключових систем забезпечення кіберзахисту. Офіційний сайт Державного центру кіберзахисту. URL: <https://scpc.gov.ua/ua/articles/324> (дата звернення: 23.07.2023)

24. Загрійчук М.Ю. Адміністративно-правові засади цифрової трансформації регіону: автореф. дис. ... юрид. політ. наук : 12.00.07 Харків, 2021. 23 с.

25. Захист дітей у цифровому середовищі: рекомендації для індустрій. Міжнародний союз електрозв'язку 2020. URL: https://thedigital.gov.ua/storage/uploads/files/news_post/2021/1/za-initsiatiivi-mintsifri-pidgotuvali-rekomendatsii-shchodo-zakhistu-ditey-u-tsifrovomu-seredovishchi/COP_Guidelines_Industry_UA_fin66.pdf (дата звернення: 11.08.2023)

26. Звіт Об'єднаного дослідницького центру (JRC), «Кібербезпека, наш цифровий якір». URL: <https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/cybersecurity-our-digital-anchor> (дата звернення: 10.11.2023)

27. Звіт про роботу системи виявлення вразливостей і реагування на кіберінциденти та кібератаки. Оперативний центр реагування на кіберінциденти державного центру кіберзахисту державної служби спеціального зв'язку та захисту інформації України. Перший квартал 2023. URL: file:///C:/Users/%D0%9B%D1%8E%D0%B4%D0%BC%D0%B8%D0%BB%D0%B0/Downloads/2023Q1_ukr.pdf (дата звернення: 23.07.2023)

28. Звіт про роботу системи виявлення вразливостей і реагування на кіберінциденти та кібератаки. Оперативний центр реагування на кіберінциденти державного центру кіберзахисту державної служби

спеціального зв'язку та захисту інформації України. Другий квартал 2023. URL: <https://scpc.gov.ua/api/files/e4eaafb7-99de-4a60-89f2-f0c05b777b69> (дата звернення: 23.07.2023)

29. Інтерпол посилює боротьбу з криптовалютними злочинами. Financial club. URL: <https://www.finclub.net/ua/news/interpol-posyliuie-borotbu-z-kryptovaliutnymy-zlochynamy.html> (дата звернення: 15.11.2023)

30. Калайда Ю.П. Можливості блокчейн-технологій у розслідуванні кримінальних правопорушень, вчинених в кіберпросторі. *Інформація і право*. № 4(39)/2021. С. 170-178. URL: <http://il.ippi.org.ua/article/view/249299> (дата звернення: 15.11.2023)

31. Категорія: Цифрові технології. Вільна енциклопедія. Вікіпедія. URL: https://uk.wikipedia.org/wiki/%D0%9A%D0%B0%D1%82%D0%B5%D0%B3%D0%BE%D1%80%D1%96%D1%8F:%D0%A6%D0%B8%D1%84%D1%80%D0%BE%D0%B2%D1%96_%D1%82%D0%B5%D1%85%D0%BD%D0%BE%D0%BB%D0%BE%D0%B3%D1%96%D1%97 (Дата звернення: 19.06.2023р.)

32. Коваленко Ю. Геномна інформація людини (ДНК): облік в умовах воєнного стану та ризики під час обробки. Офіційний сайт Української Гельсінської Спілки з прав людини. URL: <https://www.helsinki.org.ua/articles/henomna-informatsiia-liudyny-dnk-oblik-v-umovakh-voiennoho-stanu-ta-ryzyky-pid-chas-obrobky/> (дата звернення: 10.07.2023)

33. Ковальова О.В. Теоретико-правові засади інформаційного забезпечення досудового розслідування кримінальних правопорушень. дис. ... д-ра юрид. наук : 12.00.09 Кропивницький. 2023. 475 с.

34. Колодязний М.Г. Застосування сучасних технологій у сфері запобігання злочинності. *Вісник Асоціації кримінального права України*, 2020, № 1(13). С. 178-195

35. Конституція України: прийнята на п'ятій сесії Верховної Ради України 28 червня 1996 року. Відомості Верховної Ради України (ВВР), 1996,

№ 30, ст. 141. URL: <https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text> (дата звернення: 10.11.2023)

36. Концепція розвитку електронного урядування в Україні. Розпорядження Кабінету Міністрів України від 20 вересня 2017 р. № 649-р. URL: <https://zakon.rada.gov.ua/laws/show/649-2017-%D1%80#Text> (Дата звернення: 13.06.2023 р.)

37. Концепція розвитку цифрових компетентностей: схвалено розпорядженням Кабінету Міністрів України від 3 березня 2021 р. № 167-р. URL: <https://zakon.rada.gov.ua/laws/show/167-2021-%D1%80#Text> (дата звернення: 01.07.2023)

38. Концепція розвитку штучного інтелекту в Україні: Схвалено розпорядженням Кабінету Міністрів України від 2 грудня 2020 р. № 1556-р. URL: <https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text> (дата звернення: 10.07.2023)

39. Кримінальний кодекс України. Закон України від 5 квітня 2001 року. № 2341-III (Відомості Верховної Ради України (ВВР), 2001, № 25-26, ст.131). URL: <https://zakon.rada.gov.ua/laws/show/2341-14#Text> (Дата звернення: 13.06.2023 р.)

40. Литвинов, О. М. Кримінологічна стратегія як компонент стратегії національної безпеки України. *Право і безпека : Науковий журнал*. 2010. № 3. С. 137–141.

41. Маланчук П. М., Невмержицька Ю. А. Інформаційні технології в криміналістиці: крок в майбутнє. *Young Scientist*. 2017. № 11 (51). С. 918–921. URL: <https://molodyvcheny.in.ua/files/journal/2017/11/222.pdf> (дата звернення: 27.06.2023).

42. Мельничук Т.В. Кримінологічна безпека економічної діяльності : навч.-метод. посібник. Т. В. Мельничук; рец.: Є. Л. Стрельцов, Л. І. Аркуша; НУ «ОЮА». Одеса. Гельветика. 2018. 96 с.

43. Методичні рекомендації щодо реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі: Затверджено Наказом

Адміністрації Державної служби спеціального зв'язку та захисту інформації України 03 липня 2023 року № 570. URL: <https://cip.gov.ua/ua/news/nakaz-administraciyi-derzhspeczv-yazku-vid-03-07-2023-570-pro-zatverdzhennya-metodichnikh-rekomendacii-shodo-reaguvannya-sub-yektami-zabezpechennya-kiberbezpeki-na-rizni-vidi-podii-u-kiberprostorі> (дата звернення: 23.07.2023)

44. Микитчик А.В. Заходи запобігання кіберзлочинності в Україні. Кримінально-правові та кримінологічні засоби протидії злочинам проти громадської безпеки та публічного порядку. Харків, 2019. С. 137-139

45. Для безпеки киян на столичних вулицях торік облаштовано 1478 камер відеоспостереження URL: https://kyivcity.gov.ua/news/dlya_bezpeki_kiyan_na_stolichnikh_vulitsyakh_torik_o_blashtovano_1478_kamer_videosposterezhennya/ (дата звернення: 10.07.2023)

46. Мозоль С. А. Кримінологічна безпека в Україні: монографія. Харків: Константа, 2018. 482 с.

47. Мозоль С. А. Кримінологічна безпека в Україні: феномен та наукові засади забезпечення : автореф. дис. д-ра юрид. наук (д-ра наук) : 12.00.08. МВС України, Харк. нац. ун-т внутр. справ. Харків, 2018. 37с.

48. Національна стратегія сприяння розвитку громадянського суспільства в Україні на 2021-2026 роки. Указ Президента України від 27 вересня 2021 року № 487/2021. URL: <https://zakon.rada.gov.ua/laws/show/487/2021#Text> (Дата звернення: 13.06.2023 р.)

49. Пеньков С. В., Шендрік В. В. Впровадження інтернет-технологій у діяльність Національної поліції України для отримання оперативно-розшукової інформації. *Право і безпека*. 2017. № 2 (65). С. 80–85. URL: http://pb.univd.edu.ua/?action=publications&pub_id=411139&mid=8&year=2017 (дата звернення: 27.06.2023).

50. План заходів з реалізації Концепції розвитку цифрових компетентностей: затверджено розпорядженням Кабінету Міністрів України від

3 березня 2021 р. № 167-р. URL: <https://zakon.rada.gov.ua/laws/show/167-2021-%D1%80#Text> (дата звернення: 01.07.2023)

51. План заходів з реалізації Стратегії інформаційної безпеки на період до 2025 року. Розпорядження Кабінету Міністрів України від 30 березня 2023 р. № 272-р. URL: <https://zakon.rada.gov.ua/laws/show/272-2023-%D1%80#Text> (Дата звернення: 13.06.2023 р.)

52. Подзігун Г.В. Публічне адміністрування у сфері цифрової трансформації: автореф. дис. ... канд. юрид. наук : 12.00.07. Запоріжжя, 2021. 24 с.

53. Положення про організаційно-технічну модель кіберзахисту: Затверджено постановою Кабінету Міністрів України від 29 грудня 2021 р. № 1426. URL: <https://zakon.rada.gov.ua/laws/show/1426-2021-%D0%BF#Text> (дата звернення: 23.07.2023)

54. Порядок реагування суб'єктами забезпечення кібербезпеки на різні види подій у кіберпросторі: Затверджено постановою Кабінету Міністрів України від 4 квітня 2023 р. № 299. URL: <https://zakon.rada.gov.ua/laws/show/299-2023-%D0%BF#Text> (дата звернення: 23.07.2023)

55. Презентація нової електронної інтелектуальної системи аналізу «RICAS». URL: <https://univd.edu.ua/uk/news/1057> (дата звернення: 04.07.2023)

56. Прес-реліз Євростату «Заходи безпеки ІКТ, вжиті переважною більшістю підприємств у ЄС», 6/2020 – 13 січня 2020 р. «Кібератаки на критичну інфраструктуру стали новою нормою в таких секторах, як енергетика, охорона здоров'я та транспорт»; WEF, Звіт про глобальні ризики 2020.

57. Про авторське право і суміжні права. Закон України від 1 грудня 2022 року № 2811-IX. URL: <https://zakon.rada.gov.ua/laws/show/2811-20#Text> (Дата звернення: 13.06.2023 р.)

58. Про віртуальні активи: Закон України від 17 лютого 2022 року № 2074-IX. URL: <https://zakon.rada.gov.ua/laws/show/2074-20#Text> (дата звернення: 20.07.2023)

59. Про державну реєстрацію геномної інформації людини: Закон України від 9 липня 2022 року № 2391-IX. URL: <https://zakon.rada.gov.ua/laws/show/2391-20#Text> (дата звернення: 10.07.2023)

60. Про затвердження Методичних рекомендацій щодо забезпечення кіберзахисту автоматизованих систем управління технологічними процесами: Затверджено Наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України 29 травня 2023 року № 463. URL: <https://cip.gov.ua/ua/news/nakaz-administraciyi-derzhspeczv-yazku-vid-29-05-2023-463-pro-zatverdzhennya-metodichnikh-rekomendacii-shodo-zabezpechennya-kiberzakhistu-avtomatizovanikh-sistem-upravlinnya-tekhnologichnimi-procesami> (дата звернення: 23.07.2023)

61. Про Національну програму інформатизації. Закон України від 1 грудня 2022 року. № 2807-IX. URL: <https://zakon.rada.gov.ua/laws/show/2807-20#Text> (Дата звернення: 13.06.2023 р.)

62. Про основні засади забезпечення кібербезпеки України. Закон України від 5 жовтня 2017 року. № 2163-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2163-19#Text> (Дата звернення: 13.06.2023 р.)

63. Про платіжні послуги: Закон України від 30 червня 2021 року № 1591-IX. URL: <https://zakon.rada.gov.ua/laws/show/1591-20#Text> (дата звернення: 20.07.2023)

64. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року «Про Стратегію кібербезпеки України». Указ Президента України від 26 серпня 2021 року № 447/2021. URL: <https://www.president.gov.ua/documents/4472021-40013> (Дата звернення: 26.06.2023 р.)

65. Про стимулювання розвитку цифрової економіки в Україні: Закон України від 15 липня 2021 року. № 1667-IX. URL: <https://zakon.rada.gov.ua/laws/show/1667-20#Text> (дата звернення: 17.07.2023)

66. Систематичність та інтенсивність російських кібератак лишається високою – звіт. Офіційний сайт Державної служби спеціального зв'язку та

захисту інформації України. URL: <https://cip.gov.ua/ua/news/systematicity-and-intensity-of-russia-s-cyberattacks-remain-high-report> (дата звернення: 23.07.2023)

67. Стратегія забезпечення державної безпеки. Указ Президента України від 16 лютого 2022 року № 56/2022. URL: <https://www.president.gov.ua/documents/562022-41377> (дата звернення: 03.05.2023)

68. Стратегія інформаційної безпеки. Указом Президента України від 28 грудня 2021 року № 685/2021. URL: <https://zakon.rada.gov.ua/laws/show/685/2021#n14> (Дата звернення: 13.06.2023 р.)

69. Стратегія розвитку інформаційного суспільства в Україні. Розпорядження Кабінету Міністрів України від 15 травня 2013 р. № 386-р. URL: <https://zakon.rada.gov.ua/laws/show/386-2013-%D1%80#Text> (Дата звернення: 13.06.2023 р.)

70. Теплицький Б.Б. Техніко-криміналістичне забезпечення розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. автореф. дис. ... канд. юрид. наук : 12.00.09. Київ, 2021. 21 с.

71. Топчій В.В., Маркушин О.Г. Зарубіжний досвід запобігання злочинності у сфері цифрової економіки. *Юридична наука*. № 10(112)/2020. С. 201-208. URL: <https://journal-nam.com.ua/index.php/journal/article/view/589/546> (дата звернення: 10.11.2023)

72. Україна 2030Е – країна з розвинутою цифровою економікою. URL: <https://strategy.uifuture.org/kraina-z-rozvinutoyu-cifrovoyu-ekonomikoyu.html> (дата звернення: 01.07.2023)

73. Цивільний кодекс України: Закон України від 16 січня 2003 року. № 435-IV. Відомості Верховної Ради України (ВВР), 2003, №№ 40-44, ст.356. URL: <https://zakon.rada.gov.ua/laws/show/435-15#Text> (Дата звернення: 13.06.2023 р.)

74. Шеломенцев В. П. Безпека людини, суспільства і держави в Україні: кримінологічний аспект. *Боротьба з організованою злочинністю і корупцією (теорія і практика)*. 2009. № 22. С. 215–222.

75. Шеломенцев В. П. Кримінологічна безпека у кіберпросторі: система понять. *Боротьба з організованою злочинністю і корупцією (теорія і практика)*. 2010. № 23. С. 342–348.

76. Шемшученко В. Штучний інтелект у правосудді. Офіційний сайт Центру демократії та верховенства права. URL: <https://cedem.org.ua/analytics/shtuchnyj-intelekt-pravosuddia/> (дата звернення: 10.07.2023)

77. Юзікова Н.С. Інформаційна безпека у системі заходів запобігання кримінальним правопорушенням у сфері інформаційних технологій: досвід країн ЄС та США. *Електронне наукове видання «Аналітично-порівняльне правознавство»* № 5. 2023. С. 506-511. URL: <http://journal-app.uzhnu.edu.ua/article/view/290771/284400> (дата звернення: 10.11.2023)

78. Юрій І. А., Кузнєцов О. І. Перспективи та деякі особливості використання кримінальної розвідки у сфері високих технологій. *Кримінальна розвідка: методологія, законодавство, зарубіжний досвід: матеріали міжнар. наук.-практ. конф. (м. Одеса, 29 квіт. 2016 р.)*. Одеса: ОДУВС, 2016. С. 73–75.

79. Юртаєва К. В. Використання технологій штучного інтелекту в реалізації стратегій «predictive policing»: можливості, проблеми та перспективи для України. *Використання технологій штучного інтелекту у протидії злочинності* : матеріали наук.-практ. онлайн-семінару (м. Харків, 5 листоп. 2020 р.). Харків : Право, 2020. С. 99–104.

80. 14th UN Crime Congress – Kyoto, Japan (hybrid format) – 7-12 March 2021. International cooperation vital to address all forms of crime, terrorism & new & emerging forms of crime. URL: https://unis.unvienna.org/pdf/2021/Crime_Congress/06_international_cooperation_terrorism_FINAL.pdf (дата звернення: 25.09.2023)

81. Anti-Money Laundering. Palantir. URL: <https://www.palantir.com/offerings/anti-money-laundering/> (дата звернення: 01.07.2023)

82. Aptauija "Mobilo telefonu un interneta izmantošanas paradumi bernu un jauniešu vidū" (2012). Available on: (In Latvian). URL: http://www.drossinternets.lv/upload/materiali/petijumi/mob-tel_interneta_izmantosana_2012.pdf (дата звернення: 07.07.2023)

83. B. Snook, J. Eastwodd, P. Gebdreau, C. Coggin, R.M. Cullen (2007) Taking stock of criminal profiling: A narrative review and meta-analysis. *Criminal Justice and Behavior* 34, pp. 437–453

84. Batra, S., Gupta, M., Singh, J., Srivastava, D., & Aggarwal, I. (2020, November). An Empirical Study of Cybercrime and Its Preventions. In 2020 Sixth International Conference on Parallel, Distributed and Grid Computing (PDGC) (pp. 42–46).

85. Bright Sky PT. Fundação Vodafone Portugal <https://play.google.com/store/apps/details?id=pt.vodafone.BrightSky&hl=uk&gl=US&pli=1> (дата звернення: 20.07.2023)

86. CEPEJ European Ethical Charter on the use of artificial intelligence (AI) in judicial systems and their environment. Council of Europe. URL: <https://www.coe.int/en/web/cepej/cepej-european-ethical-charter-on-the-use-of-artificial-intelligence-ai-in-judicial-systems-and-their-environment> (дата звернення: 07.07.2023)

87. CERT-UA від початку року опрацювала більше двох тисяч кібератак на Україну. Офіційний сайт Державної служби спеціального зв'язку та захисту інформації України. URL: <https://cip.gov.ua/ua/news/cert-ua-vid-pochatku-roku-opracyuvala-bilshe-dvokh-tisyach-kiberatak-na-ukrayinu> (дата звернення: 23.07.2023)

88. Chris Baraniuk Exclusive: UK police wants AI to stop violent crime before it happens. *New Scientist*. <https://www.newscientist.com/article/2186512->

exclusive-uk-police-wants-ai-to-stop-violent-crime-before-it-happens/ (дата звернення: 10.07.2023)

89. Circle of 6. DevPost. URL: <https://appsagainstabuse.devpost.com/submissions/4900-circle-of-6> (дата звернення: 20.07.2023)

90. Clearview AI used nearly 1m times by US police, it tells the BBC. British Broadcasting Corporation (BBC). URL: <https://www.bbc.com/news/technology-65057011> (дата звернення: 01.12.2023)

91. Communication from the commission to the European parliament, the Council, the European economic and social committee and the committee of the regions 2030 Digital Compass: the European way for the Digital Decade. Brussels, 9.3.2021 COM(2021) 118 final. URL: <https://eufordigital.eu/wp-content/uploads/2021/03/2030-Digital-Compass-the-European-way-for-the-Digital-Decade.pdf> (дата звернення: 20.09.2023)

92. Convention on Cybercrime Budapest, 23.XI.2001. European Treaty Series - No. 185. URL: <https://rm.coe.int/1680081561> (дата звернення: 15.11.2023)

93. Cyber Security Breaches Survey 2020. Department for Digital, Culture, Media and Sport Cyber Security Breaches Survey 2020: Statistical Release URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/893399/Cyber_Security_Breaches_Survey_2020_Statistical_Release_180620.pdf (дата звернення: 03.05.2023)

94. Cybercrime. Official website of Europol. URL: <https://www.europol.europa.eu/crime-areas-and-statistics/crime-areas/cybercrime> (дата звернення: 13.07.2023)

95. D. Canter, D. Youngs (2008) Principles of Geographical Offender Profiling (New York: Toylor & Francis Group)

96. D. Shinder (2010) Profiling and categorizing cybercriminals. Available on: URL: <http://www.techrepublic.com/blog/it-security/profiling-and-categorizingcybercriminals/> (дата звернення: 07.07.2023)

97. Declaration of Principles Building the Information Society: a global challenge in the new Millennium. Document WSIS-03/GENEVA/DOC/4-E. 12 December 2003. Original: English. URL: <https://www.itu.int/net/wsis/docs/geneva/official/dop.html> (дата звернення: 15.11.2023)

98. Digital Agenda for Europe. Fact Sheets on the European Union. European Parliament. URL: <https://www.europarl.europa.eu/factsheets/en/sheet/64/digital-agenda-for-europe> (Дата звернення: 13.06.2023 р.)

99. Digital Economy and Society Index (DESI) 2020. An official website of the European Union. URL: <https://digital-strategy.ec.europa.eu/en/library/digital-economy-and-society-index-desi-2020> (дата звернення: 10.11.2023)

100. Digital Evidence Investigator PRO. The all-in-one tool to investigate mobile and computer devices. URL: <https://www.adfsolutions.com/digital-evidence-investigator-pro?hsCtaTracking=f59073e1-3bf3-4342-bb89-8e81ca0706ed%7Caba4bc59-7fd4-4dbd-98fd-0cf53607da58> (дата звернення: 01.12.2023)

101. Digital Security Risk Management for Economic and Social Prosperity OECD Recommendation and Companion Document. OECD (2015). URL: <https://www.oecd.org/digital/ieconomy/digital-security-risk-management.pdf> (дата звернення: 20.09.2023)

102. Early Pursuit against Organized crime using envier Omental scanning, the Law and Intelligent CE systems. European Commission. URL: <https://cordis.europa.eu/project/id/312651> (дата звернення: 01.07.2023)

103. Eleventh United Nations Congress on Crime Prevention and Criminal Justice. Report of the Eleventh United Nations Congress on Crime Prevention and Criminal Justice. Bangkok, 18-25 April 2005. URL: https://www.unodc.org/documents/congress/Documentation/11Congress/ACONF203_18_e_V0584409.pdf (дата звернення: 25.09.2023)

104. Enhanced EU-Ukraine cooperation in Cybersecurity. An official website of the European Union. URL: <https://www.enisa.europa.eu/news/enhanced-eu-ukraine-cooperation-in-cybersecurity> (дата звернення: 15.11.2023)

105. Eric L Piza, Brandon C Welsh, David P Farrington, and Amanda L Thomas. CCTV surveillance for crime prevention: A 40-year systematic review with meta-analysis. *Criminology & Public Policy*, 18(1):135–159, 2019.

106. Estimated by telecommunications trade association GSMA. THE Internet of things BY 2025 URL: <https://www.gsma.com/iot/wp-content/uploads/2018/08/GSMA-IoT-Infographic-2019.pdf>). (дата звернення: 10.11.2023)

107. European Cybercrime Centre. The Geneva Internet Platform's Digital Watch. URL: <https://dig.watch/actor/european-cybercrime-centre> (дата звернення: 13.07.2023)

108. European ethical Charter on the use of Artificial Intelligence in judicial systems and their environment. Adopted at the 31st plenary meeting of the CEPEJ (Strasbourg, 3-4 December 2018). European Commission for the Efficiency of Justice (CEPEJ) URL: <https://rm.coe.int/ethical-charter-en-for-publication-4-december-2018/16808f699c> (дата звернення: 07.07.2023)

109. F.T. Ngo, R. Paternoster (2011) Cybercrime Victimization: An examination of Individual and Situational level factors. *International Journal of Cyber Criminology* 5(1) (January – July), 773

110. From Likes to Convictions: Solving Social Media Crimes with Forensics. Posted by Nuris Rodriguez on December 20, 2023. Digital Forensic News & Events. URL: <https://www.adfsolutions.com/news/from-likes-to-convictions-unveiling-the-power-of-digital-forensics-in-solving-social-media-crimes> (дата звернення: 10.01.2024)

111. Global Cyber Risk Perception Survey 2018. By the Numbers: Global Cyber Risk Perception Survey. Available on. URL: <https://www.guycarp.com/insights/2018/02/by-the-numbers-global-cyber-risk-perception-survey.html> (дата звернення: 01.07.2023)

112. Global industry sectors most targeted by basic web application attacks from November 2021 to October 2022. Statista.com. Basic web application attacks: global most-targeted industries 2021-2022. Published by Ani Petrosyan, Nov 2, 2023. URL: <https://www.statista.com/statistics/221293/cyber-crime-target-industries/> (дата звернення: 04.01.2024)

113. Global number of cybercrime incidents from November 2021 to October 2022, by industry and organization size. Statista.com. Cybercrime incidents worldwide 2021-2022, by industry and organization size. Published by Ani Petrosyan, Oct 13, 2023. URL: <https://www.statista.com/statistics/194246/cybercrime-incidents-victim-industry-size/#statisticContainer> (дата звернення: 04.01.2024)

114. Global Threats Report. URL: <https://jp.security.ntt/> (дата звернення: 03.05.2023)

115. Guy Warren. URL: <https://uk.linkedin.com/in/guy-warren-itr> (дата звернення: 03.05.2023)

116. Harris, C. (2007) "Police and Soft Technology: How Information Technology Contributes to Police Decision Making" In: BYRNE, J. and REBOVICH, D.(2007). The New technology of Crime, Law and Social Control, Monsey, NY: Criminal Justice Press, p. 153-183.

117. How Can AI CCTV Cameras Prevent Crime Before It Happens? URL: <https://corefacilities.com/blog/ai-cctv-cameras-prevent-crime-before-it-happens/> (дата звернення: 20.07.2023)

118. IMPACT - International Multilateral Partnership Against Cyber Threats. URL: <https://gssd.mit.edu/search-gssd/site/impact-international-multilateral-53727-mon-07-23-2012-0910> (дата звернення: 12.08.2023)

119. International Cyber Security Protection Alliance (ICSPA). Cybil. URL: <https://cybilportal.org/actors/international-cyber-security-protection-alliance-icspa/> (дата звернення: 12.08.2023)

120. Introducing the Silent Beacon™ Panic Button. URL: <https://silentbeacon.com/> (дата звернення: 20.07.2023)

121. Jaishankar K. Establishing a Theory of Cyber Crimes. International Journal of Cyber Criminology Vol 1 Issue 2 July 2007. URL: <https://www.cybercrimejournal.com/pdf/Editoriaijccjuly.pdf> (дата звернення: 03.05.2023)

122. James Byrne, Gary Marx Technological Innovations in Crime Prevention and Policing. A Review of the Research on Implementation and Impact. *Journal of Police Studies* Volume: 3 Issue: 20 Dated: 2011 Pages: 17-40

123. John Fuller, Chris Pollette How Bluetooth Surveillance Works. URL: <https://electronics.howstuffworks.com/bluetooth-surveillance.htm> (дата звернення: 20.07.2023)

124. Joint communication to the European Parliament and the Council The EU's Cybersecurity Strategy for the Digital Decade. Brussels, 16.12.2020 JOIN(2020) 18 final. An official website of the European Union. URL: <https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0> (дата звернення: 10.11.2023)

125. K. Jaishankar (2011) *Cyber Criminology: Exploring Internet Crimes and Criminal Behavior* (Boca Raton, FL, USA: CRC Press, Taylor and Francis Group, 2011)

126. K. Rossmo (2000) *Geographic profiling* (CRS Press LLC)

127. Kethineni, S, CAO, Y, & Dodge, C (2018). «Use of bitcoin in darknet markets: Examining facilitative factors on bitcoin-related crimes». *American Journal of Criminal Justice*, 43(2), pp. 141-157.

128. McGuire, M. (2019). It ain't what it is, it's the way that they do it? Why we still don't understand cybercrime. In *The human factor of cybercrime* (pp. 3–28).

129. Most significant cases of data breach worldwide as of August 2023 (in millions), by number of compromised data records and individuals impacted. Statista.com. All-time biggest online data breaches 2023. Published by Ani Petrosyan, Jan 15, 2024. URL: <https://www.statista.com/statistics/290525/cyber-crime-biggest-online-data-breaches-worldwide/> (дата звернення: 16.01.2024)

130. Nicol Turner Lee, Caitlin Chin Police surveillance and facial recognition: Why data privacy is imperative for communities of color. URL: <https://www.brookings.edu/articles/police-surveillance-and-facial-recognition-why-data-privacy-is-an-imperative-for-communities-of-color/> (дата звернення: 01.07.2023)

131. Number of user data requests issued to Facebook by federal agencies and governments worldwide as of 2nd half 2022. Statista.com. URL: <https://www.statista.com/statistics/277230/facebooks-global-user-data-requests/#:~:text=Global%20Facebook%20user%20data%20requests%20from%20federal%20agencies%20%26%20governments%202013-2022&text=Between%20July%20and%20December%202022,over%2076%20percent%20of%20requests.> (дата звернення: 01.12.2023)

132. OECD Guidelines for the Security of Information Systems and Networks Towards a culture of security. OECD publications, 2, rue André-Pascal, 75775 PARIS CEDEX 16 PRINTED IN FRANCE. URL: <https://www.oecd.org/sti/ieconomy/15582260.pdf> (дата звернення: 20.09.2023)

133. OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security. OECD.ORG. URL: <https://www.oecd.org/sti/ieconomy/oecdguidelinesforthesecurityofinformationsystemsandnetworkstowardsacultureofsecurity.htm> (дата звернення: 20.09.2023)

134. Official site International Telecommunication Union (ITU). URL: <https://www.itu.int/en/about/Pages/default.aspx> (дата звернення: 20.09.2023)

135. Operational Technology Cybersecurity is a Global Imperative. Global Cybersecurity Alliance (ISAGCA). URL: <https://isagca.org/> (дата звернення: 12.08.2023)

136. Paul Roberts Cyberattacks on Industrial Control Systems Jumped in 2022. *The Security Ledger*. URL: <https://securityledger.com/2023/02/cyberattacks-on-industrial-control-systems-jumped-in-2022/> (дата звернення: 01.07.2023)

137. Phillips, K., Davidson, J. C., Farr, R. R., Burkhardt, C., Caneppele, S., & Aiken, M. P. (2022). Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies. *Forensic Science*, 2(2), p. 379–398.

138. Predictive policing systems widely used in US and UK, despite concerns about privacy, and flaws in the approach. URL: <https://www.privateinternetaccess.com/blog/predictive-policing-algorithms-widely-used-in-us-and-uk-despite-deep-flaws-in-the-approach/> (дата звернення: 01.07.2023)

139. Published by Stacy Jo Dixon , Sep 6, 2023. URL: <https://www.statista.com/aboutus/our-research-commitment/3088/stacy-jo-dixon> (дата звернення: 01.12.2023)

140. R. Bull, C. Cooke, R. Hatcher, J. Woodhams, C. Bilby, T. Grant (2006) *Criminal psychology: A Beginner's Guide* (Oneworld Publications, Oxford, England)

141. Recommendation of the Council on Digital Security of Critical Activities. OECD/LEGAL/0456. Adopted on: 11/12/2019. URL: <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0456> (дата звернення: 20.09.2023)

142. Resolution adopted by the General Assembly [on the report of the Second Committee (A/57/529/Add.3)] 57/239. Creation of a global culture of cybersecurity. General 31 January 2003. URL: file:///C:/Users/%D0%9B%D1%8E%D0%B4%D0%BC%D0%B8%D0%BB%D0%B0/Downloads/A_RES_57_239-EN.pdf (дата звернення: 18.07.2023)

143. Resolution adopted by the General Assembly. A/RES/54/125 26 January 2000. Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders. URL: <https://digitallibrary.un.org/record/404748#record-files-collapse-header> (дата звернення: 23.09.2023)

144. RICAS - Realtime intelligence crime analytics system. URL: <https://ricas.org/uk/> (дата звернення: 04.07.2023)

145. RiskIQ «The Evil Internet Minute 2019. URL: <https://www.microsoft.com/en-us/security/business/siem-and-xdr/microsoft-defender-threat-intelligence> (дата звернення: 03.05.2023)
146. S. Simkin, L. Ponemon, (2016) Flipping the Economics of Attacks. No: Ponemon Institute. Available on: http://www.polyscope.ch/site/assets/files/42688/06_16_53.pdf
147. SOGHOIAN, C. (2011). “The Law Enforcement Surveillance Reporting Gap” unpublished report, Center for Applied Cybersecurity Research, Indiana University, Bloomington (April 10, 2011). Available at SSRN: <http://ssrn.com/abstract=1806628>
148. Special Eurobarometer 499 : Europeans' attitudes towards cyber security (cybercrime). An official website of the European Union. URL: https://data.europa.eu/data/datasets/s2249_92_2_499_eng?locale=en (дата звернення: 10.11.2023)
149. Special Eurobarometr 390 Cyber Security. Report. 2012. Available on. URL: <https://docplayer.net/3487951-Special-eurobarometer-390-cyber-security-report.html> (дата звернення: 01.07.2023)
150. T. Hirschi (2004). Self-control and crime. In R.F. Baumeister & K.D. Vohs (Eds.), Handbook of self-regulation: Research, theory and applications (New York: Guilford Press), pp. 537–555
151. The EU's Cybersecurity Strategy for the Digital Decade. Joint communication to the European parliament and the council. Brussels, 16.12.2020 JOIN(2020) 18 final URL: <https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0> (Дата звернення: 23.06.2023 p.)
152. Tymoshenko, Y.P., Kozachenko, O.I., Kyslenko, D.P., Horodetska, M.S., Chubata, M.V., & Barhan, S.S. (2022). Latest technologies in criminal investigation (testing of foreign practices in Ukraine). Amazonia Investiga, 11(51), 149-160. <https://doi.org/10.34069/AI/2022.51.03.14>
153. United Nations Congresses on Crime Prevention and Criminal Justice 1955–2020. 65 years of achievement. URL:

https://unis.unvienna.org/pdf/2020/CrimeCongress/65-years-brochure_en.pdf (дата звернення: 17.07.2023)

154. Ushering in a new era of safety. We are NOONLIGHT. Over 3 million people protected. URL: <https://www.noonlight.com/> (дата звернення: 20.07.2023)

155. What is INTERPOL? International Criminal Police Organization. URL: <https://www.interpol.int/Who-we-are/What-is-INTERPOL> (дата звернення: 12.08.2023)

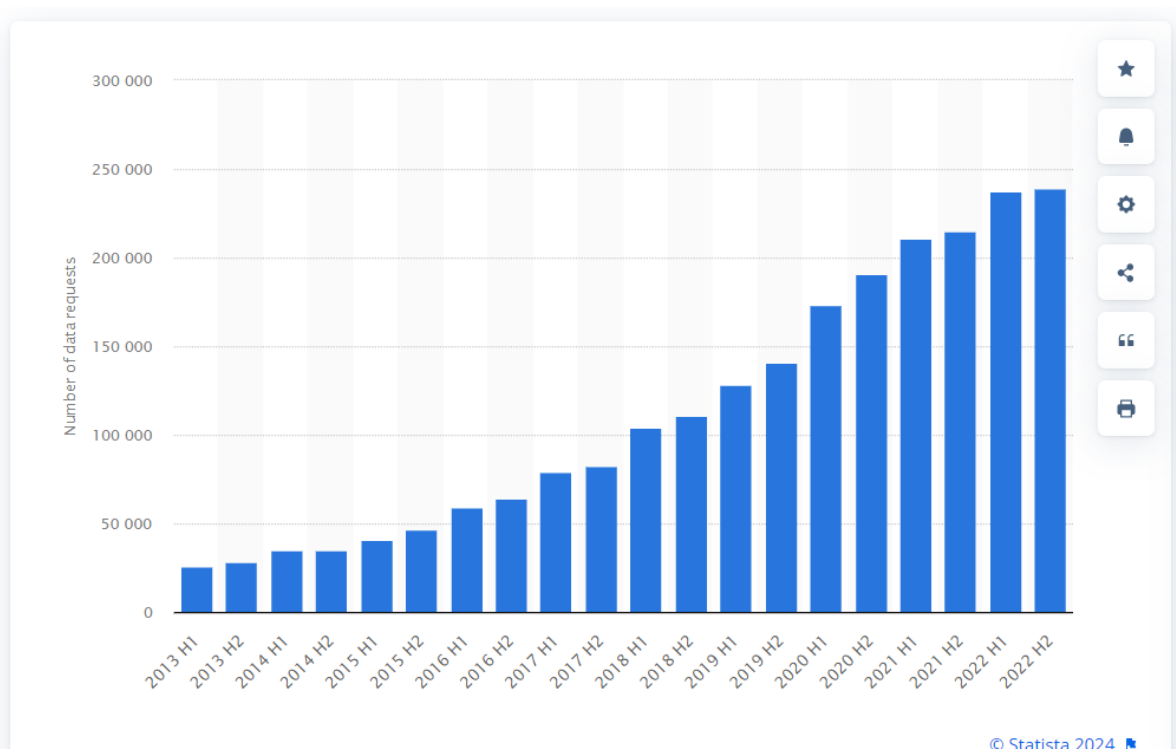
156. Zack Whittaker Police use Bluetooth messages to combat crime, target youth. URL: <https://www.zdnet.com/article/police-use-bluetooth-messages-to-combat-crime-target-youth/> (дата звернення: 20.07.2023)

ДОДАТКИ

Додаток А

Кількість запитів на дані користувачів, надісланих до Facebook в усьому світі станом на другу половину 2022 року [1]

У період з липня по грудень 2022 року Facebook отримав 239 тисяч запитів правоохоронних органів щодо інформації про користувачів. Загалом соціальна мережа видала дані користувачів для понад 76 відсотків запитів. Перше місце за кількістю запитів посідають США, на які припадає 111 тисяч запитів [2].



¹ Number of user data requests issued to Facebook by federal agencies and governments worldwide as of 2nd half 2022. Statista.com. URL: <https://www.statista.com/statistics/277230/facebook-global-user-data-requests/#:~:text=Global%20Facebook%20user%20data%20requests%20from%20federal%20agencies%20%26%20governments%202013-2022&text=Between%20July%20and%20December%202022,over%2076%20percent%20of%20requests>. (дата звернення: 01.12.2023)

²Published by Stacy Jo Dixon , Sep 6, 2023. URL: <https://www.statista.com/aboutus/our-research-commitment/3088/stacy-jo-dixon> (дата звернення: 01.12.2023)

Додаток Б

Найбільш значні випадки витоку даних у всьому світі станом на серпень 2023 року (у мільйонах), за кількістю зламаних записів даних і постраждалих осіб

Найбільшим витоком даних станом на листопад 2023 року став витік даних Sam4 у березні 2020 року, коли виявилося понад 10 мільярдів записів даних. Другий за величиною витік даних в історії на сьогоднішній день, витік даних Yahoo, стався в 2013 році. Наступним значним витоком даних став в березні 2018 року злам безпеки національної бази даних ідентифікаторів Індії Aadhaar, коли виявлено понад 1,1 мільярда записів [3].

Характеристика	Кількість постраждалих користувачів і зламаних записів
Порушення даних Sam4 (березень 2020 р.)	10,88 млрд записів
Порушення даних Yahoo (2017)*	3 мільярди рахунків
Порушення даних Aadhaar (березень 2018 р.)	1,1 млрд осіб
Витік даних Alibaba (липень 2022 р.)	1,1 млрд користувачів
Перший витік даних американської фінансової корпорації (травень 2019 р.)	885 млн користувачів
Порушення даних Verifications.io (лютий 2019 р.)	763 млн користувачів
Порушення даних LinkedIn (червень 2021 р.)	700 млн користувачів
Витік даних Facebook (квітень 2019 р.)	533 млн користувачів
Порушення даних Yahoo (2014)	500 млн рахунків
Витік даних Satwood (Marriott) (листопад 2018 р.)	500 м гостей
Порушення даних Adult Friend Finder (жовтень 2016 р.)	412,2 млн облікових записів
Витік даних MySpace (червень 2013 р.)	360 млн акаунтів
Порушення даних Exactis (червень 2018 р.)	340 млн осіб
Порушення даних Twitter (травень 2018 р.)	330 млн користувачів
Витік даних NetEase (жовтень 2015 р.)	234 млн користувачів
Витік даних Sociallarks (січень 2021 р.)	Рекорди на 200 м
Порушення даних Deep Root Analytics (червень 2017 р.)	200 мільйонів виборців США
Порушення даних Court Ventures (2013)	Особисті рекорди на дистанції 200 метрів
Порушення даних LinkedIn (червень 2012 р.)	165 млн користувачів
Витік даних Dubsplash (грудень 2018)	162 млн користувачів

³ Most significant cases of data breach worldwide as of August 2023 (in millions), by number of compromised data records and individuals impacted. Statista.com. All-time biggest online data breaches 2023. Published by Ani Petrosyan, Jan 15, 2024. URL: <https://www.statista.com/statistics/290525/cyber-crime-biggest-online-data-breaches-worldwide/> (дата звернення: 16.01.2024)

**Загальна кількість інцидентів кіберзлочинності
з листопада 2021 року по жовтень 2022 року
за галузями та розмірами організацій**

У період з листопада 2021 року по жовтень 2022 року в усьому світі було виявлено майже 16 тисяч кіберзлочинів. З цієї загальної кількості майже 700 випадків стосувалися невеликих компаній. Організації в секторі державного управління найбільше постраждали серед досліджуваних галузей, де було зареєстровано 3270 випадків кіберзлочинності. Інформаційний сектор посів друге місце, а виробництво – з приблизно 1800 інцидентами в кожній галузі [4].

Характеристика	Всього	Маленький	Великий	Невідомий
Всього	16,312	694	489	15,129
Проживання	254	4	2	248
Адміністративний	38	8	14	16
Сільське господарство	66	1	5	60
Будівництво	87	7	1	79
Освіта	496	63	15	418
Розваги	432	13	3	416
Фінанси	1,829	70	30	1,729
Охорона здоров'я	522	28	15	479
Інформація	2,105	45	110	1950
управління	9	1	0	8
Виробництво	1,814	37	24	1753
Майнінг	25	2	0	23
Інші послуги	143	7	2	134
професійний	1,396	176	54	1,166
Державне управління	3270	87	110	3,073
Нерухомість	83	15	5	63
Роздрібна торгівля	404	62	44	298
Оптова торгівля	349	13	25	311
Транспорт	117	12	6	99
Комунальні послуги	96	42	22	32
Невідомий	2,777	1	2	5,199

⁴ Global number of cybercrime incidents from November 2021 to October 2022, by industry and organization size. Statista.com. Cybercrime incidents worldwide 2021-2022, by industry and organization size. Published by Ani Petrosyan, Oct 13, 2023. URL: <https://www.statista.com/statistics/194246/cybercrime-incidents-victim-industry-size/#statisticContainer> (дата звернення: 04.01.2024)

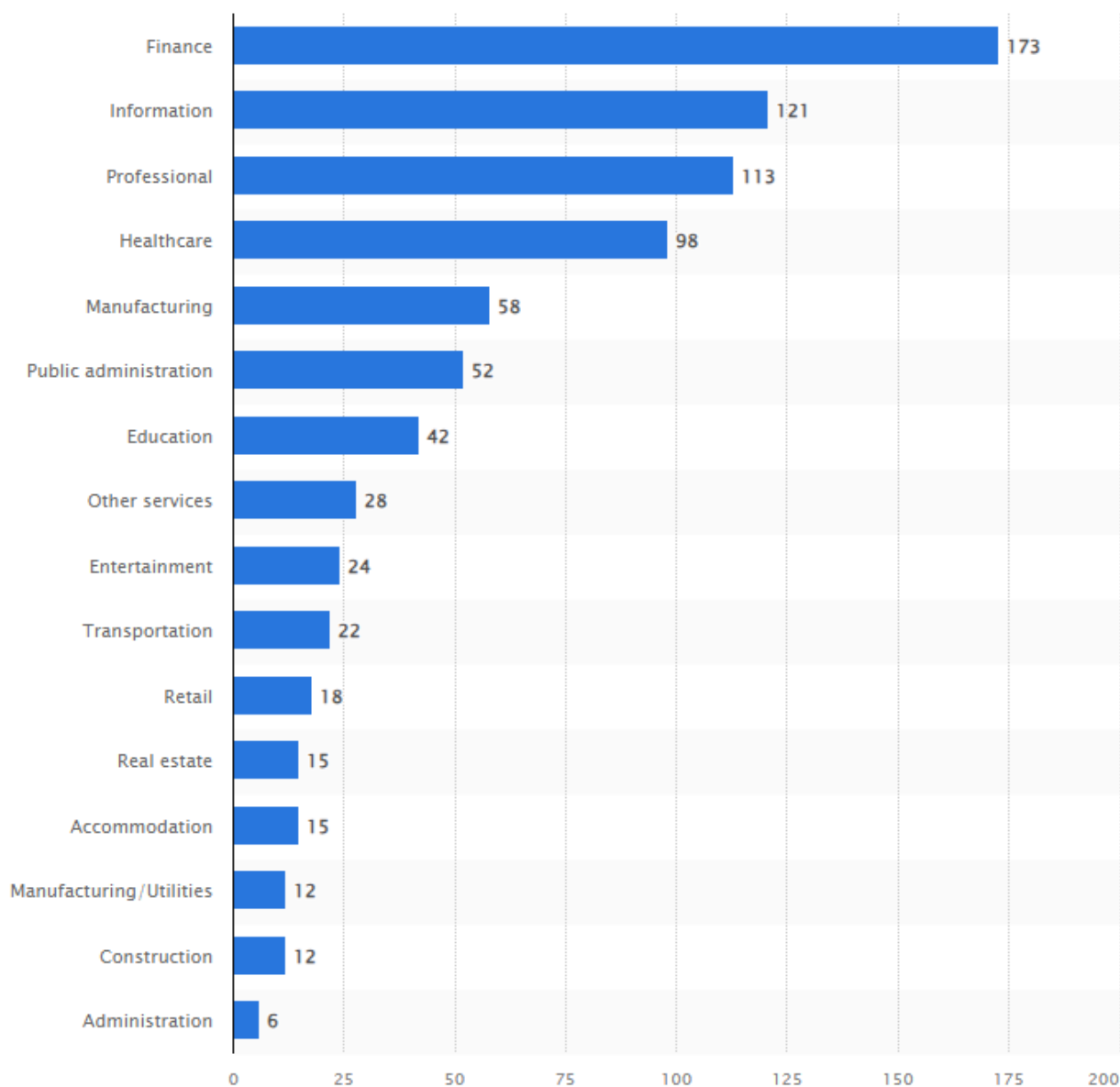
Додаток Г

Глобальні сектори промисловості, які найбільше зазнали атак базових веб-додатків з листопада 2021 року по жовтень 2022 року

У період з листопада 2021 року по жовтень 2022 року фінансова індустрія була найбільшою мішенню для атак на базові веб-додатки в усьому світі.

Установи в цьому секторі бачили 173 такі інциденти за виміряний період.

Другим за кількістю нападів був інформаційний сектор із 121 атаками, тоді як професійний сектор посів третє місце, зазнавши 113 випадків атак на базові веб-додатки [5].



⁵ Global industry sectors most targeted by basic web application attacks from November 2021 to October 2022. Statista.com. Basic web application attacks: global most-targeted industries 2021-2022. Published by Ani Petrosyan, Nov 2, 2023. URL: <https://www.statista.com/statistics/221293/cyber-crime-target-industries/> (дата звернення: 04.01.2024)

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

в яких опубліковані основні наукові результати дисертації:

1. Бенескул А. В. Характеристика кримінальних правопорушень у сфері використання цифрових технологій. *Юридичний науковий електронний журнал*. 2021. № 12. С. 511-514. URL: http://www.lsej.org.ua/12_2021/132.pdf
2. Бенескул А. В. Забезпечення кримінологічної безпеки у сфері використання цифрових технологій: міжнародно-правовий аспект. *Держава та регіони. Серія: Право*. 2022. № 3 (77). С. 132-137. URL: http://law.stateandregions.zp.ua/archive/3_2022/17.pdf
3. Бенескул А. В. Кримінологічна безпека в умовах цифрової трансформації: поняття, сутність і значення. *Ірпінський юридичний часопис: науковий журнал*. 2023. Вип. 3 (12). С. 309-317. URL: <https://ojs.dpu.edu.ua/index.php/irplegchr/article/view/125/124>
4. Бенескул А. В. Нормативно-правове закріплення застосування цифрових технологій для забезпечення кримінологічної безпеки суспільства. *Науковий вісник Ужгородського національного університету*, 2023. Серія Право. Випуск 78: частина 2. С. 145-151. URL: <http://visnyk-pravo.uzhnu.edu.ua/article/view/285996/280061>

які засвідчують апробацію матеріалів дисертації:

5. Бенескул А. В. Досвід США щодо використання цифрових технологій та штучного інтелекту при запобіганні злочинності. *Науково-практичні засади розвитку наукової думки на сучасному етапі державотворення: матеріали міжнародної науково-практичної конференції, (м. Київ, 22–23 вересня 2021 р.)*. Київ: Науково-дослідний інститут публічного права, 2021. С. 132–135.
6. Бенескул А. В. Новітні напрями вдосконалення запобігання злочинності при використанні цифрових технологій. *Взаємодія публічного та приватного права: сучасні проблеми та виклики: матеріали міжнародної*

науково-практичної конференції (м. Київ, 21–22 лютого 2022 р.). Київ: Науково-дослідний інститут публічного права, 2022. С. 39–41.

7. Бенескул А. В. Використання цифрових технологій при запобіганні злочинності та впровадження цифрової кримінології. *Актуальні проблеми імплементації наукових досягнень у практичну діяльність: матеріали міжнародної науково-практичної конференції* (м. Київ, 19–20 січня 2022 р.). Київ: Науково-дослідний інститут публічного права, 2022. С. 22–24.