УДК 343.985
DOI: 10.31733/2078-3566-2023-4-106-111

Ігор ІЄРУСАЛИМОВ©
кандидат юридичних наук, доцент

Владислав УДОВЕНКО©
аспірант

(Європейський університет, м. Київ, Україна)

АКТУАЛЬНІ ПИТАННЯ КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ, ЩО ВЧИНЯЮТЬСЯ У СФЕРІ КОМП'ЮТЕРНОЇ ІНФОРМАЦІЇ

У статті здійснено аналіз наявних наукових досліджень щодо поняття кримінальних правопорушень, що вчиняються у сфері комп'ютерної інформації, та надано своє розуміння цього явища як протиправні дії, які вчиняються з використанням комп'ютерів, мережі «Інтернет», програмного забезпечення та інших цифрових технологій. Визначено, що залежно від характеру вчиненого кримінального правопорушення, що вчиняються у сфері комп'ютерної інформації, можна виділити такі їх види: крадіжка даних, шахрайство в Інтернеті, кіберсталкінг, кібербулінг, кібертероризм, кібершантаж, хакерство та комп'ютерний злом. Надано спектр заходів, спрямованих на зменшення ризиків та попередження цих кримінальних правопорушень.

***Ключові слова*:** *кримінальні правопорушення, комп'ютерна інформація, класифікація, крадіжка даних*.

Постановка проблеми. Кримінальні правопорушення, що вчиняються у сфері комп'ютерної інформації, як специфічна категорія є дуже актуальною проблемою сьогодення, про що свідчать світові новини, статистика, проблемні питання кримінального та кримінального процесуального права. Їх розслідування (з урахуванням прогресу технологій та зростанням залежності суспільства від цифрових систем і мережі «Інтернет») набуває все більшого значення у сучасному світі.

Як правильно зазначає М. Думчиков, на сьогодні кримінальні правопорушення у сфері комп'ютерної інформації охоплюють фактично всі сфери життя суспільства, починаючи від банківської сфери, закінчуючи національною безпекою держави [1, с. 86].

На нашу думку, вони можуть призвести до серйозних наслідків для окремих осіб, організацій і навіть держав. З появою нових технологій, таких як штучний інтелект, Інтернет, блокчейн тощо виникають нові змоги для криміналістів, але й нові загрози зловживання цими технологіями. Розуміння та розслідування таких кримінальних правопорушень вимагає постійного оновлення знань і навичок.

Комп'ютерні правопорушення, що вчиняються у сфері комп'ютерної інформації, можуть бути вчинені з будь-якого куточка світу і спрямовані на будь-яку кількість потенційних потерпілих. Відповідно, їх розслідування потребує співпраці між правоохоронними органами різних країн, обміну інформацією та спільних дій. Також вони можуть становити загрозу для національної безпеки країн. Наприклад, кібератаки на критичну інфраструктуру, військові системи можуть мати серйозні наслідки для держави. Розслідування таких злочинів є важливим елементом забезпечення національної безпеки. У сучасному цифровому світі важливо захищати особисті дані

© І. Ієрусалимов, 2023
ORCID iD: https://orcid.org/0000-0003-3163-982X
law.kafedra@e-u.edu.ua

© В. Удовенко, 2023
ORCID iD: https://orcid.org/0009-0008-7986-8449
Researcher iD https://www.researchgate.net/profile/Vladyslav-Udovenko
udaffchik@gmail.com

користувачів. Крадіжки особистої інформації, порушення конфіденційності даних та інші злочини, пов'язані з комп'ютерною інформацією, стають все поширенішими. Розслідування таких злочинів допомагає забезпечити захист особистих даних та притягнення винуватих осіб до відповідальності.

Отже, актуальність теми розслідування кримінальних правопорушень у сфері комп'ютерної інформації пов'язана зі зростанням кіберзлочинності, зі швидким технологічним прогресом, глобалізацією Інтернету та необхідністю захисту національної безпеки та особистих даних. Розслідування таких злочинів вимагає постійного оновлення знань, співпраці між країнами та вдосконалення методів та інструментів розслідування.

Аналіз публікацій, в яких започатковано вирішення цієї проблеми. Питання кримінальних правопорушень, що вчиняються в сфері комп'ютерної інформації та їх розслідування розглядали такі вчені, як Дж. Арас, Г. Власова, О. Користін, М. Літвінов, Р. Лук'янчук, В. Марков, М. Ожеван, Ю. Онищенко, О. Орлов, П. Пушкаренко, К. Рудой, Є. Скулиш, В. Хахановський та ін.

Мета статті: висвітлення сучасних наукових підходів до визначення поняття кримінальних правопорушень, що вчинюються у сфері комп'ютерної інформації, та формування на підставі цього авторського бачення змісту вказаного поняття.

Виклад основного матеріалу. Під кримінальними правопорушеннями, що вчиняються у сфері комп'ютерної інформації, В. Боглов розуміє передбачене кримінальним законодавством противоправне, винне порушення чужих прав та інтересів щодо автоматизованих систем обробки даних, повноцінного впливу, що підлягають правовій охороні майнових прав та інтересів, громадської та державної безпеки [2, с. 156].

Проте О. Амелін вважає, що в юридичному сенсі таких кримінальних правопорушень немає, але при цьому наголошує, що багато традиційних видів злочинів удосконалилися внаслідок залучення коштів обчислювальної техніки, і отже, можна говорити лише про комп'ютерні аспекти злочинів без виділення їх в окрему групу [3, с. 6].

Заборонені кримінальним законом суспільно-небезпечні умисні, винні та противоправні діяння, спрямовані на порушення недоторканості комп'ютерної інформації, яка охороняється законом, та її матеріальних носіїв, що завдають шкоду правам та інтересам окремих осіб, державної та громадської безпеки вважає О. Миколенко [4, с. 104].

Пропонує під цим поняттям М. Думчиков розуміти – умисні суспільно небезпечні, протиправні, винні діяння, що посягають та заподіюють шкоду суспільним відносинам, які регламентують порядок зберігання, поширення, використання інформації та їх захист [1, с. 90].

На нашу думку, кримінальні правопорушення у сфері комп'ютерної інформації є протиправні дії, які вчиняються з використанням комп'ютерів, мережі «Інтернет», програмного забезпечення та інших цифрових технологій. Основною характеристикою цих кримінальних правопорушень є використання технології та комп'ютерних мереж як засобу для їх вчинення. У сучасному світі кіберзлочини у сфері комп'ютерної інформації є серйозною загрозою, яка постійно зростає як за поширеністю, так і за складністю.

Вважаємо, що залежно від характеру вчиненого кримінального правопорушення у сфері комп'ютерної інформації можна виділити такі їх види:

крадіжка даних. Наприклад, незаконне отримання, використання або розголошення комерційних таємниць, особистих даних або державних таємниць. Це може стосуватися бізнесів, урядових установ або окремих осіб. Згідно з дослідженнями, в 2016 році викрадення даних завдало збитків у розмірі 16 мільярдів доларів 15,4 мільйонам споживачів у Сполучених Штатах. У тому ж році британська організація з запобігання шахрайства Cifas зафіксувала майже 173 тисячі випадків шахрайства, пов'язаних з особистими відомостями у Великобританії. Це найбільша кількість випадків шахрайства за останні 13 років [5];

шахрайство в Інтернеті, що містить різноманітні види обману та недобросовісної діяльності, які вчиняються через Інтернет з метою заволодіння незаконною вигодою або шахрайства над особою, зокрема отримання логіна і пароля, інших особистих даних для використання в платіжних системах, шахрайство з

кредитними картками, через отримання номера карти, терміну дії та CVV-код, створення фіктивних інтернет-магазинів. На жаль, шахрайство було і в мирні часи, а в умовах війни схеми злодіїв отримали нові втілення. Наприклад, на Вінниччині 31-річний громадянин України збирав в Інтернеті гроші нібито на обладнання для військового шпиталю. За час своєї діяльності шахраю вдалося виманити 53 благодійні внески, проте ці кошти були витрачені аферистом на власні потреби. Для своєї шахрайської діяльності зловмисник створив фейкові сторінки в соціальних мережах, де розміщував справжні дописи про збір грошей, однак в оголошеннях змінював банківські реквізити на власні. Наразі злочинець затриманий, йому пред'явлено звинувачення за статтею 190 КК України [6];

кіберсталкінг та кібербулінг належать до переслідування, зловживання, цькування або залякування людей за допомогою електронних засобів комунікації, таких як соціальні мережі, електронна пошта, повідомлення та форуми, створюючи для цього фейкові акаунти, повідомлення на мобільний телефон та в різні месенджери. Основні риси кібербулінгу: запостити образливі або непристойні повідомлення про когось; поширення чуток, лайки, негативних коментарів або фотографій з наміром нашкодити чи засмутити особу, створення фейкових акаунтів, підробка особистості, що призводить до дискредитації та сорому; інтимне шантажування. Юридично це можна кваліфікувати за різними статтями, зокрема, якщо сталкер погрожує вбивством і якщо такі погрози дійсно були в повідомленнях. Також можна використовувати статтю про порушення недоторканності приватного життя, якщо, наприклад, злочинець незаконно зберігав, збирав, використовував, знищував чи поширював конфіденційну інформацію про особу або незаконно її змінював [7];

кібертероризм – кібертерористичні дії мають на меті завдати шкоди комп'ютерним системам, мережам, критичній інфраструктурі або впливати на функціонування технологічних систем з метою спричинення паніки, хаосу або викликання серйозних наслідків. На сьогодні вже було багато випадків кібератак, які можуть кваліфікуватися як кібертероризм. Найбільше ураження за допомогою Троянської програми відбулося 14 квітня 2017 року, коли система оновлення програми M. E. Doc була заражена вірусом сімейства Petya. Внаслідок атаки була заблокована діяльність таких підприємств, як аеропорт «Бориспіль», ЧАЕС, Укртелеком, Укрпошта, Ощадбанк, Укрзалізниця та низки інших великих підприємств [8];

кібершантаж – використання комп'ютерних систем або мереж для шантажу, зокрема шантажу через розголошення особистої інформації, блокування доступу до системи або поширення негативної інформації з метою отримання вигоди або контролю над потерпілим;

хакерство та комп'ютерний злом. Зокрема, хакерство містить незаконне отримання доступу до комп'ютерних систем і мереж з метою зміни, крадіжки або руйнування даних. Хакери можуть використовувати різні методи, включно із зламом паролів, використанням вразливостей програмного забезпечення та інженерінгом соціальних мереж.

Це лише кілька прикладів злочинів у сфері комп'ютерної інформації, і список може бути набагато ширшим.

Запобігання кримінальним правопорушенням у сфері комп'ютерних технологій містить широкий спектр заходів, спрямованих на зменшення ризиків та попередження протиправних дій. Ось деякі важливі аспекти запобігання злочинам у цій сфері:

– кібербезпека: Забезпечення ефективного захисту комп'ютерних систем і мереж від несанкціонованого доступу, вірусів, троянських програм та інших шкідливих атак. Це встановлення сильних паролів, регулярне оновлення програмного забезпечення, використання антивірусного захисту, фаєрволів та інших технічних заходів безпеки;

– навчання та освіта: інформування користувачів про потенційні загрози та методи обману, які використовуються злочинцями. Навчання основам кібербезпеки, правилам безпечного використання Інтернету та комп'ютерних технологій;

– свідоме використання соціальних мереж: попередження про ризики, пов'язані з розміщенням особистої інформації в соціальних мережах та встановлення обмежень доступу до неї. Підтримка свідомого та відповідального використання соціальних мереж, особливо серед дітей та підлітків;

– захист особистих даних: використання сильних паролів, шифрування даних, обмеження доступу до особистої інформації та регулярна перевірка наявності підозрілих

дій або несподіваних активностей у банківських або фінансових облікових записах;

– законодавчий захист: удосконалення законодавства щодо кіберзлочинності, встановлення жорстких санкцій для злочинів у сфері комп'ютерних технологій, а також регулювання використання технологій і захисту особистих даних;

– міжнародна співпраця: зміцнення співпраці між державами та міжнародними організаціями у сфері кібербезпеки, обмін даними та інформацією про кіберзлочини, спільні розслідування та притягнення злочинців до відповідальності;

– співпраця з приватним сектором: залучення та співпраця з компаніями, провайдерами інтернет-послуг та іншими представниками приватного сектора для спільного виявлення загроз, обміну інформацією та розробки заходів захисту;

– своєчасне реагування: забезпечення належного розслідування, збереження доказів та притягнення винуватих осіб до відповідальності;

– створення культури кібербезпеки: залучення громадськості та підвищення свідомості про кіберзагрози, поширення правил безпеки та рекомендацій щодо захисту особистих даних та інформаційної безпеки.

Ці заходи спільно сприяють зменшенню ризиків кіберзлочинності та попередженню протиправних дій у сфері комп'ютерних технологій. Важливо прагнути до постійного вдосконалення і адаптації заходів запобігання відповідно до технологій та загроз, що змінюються.

Розслідування кримінальних правопорушень у сфері комп'ютерних технологій являє собою складність та виклики для правоохоронних органів та служб безпеки, зокрема анонімність в Інтернеті. Кіберзлочинці можуть залишати сліди через анонімні проксі-сервери, використання хакерських технік або шифрування, що ускладнює відстеження їхньої справжньої ідентичності та місцеперебування.

Глобальний характер, що виявляється в можливості злочинців здійснювати атаки з будь-якої точки світу, перетинаючи юрисдикційні межі, ускладнює співпрацю та обмін інформацією між правоохоронними органами різних країн. Кіберзлочинці постійно вдосконалюють свої техніки та використовують нові вразливості в системах для вчинення кримінальних правопорушень. Розслідування вимагає висококваліфікованих спеціалістів, які розуміють складні технічні аспекти кіберзлочинності.

Ці види кримінальних правопорушень можуть мати велику кількість електронних доказів, таких як журнали ведення, відомості про мережевий трафік, електронні повідомлення та інше. Аналіз цих доказів може бути складним та ресурсомістким завданням.

Їх розслідування вимагає наявності достатніх ресурсів, технічного обладнання та спеціалістів. Дефіцит ресурсів і фінансування може ускладнювати проведення розслідувань. Забезпечення потрібного обладнання, програмного забезпечення та персоналу може бути викликом для правоохоронних органів, особливо в умовах швидкого технологічного розвитку.

Також важливо відзначити високу мобільність та адаптивність кіберзлочинців. Вони швидко адаптуються до нових захисних технологій та використовують нові методи атак, що вимагає постійного оновлення знань та навичок у сфері кібербезпеки. Крім того, складність міжнародної співпраці та обміну інформацією між правоохоронними органами різних країн може ускладнювати розслідування кримінальних правопорушень у сфері комп'ютерної інформації, особливо коли злочинці використовують анонімність та перетинають юрисдикційні межі.

Усі ці фактори викликають потребу в постійному розвитку та поліпшенні спеціалізованих підрозділів з кібербезпеки в правоохоронних органах та сприяють необхідності співпраці між різними суб'єктами, включно з урядовими органами, приватними компаніями.

Висновки. Отже, кримінальні правопорушення, що вчиняються у сфері комп'ютерної інформації, стають все більш поширеними, складними і руйнівними. Вони мають значний вплив на окремих осіб, організації та суспільство загалом, призводять до фінансових збитків, порушення приватності, крадіжок особистих даних, загроз для критичної інфраструктури та національної безпеки. Правоохоронні органи та служби безпеки стикаються з численними складнощами під час їх розслідування.

Список використаних джерел

1. Думчиков М. О. Кримінальні правопорушення в сфері комп'ютерної інформації: ретроспективний аналіз. *Науковий вісник Міжнародного гуманітарного університету. Серія : Юриспруденція.* 2022. № 57. С. 86–90.

2. Болгов В. М., Гадіон Н. М., Гладун О. З. Організаційно-правове забезпечення протидії кримінальним правопорушенням, що вчиняються з використанням інформаційних технологій : науково-практ. посіб. Київ : Національна академія прокуратури України, 2015. 202 с.

3. Амелін О. М. Визначення кіберзлочинів у національному законодавстві. *Науковий часопис Національної академії прокуратури України*. 2016. № 3. С. 1–12.

4. Миколенко О. М. Деякі особливості розслідування злочинів у сфері використання електроннообчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. *Кібербезпека в Україні: правові та організаційні питання* : матеріали Всеукр. наук.-практ. конф. (м. Одеса, 21 жовт. 2016 р.). Одеса : ОДУВС, 2016. С. 155-157

5. Викрадення даних. URL: https://www.eset.com/ua/support/information/entsiklopediya-ugroz/krazha-dannykh/.

6. Реальні історії шахрайства в інтернеті в умовах війни. URL: https://it-kharkiv.com/realni-istoriyi-shahrajstva-v-interneti-v-umovah-vijny/.

7. Кібербулінг: дев'ять запитань, відповіді на які ви могли не знайти. URL: https://tsn.ua/ukrayina/kiberbuling-dev-yat-zapitan-vidpovidi-na-yaki-vi-mogli-ne-znati-2246665.html

8. Концепція інформаційної безпеки України. URL: https://www.osce.org/uk/fom/ 175056?download=true

Надійшла до редакції 07.12.2023

References

1. Dumchykov, M. O. (2022) Kryminalni pravoporushennia v sferi kompiuternoi informatsii: retrospektyvnyi analiz [Criminal offenses in the field of computer information: a retrospective analysis]. *Naukovyi visnyk Mizhnarodnoho humanitarnoho universytetu. Seriia : Yurysprudentsiia*. № 57, pp. 86–90. [in Ukr.].

2. Bolhov, V. M., Hadion N. M., Hladun O. Z. (2015) Orhanizatsiino-pravove zabezpechennia protydii kryminalnym pravoporushenniam, shcho vchyniaiutsia z vykorystanniam informatsiinykh tekhnolohii [Organizational and legal provision of combating criminal offenses committed with the use of information technologies] : naukovo-prakt. posib. Kyiv : Natsionalna akademiia prokuratury Ukrainy, 202 p. [in Ukr.].

3. Amelin, O. M. (2016) Vyznachennia kiberzlochyniv u natsionalnomu zakonodavstvi [Definition of cybercrime in national legislation]. *Naukovyi chasopys Natsionalnoi akademii prokuratury Ukrainy*. № 3, pp. 1–12. [in Ukr.].

4. Mykolenko O. M. (2016) Deiaki osoblyvosti rozsliduvannia zlochyniv u sferi vykorystannia elektronnoobchysliuvalnykh mashyn (kompiuteriv), system ta kompiuternykh merezh i merezh elektrozviazku. [Some features of the investigation of crimes in the field of the use of electronic computing machines (computers), systems and computer networks and telecommunication networks]. *Kiberbezpeka v Ukraini: pravovi ta orhanizatsiini pytannia: materialy Vseukr. nauk.-prakt. konf. (m. Odesa, 21 zhovt. 2016 r.)*. Odesa : ODUVS, 233 p. [in Ukr.].

5. Vykradennia danykh [Data theft]. URL: https://www.eset.com/ua/support/ information/entsiklopediya-ugroz/krazha-dannykh/ [in Ukr.].

6. Realni istorii shakhraistva v interneti v umovakh viiny [Real stories of fraud on the Internet in the conditions of war]. URL: https://it-kharkiv.com/realni-istoriyi-shahrajstva-v-interneti-v-umovah-vijny/ [in Ukr.].

7. Kiberbulinh: deviat zapytan, vidpovidi na yaki vy mohly ne znaity [Cyberbullying: Nine Questions You Might Not Have Answered]. URL: https://tsn.ua/ukrayina/kiberbuling-dev-yat-zapitan-vidpovidi-na-yaki-vi-mogli-ne-znati-2246665.html [in Ukr.].

8. Kontseptsiia informatsiinoi bezpeky Ukrainy [Concept of information security of Ukraine]. URL: https://www.osce.org/uk/fom/175056?download=true [in Ukr.].

ABSTRACT

Ihor Iierusalymov, Vladyslav Udovenko. Current issues of criminal offenses committed in the sphere of computer information. The article highlights the relevance of the investigation of criminal offenses committed in the field of computer information, due to the growth of this type of crime, rapid technological progress, globalization of the Internet and the need to protect national security and personal data. The purpose of the article is to highlight modern scientific approaches to the definition of the concept of criminal offenses committed in the field of computer information and to form the content of this concept based on this author's vision. For this, an analysis of available scientific research was carried out regarding the concept of criminal offenses committed in the field of computer information, and an understanding of this phenomenon was provided, as illegal actions that are committed using computers, the Internet, software and other digital technologies. It was determined that depending on the nature of the criminal offense committed in the field of computer information, the following types can be

distinguished: data theft. Internet fraud, cyber stalking, cyber bullying, cyber terrorism, cyber blackmail, hacking and hacking. It is noted that the investigation of these criminal offenses presents complexity and challenges for law enforcement agencies and security services. For the effective prevention and counteraction of criminal offenses committed in the field of computer information, a range of measures aimed at reducing risks and preventing illegal actions is provided, in particular, cyber security: training and education: conscious use of social networks: protection of personal data: legal protection, international cooperation: cooperation with the private sector: timely response: ensuring proper investigation, preservation of evidence and prosecution of those responsible, creating a culture of cyber security and the content of each is disclosed.

***Keywords*:** *criminal offenses, computer information, classification, data theft*.

УДК 343.126.1.06
DOI: 10.31733/2078-3566-2023-4-111-117

Дмитро КОЛОДЧИН©
кандидат юридичних наук
(ПрАТ «Вищий навчальний заклад «Міжрегіональна Академія управління персоналом», м. Київ, Україна)

СТАН НАУКОВОГО РОЗРОБЛЕННЯ ПРОБЛЕМИ ДОСЛІДЖЕННЯ ЗЛОЧИННОСТІ В ПЕНІТЕНЦІАРНІЙ СФЕРІ УКРАЇНИ

У статті розглянуто сучасний стан наукового дослідження злочинності в пенітенціарній сфері України. Виокремлено їхні чотири періоди: перший період (1991–1995 рр.); другий період (1995–2004 рр.); третій період (2004–2013 рр.); четвертий період розпочався у 2014 році і триває донині. Подано аналіз наукових праць вітчизняних вчених щодо сучасного стану злочинності в пенітенціарній сфері України. Доведено, що злочинність у пенітенціарній сфері України, а також вивчення нормативно-правових джерел з означеної проблематики дають підстави стверджувати, що ця тема дослідження є нагальним питанням сьогодення, має теоретико-прикладний характер, а тому потребує активізації науковців у цьому напрямі.

***Ключові слова*:** *стан, періоди, дослідження, засуджений, місце несвободи, злочинність, пенітенціарна сфера*.

Постановка проблеми. Проблема дослідження злочинності в пенітенціарній сфері України має власну писану історію. Розглядається вона вченими, як правило, одночасно з проблемою виникнення злочинності та створенням перших в'язниць. Виконані останнім часом дослідження у сфері виконання та відбування покарань свідчить про те, що сьогодні особливо актуальним стало питання запобігання злочинності в пенітенціарній сфері. До речі, дослідженням встановлено, що засуджений користується всіма правами людини і громадянина, за винятком обмежень, які визначені законом і встановлені вироком суду.

Вивчення стану наукового розроблення проблеми дослідження злочинності в пенітенціарній сфері України створює передумови на науковому рівні проаналізувати монографічні праці і наукові статті щодо цього і надати ґрунтовне пояснення причин і умов вчинення кримінальних правопорушень в місцях несвободи ДКВС України та уповноважених органах з питань пробації Державної установи «Центр пробації» як засудженими, так і персоналом.

Крім того, вивченню стану наукового розроблення проблеми дослідження злочинності в пенітенціарній сфері України сприяють також і суттєві зміни в державній політиці у сфері виконання покарань та пробації Міністерства юстиції України, як правонаступника Державної пенітенціарної служби України, сутність яких спрямована на захист прав і свобод засуджених, дотримання в місцях несвободи та в уповноважених органах з питань пробації міжнародних стандартів поводження з ними, створення

ORCID iD: https://orcid.org/0000-0002-0820-4409
kolodchin005@ukr.net