УДК 343.9
DOI 10.33244/2617-4154.1(10).2023.187-194

В. В. Топчій,
д-р юрид. наук, професор,
заслужений юрист України
e-mail: tv1959@ukr.net
ORCID ID 0000-0003-4596-6469;
О. М. Бодунова,
канд. юрид. наук, доцент,
Державний податковий університет
e-mail: olesalasuk@gmail.com
ORCID ID 0000-0001-9179-5985

СИСТЕМА КРИМІНАЛЬНИХ ПРАВОПОРУШЕНЬ У СФЕРІ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ: МІЖНАРОДНО-ПРАВОВИЙ ВИМІР

У статті досліджується система кримінальних правопорушень у сфері інформаційних технологій відповідно до норм міжнародного права. Зазначено, що впродовж останнього двадцятиліття у світі триває процес формування інформаційного суспільства, а тому все більше розвиваються обчислювальні та інформаційні мережі — унікальне поєднання комп'ютерів і комунікацій. З кожним днем більш активно розвиваються сучасні інформаційні технології і в Україні. Людська цивілізація на межі тисячоліть вступила в еру інформації. Світовою системою комп'ютерних комунікацій щодня користуються сотні мільйонів людей. Це надає нові можливості розвитку національної культури, освіти, науки й економіки.

Проте технологічний прогрес і впровадження інформаційних технологій у всі сфери життєдіяльності суспільства має негативний ефект, оскільки це призводить до збільшення кількості кримінальних правопорушень. Також це дає змогу вчиняти кримінальні правопорушення новими, нетрадиційними способами.

Особливо в умовах ведення повномасштабної війни росії проти України використання інформаційних технологій під час вчинення кримінальних правопорушень є звичним явищем для окупантів, що зумовлює розширення переліку кримінально протиправних діянь, які вчиняються у сфері інформаційних технологій.

Зроблено висновок, що з розвитком технічного прогресу видозмінюється і злочинність, яка набуває нових, раніше невідомих форм. Так, з виникненням у середині XX століття електронно-обчислювальних пристроїв поняття злочинності в цій сфері неодмінно пов'язувалося з предметом кримінально протиправного впливу або предметом кримінального правопорушення, яким є комп'ютер. Об'єднання комп'ютерів у мережі (локальні, глобальні) надало можливість використовувати ЕОМ як засіб кримінального правопорушення, а місцем його вчинення став кіберпростір.

Зважаючи на викладене, у міжнародних нормативно-правових актах універсальне коло кримінальних правопорушень у сфері інформаційних відносин досі не визначене. Це пов'язано з динамічним розвитком злочинності, виникненням нових видів кримінальних правопорушень, що вчиняються у сфері інформаційних технологій. Тому на сьогодні актуальним питанням залишається розроблення єдиної кримінальної стратегії, пов'язаної з комп'ютерними кримінальними правопорушеннями, їх поняттям та системою.

Ключові слова: *злочинність у сфері інформаційних технологій, комп'ютерні кримінальні правопорушення, інформаційне суспільство, комп'ютерне шахрайство, інформаційні мережі.*

Метою цієї статті є теоретичний аналіз та дослідження системи кримінальних правопорушень у сфері інформаційних технологій відповідно до норм міжнародного права.

Постановка проблеми. Упродовж останнього двадцятиліття у світі триває процес формування інформаційного суспільства, а тому все більше розвиваються обчислювальні та інформаційні мережі – унікальне поєднання комп'ютерів і комунікацій. З кожним днем більш активно розвиваються сучасні інформаційні технології і в Україні. Людська цивілізація на межі тисячоліть вступила в еру інформації. Світовою системою комп'ютерних комунікацій щодня користуються сотні мільйонів людей. Це надає нові можливості розвитку національної культури, освіти, науки й економіки [1, с. 8].

Проте технологічний прогрес і впровадження інформаційних технологій у всі сфери життєдіяльності суспільства має негативний ефект, оскільки це призводить до збільшення кількості кримінальних правопорушень. Також це дає змогу вчиняти кримінальні правопорушення новими, нетрадиційними способами.

Крім того, що кримінальні правопорушення, які вчинені з використанням переваг найсучасніших технологій, завдають великих економічних збитків, суспільство стає все більш залежним від роботи автоматизованих систем у різноманітних сферах життя – від управління Збройними силами України, підприємствами, організаціями, відомствами, рухом літаків і поїздів до медичного обслуговування населення та національної безпеки. Іноді навіть незначний збій у функціонуванні таких систем може призвести до реальної загрози життю людей. Стрімке зростання глобальних комп'ютерних і телекомунікаційних мереж, а також можливість підключення до них через звичайні телефонні лінії посилюють можливості їх використання для незаконної діяльності [2].

Особливо в умовах ведення повномасштабної війни росії проти України використання інформаційних технологій під час вчинення кримінальних правопорушень є звичним явищем для окупантів, що зумовлює розширення переліку кримінально протиправних діянь, які вчиняються у сфері інформаційних технологій.

Аналіз останніх досліджень і публікацій. Кримінальним правопорушенням у сфері інформаційних технологій, їх системі приділялася суттєва увага у наукових працях Е. Аверьянової, В. Болгова, С. Бородіна, В. Вєхова, Н. Гадіон, О. Гладуна, В. Голубєва, А. Гребєнькова, О. Григорьєва, Г. Долженкова, М. Журби, І. Карася, В. Кіютіна,

І. Клепицького, О. Книжечко, О. Користіна, Л. Краснова, В. Крачевського, М. Литвинова, Ю. Ляпунова, С. Максимова, А. Новікова, П. Смагіна, В. Хахановського, І. Юрченка та інших. Проте до сьогодні залишаються не повністю дослідженими питання щодо системи кримінальних правопорушень у сфері інформаційних технологій як за законодавством України, так і відповідно до міжнародно-правових договорів. У зв'язку з цим актуальними є питання щодо аналізу норм міжнародного права та рекомендацій зарубіжних експертів стосовно класифікації кримінально протиправних діянь цієї категорії.

Виклад основного матеріалу. Варто зазначити, що кримінальні правопорушення у сфері інформаційних технологій завдають значних збитків розвиненим у технічному відношенні країнам, оскільки в цих країнах з початком процесу інформатизації суспільства створюються сприятливі умови для вчинення таких протиправних діянь. Зокрема, глобальна комп'ютерна мережа «Інтернет» надає можливість увійти до будь-якої світової відомчої комп'ютерної системи, зокрема і військової. До того ж це можна зробити майже з будь-якої точки світу. Порівняно з розвиненими країнами національна безпека України досі ще залежить від комп'ютерних мереж значно менше: комп'ютерних кримінальних правопорушень найбільше зазнає у нас фінансово-кредитна сфера. Але уже відчутний вплив кримінальних правопорушень і на інші сфери: екологічні, економічні, транспортні тощо. Так, впровадження електронних сервісів в органах державної влади та місцевого самоврядування, поширення телекомунікаційної мережі, впровадження системи електронних платежів, використання автоматизованих баз даних у діяльності правоохоронних органів та у військовій справі значно розширили сферу діяльності комп'ютерних злочинців.

Саме тому підтримуємо думку науковців, що комп'ютерна злочинність є міжнародним явищем, рівень якої тісно пов'язаний з економічним рівнем розвитку суспільства в різних державах та регіонах. При цьому менш розвинені в технічному відношенні країни завдяки діяльності міжнародних правоохоронних організацій мають можливість використати досвід більш розвинутих країн для запобігання та викриття комп'ютерних кримінальних правопорушень. Загальні тенденції, кримінально протиправні засоби та заходи запобігання є в різні відрізки часу однаковими для різних країн, що базується на єдності технічної, програмної та методичної бази цих кримінальних правопорушень [3, с. 137].

Відмітимо, що перше ґрунтовне дослідження проблеми злочинності у сфері інформаційних технологій на міжнародному рівні було зроблено Організацією економічного співробітництва та розвитку (далі – ОЕСР), яка з 1983 по 1985 роки вивчала можливості гармонізації норм, що передбачають кримінальну відповідальність за кіберзлочини. Висновки ОЕСР викладені у доповіді вказаної організації «Злочини, пов'язані з комп'ютером: аналіз правової політики», в якій проаналізовано чинне законодавство, надано пропозиції щодо його реформування, а також рекомендовано мінімальний перелік діянь, які підлягають криміналізації:

– злам, зміна, видалення, приховування комп'ютерних даних та/або комп'ютерних програм, вчинені умисно, з метою протиправного переміщення грошових коштів чи інших матеріальних цінностей;

– злам, зміна, видалення, приховування комп'ютерних даних та/або комп'ютерних програм, вчинені умисно з метою підроблення;

– злам, зміна, видалення, приховування комп'ютерних даних та/або комп'ютерних програм, вчинені умисно з метою перешкодити функціонуванню комп'ютера та/або телекомунікаційних систем;

– порушення виняткових прав власника комп'ютерної програми з метою комерційної експлуатації цієї програми або її продажу;

– доступ до комп'ютерних даних або даних телекомунікаційних систем, а також їх перехоплення, вчинене навмисно без дозволу особи, відповідальної за функціонування системи, або з порушенням вимог безпеки, або з протиправними намірами [1].

1986 року в Парижі група експертів Організації економічного співробітництва та розвитку кримінальні правопорушення у сфері інформаційних технологій визначила як «будь-яку незаконну, неетичну або заборонену поведінку щодо автоматизованої обробки і або передачі даних».

13 вересня 1989 року Радою Європи прийнято Рекомендацію No R89 (9) Комітету міністрів Ради Європи щодо кримінальних правопорушень, які пов'язані з комп'ютерними технологіями, де було зроблено першу спробу визначити поняття і коло кримінальних правопорушень, пов'язаних з використанням комп'ютерів [4].

У Рекомендаціях № R (95)13 щодо проблем кримінального процесуального права, які пов'язані з інформаційними технологіями, Рада Європи словосполучення «злочин з використанням комп'ютера» замінила на «злочин, пов'язаний з використанням комп'ютерних технологій». У цьому документі наголошується, що кримінальні правопорушення, пов'язані з використанням інформаційних технологій, можуть вчинятися не тільки за допомогою окремого комп'ютера, а й комп'ютерної системи, що може бути як об'єктом, так і середовищем вчинення кримінального правопорушення [5, с. 96–97].

З 1985 по 1989 роки Спеціальний Комітет експертів Ради Європи з питань злочинності, пов'язаної з комп'ютерами, розробляв Рекомендацію № 89, затверджену Комітетом міністрів Ради Європи 13 вересня 1989 року. Вона містить перелік правопорушень, рекомендований країнам-учасницям ЄС для розроблення єдиної кримінальної стратегії, пов'язаної з комп'ютерними програмами народного консенсусу з питань криміналізації деяких кримінальних правопорушень, пов'язаних з комп'ютерами. Рекомендація містить два списки злочинів: «мінімальний» та «факультативний (додатковий)». До «мінімального» входять діяння, які обов'язково повинні бути заборонені міжнародним законодавством і підлягають переслідуванню в судовому порядку. Зокрема, це:

– комп'ютерне шахрайство. Створення, зміна, знищення або пошкодження комп'ютерних даних чи комп'ютерних програм, або інше втручання у хід обробки даних, яке впливає на результат обробки даних так, що завдає економічні або майнові втрати іншій особі, яке здійснюється з метою забезпечення незаконної економічної користі для себе чи інших осіб;

– підроблення комп'ютерної інформації. Створення, зміна, знищення, приховування комп'ютерних даних чи комп'ютерних програм або інше втручання у хід обробки даних різними способами, або створення таких умов, які, згідно з національним законодавством, будуть становити таке правопорушення, як підробка;

– пошкодження комп'ютерних даних чи комп'ютерних програм. Несанкціоноване знищення, пошкодження, погіршення комп'ютерних даних чи комп'ютерних програм;

– комп'ютерний саботаж. Створення, зміна, знищення або приховування комп'ютерних даних чи комп'ютерних програм або інше втручання в комп'ютерні системи з метою перешкоджання функціонуванню комп'ютера або телекомунікаційних систем;

– несанкціонований доступ. Несанкціонований доступ до комп'ютерної системи або мережі з порушенням засобів захисту;

– несанкціоноване перехоплення. Несанкціоноване перехоплення даних, що йдуть до мережі, від мережі або усередині мережі, здійснене із застосуванням технічних засобів зв'язку;

– несанкціоноване відтворення захищених комп'ютерних програм. Протиправне відтворення, розповсюдження чи публічне передавання комп'ютерної програми, захищеної відповідно до закону [6, с. 14–17].

«Додатковий» список містить ті правопорушення, за якими досягнення міжнародної згоди виявляється складним. Зокрема, це:

1) зміна комп'ютерних даних чи комп'ютерних програм. Несанкціонована зміна комп'ютерних даних або комп'ютерних програм;

2) комп'ютерне шпигунство. Придбання з використанням протиправних засобів або шляхом несанкціонованого розкриття, передавання або використання торговельної чи комерційної таємниці з метою заподіяння економічного збитку особі, яка має право на таємницю, або отримання незаконної економічної переваги для себе чи третьої особи;

3) протиправне використання комп'ютера. Несанкціоноване використання комп'ютерної системи або мережі, якщо воно:

– вчиняється в умовах значного ризику втрат для особи, яка має право використовувати систему, шкодить системі або її функціонуванню;

– вчинено з метою заподіяння шкоди особі, яка має право використовувати комп'ютер;

4) протиправне використання захищеної комп'ютерної програми. Використання захищеної законом комп'ютерної програми без дозволу або її незаконне відтворення з метою отримання економічної вигоди для себе чи третьої особи або з наміром заподіяти шкоду законному власнику програми [6, с. 14–17].

Управління ООН з наркотиків і злочинності в опублікованому 2013 року звіті «Всебічне дослідження проблеми кіберзлочинності та відповідних заходів з боку держав-членів, міжнародного співтовариства і приватного сектора» з цього приводу зазначає, що поняття «кіберзлочинність» залежить від контексту і мети вживання цього терміна. Водночас, хоча основу цього поняття становлять кримінальні правопорушення проти конфіденційності, цілісності та доступності даних, проте до нього включають і

будь-які дії, спрямовані на нелегальне вилучення прибутку, контент-злочини та інші протиправні діяння в кіберпросторі. При цьому, як зазначають автори звіту, у створенні універсального визначення кіберзлочинності немає потреби, оскільки з метою міжнародного співробітництва з розслідування злочинів набагато важливіше гармонізувати норми, що належать до збирання та подання електронних доказів. Така необхідність не обмежується терміном «кіберзлочин», оскільки на електронних носіях і в електронних комунікаціях може міститися інформація, що належить до будь-якого виду кримінальних правопорушень, вчинених як у кіберпросторі, так і поза ним [1].

Висновки. З огляду на викладене доходимо висновку, що з розвитком технічного прогресу видозмінюється й злочинність, яка набуває нових, раніше невідомих форм. Так, з виникненням у середині XX століття електронно-обчислювальних пристроїв поняття злочинності в цій сфері неодмінно пов'язувалося з предметом кримінально протиправного впливу або предметом кримінального правопорушення, яким є комп'ютер. Об'єднання комп'ютерів у мережі (локальні, глобальні) надало можливість використовувати ЕОМ як засіб кримінального правопорушення, а місцем його вчинення став кіберпростір.

Зважаючи на вищевикладене, у міжнародних нормативно-правових актах універсальне коло кримінальних правопорушень у сфері інформаційних відносин досі не визначене. Це пов'язано з динамічним розвитком злочинності, виникненням нових видів кримінальних правопорушень, що вчиняються у сфері інформаційних технологій. Тому на сьогодні актуальним питанням залишається розроблення єдиної кримінальної стратегії, пов'язаної з комп'ютерними кримінальними правопорушеннями, їх поняттям і системою.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Інформаційна діяльність в правознавстві: монографія. К.: Наука і життя, 2007. 244 с.

2. Круль С. М. Злочини у сфері інформаційних технологій: національний та міжнародний аспекти. *Актуальні проблеми вдосконалення чинного законодавства України*. 2008. Вип. 20. С. 200–204. URL: http://nbuv.gov.ua/UJRN/apvchzu_2008_20_32

3. Біленчук П. Д., Задояний М. Т. основи криміналістики: інноваційні технології та основи організації розслідування злочинів: навчальний посібник. Черкаси: Східноєвропейський ун-т економіки і менеджменту, 2008. 193 с.

4. Амелін О. Злочини у сфері інформаційних відносин в міжнародно-правових актах. *Науковий часопис Національної академії прокуратури України.* 2016. № 2. С. 1–9. URL: http://www.chasopysnapu.gp.gov.ua/ua/pdf/10-2016/01/amelin.pdf

5. Про проблеми кримінально-процесуального права, пов'язані з інформаційними технологіями: Рекомендації Ради Європи No R (95) 13 від 11 вересня 1995 року. *Правова інформатика*. 2006. № 3(11). С. 96–97.

6. Болгов В. М., Гад Н. М. Організаційно-правове забезпечення протидії кримінальним правопорушенням, що вчиняються з використанням інформаційних технологій: наук.-практ. посіб. С. 14–17.

REFERENCES

1. Informatsiina diialnist v pravoznavstvi: monohrafiia. K.: Nauka i zhyttia, 2007. 244 s.

2. Krul C. M. Zlochyny u sferi informatsiinykh tekhnolohii: natsionalnyi ta mizhnarodnyi aspekty. *Aktualni problemy vdoskonalennia chynnoho zakonodavstva Ukrainy.* 2008. Vyp. 20. S. 200–204. URL: http://nbuv.gov.ua/UJRN/apvchzu_2008_20_32

3. Bilenchuk P. D., Zadoianyi M. T. osnovy kryminalistyky: innovatsiini tekhnolohii ta osnovy orhanizatsii rozsliduvannia zlochyniv: navchalnyi posibnyk. Cherkasy: Skhidnoievropeiskyi un-t ekonomiky i menedzhmentu, 2008. 193 s.

4. Amelin O. Zlochyny u sferi informatsiinykh vidnosyn v mizhnarodno-pravovykh aktakh. *Naukovyi chasopys Natsionalnoi akademii prokuratury Ukrainy*. 2016. № 2. S. 1–9. URL: http://www.chasopysnapu.gp.gov.ua/ua/pdf/10-2016/01/amelin.pdf

5. Pro problemy kryminalno-protsesualnoho prava, poviazani z informatsiinymy tekhnolohiiamy: Rekomendatsii Rady Yevropy No R (95) 13 vid 11 veresnia 1995 roku. *Pravova informatyka*. 2006. № 3(11). S. 96–97.

6. Bolhov V. M., Had N. M. Orhanizatsiino-pravove zabezpechennia protydii kryminalnym pravoporushenniam, shcho vchyniaiutsia z vykorystanniam informatsiinykh tekhnolohii: nauk.-prakt. posib. S. 14–17.

Topchii V., Bodunova O. The System of Criminal Offenses in the Field of Information Technologies: the International Legal Dimension

The article examines the system of criminal offenses in the field of information technologies in accordance with the norms of international law. It is noted that during the last twenty years, the process of forming an information society continues in the world, and therefore computing and information networks are increasingly developing - a unique combination of computers and communications. Every day, modern information technologies are developing more actively in Ukraine as well. Human civilization has entered the era of information at the turn of the millennium. Hundreds of millions of people use the world's computer communications system every day. This provides new opportunities for the development of national culture, education, science and economy.

However, technological progress and the introduction of information technology into all areas of society's life have a negative effect, as it leads to an increase in the number of criminal offenses. It also makes it possible to commit new criminal offenses in unconventional ways.

Especially in the conditions of Russia's full-scale war against Ukraine, the use of information technologies in the commission of criminal offenses is a common phenomenon for the occupiers, which leads to the expansion of the list of criminally illegal acts committed in the field of information technologies.

It was concluded that with the development of technical progress, crime also changes, which acquires new, previously unknown forms. Thus, with the emergence of electronic computing devices in the middle of the 20th century, the concept of crime in this area was necessarily associated with the subject of criminally unlawful influence or the subject of a criminal offense, which is a computer. The combination of computers in the network (local,

global) made it possible to use computers as a means of criminal offense, and cyberspace became the place of its commission.

Considering the above, the universal range of criminal offenses in the field of information relations has not yet been defined in international legal acts. This is due to the dynamic development of crime, the emergence of new types of criminal offenses committed in the field of information technologies. Therefore, the development of a unified criminal strategy related to computer criminal offenses, their concept and system remains an urgent issue today.

***Key words**: crime in the field of information technologies, computer criminal offenses, information society, computer fraud, information networks.*

Стаття надійшла до редколегії 9 січня 2023 року