УДК 343.9
DOI 10.33244/2617-4154.1(10).2023.180-186

Н. А. Лугіна,
канд. юрид. наук, доцент
e-mail: natali.lugina7@gmail.com
ORCID ID 0000-0001-6005-2943;
А. М. Лучук,
здобувач першого (бакалаврського) рівня освіти,
Державний податковий університет
e-mail: luchanas2612@gmail.com
ORCID ID 0000-0001-8229-0571

ПОРІВНЯЛЬНИЙ АНАЛІЗ ВІТЧИЗНЯНОГО ТА ЄВРОПЕЙСЬКОГО ЗАКОНОДАВСТВА З ПИТАНЬ ЗАПОБІГАННЯ КІБЕРЗЛОЧИННОСТІ

У статті розглянуто проблемні аспекти, що виникають під час запобігання кіберзлочинності в Україні. Проаналізовано різні визначення поняття кіберзлочинів, серед яких наведено законодавче визначення поняття «кіберзлочин». Наведено класифікацію кіберзлочинів, надану Будапештською Конвенцією про кіберзлочинність. Зосереджено увагу на національній законодавчій базі, що регулює питання боротьби з кіберзлочинністю та міжнародних нормативно-правових актах з цього питання. Акцентовано увагу на міжнародно-правовому співробітництві в роботі щодо попередження та протидії транскордонним та транснаціональним кіберзлочинам. Встановлено загальні та спеціальні причини неефективності запобіжної діяльності у сфері кіберзлочинності в Україні. Запропоновано шляхи подолання виявлених проблем.

Сьогодні важко сперечатися щодо питання важливості мережі «Інтернет» у нашому житті. Інтернет відкриває перспективи для саморозвитку, отримання нових знань, пошуку роботи тощо. Цей ресурс використовуємо щодня, навіть свій вільний час можемо проводити на його просторах. Але пропри це інтернет має й іншу сторону, ту, в якій щодня, щогодини вчиняються кримінальні правопорушення, адже платформа забезпечує користувачів повною анонімністю та не обмежує їх у своїх діях.

Наприклад, 2018 року в Україні працівники Департаменту кіберполіції Національної поліції України були залучені до більше ніж одинадцяти тисяч кримінальних проваджень, пов'язаних з кримінальними правопорушеннями у сфері новітніх інформаційних технологій. Упродовж року було встановлено, що найбільша кількість протиправних діячів перебуває в Києві, а також на території Одеської, Миколаївської та Львівської областей.

Хоч і всі науковці достатньо ґрунтовно розкривають проблему у своїх дослідженнях, необхідно все ж таки узагальнити накопиченні знання, зануритися у саму історію виникнення та розвитку кіберзлочинності для можливості аналізу дій злочинців відносно розвитку технологій.

Проаналізувавши наукові дослідження та досвід різних країн у боротьбі з таким явищем, можна стверджувати, що ця проблема є чи не найнебезпечнішою у XXI столітті і є нагальна потреба вдосконалення законодавства та проведення роз'яснювальних дій у суспільстві задля подальшого запобігання створенню нових груп кіберзлочинців та розповсюдженню такого явища.

Ключові слова: *запобігання кіберзлочинності, кіберзлочинність в Україні, протидія злочинності, кіберзлочини, зарубіжне законодавство, проблеми протидії кібезлочинності у країнах Європейського Союзу.*

Метою статті є теоретичне дослідження вітчизняного та Європейського законодавства з питань запобігання кіберзлочинності.

Постановка проблеми. Процес становлення України як демократичної, правової, економічної та соціально розвиненої країни супроводжується певними негативними, дестабілізуючими явищами, які притаманні будь-якій державі. Одним з таких явищ виступає поява злочинності, яка являє собою різновид об'єктивно небезпечної поведінки, що несе загрозу для особи, держави, бізнесу і суспільства [1]. Розвиток сучасних комп'ютерних технологій привносить у життя громадян не лише нові прогресивні можливості, але й ряд небезпечних аспектів, які знаходять своє відображення у кіберзлочинності. За допомогою доступу до мережі «Інтернет» були як модифіковані раніше відомі злочини – крадіжки, онлайн-шахрайства, вимагання, розповсюдження дитячої порнографії, так і з'явилися абсолютно нові, раніше не відомі види злочинів – скімінг, фішинг, кардінг, вішинг, шимінг та інші. Зважаючи на те, що кіберзлочини можуть вчинятися на території однієї держави, так і інших держав, до злочинних угруповань можуть входити представники різних національностей, перед міжнародним співтовариством постало питання боротьби з кіберзлочинністю. Характеристика кіберзлочинів як соціальних явищ передбачає їх актуальність для всього суспільства і потребує наявності стратегії держави в усіх сферах запобігання кіберзлочинності.

Виклад основного матеріалу. Що ж саме являє собою кіберзлочин? Думки науковців щодо цього різняться. Так, наприклад, О. Копатін та Є. Скулишин визначають кіберзлочини як злочини, пов'язані з використанням кібернетичних комп'ютерних систем, та злочини у кіберпросторі. Натомість, В. М. Болгов зазначає, що кіберзлочини – це сукупність передбачених чинним законодавством кримінально караних суспільно небезпечних діянь (дій чи бездіяльності), що посягають на право захисту від несанкціонованого поширення і використання інформації, негативних наслідків впливу інформації чи функціонування інформаційних технологій [1].

Законодавче визначення поняття «кіберзлочин» міститься у ст. 1 ЗУ «Про основні засади забезпечення кібербезпеки України», відповідно до якої кіберзлочин

(комп'ютерний злочин) – суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України [1]. Будапештською Конвенцією (Конвенція про кіберзлочинність) було класифіковано кіберзлочини на чотири групи, пізніше був прийнятий Додатковий протокол, тому нині таких груп п'ять. До першої групи віднесено злочини проти доступності, конфіденційності, цілісності комп'ютерних даних і систем (незаконний доступ, незаконне перехоплення, втручання в систему, втручання в дані). Друга група – злочини, пов'язані з використанням комп'ютера як засобу скоєння злочинів (засобу маніпуляцій з інформацією). У цю групу входять комп'ютерне підроблення та комп'ютерне шахрайство. Третя група – злочини, пов'язані з контентом – тобто з вмістом даних, розміщених у комп'ютерних мережах (найпоширеніші серед них – злочини, пов'язані з дитячою порнографією). Четверта група – злочини, пов'язані з порушенням авторського права і суміжних прав (встановлення таких порушень віднесено документом до компетенції національних законодавств держав). П'ята група злочинів зафіксована в окремому протоколі – це вчинені за допомогою комп'ютерних мереж акти расизму та ксенофобії [3].

Завдання профілактики кіберзлочинів вирішується спеціальними державними органами у відповідних формах попереджувальної діяльності, серед яких розробка системи заходів у суспільстві, направлених на попередження злочинності (соціальних, економічних, правових); координація діяльності правоохоронних і громадських організацій у ході реалізації комплексних програм боротьби зі кіберзлочинністю тощо. Суб'єкти запобігання кіберзлочинності мають утворювати цілісну у функціональному й організаційному відношенні систему [3]. Проте статистика вчинюваних кіберзлочинів в Україні доводить, що діяльність із запобігання не є достатньо ефективною. Серед низки проблемних аспектів, які не дозволяють знизити кількість ймовірних кіберзлочинів до мінімуму, можна виділити загальні та спеціальні причини.

До загальних можна віднести такі: по-перше, можливості співробітників правоохоронних органів є достатньо обмеженими через велику завантаженість. Так, наприклад, у жовтні 2021 року було виявлено близько 299 160 кримінальних правопорушень [2, с. 67]. На сьогодні спостерігається тенденція більш активного звернення населення до правоохоронних і судових органів за відновленням порушених прав та отриманням компенсації за заподіяну шкоду [3]. Працівники уповноважених органів ледве встигають займатися звичними злочинами, не говорячи про вже про кіберзлочинність.

Щодо спеціальних причин, які є характерними саме для запобігання кібезлочинам, по-перше, технічне оснащення органів та спеціалістів не відповідає належному рівню. Водночас як кіберзлочинці використовують найновітніші технології під час вчинення протиправних дій, запобіжна та розслідувальна діяльність здійснюється на застарілих комп'ютерах та іншій техніці.

По-друге, оскільки кіберзлочинність зазвичай має міжнародний характер і може вчинюватися особами різних національностей і з території різних держав, досить важливого значення набуває міжнародне співробітництво. Європейським Союзом, крім

раніше названих, прийняті інші акти, що регулюють питання боротьби з кіберзлочинністю – Директива про боротьбу із сексуальною експлуатацією дітей в інтернеті та дитячою порнографією (2011 рік), Пропозиція про тимчасове регулювання обробки персональних та інших даних з метою боротьби із сексуальним насильством над дітьми (2020 рік) та інші. Крім того, з метою об'єднання європейської експертизи в галузі кіберзлочинності для підтримки розслідувань з питань кіберзлочинності Європолом був створений ключовий орган боротьби з кіберзлочинністю в ЄС – Європейський центр з кіберзлочинності. Незважаючи на те, що Україною було ратифіковано ряд міжнародних договорів, що гарантують співробітництво у боротьбі з кіберзлочинністю, на практиці взаємодія з іншими країнами зумовлює значну кількість бюрократичних процедур, які уповільнюють процес запобігання кіберзлочинам [4].

По-третє, відсутність значних успіхів у боротьбі з кіберзлочинністю пояснюється низьким рівнем комп'ютерної грамотності населення через обмежений доступ до інтернет-комунікацій. Так, за даними Міністерства цифрової трансформації, 4 мільйони українців живуть у населених пунктах, де немає жодного інтернет-провайдера. Ще 1,5 млн українців проживають на околицях населених пунктів, де провайдери є, але вартість підключення занадто дорога і часто перевищує кілька тисяч гривень. Усього понад 17 тисяч населених пунктів в Україні не мають інтернет-інфраструктури [6]. Недостатній рівень знань у галузі інформаційних технологій робить значну частку населення нашої країни вразливими перед злочинцями, які використовують новітні інформаційні досягнення та кіберзлочинцями.

Кіберзлочинність – один з найпоширеніших видів злочинності не тільки в Україні, а й в інших куточках світу. Майже кожен у світі чув про кіберзлочинність і навіть стикався з нею особисто. Кіберзлочинність охоплює різні види злочинів, скоєних за допомогою комп'ютерів та інтернету. З огляду на стрімкий цифровий розвиток суспільства виникає потреба у створенні ефективного механізму захисту персональних даних в інтернеті [5].

Згідно з дослідженнями «Лабораторії Касперського» в реальному часі багато країн світу щодня зазнають численних кібератак. Більшість кібератак було здійснено в таких країнах, як Франція, Німеччина, Бразилія, США та Китай [7].

Варто зазначити, що у країнах ЄС активно створюються спеціальні органи з боротьби з кіберзлочинністю. Загалом ці органи можна розділити на дві групи. Першу групу складають органи, які займаються розробкою та реалізацією національних стратегій боротьби з кіберзлочинністю. Другу – складають суб'єкти, які запобігають і розслідують злочини, скоєні у кіберпросторі.

Стратегія кібербезпеки ЄС була прийнята в 2013 році. Її характеристика полягає в тому, що стратегія охоплює різні аспекти кіберпростору, включаючи внутрішній ринок, судову систему, а також внутрішню та зовнішню політику. Разом зі стратегією розроблено та прийнято законодавчу пропозицію щодо посилення безпеки інформаційних систем ЄС. Пріоритетами міжнародної політики ЄС у кіберпросторі є:

– свобода та відкритість: стратегія визначає принципи реалізації основних прав людини та громадянина у кіберпросторі;

– застосування законодавства ЄС у кіберпросторі тією ж мірою, що й у фізичному світі. Відповідальність за безпеку кіберпростору несе суспільство в цілому: від звичайних громадян до всієї держави;

– розвиток потенціалу кібербезпеки через співпрацю з міжнародними партнерами та організаціями, приватним сектором і громадянським суспільством.

Для посилення кібербезпеки Європейського Союзу у вересні 2017 року Європейська комісія запропонувала пакет заходів, включаючи створення Агентства ЄС з кібербезпеки та запровадження сертифікатів на цифрові продукти та послуги, вироблені в ЄС. Сьогодні це агентство успішно діє у країнах – членах ЄС. Відповідно до стратегії ЄС Агентство ЄС з кібербезпеки також базується на прийнятій Директиві ЄС щодо інформаційної безпеки [8]. У рамках директиви ЄС було створено Групу реагування на кіберінциденти як групу стратегічного співробітництва, в якій країни-члени ЄС співпрацюють, обмінюються інформацією та домовляються про те, як директиву слід послідовно впроваджувати в ЄС. Група реагування на кіберінциденти також надає стратегічні рекомендації центральній мережі CSIRT ЄС. До групи реагування на кіберінциденти входять представники відповідних національних міністерств та національних органів кібербезпеки.

Висновки. Отже, кіберзлочин – це кримінально карана діяльність, вчинена із застосуванням комп'ютера, пристрою із мережевим з'єднанням або інтернет-мережі. У середовищі, де постійно виникають і розвиваються кіберзагрози, залишатися беззахисним неможливо, саме тому поточна ситуація у світі вимагає постійного вдосконалення методів боротьби з кіберзлочинністю та спонукає до побудови державної моделі забезпечення кібербезпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Кількість кіберзлочинів в Україні зросла вдвічі за останні п'ять років – Opendatabot. URL: https://mind. ua/news/20203511-kilkist-kiberzlochiniv-v-ukrayini-zrosla-vdvichi-za-ostanni-p-yat-rokiv-opendatabot (дата звернення: 14.09.2022).

2. Дручек О. В. Профайлінг як метод забезпечення державної безпеки і громадського порядку: проблеми застосування. *Науковий вісник публічного та приватного права*. К., 2018. С. 132–136.

3. Про Національну поліцію: Закон України від 02.07.2015 № 580-VIII. *Відомості Верховної Ради України*. 2015. № 40–41. С. 379.

4. Про ратифікацію Конвенції про кіберзлочинність: Закон України від 07.09.2005 № 2824-IV. *Відомості Верховної Ради України*. 2006. № 5, 5–6. С. 128, 71.

5. Офіційний сайт кіберполіції України. URL: https://cyberpolice.gov.ua/contacts/ (дата звернення: 21.09.2022).

6. Про оперативно-розшукову діяльність: Закон України від 18.02.1992 № 2135-XII. *Відомості Верховної Ради України.* 1992. № 22. Ст. 303.

7. Елементи для створення глобальної культури кібербезпеки від 20 грудня 2002 р. URL: http://zakon.rada.gov.ua/laws/show/995_b42

8. Савчук Н. В. Світовий досвід державного регулювання ринку інтернет-послуг. *Формування ринкових відносин в Україні*. 2012. № 4. С. 24–28.

REFERENCES

1. Kil`kist` kiberzlochy`niv v Ukrayini zrosla vdvichi za ostanni pyat` rokiv – Opendatabot [The number of cybercrimes in Ukraine has doubled in the last five years]. URL: https://mind.ua/ news/20203511-kilkist-kiberzlochiniv-v-ukrayini-zrosla-vdvichi-za-ostanni-p-yat-rokiv-opendatabot [in Ukr.].

2. Druchek, O. V. (2018). Profajling yak metod zabezpechennya derzhavnoyi bezpeky` i gromads`kogo poryadku: problemy` zastosuvannya [Profiling is a method of securing state security and a public order: problems of application]. *Naukovyi visnyk publichnogo ta pry`vatnogo prava* (Scientific Bulletin of Public and Private Law), 132–136 [in Ukr.].

3. Pro Natsionalnu politsiiu: Zakon Ukrainy vid 02.07.2015 № 580-VIII [On the National Police: Law of Ukraine No. 580-VIII of July 02, 2015]. *Vidomosti Verkhovnoi Rady Ukrainy* (Bulletin of the Verkhovna Rada of Ukraine), 40–41, Art. 379 [in Ukr.].

4. Pro ratyfikatsiiu Konventsii pro kiberzlochynnist [Ratification of the Convention on Cybercrime: Law of Ukraine] vid 07.09.2005 № 2824-IV. *Vidomosti Verkhovnoi Rady Ukrainy* (Bulletin of the Verkhovna Rada of Ukraine), 5. St. 71 [in Ukr.].

5. Oficijny`j sajt kiberpoliciyi Ukrayiny` [Official site of the cyberpolice of Ukraine]. URL: https:// cyberpolice.gov.ua/contacts/ [in Ukr.].

6. Pro operatyvno-rozshukovu diialnist: Zakon Ukrainy vid 18 liutoho 1992 roku № 2135-XII [On search operations: Law of Ukraine]. *Vidomosti Verkhovnoi Rady Ukrainy* (Bulletin of the Verkhovna Rada of Ukraine), 22. St. 303 [in Ukr.].

7. Elementy dlia stvorennia hlobal'noi kul'tury kiberbezpeky vid 20 hrudnia 2002 r. URL: http://zakon.rada.gov.ua/laws/show/995_b42

8. Savchuk, N. V. (2012). Svitovyi dosvid derzhavnoho rehuliuvannia rynku internet-posluh [The World experience of state regulation of the market of Internet-services]. *Formuvannia rynkovykh vidnosyn v Ukraini* [The formation of market relations in Ukraine], no, 4, 24–28 [in Ukrainian].

N. Luhina, A. Luchuk. Comparative Analysis of Domestic and European Legislation on Cybercrime Prevention

This article examines problematic aspects that arise during the prevention of cybercrime in Ukraine. Various definitions of the concept of cybercrime are considered, among which the legislative definition of the concept of "cybercrime" is given. The classification of cybercrimes provided by the Budapest Convention on Cybercrime is presented. Attention is focused on the national legislative framework that regulates the fight against cybercrime and international legal acts on this issue. Attention is focused on international legal cooperation in the prevention and counteraction of cross-border and transnational cybercrimes. The general and special reasons for the ineffectiveness of preventive activities in the field of cybercrime in Ukraine have been established. Ways to overcome the identified problems are proposed.

Today it is difficult to argue about the importance of the Internet in our lives. The Internet opens up prospects for self-development, gaining new knowledge, finding a job, etc. We use this resource every day, we can even spend our free time on its spaces. But, despite this, the Internet has another side, the one in which criminal offenses are committed every day, every hour, because the platform provides users with complete anonymity and does not limit their actions.

For example, in 2018, in Ukraine, employees of the Cyber Police Department of the National Police of Ukraine were involved in more than eleven thousand criminal proceedings related to criminal offenses in the field of the latest information technologies. During the year, it was established that the largest number of illegal actors is located in Kyiv, as well as in the Odesa, Mykolaiv, and Lviv regions.

Although all scientists sufficiently thoroughly reveal the problem in their research, it is still necessary to generalize the accumulated knowledge, to dive into the very history of the emergence and development of cybercrime in order to analyze the actions of criminals in relation to the development of technologies.

Having analyzed scientific research and the experience of various countries in the fight against this phenomenon, it can be stated that this problem is almost the most dangerous in the 21st century and there is an urgent need to improve legislation and carry out explanatory actions in society, in order to further prevent the creation of new groups of cybercriminals and spread of this phenomenon.

***Key words**: prevention of cybercrime, cybercrime in Ukraine, combating crime, cybercrime, foreign legislation, problems of combating cybercrime in the countries of the European Union.*

Стаття надійшла до редколегії 4 січня 2023 року