УДК 343.9
DOI https://doi.org/10.32782/apdp.v96.2022.4

Т. Д. Лисько, В. В. Меланіч, Ю. В. Славіта

ПРОТИДІЯ КІБЕРЗЛОЧИННОСТІ: СУЧАСНИЙ СТАН ВІТЧИЗНЯНОГО ЗАКОНОДАВСТВА ТА ДОСВІД ЗАРУБІЖНИХ КРАЇН

Постановка проблеми. Сучасні світові тенденції розвитку кіберзлочинності та її збільшення свідчать про зростання значення боротьби з нею. Це зумовлює віднесення окремих груп суспільних відносин у кіберсфері до компетенції правового регулювання. Ці питання є особливо актуальними з точки зору забезпечення національної безпеки та, відповідно, надання суспільно небезпечним діям статусу кримінальних правопорушень у кіберсфері та встановлення за їх вчинення кримінальної відповідальності. Слід констатувати, що Україна наразі слабо залучена в процес боротьби з кіберзлочинністю і вразлива до атак у сфері інформаційної безпеки. Важливість протидії використанню комп'ютерних технологій у кримінальній протиправній діяльності на даному етапі розвитку української держави не викликає сумнівів. Крім того, загрозою демократичним перетворенням в Україні та її національній безпеці є ступінь комп'ютеризації та одночасно можливості, які відкриваються злочинцям, а також тенденція до зростання кількості кримінальних правопорушень у сфері комп'ютерних інформаційних технологій.

Аналіз останніх досліджень і публікацій. Тенденції розвитку та протидії кіберзлочинності останнім часом викликають інтерес як у науковців, так і в практиків. Вони знайшли відображення в працях таких учених як М.В. Гуцалюк, М.О. Кравцова, В.В. Марков, А.І. Марущак, Є.Д. Скулиш, О.В. Таволжанський та ін. Тим не менше, все ще існує потреба в дослідженнях, щоб отримати цілісне бачення цієї проблеми.

Метою статті є дослідження перспектив розвитку кіберзлочинності. Зокрема, ставимо за мету визначити правову природу кіберзлочинності, специфіку цієї категорії у вітчизняній та світовій науці. Виходячи з цього, необхідно визначити основні причини та прояви, а також відповідні контрзаходи.

Виклад основного матеріалу дослідження. На сучасному етапі розвитку людського суспільства інформація є важливим стратегічним ресурсом, який потребує захисту. Все частіше вона стає об'єктом кримінальних протиправних посягань. Комплексне і широкомасштабне використання інформаційних технологій на основі персональних комп'ютерів, інформаційно-обчислювальних мереж і комп'ютерних систем зв'язку відкрило людству шлях до нового етапу розвитку – етапу інформаційного суспільства. Наслідком цього є поява нового виду злочинності – комп'ютерної або кіберзлочинності [1, с. 108].

Використання сучасних інформаційних технологій здійснюється сьогодні практично в усіх сферах суспільного життя, включаючи державні та недержавні структури, що висуває проблему боротьби з кіберзлочинністю на перший план. Окрім прямої шкоди від несанкціонованого доступу до інформації, її поширення,

зміни, знищення тощо, кіберзлочинність є джерелом загроз національній безпеці, бізнесу, правам та інтересам людини. Тому вітчизняним законотворцям та дослідникам варто враховувати досвід України та передових країн світу, оскільки це є свідченням існування такої загрози в майбутньому для будь-якої країни світу.

У Законі України "Про основні засади забезпечення кібербезпеки України" під кіберзлочинністю розуміється сукупність кіберзлочинів, а кіберзлочин (комп'ютерний злочин) – суспільно небезпечна злочинна діяльність у кіберпросторі та/або при його використанні, за яку настає відповідальність, передбачена Законом України про кримінальну відповідальність та/або визнана кримінальним правопорушенням міжнародними договорами України [2].

Термін «кіберзлочинність» охоплює коло кримінальних правопорушень у віртуальному середовищі та регулюється міжнародним правом [3, с. 332-337]. Кіберзлочинність – це злочинність у так званому «віртуальному просторі». Віртуальний простір можна визначити як комп'ютерно змодельований простір, у якому інформація про людей, об'єкти, факти, події, явища та процеси, оброблена локальними та глобальними комп'ютерними мережами, представлена в математичній, символічній чи іншій формах. Це відомості, що зберігаються в пам'яті фізичного або віртуального пристрою, а також інші носії, спеціально призначені для їх зберігання, обробки та передачі.

Відповідно до Конвенції про кіберзлочинність [4], кіберзлочини поділяються на такі категорії:

1) злочини проти конфіденційності, цілісності та доступності комп'ютерних даних і систем. До них належать:

– незаконний доступ під яким слід розуміти навмисний несанкціонований доступ до всієї комп'ютерної системи чи її частини з метою отримання комп'ютерних даних або з будь-якою іншою недобросовісною метою;

– підробка даних, навмисне пошкодження, знищення, фальсифікація, зміна або приховування комп'ютерної інформації без права на це;

– втручання в систему, тобто умисне втручання у функціонування комп'ютерної системи шляхом введення, передачі, пошкодження, знищення, погіршення, підміни або приховування комп'ютерних даних без права на це;

– використовувати пристроїв не за призначенням, а саме їх виготовлення, продаж, придбання для використання, розповсюдження або надання для використання іншим чином;

2) правопорушення, пов'язані з інформаційним змістом, зокрема дитячою порнографією, расизмом і ксенофобією;

3) злочини, пов'язані з використанням комп'ютерів, включаючи підробку та шахрайство, вчинені з використанням комп'ютерів;

4) кримінальні правопорушення, пов'язані з порушенням авторського права і суміжних прав, наприклад незаконне тиражування та використання комп'ютерних програм.

Стратегія державних підходів і механізмів удосконалення інформаційних систем покликана сприяти зменшенню масштабів кіберзлочинності та закласти основні положення національної політики протидії кіберзлочинності в міжнародному

кіберпросторі. Враховуючи міжнародний характер кіберзлочинності, гармонізація національного законодавства є ключовою для боротьби з нею. Проте при гармонізації необхідно враховувати регіональні вимоги та можливості. Важливість регіональних аспектів у реалізації стратегій боротьби з кіберзлочинністю підкреслює той факт, що багато правових і технічних стандартів були узгоджені між країнами світу. Глобальна програма кібербезпеки базується на п'яти основних принципах: 1) юридичний позов; 2) техніко-процедурні заходи; 3) організаційні структури; 4) створити потенціал; 5) міжнародне співробітництво. Зрозуміло, що українська система державних механізмів боротьби з кіберзлочинністю має застосовувати всі ці принципи.

Дуже важливо розуміти глобальний характер проблеми кіберзлочинності. Так, кібератаки вже зараз паралізують роботу не лише приватних структур, а й державних органів. Немає жодної країни у світі, яка була б захищена від таких атак.

При розробці засобів і методів боротьби з кіберзлочинністю слід враховувати латентність цього виду злочинності. За оцінками експертів, латентність «комп'ютерних злочинів» у США сягає 80%, у Великобританії – 85%, у Німеччині – 75%, в Україні – понад 90% [5]. За даними Symantec Security, міжнародної служби захисту від кіберзагроз, 12 людей у всьому світі стають жертвами кібератак щосекунди, і щороку в усьому світі реєструється близько 556 мільйонів кіберзлочинів, збитки від яких складають понад 100 мільярдів доларів. США [6, с. 46].

Кіберзлочинність може завдати шкоди інтересам як держави, так і конкретної людини. Безумовно, специфіка функціонування інформаційних систем, особливо Інтернету, вимагає об'єднання зусиль різних державних і приватних суб'єктів [7, с. 11], для вирішення найактуальніший проблем кібербезпеки, але саме держава повинна і здатна здійснювати комплексні заходи протидії вчиненню кіберзлочинів, створювати умови захисту для тих, хто є найбільш уразливим перед атаками кіберзлочинців (наприклад, банки, фізичні особи) та зосереджувати зусилля на створенні більш надійної системи захисту інформації.

Наразі провідні країни світу активно розширюють та створюють у збройних силах та спецслужбах підрозділи, покликані забезпечити розвиток наступальних можливостей у кіберпросторі. Так, у США, крім уже діючого Центру національної кібербезпеки (National Cyber Security Center), було сформовано Об'єднане кіберкомандування (Unified US Cyber Command) у складі збройних сил, яке на глобальному рівні має координувати зусилля всіх структур Пентагону під час бойових дій, надавати відповідну підтримку цивільним федеральним установам, а також взаємодіяти з аналогічними за завданнями відомствами інших [8]. Водночас ці організації є частково підконтрольними відомствами, оскільки вищим керівним органом є Рада національної безпеки зі спеціальним 60 комітетом, до сфери відповідальності якого входить реалізація інформаційної стратегії [9, с. 239], у тому числі боротьба з кіберзлочинністю.

У Великій Британії реалізуються програми зі створення кіберзброї, щоб забезпечити стійкість уряду проти зростаючих кіберзагроз [10].

В Австралії створено координаційну групу безпеки електронної пошти (ESCG). Основним завданням цієї групи є створення надійного електронного робочого простору як для державного, так і для приватного секторів [11, с. 84].

Для ефективної боротьби з кіберзлочинністю в Україні, за прикладом іноземних держав, необхідно: створити політичну основу (концептуальний рівень), удосконалити законодавчу систему (законодавчий рівень), створити систему органів, основними якими є функції полягають у забезпеченні захисту України від кіберзлочинності [12, с. 54]. У 2016 році було зроблено перші кроки до розробки політичної основи та тематичної системи забезпечення кібербезпеки. Зокрема, на концептуальному та інституційному рівні у березні 2016 року Уряд України затвердив Стратегію кібербезпеки України, метою якої було створення національної системи кібербезпеки; у червні 2016 року Президент України підписав Указ про створення Національного координаційного центру з кібербезпеки. Першим етапом його роботи був аналіз і розробка галузевих індикаторів стану кібербезпеки; у вересні 2016 року Верховна Рада України прийняла в першому читанні Закон «Про Основи забезпечення кібербезпеки України» [13, с. 124].

Вважаємо, що в новій Стратегії слід врахувати основні стратегічні принципи, визначені у Стратегії національної безпеки України на 2020 рік (ст. 4) – стримування, стабільність та взаємодія [14]. Згідно зі Стратегією, подальший розвиток національної системи кібербезпеки на засадах стримування, кіберпротистояння та взаємодії передбачає посилення спроможності національної системи кібербезпеки запобігати збройній агресії проти України в кіберпросторі або використовувати її для нейтралізації спецслужб та підривної діяльності, а також для мінімізації загроз кіберзлочинності та кібертероризму [15].

Висновки. Отже, слід зазначити, що кіберзлочинність сьогодні є суттєвою загрозою інформаційній безпеці України. Окрім змін у кримінальному законодавстві, комплексна боротьба з кіберзлочинністю потребує гармонізації національного кримінального законодавства про кіберзлочинність із міжнародним, що позитивно вплине на стан боротьби та запобігання кіберзлочинності; якнайшвидшої імплементації положення Конвенції про кіберзлочинність, призначивши орган для цілодобового прийому запитів і повідомлень про кіберзлочини та надання негайної допомоги в розслідуванні або переслідуванні таких кримінальних правопорушень; налагодження взаємодії вітчизняних правоохоронних органів з правоохоронними органами інших держав; підвищення рівня знань працівників оперативних підрозділів, працівників органів слідства, прокуратури, суддів у сфері інформаційних технологій та кібербезпеки, особливо в сферах збирання та дослідження електронних доказів, як це передбачено положеннями згадуваної Стратегії.

Зважаючи на негативні наслідки кіберзлочинності та світові тенденції, на сьогодні залишається актуальним подальше вдосконалення за основними напрямами боротьби з нею. Вважаємо, що це суттєво підвищить ефективність та результативність протидії зазначеним кримінальним правопорушенням та сприятиме захисту інформаційної безпеки, особливо в умовах розвитку інформаційного суспільства та цифрової держави.

Література

1. Марков В.В. До питання щодо зарубіжного досвіду протидії кіберзлочинності. *Право і безпека*. 2015. № 2(57). С. 107–113.

2. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 р. № 2163-VIII : станом на 17 серп. 2022 р. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 21.12.2022).

3. Голіна В.В., Головкін Б.М. Кримінологія: Загальна та Особлива частини : навчальний посібник. Х. : Право, 2014. 513 с.

4. Конвенція про кіберзлочинність : Конвенція Ради Європи від 23.11.2001 р. : станом на 7 верес. 2005 р. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text (дата звернення: 21.12.2022).

5. Рівень проникнення Інтернету в світі за станом на вересень 2018 року з розбивкою по регіонах. Statista. URL: https://www.statista.com/statistics/269329/penetration-rate-of-the-internetbyregion/ (дата звернення: 13.12.2022).

6. Бельський Ю. Щодо визначення поняття кіберзлочину. *Юридичний вісник*. 2014. № 6. С. 414–418.

7. Роговець В. Інформаційні війни в сучасному світі: причини, механізми, наслідки. *Персонал.* 2015. № 5. С. 10–17.

8. Department of Defense: Report on Strategic Communication. URL: http://www.au.af.mil/au/awc/awcgate/dod/dod_report_strategic_communication_1 1feb10.pdf (дата звернення: 13.12.2022).

9. Djerf-Pierre Monika. Squaring the Circle: Public Service and Cmmercial News on Swedish Television. *Journalism Studies*. 2018. 1(2). P. 239–260.

10. Kessel J. M. and Mozur P. How China Is Changing Your Internet. New York Times. 2016. URL: https://www.nytimes.com/video/technology/100000004574648/chinainternetwechat.html (дата звернення: 13.12.2022).

11. Sanders Karen, Canel Crespo María José and Holtz-Bacha Christina. Communicating Governments: A Three-Country Comparison of How Governments Communicate with Citizens. *The International Journal of Press/Politics*. 2017. 16(4). 547 p.

12. Бутузов В. Протидія комп'ютерній злочинності в Україні (системно-структурний аналіз): монографія. Київ : КИТ, 2010. 148 с.

13. Голубєв В.О. Розслідування комп'ютерних злочинів: монографія. Запоріжжя : Гуманітарний університет "ІДМУ", 2003. 296 с.

14. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України" : Указ Президента України від 26.08.21 р. № 447. URL: https://www.president.gov.ua/documents/4472021-40013 (дата звернення: 13.12.2022).

15. Про затвердження плану заходів на 2017 рік з реалізації Стратегії кібербезпеки України: Розпорядження Кабінету Міністрів України від 10.03.17 р. № 155-р. URL: https://zakon. rada.gov.ua/laws/show/155-2017-%D1%80#Text (дата звернення: 13.12.2022).

Анотація

Лисько Т. Д., Меланіч В. В., Славіта Ю. В. **Перспективи (тенденції) розвитку та заходи протидії кіберзлочинності.** – Стаття.

Сучасні світові тенденції розвитку кіберзлочинності та їх активізація свідчать про зростання значення боротьби з нею для подальшого розвитку суспільства, що в свою чергу зумовлює віднесення окремих груп суспільних відносин у кіберсфері до сфери правового регулювання. Дана проблема є особливо актуальною з точки зору забезпечення національної безпеки та, відповідно, суспільно небезпечних дій, які мають набувати статусу кримінальних правопорушень у кіберсфері та тягти за собою відповідну кримінальну відповідальність. Зважаючи на зростання кількості кібератак, необхідно не лише вивчити світові тенденції розвитку кіберзлочинності, створити ефективне нормативно-правове забезпечення, а й запровадити систему заходів із запобігання та захисту від кіберзлочинності.

Стаття присвячена дослідженню тенденцій розвитку кіберзлочинності, яка становить загрозу інформаційній безпеці країни. Визначено місце та роль кібербезпеки в системі національної безпеки. Надано рекомендації щодо вдосконалення системи захисту та боротьби з кіберзлочинністю. У статті визначено необхідність забезпечення інформаційної безпеки, яка визначається відповідними факторами. Зазначається, що комплексна боротьба з кіберзлочинністю потребує певних заходів, зокрема гармонізації національного кримінального законодавства про кіберзлочинність із міжнародним, імплементації окремих положень Конвенції про кіберзлочинність та налагодження взаємодії між правоохоронними органами України та правоохоронними органами інших країн для покращення обміну інформацією з метою ефективної протидії кіберзлочинності.

Ключові слова: кібербезпека, інформаційна безпека, кіберзлочинність, кіберпростір, комп'ютерна злочинність, протидія, законодавство.

Summary

Lysko T. D., Melanich V. V., Slavita Yu. V. **Combating cybercrime: the current state of domestic legislation and the experience of foreign countries.** – Article.

Modern world trends in the development of cybercrime and their intensification testify to the growing importance of combating it for the further development of society, which in turn determines the assignment of certain groups of social relations in the cyber sphere to the competence of legal regulation. This problem is particularly relevant from the point of view of ensuring national security and, accordingly, socially dangerous actions, which should acquire the status of criminal offenses in the cyber sphere and entail the corresponding legal responsibility. Considering the growing number of cyberattacks, it is necessary not only to study the global trends in the development of cybercrime, to create effective regulatory and legal support, but also to introduce a system of measures to prevent and protect against cybercrime.

The article is devoted to the study of trends in the development of cybercrime, which poses a threat to the information security of the country. The place and role of cyber security in the national security system is defined. Recommendations on improving the system of protection and combating cybercrime are provided. The article defines the need to ensure information security, which is determined by relevant factors. It is noted that the comprehensive fight against cybercrime requires certain measures, in particular, the harmonization of national criminal legislation on cybercrime with the international one, the implementation of certain provisions of the Convention on Cybercrime and the establishment of interaction between national legislation. law enforcement agencies and law enforcement agencies of other countries and to improve the exchange of information between law enforcement agencies.

Key words: cyber security, information security, cyber crime, cyber space, computer crime, countermeasures, legislation.