РОЗДІЛ 8
КРИМІНАЛЬНЕ ПРАВО ТА КРИМІНОЛОГІЯ; КРИМІНАЛЬНО-ВИКОНАВЧЕ ПРАВО

УДК 343.2
DOI https://doi.org/10.32782/2307-3322/2020.60.30

БОРОТЬБА З КІБЕРЗЛОЧИННІСТЮ: НАПРЯМИ ВДОСКОНАЛЕННЯ КРИМІНАЛЬНОГО ЗАКОНОДАВСТВА УКРАЇНИ

COMBATING CYBERCRIME: DIRECTIONS FOR IMPROVING THE CRIMINAL LEGISLATION OF UKRAINE

Гладка Н.М.,
кандидат юридичних наук (доктор філософії),
завідувач кафедри загальних дисциплін
Вінницького навчально-наукового інституту
Університету державної фіскальної служби України

Стаття присвячена розгляду актуальних проблем удосконалення кримінального закону України в частині відповідальності за злочини, які вчиняються у кіберпросторі. Статистичні дані свідчать, що кіберзлочинність набирає вкрай загрозливих масштабів як для світового співтовариства, так і для України. У зв'язку зі значним поширенням кіберзлочинності, виникненням нових форм і видів протиправних діянь, які вчиняються у кіберпросторі, зростанням масштабів завданих збитків, значною небезпекою для суспільства досить актуальною є проблема реформування та вдосконалення кримінального закону в частині відповідальності за злочини, які вчиняються у кіберпросторі.

Проаналізувавши основні положення кримінального закону, автор наголошує на тому, що чинна вітчизняна нормативно-правова база лише частково задовольняє потреби часу та не завжди охоплює всі ключові елементи, необхідні для ефективної протидії кіберзлочинам усіх рівнів складності. Автором охарактеризовано найпоширеніші злочини, які здійснюються у кіберпросторі (хакінг, шахрайські операції з криптовалютою, крадіжка даних, інформації, інтелектуальної власності, торгівля людьми, продаж зброї, наркотиків тощо), наведено приклади відносно нових суспільно небезпечних діянь, таких як тролінг, віртуальний мобінг, кіберпереслідування, фармінг.

Автор наголошує на необхідності здійснення цілеспрямованої роботи з удосконалення законодавства в частині відповідальності за злочини, які вчиняються у кіберпросторі, із залученням фахівців у сфері інформаційних технологій у взаємодії та координації зусиль науковців, представників правоохоронних органів, спецслужб, судової системи у боротьбі з кіберзлочинністю.

Ключові слова: кіберзлочин, кіберзлочинність, злочини у сфері інформаційно-комунікаційних технологій, кіберзлочинець, кіберпростір, боротьба з кіберзлочинністю.

The article is devoted to the overview of current directions of improvement of the criminal law of Ukraine in the part of responsibility for crimes committed in cyberspace. Statistics show that cybercrime is gaining enormous proportions both for the international community and for Ukraine. Due to the widespread cybercrime, the emergence of new forms and types of wrongdoing committed in cyberspace, the increasing scale of damage caused, the problem of reforming and improving the criminal law in relation to criminal offenses committed in cybercrime is quite relevant to society. .

The legal basis for combating cybercrime in Ukraine consists of international normative acts, the Constitution of Ukraine, the Criminal Code of Ukraine, the Laws of Ukraine "On the basic principles of cybersecurity of Ukraine", "On information", "On protection of information in information and telecommunication systems", "On the basics national security" and other regulations. Analysing the main provisions of the criminal law, the author emphasizes that the current domestic regulatory framework only partially meets the needs of the time and does not always cover all the key elements necessary to effectively counter cybercrime at all levels of complexity.

The author describes the most common crimes committed in cyberspace (hacking, cryptocurrency fraud, data theft, data leakage, manipulation of data, information or intellectual property, human trafficking, sale of weapons, drugs, etc.). such as trolling, virtual mobbing, cyber-harassment, phasing, and more. The author emphasizes the necessity of purposeful work of improving the legislation in part with regard to responsibility for crimes committed in cyberspace with the involvement of specialists in the field of information technology, and considers that one of the priority areas is the organization of interaction and coordination of efforts of law enforcement agencies and special forces in fighting cybercrime.

Key words: cybercrime, crimes in the field of information and communication technologies, cyberspace, fight against cybercrime.

Постановка проблеми. У світі вчиняється значна кількість злочинів у кіберпросторі з використанням інформаційно-комунікаційних технологій, програмних, програмно-апаратних засобів, інших технічних і технологічних засобів та обладнання. Інформаційно-комунікаційні технології впроваджуються і розвиваються набагато швидше, ніж законодавці та правоохоронні органи можуть на це реагувати. Кількість кіберзлочинів щороку зростає, тож боротьба з кіберзлочинністю – одна з найактуальніших проблем, яка гостро стоїть перед усією світовою спільнотою, в тому числі і перед Україною.

Статистичні дані українських правоохоронних органів свідчать про те, що в нашій державі вчиняються всі основні кіберзлочини (шахрайство, несанкціонований доступ до персональної інформації користувачів та автоматизованих баз даних, поширення порнографії, продаж зброї чи наркотиків тощо), і щороку їх кількість зростає. Крім того, кількість виявлених кіберзлочинів в Україні збільшується в середньому на 2,5 тисячі кожного року [4]. Так, протягом 2018 року працівники Національної поліції були залучені до розслідування 11 тисяч кримінальних проваджень, виявили 6 тисяч злочинів, вчинених у сфері використання високих інформаційних технологій (з них 2398 – у сфері платіжних систем, 1598 – у сфері е-комерції, 1325 – у сфері кібербезпеки) [7]. Держава не завжди реально обізнана з масштабами кіберзлочинності, адже більшість таких злочинів залишаються незафіксованими та не публікуються в офіційних звітах державних органів.

Слід зазначити, що для боротьби з кіберзлочинністю одним із найважливіших інструментів є законодавче врегулювання правових механізмів попередження кіберзлочинності, виявлення та розслідування кіберзлочинів. Тож перед українським законодавцем постає дуже важливе завдання – удосконалити кримінальний закон для приведення у відповідність із міжнародними нормативно-правовими документами та врахувати виклики сучасного суспільства.

Аналіз останніх досліджень і публікацій. Проблема правового регулювання боротьби з кіберзлочинністю в Україні є однією із першочергових. Питання правового регулювання боротьби із кіберзлочинністю розглядали такі вчені, як О. Амелін, М. Гуцалюк, В. Бурячок, А. Войціховський, В. Гавловський, Р. Джансараєва, В. Дзюндзюк, Д. Дубов, О. Користін, М. Кравцова, С. Демедюк, М. Літвінов, Р. Лук'янчук, В. Пилипчук, М. Погорецький, В. Хахановський та інші. У зв'язку зі значним поширенням кіберзлочинності, виникненням нових форм і видів протиправних діянь, які вчиняються у кіберпросторі, зростанням масштабів завданих збитків значною небезпекою для суспільства й досить актуальною є проблема реформування та вдосконалення кримінального закону в частині відповідальності за злочини, які вчиняються у кіберпросторі.

Мета статті – здійснити аналіз положень кримінального закону України в частині відповідальності за злочини, які вчиняються у кіберпросторі, та визначити напрями вдосконалення чинного законодавства.

Виклад основного матеріалу. Кіберзлочинність пов'язана із появою та поширенням глобальної мережі Інтернет, розвитком новітніх інформаційних технологій, інформаційно-телекомунікаційних систем. Особлива природа інтернету забезпечує глобальність і відносну анонімність для її користувачів, що сприяє швидкому поширенню протиправних діянь в інформаційній мережі. Зі значним поширенням кіберзлочинів виникає потреба вдосконалення правового регулювання боротьби з кіберзлочинністю.

Масштаби світової кіберзлочинності вражають. Наприклад, за прогнозами Cybersecurity Ventures (однієї з провідних компаній США, яка займається дослідженнями у сфері електронної комерції), збитки від кіберзлочинності до 2021 року будуть коштувати світу 6 трильйонів доларів щорічно [1]. За даними компаній Bromium і McGuire доходи від кіберзлочинності у всьому світі становили не менше 1,5 трильйонів доларів у 2018 році (з них 860 мільярдів доларів принесли злочинцям незаконні / нелегальні інтернет-платформи, 500 мільярдів доларів – крадіжки комерційної таємниці, 160 мільярдів доларів – торгівля даними, 1,6 мільярда доларів – зловмисне програмне забезпечення тощо).

Кіберзлочинність завдає значних збитків і нашій державі. Так, хакерська атака у червні 2017 року, яка здійснювалася за допомогою вірусної програми "Petya.A", порушила роботу багатьох стратегічних українських державних і приватних підприємств, зокрема аеропорту Бориспіль, Укртелекому, Укрзалізниці, Кабінету Міністрів України тощо. Експерти Міжнародного валютного фонду підрахували, що економічні втрати від атаки вірусу "NotPetya" склали 850 мільйонів доларів [3, с. 119].

Згідно з дослідженням, протягом останніх років значно зросла кількість злочинів, які вчиняються за допомогою соціальних мереж та у соціальних мережах. Економіка кіберзлочинності «заробляє» на таких злочинах близько 3,25 мільярдів доларів щороку [2]. Очевидно, що кіберзлочинність набирає вкрай загрозливих масштабів для світового співтовариства, тож боротьба з нею – одне із найважливіших завдань. На думку автора, одним із пріоритетних напрямів є удосконалення кримінального закону в частині боротьби з кіберзлочинністю, внесення змін до діючого законодавства, ратифікація та імплементація міжнародних правових актів.

Правову основу боротьби з кіберзлочинністю становлять міжнародні нормативно-правові акти, Конституція України, Кримінальний кодекс України, Закони України «Про основні засади забезпечення кібербезпеки України», «Про інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про основи національної безпеки» та інші нормативні акти. Україна ратифікувала ряд нормативно-правових міжнародних документів, це Конвенція Організації Об'єднаних Націй проти транснаціональної організованої злочинності (United Nations Convention against Transnational Organized Crime) [5], Європейська конвенція про взаємну допомогу у кримінальних справах (European Convention on Mutual Assistance in Criminal Matters) [9] Конвенція про кіберзлочинність (Convention on Cybercrime) [10] тощо.

Одним із найважливіших інструментів правового регулювання боротьби із кіберзлочинністю, як у світі, так і в Україні є Конвенція про кіберзлочинність (Convention on Cybercrime). Конвенція містить найповнішу на сьогоднішні день класифікацію кіберзлочинів, відповідно до якої кіберзлочини розмежовуються залежно від об'єкта посягання на

1) правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем; 2) правопорушення, пов'язані з комп'ютерами; 3) правопорушення, пов'язані зі змістом; 4) правопорушення, пов'язані з порушенням авторських і суміжних прав [10].

Прийняття Кримінального кодексу України 2001 року стало новим етапом правового регулюванні боротьби з кіберзлочинністю у вітчизняному законодавстві. У Кримінальному кодексі України міститься розділ 16 «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку». Так, несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку передбачає покарання за створення та розповсюдження вірусів незалежно від мети таких дій (ст.ст. 361, 361-1) [6].

Кримінальна відповідальність передбачена за 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. Передбачаються санкції за зловживання правом доступу до інформації та у разі, якщо працівник компанії, використовуючи свої службові обов'язки, надав доступ до бази даних клієнтів своєї компанії стороннім особам чи компаніям-конкурентам (ст.ст. 362, 362-1).

Відповідно до ст. 363, 363-1 відповідальність настає за 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, та перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку [6].

Тривалий час у чинному законодавстві України були відсутні терміни «кіберзлочин» і «кіберзлочинність», що негативно позначалося на розвитку кримінальної науки, на практичній роботі правоохоронних органів, судовій діяльності. Тому дуже важливим стало прийняття Закону України «Про основні засади забезпечення кібербезпеки України», який набув чинності 9 травня 2018 року. У цьому нормативно-правовому акті поняття кіберзлочину визначається як 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, та поняття кіберзлочинності як сукупності кіберзлочинів (ч.ч. 8, 9 ст. 1). Крім того, одним із основних принципів кібербезпеки визачено принцип невідворотності покарання за вчинення кіберзлочинів [8].

Виходячи з того, як визначає поняття «кіберзлочин» український законодавець, можна припустити, що будь-яке протиправне діяння, відповідальність за яке передбачена кримінальним законом, можна назвати «кіберзлочином», якщо воно вчинене у кіберпросторі або з його використанням (крадіжка, шахрайство, торгівля людьми, продаж наркотиків, зброї тощо).

Зі стрімким розвитком інформаційних технологій виникають нові форми та види кіберзлочинів, зростає їх кількість. Кібертероризм, хакінг, злочинні операції з криптовалютою, крадіжка даних, інформації чи інтелектуальної власності, продаж зброї чи наркотиків в інтернеті – це далеко не повний перелік поширених кіберзлочинів. Особливу загрозу як для окремої держави, так і для всього світу може становити використання інформаційних технологій терористичними групами і терористами для досягнення своїх цілей. Кібертероризм може включати використання інформаційних технологій для організації та виконання атак проти телекомунікаційних мереж, інформаційних систем і комунікаційної інфраструктури або обмін інформацією, а також загрози з використанням засобів електрозв'язку. Прикладами можуть слугувати злом інформаційних систем, внесення вірусів у вразливі мережі, дефейс веб-сайтів, DoS-атаки, терористичні загрози, спричинені електронними засобами зв'язку.

Одним із найпоширеніших кіберзлочинів як в усьому світі, так і в Україні є шахрайство. Останнім часом в Україні значно зросла злочинна діяльність у електронній комерції та виникли нові її форми: шахрайські продажі через інтернет-аукціони чи роздрібні сайти або через підроблені веб-сайти, які можуть пропонувати товари чи послуги, яких насправді не існує; шахрайство з масовим маркетингом і шахрайство споживачів (фішинг- шахрайства – використання шахрайських електронних листів, замаскованих під законні електронні листи, які запитують або надсилають особисту або корпоративну інформацію у користувачів, наприклад паролі або банківські рахунки; фармінг відбувається там, де користувача направляють на підроблений веб-сайт, іноді з фішинг-електронних листів, для введення його особистих даних та інші види шахрайств).

Надзвичайно поширеними в Україні є злочини у сфері інтелектуальної власності, причому переважна більшість таких злочинів (піратство, підробка) вчиняється у кіберпросторі. Значних збитків можуть завдавати та нести суспільну небезпеку незаконне вторгнення в комп'ютерні мережі (злом або хакінг); порушення або погіршення функціональності комп'ютера та мережевого простору (зловмисне програмне забезпечення та атаки відмови в сервісі (DOS) або розповсюджені відмови в обслуговуванні (DDOS) можуть становити суспільну небезпеку та завдавати значних збитків. Злочинці використовують спеціальне програмне забезпечення (віруси, черви, троянці, шпигунське програмне забезпечення). Зловмисне програмне забезпечення може бути руйнівним, наприклад видаляти файли

або спричиняти збої в системі, але також може використовуватися для крадіжки особистих даних.

Відносно новими видами злочинів є суспільно небезпечні діяння, пов'язані з розвитком соціальних мереж (кібер-знущання або тролінг, віртуальний мобінг, кіберпереслідування), які вчиняються у/або через соціальні мережі. Кіберзлочинці часто використовують у своїй злочинній діяльності так звану темну мережу або Даркнет, що значно ускладнює виявлення та розслідування кіберзлочинів. У Даркнеті файлообмін здійснюється анонімно, оскільки IP-адреси недоступні публічно. У Даркнеті натепер існують численні програми анонімних мереж: Tor, I2P, RetroShare, Freenet, GNUnet та інші [2].

Висновки. Вдосконалення нормативно-правового регулювання боротьби з кіберзлочинністю в Україні є досить актуальним і важливим, адже сьогодні практично усі державні та недержавні процеси відбуваються із застосуванням інструментів кіберспростору, а з розвитком інформаційних технологій злочинність у кіберпросторі набуває загрозливих масштабів – кількість злочинів зростає, виникають нові види злочинів і способи їх вчинення.

Чинна вітчизняна нормативно-правова база у сфері протидії злочинам у кіберпросторі лише частково задовольняє потреби часу та не завжди охоплює всі ключові елементи, необхідні для ефективної протидії кіберзлочинам усіх рівнів складності. Одним із пріоритетних напрямів такої роботи має стати організація взаємодії і координації зусиль науковців і практиків (правоохоронців, працівників спецслужб, судової системи) у боротьбі з кіберзлочинністю.

Такі держави як США, Великобританія, Японія, Китай досягли значних успіхів у боротьбі з кіберзлочинністю, попередженні, виявленні та розслідуванні кіберзлочинів. У цих країнах досить розвинена законодавча база, яка регулює сферу боротьби з кіберзлочинністю, тож для України важливою є готовність співпрацювати та вносити необхідні зміни у вітчизняне законодавство, які відповідатимуть стандартам, встановленим на європейському та світовому рівнях. Враховуючи міжнародний характер кіберзлочинності, у боротьбі з нею важливе значення має співпраця зі світовим товариством, імплементація міжнародних документів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Global Cybercrime Damages Predicted To Reach $6 Trillion Annually By 2021. URL:https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/(дата звернення: 05.01.2020).
2. Hyper-connected web of profit emerges, as global cybercriminal revenues hit $1.5 trillion annually. URL: https://www.bromium.com/press-release/hyper-connected-web-of-profit-emerges-as-global-cybercriminal-revenues-hit-1-5-trillion-annually/ (дата звернення: 05.01.2020)
3. Гуцалюк М.В. Сучасні тенденції організованої кіберзлочинності Журнал «Інформація і право». № 1(28). 2019. с. 119.
4. Кількість кіберзлочинів збільшується на 2,5 тисячі в рік – голова Кіберполіції. URL: https://www.epravda.com.ua/news/2018/01/15/633010/ (дата звернення: 08.01.2020).
5. Конвенція Організації Об'єднаних Націй проти транснаціональної організованої злочинності : Резолюція 55/25 Генеральної Асамблеї від 15 листопада 2000 року. URL: http://zakon5.rada.gov.ua/laws/show/995_789 (дата звернення: 05.01.2020).
6. Кримінальний кодекс України. *Відомості Верховної Ради України* (ВВР), 2001, № 25–26, ст. 131. URL: https://zakon.rada.gov.ua/laws/show/2341-14 (дата звернення: 08.01.2020).
7. Підсумки 2019 року в цифрах. URL: https://cyberpolice.gov.ua/results/2018/.
8. Про основні засади забезпечення кібербезпеки України : Закон України (*Відомості Верховної Ради* (ВВР), 2017, № 45, ст. 403. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 08.01.2020).
9. Про ратифікацію Європейської конвенції про взаємну допомогу у кримінальних справах (1959 рік) та Додаткового протоколу 1978 року до Конвенції № 1433-IV : Закон України від 04.02.04 р. URL: http://zakon0.rada.gov.ua/laws/show/44/98-%D 0%B2%D1%80 (дата звернення: 08.01.2020).
10. Про ратифікацію Конвенції про кіберзлочинність : Закон України від 07.09.05 р. № 2824-IV (2824-15). URL: http://zakon2.rada.gov.ua/laws/show/2824-15 (дата звернення: 08.01.2020).
11. Савінова Н.А. Кримінально-правове забезпечення розвитку інформаційного суспільства в Україні: теоретичні та практичні аспекти : монографія. Н.А. Савінова. К. : ДКС. 2011. 342 с.