УДК 343
DOI https://doi.org/10.32782/2524-0374/2022-5/113

СТАНОВЛЕННЯ ТА ГЕНЕЗА КРИМІНАЛЬНОЇ ВІДПОВІДАЛЬНОСТІ ЗА КРИМІНАЛЬНІ ПРАВОПОРУШЕННЯ У КІБЕРПРОСТОРІ НА ТЕРНАХ УКРАЇНИ

FORMATION AND GENESIS OF CRIMINAL LIABILITY FOR CRIMINAL OFFENSES IN CYBERSPACE IN UKRAINE

Думчиков М.О., старший викладач
кафедри кримінально-правових дисциплін та судочинства
Навчально-науковий інститут права Сумського державного університету

Каріх І.В., старший викладач
кафедри кримінально-правових дисциплін та судочинства
Навчально-науковий інститут права Сумського державного університету

Статтю присвячено становленню кримінальної відповідальності за кримінальні правопорушення які вчиняються у кіберпросторі. Проаналізовано, що в умовах стрімкого розвитку інформаційного суспільства в Україні, коли електронно обчислювальні машини та телекомунікаційні системи поширюються всюди, все більше викликів постає перед кримінально правовою охороною кіберпростору. Проаналізовано законодавче та доктринальне визначення понять кіберпростір та кіберзлочин. Перелічено, які групи кримінальних правопорушень вчинених у кіберпросторі передбачені Конвенцією Ради Європи та чинним Кримінальним кодексом України. Висвітлено стан нормативно правового регулювання і протидії цьому негативному та протиправному явищу. Визначено статистичну динаміку кримінальних правопорушень які вчиняються у кіберпросторі. Наголошено, що суспільна небезпека кіберзлочинів, полягає у завданні шкоди як окремому громадянину так і державі в цілому. Визначено та проаналізовано 5 етапів становлення кримінальної відповідальності за правопорушення вчинені у кіберпросторі. Надано характеристику окремим підвидам кіберзлочинів таких, як фішинг, скамінг, чорний рефаундінг та кардинг. Наголошено, що 16 розділ особливої частини Кримінального кодексу України, не обмежується іншими кримінальними правопорушеннями які вчиняються у кіберпросторі та містяться в інших розділах. Проаналізоване законодавче визначення кіберпростору та кіберзлочину та визначені їх основні ознаки. Наголошено на такій ознаці кіберзлочинів, як латентність. Проаналізовано, що внаслідок складного та специфічного характеру кіберзлочинів не існує певної уніфікованої моделі, щодо виявлення усіх можливих категорій загроз, про що і свідчить невтішна статистика. Сучасна модель кіберзлочинності швидко трансформується і якісно пристосовується до реалій сьогодення, а отже перед суспільством постають нові виклики які потребують як законодавчого регулювання так і координації правоохоронних органів з метою захисту суспільства та кіберпростору в цілому. Крім цього наголошуємо, що в сучасному світі проблеми кіберзлочинності не можуть бути вирішні без правових контрзаходів та міжнародної співпраці.

Ключові слова: кіберзлочин, кіберпростір, кримінальне правопорушення у кіберпросторі, кіберзахист, кардинг, фішинг.

The article is devoted to the establishment of criminal liability for criminal offenses committed in cyberspace. It is analyzed that in the conditions of rapid development of the information society in Ukraine, when electronic computers and telecommunication systems are spreading everywhere, more and more challenges are facing the criminal law protection of cyberspace. Legislative and doctrinal definitions of cyberspace and cybercrime are analyzed. The groups of criminal offenses committed in cyberspace are listed under the Council of Europe Convention and the current Criminal Code of Ukraine. The state of normative legal regulation and counteraction to this negative and illegal phenomenon is covered. The statistical dynamics of criminal offenses committed in cyberspace is determined. It is emphasized that the public danger of cybercrime is to harm both the individual citizen and the state as a whole. 5 stages of criminal liability for offenses committed in cyberspace have been identified and analyzed. Some subtypes of cybercrime, such as phishing, scamming, black refounding and carding, are described. It is emphasized that Section 16 of the Special Part of the Criminal Code of Ukraine is not limited to other criminal offenses committed in cyberspace and contained in other sections. The legislative definition of cyberspace and cybercrime is analyzed and their main features are determined. Emphasis is placed on such a feature of cybercrime as latency. It is analyzed that due to the complex and specific nature of cybercrime, there is no unified model for identifying all possible categories of threats, as evidenced by disappointing statistics. The modern model of cybercrime is rapidly transforming and qualitatively adapting to the realities of today, and therefore society faces new challenges that require both legislation and coordination of law enforcement agencies to protect society and cyberspace as a whole. In addition, we emphasize that in today's world the problems of cybercrime cannot be solved without legal countermeasures and international cooperation.

Key words: cybercrime, cyberspace, criminal offense in cyberspace, cyber defense, carding, phishing.

Сьогодні ми живемо в епоху інформаційного суспільства, коли фактично електронно обчислювані машини та телекомунікаційні системи охоплюють усі сфери життєдіяльності, як держави в цілому, так і кожного окремого громадянина зокрема. Разом з тим запровадження глобальної діджиталізації в суспільство, поставило певні виклики, щодо можливостей зловживання інформаційними та телекомунікаційними технологіями. Наразі жертвами зловмисників, які здійснюють свою діяльність у віртуальному просторі (кіберсередовищі), можуть стати не лише окремі громадяни, але й цілі держави. При цьому безпека десятків тисяч користувачів, може виявитися залежною лише від декількох зловмисників. Варто зауважити, що кількість кримінальних правопорушень у кіберпросторі, зростає пропорційно кількості користувачів мережі Інтернет та кількості телекомунікаційних систем.

Наразі кіберзлочинність є напевно однією з найбільших глобальних загроз, як для України так і для усього світу. За даними всесвітнього огляду економічних злочинів Pricewater house Coopers (PWC) за 2021 рік, кримінальні правопорушення у кіберпросторі показали найвищий рівень за весь період публікаційних оглядів. Так рівень злочинності збільшився з 24 % у 2014 році, до 39 % у 2021 році, тим самим посівши 2 місце серед економічних кримінальних правопорушень у світі, залишивши позаду кримінальні правопорушення пов'язані з легалізацією грошових коштів отриманих незаконним шляхом та різні корупційні кримінальні правопорушення. Однак зазначені дані не в повній мірі відповідають дійсності, адже кримінальні правопорушення вчинені в кіберпросторі є дуже латентним за своїм за своєю ознакою, тому реальна картина та реальна статистика набагато більша. Це зумовлене перш за все, відсутністю чітких методів збирання даних про вчинення кримінальних правопорушень в кіберпросторі та певні характерні особливості зазначеного виду кримінальних правопорушень [1].

Перший злочин здійснений із використанням комп'ютера в колишньому Союзі Радянських Соціалістичних Республік

був зареєстрований у 1979 році у Вільнюсі, ним стало розкрадання, збитки від якого складали 78584 карбованців. Цей факт був занесений у міжнародний реєстр правопорушень подібного роду і став своєрідним початком розвитку нового виду злочинів у колишньому СРСР [2].

Стосовно самого поняття кіберзлочинності та підходів його визначення, варто зауважити, що більшість авторів та вчених пов'язує його перш за все з специфічним предметом вчинення кримінального правопорушення – комп'ютером або з самим місцем його вчинення – кіберпростором.

Перший етап 2001–2005. Перша спроба врегулювання кримінальних правопорушень в законодавстві України була в кримінальному кодексі 2001 року. Так в главі 16 кримінального кодексу України «Злочини у сфері використання електронно-обчислювальних машин, систем та комп'ютерних мереж» було визначено 3 види кримінальних правопорушень у кіберпросторі, зокрема [3]:

Стаття 361. Незаконне втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж;

1. Стаття 362. Викрадення, привласнення, вимагання комп'ютерної інформації або заволодіння нею шляхом шахрайства чи зловживання службовим становищем;
2. Стаття 363. Порушення правил експлуатації автоматизованих електронно-обчислювальних систем [3].

Варто зауважити, що фактично законодавець визначає предмет кримінальних правопорушень у кіберпросторі, і відносить до нього ЕОМ та комп'ютерні мережі. Однак в той же час на законодавчому рівні залишається неврегульованим питання щодо визначення поняття кіберпростору та кіберзлочину. В той же час деякі науковці визначають доктринальне визначення кіберзлочину.

Зокрема, П.Д. Біленчук та М.А. Зубань визначають кіберзлочин як суспільно небезпечну діяльність або бездіяльність, яка здійснюється з використанням сучасних технологій і засобів комп'ютерної техніки, з метою завдання шкоди майновим або суспільним інтересам держави, підприємств, відомств, організацій, кооперативів, громадським організаціям і громадянам, а також правам особи [4, с. 6].

Батурін Ю.М. визначає кіберзлочини, як злочини основним предметом яких є комп'ютер [5].

Другий етап 2005–2009. В 2005 році Україна ратифікувала «конвенцію про кіберзлочинність», однак навіть в конвенції не визначалося поняття кіберзлочину та кіберпростор. Конвенція визначала види кримінальних правопорушень у кіберпросторі, зокрема [6]:

1) правопорушення проти конфіденційності;
2) правопорушення пов'язані з комп'ютером;
3) правопорушення пов'язані зі змістом;
4) порушення пов'язані з порушенням авторських та суміжних прав.

Зокрема, правопорушення проти конфіденційності включали в себе: незаконний доступ, нелегальне перехоплення, втручання в данні, втручання в систему та зловживання пристроями. Фактично правопорушення проти конфіденційності які закріплені в конвенції, відображалися в 16 главі особливої частини кримінального кодексу України. До таких кримінальних правопорушень можна було віднести різного роду проникнення в комп'ютерну або телекомунікаційну мережу, протизаконне перенаправлення Інтернет трафіку, створення, використання та розповсюдження шкідливого програмного забезпечення, збут інформації з обмеженим доступом та несанкціоновані дії з інформацією, яка зберігається в ЕОМ.

Правопорушення пов'язані з комп'ютером, включають в себе підробку пов'язану з комп'ютером та шахрайство пов'язане з комп'ютером. Такі правопорушення знайшли відображення в ККУ в 200ст., 358ст., та 190ст. Зокрема, до таких дій можна віднести будь які види віртуального шахрайства; «скам», «фішинг», підроблення електронних документів для отримання кредитів, підроблення документів для відкриття рахунків в електронних платіжних система, тощо.

Стаття 9 «конвенції про кіберзлочинність» визначає як правопорушення -вироблення, пропонування, розповсюдження, здобуття та володіння дитячої порнографії. Зокрема, ст. 301 встановлює відповідальність за одержання доступу до дитячої порнографії, її придбання, зберігання, ввезення, перевезення чи інше переміщення, виготовлення, збут і розповсюдження. Так само зазначається, що одержання доступу до дитячої порнографії з використанням інформаційно-телекомунікаційних систем або технологій слід вважати умисним, якщо доведено, що особа усвідомлювала, що у такий спосіб вона отримає доступ до дитячої порнографії [3].

Статтею 176 ККУ встановлюється відповідальність за порушення авторського права та суміжних прав, аналогічну статтю містить «конвенції про кіберзлочинність», однак, основною відмінністю є використання комп'ютера як предмета кримінального правопорушення.

Основною характеристикою другого етапу можна виділити фактичне розширення переліку кримінальних правопорушень, які вчиняються в кіберпросторі, однак одночасно спостерігається фактична відсутність регулювання як кіберпростору в цілому, так і окремих видів кіберзлочинів. Велика кількість кримінальних правопорушень визначених в ККУ, які фактично вчиняються в кіберпросторі, кваліфікуються без визначення специфічного знаряддя кримінального правопорушення, способу вчинення та предмета кримінального правопорушення. На нашу думку визначення зазначених факультативних ознак, є основним при кваліфікації кримінальних правопорушень вчинених в кіберпросторі.

Третій етап 2009-2015. Поява криптовалюти, стрімкий розвиток електронних платіжних систем, систем електронної комерції, соціальних мереж та діджиталізації суспільства в цілому, поставив нові загрози у кіберпросторі. Якщо, перший та другий етапи характеризувалися здебільшого кримінальними правопорушеннями пов'язаними з проникненням в системи ЕОМ та телекомунікаційні системи, а також створенням, розповсюдженням та збутом шкідливого програмного забезпечення, то для третього етапу характерні економічний характер зазначених кримінальних правопорушень.

Набувають популярність такі кримінальні правопорушення як «кардинг», «скамінг», «фішинг» та «чорний рефаундінг».

Кардинг – використання в операціях рекві-зитів платіжних карт, отриманих зі зламанихсерверів інтернет-магазинів, платіжних і роз- рахункових систем, а також із персональнихкомп'ютерів (безпосередньо або через програ-ми віддаленого доступу, «трояни», «боти») [7, с. 75].

Фішинг (англ. Phishing) – це вид шахрайства, метою якого є отримання конфіденційної інформації довірливих чи неуважних користувачів мережі персональних даних клієнтів онлайнових аукціонів, сервісів з переказу або обміну валюти, інтернет-магазинів тощо [8].

Скамінг – різновид шахрайства, яке здійснюється переважно в онлайн середовищі, та полягає в розсилці повідомлень через емейл адреси та соціальні мережі в яких міститься заздалегідь неправдива інформація. Наприклад, одержувачу листа повідомляють, що він став переможцем лотереї, і для отримання виграшу йому необхідно переказати невелику суму на вказаний рахунок. Також часто користувачам пропонують інвестувати офшорні підприємства та нерухомість.

Чорний рефаундінг – система повернення частини або повної суми коштів продавцем покупцю, якщо той незадоволений якістю товару і надав докази браку такого товару.

Четвертий етап 2015–2020. Четвертий етап характеризується одразу двома визначними факторам, по – перше це створення спеціалізованого правоохоронного органу «Департаменту кіберполіції Національної поліції України» 5 жовтня 2015 року, та прийняття Закону України «Про основні засади забезпечення кібербезпеки України».

Законом встановляться основні поняття такі як, кіберпростір, кібербезпека, кіберзлочин, кібератака, кіберзагроза та інші. Зокрема, під кіберпростором слід розуміти – середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних. Виходячи з законодавчого визначення кіберпростору, можемо визначити певні характерні йому ознаки [9]:

– віртуальний просторій;
– він є комунікативним середовищем;
– утворюється за допомогою електронних комунікацій та мережі Інтернет.

В свою чергу кіберзлочин (комп'ютерний злочин) законодавець визначає, 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. До основних ознак кіберзлочину законодавець в свою чергу відносить:

– суспільна небезпечність;
– винність;
– вчиняється у кіберпросторі.

П'ятий етап 2020 – теперішній час. П'ятий етап можна охарактеризувати стрімким розвитком Інтернет – суспільства, появою нових методів та сервісів онлайн платежів, переходом бізнесу від традиційних методів його ведення до електронної комерції та впровадження віртуальних валют у світову економіку. Така динаміка перш за все зумовлена світовою пандемією COVID – 19, яка фактично змінила правила гри. Все більше різного роду послуг почали надаватися онлайн, уряди держав почали створювати та розвивати систему електронного урядування, банківські перекази почили відтіснятися електронними платіжними система, а соціальні мережі фактично почали виступати повноцінними торгівельними майданчиками. Звичайно, що такі тренди породили нові види кіберзлочинів, а їх кількість суттєво збільшилася. Зокрема, «скамінг» набуває все більш масового характеру і становить приблизно 50% від усіх кіберзлочинів, а самі кіберзлочини стають більш латентними. Лише за 2021 рік кількість зареєстрованих кіберзлочинів зросла на 25%. Згідно даних офісу генеральної прокуратури за 2021 рік було опубліковано 3147 кримінальні правопорушення які були вчинені кіберпросторі, та вручено 2125 повідомлень про підозру. Для статистики за 2014 рік було опубліковано 443 кримінальні правопорушення у зазначеній сфері та вручено 201 підозру. Варто зауважити, що статистична інформація, обмежена лише 16 розділом особливої частини ККУ, і не містить інформації про інші «традиційні» види кіберзлочинів які містяться в інших розділах особливої частини ККУ.

Така невтішна статистика говорить про стрімку динаміку розвитку кіберзлочинної сфери. На нашу думку, в епоху діджиталізації суспільства треба більше уваги приділяти безпеці у кіберпросторі. Це зумовлено перш за все тим, що спільнота все більше сфер суспільного життя переносить у кіберпростір, що відкриває все нові і нові можливості для реалізації кіберзлочинцями своїх протиправних намірів. З огляду на це, вважаємо за потрібне побудову нової національної моделі забезпечення кібербезпеки держави в цілому та кожного громадянина, підприємства, організації зокрема. Така модель повинна будуватися на чіткій координації між системами правоохоронних органів, органів фінансового моніторингу та судової системи, а також їх задовільне, як кадрове так і матеріально – технічне забезпечення.

ЛІТЕРАТУРА

1. Офіційний веб-ресурс PricewaterhouseCoopers. URL: https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/cyber-year-in-retrospect.html
2. Батурин Ю.М. Проблемы компьютерного права. 1991. 272 с. URL: http://ndki.narod.ru/liblary/books/Baturin.html
3. Кримінальний кодекс України : Закон України від 05.04.2001 № 2341-II / *Верховна Рада України*. URL: http://zakon2.rada.gov.ua/laws/show/2341-14
4. Біленчук П.Д., Зубань М.А. Комп'ютерні злочини: соціально-правові та кримінолого-криміналістичні аспекти. Українська академія внутрішніх справ. 1994. с. 6
5. Батурин Ю.М., Жодзишский А.М. Компьютерная преступность и компьютерная безопасность. 1991. 160 с. URL: http://lawlibrary.ru/izdanie14201.html
6. Конвенція Ради Європи про кіберзлочинність: від 21.11.2001 URL: http://zakon.rada.gov.ua/laws/show/994_575
7. А.А. Русецький. Теоретико – правовий аналіз понять «кіберзлочин» і «кіберзлочинність». *Право і безпека*. 2017. № 1 (64). С. 74–78.
8. Що таке фішинг? URL: https://uk.wikipedia.org/wiki/Фішинг
9. Про основні засади забезпечення кібербезпеки України : Закон України від. 05.10.2017 № 2163-VIII.