ЮРИДИЧНІ НАУКИ

DOI: https://doi.org/10.32839/2304-5809/2022-8-108-6
УДК 343.2/.7

Любавіна В.П.[1]
Університет державної фіскальної служби України

СУТНІСТЬ КІБЕРЗЛОЧИННОСТІ ТА СПОСОБИ БОРОТЬБИ

Анотація. У статті розкрита сутність протиправних дій у сфері інноваційних технологій, що завдають шкоди інтересам нашої держави, організаціям та громадянам в цілому. Проаналізовано, що однією з основних проблем боротьби з кіберзлочинами є прогалини у чинному законодавстві. У статті розкрита сутність «кіберзлочинності», розглядаються особливості злочинів у сфері комп'ютерної інформації відповідно до чинного кримінального законодавства України, проведений аналіз особистості комп'ютерного злочинця. Також висвітлені окремі види кіберзлочинів. Інформаційні технології роблять людей більш вразливими перед широким спектром загроз, і тому автором запропоновані також запобіжні заходи, які можуть прийняти користувачі Інтернету та комп'ютерів, щоб захиститися від кібератак.

Ключові слова: кіберзлочинність, кіберзлочини, інноваційні технології, комп'ютерна інформація, особистість комп'ютерного злочинця, інформаційні злочини, сучасні інформаційні технології.

Lyubavina Victoria
University of the State Police of Ukraine

THE ESSENCE OF CYBERCRIME AND METHODS OF FIGHTING IT

Summary. The article reveals the essence of illegal actions in the field of innovative technologies that harm the interests of our state, organizations and citizens as a whole. It has been analyzed that one of the main problems in the fight against cybercrimes are gaps in the current legislation. The article reveals the essence of "cybercrime", considers the specifics of crimes in the field of computer information in accordance with the current criminal legislation of Ukraine, and conducts an analysis of the personality of a computer criminal. Certain types of cybercrimes are also highlighted. Information technology makes people more vulnerable to a wide range of threats, and therefore the author also suggests precautions that Internet and computer users can take to protect themselves from cyberattacks. The peculiarity of cybercrime is that criminals can operate from almost anywhere in the world and mask their tracks relatively well. In addition, the crime scene does not necessarily have to coincide with the crime scene. Thus, we believe that in order to counteract crimes committed with the use of modern information technologies in our state, it is necessary to constantly increase the security of information systems, develop modern information technologies, improve legislation in the field of information crimes, develop competitive means of informatization, expand international cooperation of Ukraine in the field safe use of information resources. In today's world, cybercrime is a serious threat to society and its information security. Cybercrime creates a complex of social problems that require immediate response and effective resolution. With the improvement of information technologies, cybercrime is also improving, which is manifested in many spheres of life and activity of a person and society as a whole. Therefore, the conducted analysis does not cover all the problems related to the cyber security of society and the state. Moreover, with the development of information and telecommunication technologies, new ways of committing crimes and methods of countering law enforcement agencies will appear.

Keywords: cybercrime, cybercrimes, innovative technologies, computer information, the personality of a computer criminal, information crimes, modern information technologies.

Постановка проблеми. З кожним днем кіберзлочини отримують все більшу розповсюдженість. Насамперед це пов'язано із недосконалістю чинного законодавства України в області здійснення розслідування злочинів у сфері комп'ютерної інформації, а також щодо можливістю перегляду та внесення змін до законодавства України. На сьогоднішній день використання інформаційних технологій не має меж. Майже кожен чув про таке явище, як кіберзлочинність і можливо навіть особисто з нею зіштовхувався. Комп'ютери, мобільні телефони та Інтернет змінили сучасну життя. Вони дають населенню безліч переваг.

Однак інформаційні технології також роблять людей більш уразливими перед широким спектром загроз, а вони, у свою чергу, можуть призвести до фінансових втрат або завдати шкоди репутації особистості.

Аналіз останніх досліджень і публікацій. За останні роки було написано і опубліковано ряд монографічних робіт, присвячених дослідженню різних аспектів провини і її форм, таких авторів як: В.І. Антипов, Е.Л. Кочкіна, О.В. Манжай, В.А. Москальчук, К.М. Євдокимов, Г.А. Гундеріч, Є.В. Полікарпова, А.М. Пахомов, Н.В. Савчук.

Ціль статті полягає в аналізі сутності та особливості кіберзлочинів в Україні. Кіберзлочини частіше відбуваються заради економічних цілей. Це може бути, наприклад, нанесення економічної шкоди у вигляді крадіжки коштів та конфіденційної інформації. До інших видів цілей відносяться політичні – заподіяння шкоди основним державним і політичним інститутам, що

[1] ORCID: https://orcid.org/0000-0003-4715-1749

© Любавіна В.П., 2022

підриває систему владних відносин і довіри до влади. Третій вид цілей – ідеологічні: поширення ідей та ідеологій з метою вербування інтернет-користувачів у ряди, наприклад, радикальних терористичних та націоналістичних угруповань. Зрештою, до четвертого виду цілей ми відносимо соціально-психологічні, такі як нанесення морального, психологічного шкоди громадянам.

Виклад основного матеріалу. Щодо наукових підходів до визначення понять «кіберзлочин» і «кіберзлочинність» слід пояснити, що частина вчених пов'язує їх із специфічним предметом злочину – комп'ютером (комп'ютерною технікою) чи комп'ютерними даними та способом вчинення злочину – з використанням вищевказаних предметів для вчинення злочину [6, с. 338] або з певним місцем його вчинення, яким є кіберпростір [1, с. 17], віртуальний простір [2, с. 173].

Кіберзлочинність – це явище у всьому світі, яке не зупиняється ні на кордонах країни, ні за зачиненими дверима. Вона може відбуватися скрізь, де люди використовують комп'ютери, смартфони та інші ІТ-пристрої – в компаніях, державних установах, університетах, вдома та в дорозі.

Слід зауважити, що незначна помилка в керуванні цифровим життям може «відкрити двері» для кіберзлочинців. Злочини, у яких злочинці використовують сучасні інформаційні технології, у широкому сенсі називаються кіберзлочинністю. Отже, кіберзлочинність – це спроба шахрайства, яка досягає потенційну жертву електронною поштою.

Однак у більш вузькому значенні цей термін включає злочини, націлені на самі комп'ютерні системи та мережі. Це також може бути кібершпигунство або кібертероризм.

Таким чином, протиправні дії у сфері інноваційних технологій, що здійснюються з використанням мережі Інтер немає та комунікаційних пристроїв, на даний час все частіше стали застосовуватися в злочинних цілях проти інтересів різних держав, у тому числі і України, організацій та громадян. Кібершахрайство, інформаційні блокади, тероризм, комп'ютерний шпигунство, неправомірний доступ до особистої інформації (акаунти в соціальних мережах, електронні пошти) та інші злочинні посягання завдають значної майнової шкоди, зазіхають на національну безпеку держави.

Особливість кіберзлочинності полягає в тому, що злочинці можуть діяти практично з будь-якої точки світу та відносно добре маскувати свої сліди. Крім того, місце злочину не обов'язкове має збігатися з місцем скоєння злочину.

Саме проблемі інформаційної (комп'ютерної) безпеки в державі повинна приділятися особливу увага. Варто зазначити, що держави приймають заходи щодо об'єднання зусиль у сфері боротьби з кіберзлочинцями. Наприклад, у 2009 р. в Естонії відкрився Центр колективної кібербезпеки під керівництвом НАТО. 25 січня 2018 р. розпочав роботу Глобальний центр з питань кібербезпеки під егідою Всесвітнього економічного форуму у Давосі.

У сфері правового регулювання кіберзлочинності окремої уваги заслуговує на проект конвенції ООН «Про співробітництво у сфері протидії інформаційної злочинності», створений російськими розробниками. В ньому представлені цілі, які полягають у профілактиці виявлення злочинів на інформаційній сфері на ранніх стадіях, забезпечення караності даних порушень, безпосереднє співробітництво країн у вирішенні подібних питань, що полягає у створенні та розвитку кадрів та надання допомоги один одному (ст. 1). У цій конвенції докладно розкриваються специфічних інформаційних термінів. Наприклад, «бот-мережа» означає два і більше пристроїв ІКТ, в модуль яких завантажені вірусні програми, управління якими проводиться таємно. Встановлено також відповідальність за незаконне отримання інформації у електронної форми (гл. 2).

Для ефективності боротьби з подібними інцидентами, у ст. 57 Конвенції кожному державі пропонується сформувати інформаційний центр, який буде працювати цілодобово [4].

Аналізуючи цю Конвенцію, необхідно зазначити, що в ній зібрано значна кількість відомостей, завдяки яким можна вдосконалити заходи щодо боротьби з кіберзлочинністю. У ній: представлена конкретна програма по здійсненню навчання кваліфікованих спеціалістів, які займаються здійсненням інформаційної безпеки; акцентується увага на необхідності проведення усіма країнами єдиної політики у боротьбі з кіберзлочинністю та активної взаємодопомоги.

Крім того, доповідь Групи урядових експертів з досягнень у сфері інформатизації та телекомунікацій у контексті міжнародної безпеки щорічно представляється Генеральним Секретарем, де країни-учасниці дають звіт про проведені заходи в галузі інформаційної безпеки.

Тому, саме прийняття національних стратегій у сфері кібербезпеки стало невід'ємною частиною політики держав. Наприклад, у Німеччині існує федеральне агентство Національний центр кібербезпеки, здійснює захист національної інфраструктури від кібератак. Під кіберзлочинністю слід розуміти соціально-правовий феномен, що проявляється в забороненій законом про кримінальну відповідальність предметній діяльності (кримінальній активності) частини населення з використанням електронно-обчислювальних машин (комп'ютерів), телекомунікаційних систем, комп'ютерних мереж і мереж електрозв'язку [5, с. 19].

В Україні з метою своєчасного реагування на нові кібератаки правоохоронні органи орієнтовані на ведення моніторингу ситуації, що складається в мережі Інтернет, підвищення кваліфікації співробітників, методичне забезпечення їх діяльності.

Таким чином, вважаємо, що з метою протидії злочинів, скоєних з використанням сучасних інформаційних технологій у нашому державі слід постійно підвищувати безпеку інформаційних систем, розвивати сучасні інформаційні технології, удосконалювати законодавство у сфері інформаційних злочинів, розвивати конкурентоспроможні засоби інформатизації, розширювати міжнародне співробітництво України у сфері безпечного використання інформаційних ресурсів.

Необхідно врахувати, що в епоху стрімкого та активного розвитку цифровізації інформаційні технології стають невід'ємною частиною повсякденного життя будь-якого громадянина,

робітників процесів та діяльності державних органів та бізнесу, тому особливе увагу потрібно приділяти особистої кібербезпеки.

Очевидно, що Україна знаходиться на початковому етапі впровадження інститутів та механізмів у сфері кібербезпеки, проте певна законодавча база вже створена, і тому необхідно її дотримуватися та вдосконалювати.

З кожним днем кіберзлочини отримують все більшу поширеність,

їх кількість значно збільшується. Виникає все більше нових видів злочинів, до кожного з яких потрібно підбирати відповідні методи боротьби, що викликає певні проблеми, насамперед тому, що спіймати кібершахрая набагато складніше, ніж звичайного злочинця.

Боротьба з кіберзлочинністю ускладнюється цілою низкою факторів:

– кіберзлочинці – це не звичайні шахраї, а добре навчені та зазвичай ховаються за екраном свого комп'ютера. Таку особу вирахувати набагато складніше, ніж звичайного злочинця;

– зіткнувшись з кіберзлочинами, співробітники правоохоронних органів потребують допомоги висококваліфікованих спеціалістів у сфері програмування, в яких, як і раніше, відчувається брак;

– досить важко здійснювати контроль за вже існуючими, постійно оновлюються і знову виникають видами кіберзлочинності.

У сучасному світі кіберзлочинність є серйозною загрозою суспільству та його інформаційною безпекою. Кіберзлочинність породжує комплекс соціальних проблем, які вимагають негайного реагування та ефективного дозволу.

Найбільша частина кіберзлочинності залишається за рамками статистики – можна з упевненістю стверджувати, що до офіційної статистики потрапляє лише десять, у кращому разі двадцять відсотків скоєних діянь.

Структура кіберзлочинності відрізняється помітно у різних країнах залежно, передусім, від характеру і рівня розвитку інформаційних технологій, поширення мережі Інтернет, використання електронних сервісів та електронної комерції тощо. Структура кіберзлочинності злочинності, наприклад, США, виглядає так. За даними одного з досліджень, 44% склали крадіжки грошей з електронних рахунків, 16% – пошкодження програмного забезпечення, стільки ж – викрадення секретної інформації, 12% – фальсифікація інформації, 10% – замовлення послуг за чужий рахунок [8, с. 38].

Для проведення максимально ефективної політики у сфері протидії кіберзагрозам необхідно у повній мірою використовувати досягнення та ресурси набирає обертів процесу цифровізації. Цифровізація може зіграти важливу роль у політиці щодо забезпечення національної та інформаційної безпеки країни. Правильне впровадження та використання цифрових нововведень значно спростить завдання захисту як персональних даних користувача, так і секретних матеріалів державного рівня та значення [9, с. 259].

З удосконаленням інформаційних технологій вдосконалюється і кіберзлочинність, яка знаходить прояв у багатьох сферах життя та діяльності людини та суспільства в цілому.

Захист від цього виду злочинів передбачає кореляцію зусиль на рівні міжнародного співробітництва та взаємодії.

Для проведення ефективної політики по боротьбі з інформаційними правопорушеннями та кіберзлочинами можуть бути вжиті такі заходи:

1) удосконалення технологій, що діють виявленню кіберзлочинів у мережі, а також способів проведення розслідувань даних правопорушень;

2) максимально широке використання технології блокчейн для протистояння кіберзагроз;

3) розвиток ресурсів штучного інтелекту та їх послідовне впровадження у сферу розслідування кіберпресту полінь;

4) посилення відповідальності за вчинення кіберзлочинів;

5) цілеспрямована боротьба з кібертероризмом у всіх його можливих формах та проявах.

Висновки з дослідження і перспективи подальшого наукового пошуку. Отже, проведений аналіз охоплює далеко не всі проблеми, пов'язані з кібербезпекою суспільства і держави. Більше того, з розвитком інформаційно-телекомунікаційних технологій з'являтимуться нові способи скоєння злочинів та методи протидії правоохоронним органам.

Безумовно, не можна просто обмежити до тих чи інших інтернет-сервісів. Без належного правового регулювання проблему вирішити неможливо, необхідно підвищувати відповідальність за розміщення в мережі забороненого контенту, формувати правові та організаційно-технічні механізми протидії протиправної діяльності в даній сфері. Перш за все, слід зауважити, що держава веде активну політику в рамках протидії кіберзлочинності та злочинам, що вчиняються з використанням інформаційно-телекомунікаційних технологій.

Однак на даний момент це заходи не профілактичні, не запобігають і не запобігають зазначений вид злочинних посягань, а, по більшій частині, – контрзаходи у відповідь на вже скоєні злочини або дії, спрямовані на їх припинення. Як би це сумно не звучало, сучасний злочинець значно швидше освоює простори Інтернету, активніше вивчає, розробляє та застосовує нові технічні розробки.

Список літератури:

1. Бутузов В. М. Співвідношення понять «комп'ютерна злочинність» та «кіберзлочинність». *Інформаційна безпека людини, суспільства, держави*. 2010. № 1(3). С. 16–18.
2. Іванченко О. Ю. Кримінологічна характеристика кіберзлочинності, запобігання кіберзлочинності на національному рівні. *Актуальні проблеми вітчизняної юриспруденції*. 2016. Вип. 3. С. 172–177.
3. Книженко О. О. Сучасний стан злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж і мереж електрозв'язку в Україні. *Бюлетень Міністерства юстиції України*. 2014. № 7. С. 122–127.
4. Конвенція про кіберзлочинність : міжнародний документ від 23.11.2001 // База даних «Законодавство України» / Верховна Рада України. URL: http://zakon.rada.gov.ua/laws/show/994_575

5. Кравцова М. О., Литвинов О. М. Запобігання кіберзлочинності в Україні : монографія. Харків : Панов, 2016. 212 с.
6. Манжай О. В. Використання кіберпростору в оперативно-розшуковій діяльності. *Право і Безпека*. 2009. № 4. С. 215–219.
7. Савчук Н. В. Кіберзлочинність: зміст та методи боротьби. *Теоретичні та прикладні питання економіки* : зб. наук. пр. Київ : Вид.- поліграф. центр «Київ. ун-т», 2009. Вип. 19. С. 338–342.
8. Селіко Ю., Прохоров А. Inernet – відмичка для комп'ютера. *Комп'ютер-прес*. 2002. № 3.
9. Шинкарецька Г. Г., Берман А. М. Цифровізація та проблема забезпечення національної безпеки. *Освіта і право*. 2020. № 5. С. 254–260.

References:

1. Butuzov V. M. (2010) Spivvidnoshennia poniat «kompiuterna zlochynnist» ta «kiberzlochynnist» [Correlation of the concepts "computer crime" and "cybercrime]. *Informatsiina bezpeka liudyny, suspilstva, derzhavy,* no. 1(3), pp. 16–18. (in Ukrainian)
2. Ivanchenko O. Y. (2016) Kryminolohichna kharakterystyka kiberzlochynnosti, zapobihannia kiberzlochynnosti na natsionalnomu rivni [Actual problems of domestic jurisprudence Criminological characteristics of cybercrime, prevention of cybercrime at the national level]. *Aktualni problemy vitchyznianoi yurysprudentsii,* vol. 3, pp. 172–177. (in Ukrainian)
3. Knyzhenko O. O. (2014) Suchasnyi stan zlochyniv u sferi vykorystannia elektronno-obchysliuvalnykh mashyn (kompiuteriv), avtomatyzovanykh system, kompiuternykh merezh i merezh elektrozviazku v Ukraini [Current state of crimes in the sphere of use of electronic computing machines (computers), automated systems, computer networks and telecommunication networks in Ukraine.]. *Bulletin of the Ministry of Justice of Ukraine*, no. 7, pp. 122–127. (in Ukrainian)
4. Konventsiia pro kiberzlochynnist: mizhnarodnyi dokument vid 23.11.2001 [Convention on cybercrime: an international document]. Database "Legislation of Ukraine" / Verkhovna Rada of Ukraine. Available at: http://zakon.rada.gov.ua/laws/show/994_575
5. Kravtsova M. O., Litvinov O. M. (2016*) Zapobihannia kiberzlochynnosti v Ukraini: monohrafiia* [Prevention of cybercrime in Ukraine: monograph]. Kharkiv: Panov, p. 212. (in Ukrainian)
6. Manzhai O. V. (2009) Vykorystannia kiberprostoru v operatyvno-rozshukovii diialnosti [The use of cyberspace in operational and investigative activities]. *Pravo i Bezpeka*, no. 4, pp. 215–219. (in Ukrainian)
7. Savchuk N. V. (2009) Kiberzlochynnist: zmist ta metody borotby [Cybercrime: content and methods of combat]. *Teoretychni ta prykladni pytannia ekonomiky: zb. nauk. pr.*, vol. 19, pp. 338–342. (in Ukrainian)
8. Seliko Yu., Prokhorov A. (2002) Inernet – vidmychka dlia kompiutera [Inernet – a lock for a computer Computer-press]. *Kompiuter-pres*, no. 3. (in Ukrainian)
9. Shinkaretska H. G., Berman A. M. (2020) Tsyfrovizatsiia ta problema zabezpechennia natsionalnoi bezpeky [Digitization and the problem of ensuring national security]. *Education and law*, no. 5, pp. 254–260. (in Ukrainian)