УДК 343
DOI https://doi.org/10.32841/2307-1745.2022.55.14

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

КРИМІНАЛЬНО-ПРАВОВА ХАРАКТЕРИСТИКА ПОНЯТТЯ ТА ВИДІВ КІБЕРЗЛОЧИНІВ

Анотація. Кіберзлочини сьогодні є дуже актуальною проблемою як на державному рівні так і на рівні окремого громадянина. Про її актуальність свідчать новини по всьому світу, статистика кримінальних проваджень, проблеми в кримінальному процесі, а також проблемні питання науки кримінального права. Все це пов'язано перш за все з тим, що комп'ютерні злочини є дуже специфічною категорією, яка постійно розвивається одночасно технічним прогресом.

Статтю присвячено дослідженню доктринальних підходів щодо визначення поняття кіберзлочину, та визначення основних видів кіберзлочинів. Метою статті є дослідження феномену кіберзлочинів, визначення поняття кіберзлочину та видів зазначених кримінальних правопорушень, надати загальну характеристику кіберзлочинам. Об'єктом дослідження є суспільні відносини, що виникають у кіберпросторі, а також використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.

Методологічною базою для написання даної статті було використано різні методи наукового пізнання. Зокрема метод порівняння та аналогії застосовано для дослідження правового регулювання різних видів кіберзлочинів. Метод спостереження було використано для ознайомлення із сутністю кіберзлочинів та загальною специфікою цього явища. Метод узагальнення було використано для дослідження різних видів кіберзлочинів.

У статті розглянуто доктринальні визначення дефініції поняття кіберзлочин як вітчизняних так і зарубіжних науковців, зокрема прослідковується, що більшість науковців ототожнює поняття кіберзлочин та комп'ютерний злочин. Надано авторське визначення кіберзлочину, а саме умисні суспільно небезпечні, протиправні, винні діяння, що посягають та заподіюють шкоду суспільним відносинам які регламентують порядок зберігання, розповсюдження, використання інформації та їх захист у кіберпросторі.

Наголошено що злочини в сфері комп'ютерної інформації та злочини з використанням ЕОМ є різновидом кіберзлочинів, а не тотожними кримінальними правопорушеннями.

У статті проаналізовано різні підходи до класифікації кіберзлочинів як на міжнародному та загальнодержавному рівні, так і на доктринальному рівні, та було запропоновано авторську класифікацію кіберзлочинів. Зокрема, класифікувати кіберзлочини, за об'єктом заподіяння шкоди: кримінальні правопорушення у сфері використання платіжних систем; шахрайства сфері комп'ютерної інформації; кримінальні правопорушення у сфері інтелектуальної власності; кримінальні правопорушення у сфері інформаційної безпеки; злочини проти основ національної безпеки та оборони держави.

Ключові слова: кіберзлочини, злочини в сфері комп'ютерної інформації, комп'ютерні злочини, кіберпростір, кримінальні правопорушення в сфері комп'ютерної інформації.

Актуальність. Поняття кіберзлочинність є поки що незвичним для правоохоронних органів, проте злочинні дії, в яких використовується кіберпростір, несе у собі велику суспільну небезпеку. Транснаціональний характер кримінально протиправної діяльності з використанням кіберпростору дає підстави вважати, що розробка загальної політики з основних питань має бути частиною будь-якої стратегії боротьби з кіберзлочинністю. Сьогодні значну частку в загальному обсязі кримінальних правопорушень починають займати кримінальні правопорушення які вчиняються у кіберпросторі або як їх називають кіберзлочини. Варто зауважити, що зростанню та розвитку кіберзлочинності сприяє перш за все сама природа цього виду кримінального правопорушення. Така природа базується, як на відкритому та загальнодоступному характері мережі Інтернет так і на безкарності осіб які скоюють такі кримінальні правопорушення.

Аналіз останніх досліджень і публікацій. Вперше на міжнародному рівні згадування про кіберзлочин було використано в конвенції про кіберзлочинність 2001 року, однак визначення в конвенції не надається. Законом України «про основні засади забезпечення кібербезпеки України» визначає кіберзлочин 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. Крім того законом йде ототожнення кіберзлочину з комп'ютерним злочином [1].

Варто проаналізувати думку зарубіжних та вітчизняних науковців, щодо визначення дефініції кіберзлочин. Так О. Копан в словнику термінів із кібербезпеки надає визначення кіберзлочину як протиправне втручання в роботу кібернетичних систем, основною управляючою ланкою яких є комп'ютер, створення та використання в злочинних цілях певної кібернетичної системи, використання в злочинних цілях існуючих кібернетичних систем [2, с. 101].

М.В. Кочаревський співвідносить поняття кіберзлочин та злочин в сфері компьютерної інформації і визначає як однин з видів злочинів в сфері інформаційної безпеки, що передбачені КК України, суспільно небезпечні, винні, вчинені суб'єктом злочину діяння, які заподіюють шкоду, забезпеченим засобами обчислювальної техніки, відносинам у сфері реалізації інформаційної потреби [3, с. 11].

Тропіна зазначає, що під кіберзлочином варто розуміти певну сукупність кримінальних правопорушень, що вчиняються в кіберпросторі за допомогою або через комп'ютерні системи чи комп'ютерні мережі, а також інших засобів доступу до кіберпростору в межах комп'ютерних систем або мереж і проти комп'ютерних систем, комп'ютерних мереж і комп'ютерних даних [4, с. 29].

Бессонов В.А. під кіберзлочинами розуміє передбачене кримінальним законодавством противоправне, винне порушення чужих прав та інтересів щодо автоматизованих систем обробки даних, повноцінного впливу, що підлягають правовій охороні майнових прав та інтересів, громадської та державної безпеки [5].

Разом з тим С. Буяджи зауважує та визначає кіберзлочинність як сукупність окреслених кримінальним законом вчинків, скоєних на тій чи іншій території або щодо об'єктів, розташованих на ній, за відповідний період часу, вчинених у віртуальному просторі шляхом деструктивного впливу на комп'ютерні системи, комп'ютерні мережі й комп'ютерні дані [6, с. 45].

Дворецький М.Ю. ототожнює поняття кіберзлочину та злочину в сфері компьютерної інформації та розуміє під ним заборонені кримінальним законом суспільно – небезпечні умисні, винні та противоправні діяння, які спрямовані на порушення недоторканості комп'ютерної інформації, яка охороняється законом та її матеріальних носіїв, що завдають шкоду правам та інтересам окремих осіб та державної та громадської безпеки [7].

На думку М. Погорецького і В. Шеломенцева кіберзлочини можна розглядати у широкому та вузькому значенні. У широкому розумінні кіберзлочини – це: кримінальні посягання, об'єктивна сторона яких відбувається у кіберпросторі, а об'єктом посягання є суспільні відносини у різноманітних сферах людської діяльності, пов'язані з використанням ресурсів кіберпростору.

У вузькому розумінні під кіберзлочинами пропонується розуміти кримінальні посягання з використанням кіберпростору на відносини керування певними процесами, пов'язаними з використанням комп'ютерних систем [8, с. 91].

В.Б. Боровиків комп'ютерні злочини визначає як навмисні суспільно небезпечні діяння, які заподіюють шкоду або створюють загрозу заподіяння шкоди суспільним відносинам, що регулює безпечне виробництво, зберігання, використання або поширення інформації або інформаційних ресурсів [9].

Пропонуємо під кіберзлочинами розуміти умисні суспільно небезпечні, протиправні, винні діяння, що посягають та заподіюють шкоду суспільним відносинам які регламентують порядок зберігання, розповсюдження, використання інформації та їх захист у кіберпросторі.

Визначення мети дослідження. У цій роботі вважаємо за доцільне, взявши за основу поняття кіберзлочину, визначити основні ознаки які притаманні кіберзлочинам та здійснити класифікацію кіберзлочинів.

Виклад основного матеріалу дослідження. Аналізуючи правовий аспект кіберзлочинів, варто зауважити, що злочини в сфері комп'ютерної інформації та злочини, що скоються за допомогою комп'ютерних технологій є видами кіберзлочинів, а не ідентичними поняттями.

Суспільна небезпека кіберзлочинів полягає у тому, що неправомірний доступ до комп'ютерної інформації може шкодити діяльності різноманітних систем державної оборони країни, системи муніципальної діяльності міста, енергетичної системи чи банківського сектору. Одночасно різного типу дії щодо спотворення достовірної інформації можуть призвести до проблем як загальнонаціонального характеру так і заподіяти шкоду правам та законним інтересам окремих осіб.

Відповідно до конвенції про кіберзлочинність 2001 року, яку Україна ратифікувала у 2005 році, визначається 4 види злочинів в сфері комп'ютерної інформації, які визначаються за їх родовим об'єктом [9]:

1) злочини проти конфіденційності інформації;

2) злочини пов'язані з використанням комп'ютера;

3) злочини пов'язані зі змістом інформації яка міститься на електронних носіях та інтернет мережі;

4) злочини пов'язані з порушенням авторських та суміжних прав.

В свою чергу кримінальний кодекс України містить дещо іншу класифікацію злочинів в сфері комп'ютерної інформації. Зокрема розділ 16 кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку включає 6 видів злочинів в сфері комп'ютерної інформації [10]:

Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку.

1. Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут.

2. Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації.

3. 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.

4. 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.

5. Перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку.

Варто зауважити, що перелік злочинів в сфері комп'ютерної інформації якій міститься в кримінальному кодексі України, не висвітлює весь спектр вчинюваних злочинних дій в кіберпросторі.

Серед науковців існує чимало класифікацій кіберзлочинам. Так зокрема О.Г. Волеводза вважає, що всі кіберзлочини можна поділити на [11, с. 311]:

Кримінальні правопорушення в сфері комп'ютерної інформації, які посягають на інформаційні комп'ютерні відносини;

– кримінальні правопорушення в інформаційному комп'ютерному просторі, які посягають на відносини реалізації прав на інформаційні ресурси;

– інші кримінальні правопорушення, для яких характерне використання комп'ютерної інформації або її складових елементів.

Водночас деякі науковці, зокрема професор Савченко А.В., вважають, що крім кримінальних правопорушень, зазначених у вищевказаному звіті, під категорію кіберзлочинів можуть підпадати й інші злочини, передбачені КК України, за умови, що знаряддям їх вчинення будуть інформаційні мережеві технології та (або) їх наслідки позначатимуться у кіберпросторі [12, с. 154].

Зокрема до таких кримінальних правопорушень вчинених у кіберпросторі автор відносить: державну зраду, шпигунство, диверсію, порушення таємниці голосування, незаконне розголошення лікарської таємниці, розголошення комерційної та банківської темниці, сутенерство та інші. Фактично можна стверджувати, що в кожному розділі особливої чистини кримінального кодексу України є кримінальні правопорушення які можуть вчинятися у кіберпросторі за допомогою ЕОМ та іншого програмного забезпечення.

Дуже цікавою, на нашу думку, є класифікація кіберзлочинів, запропонована В. Б. Дзюндзюком [13]:

1) злочини проти конституційних прав і свобод людини та громадянина, такі як порушення недоторканості приватного житла, порушення таємниці листування, телефонних переговорів, поштових, телеграфних та інших повідомлень, порушення авторських і суміжних прав;

2) злочини проти життя та здоров'я. Різноманітні рецепти виготовлення наркотичних та інших психотропних речовин за домашньою технологією виготовлення, з подальшим їх розповсюдженням;

3) злочини проти честі та гідності особи. Розповсюдження конференційної компрометуючої інформації та різного роду наклепів;

4) злочини проти власності. Різного роду кримінальні правопорушення в сфері платіжних та банківських систем;

5) злочини у сфері комп'ютерної інформації, такі як неправомірний доступ до інформації, створення, використання та розповсюдження шкідливих програм;

6) злочини проти суспільної моральності;

7) злочини проти безпеки держави. Із зростанням використання мережі Інтернет у державних структурах стає можливим нелегально дістати доступ не лише до приватної та корпоративної інформації, а й до інформації, що є державною таємницею, також стає можливим скоювати такі злочини, як шпигунство, державна зрада або розголошення державної таємниці.

Зауважмо, що кіберзлочинність не стоїть на місці, з'являються та будуть з'являтись нові види кримінальних правопорушень які вчиняються у кіберпросторі. Однак наразі вважаємо, серед найбільш характерних видів кіберзлочинів можна виділити наступні:

1. *Кримінальні правопорушення у сфері використання платіжних систем*:
   - скімінг;
   - кардинг;
   - enroll;
   - кеш-трепінг.
2. *Шахрайства сфері комп'ютерної інформації*:
   - фішинг;
   - шахрайство в сфері проведення інтернет аукціонів;
   - використання фіктивних суб'єктів електронної комерції.
3. *Кримінальні правопорушення у сфері інтелектуальної власності*:
   - інтернет піратство;
   - кардшарінг.
4. *Кримінальні правопорушення у сфері інформаційної безпеки*:
   - підроблення комп'ютерної інформації;
   - створення шкідливого програмного забезпечення;
   - розповсюдження шкідливого програмного забезпечення;
   - продаж шкідливого програмного забезпечення;
   - пошкодження комп'ютерних даних чи даних комп'ютерних програм;
   - зміна комп'ютерних даних чи даних комп'ютерних програм;
   - комп'ютерне шпигунство;
   - протиправне використання захищеної інформації.
5. *Злочини проти основ національної безпеки та оборони держави*:
   - шпигунство;
   - кібертероризм.

Отже, така значна кількість видів кіберзлочинів свідчить про те, що масштаби кіберзлочинності збільшуються. Тим самим зростає необхідність взаємодії держави із суспільством і міжнародною спільнотою з метою подолання цього негативного явища [14].

Підсумовуючи вищевикладене, варто наголосити, що наразі кіберзлочини є найбільш прогресивним види кримінальних правопорушень, які охопила практично всі сфери життєдіяльності людини, шкоди вид кіберзлочнів зазнають як держава в цілому так і окремі громадяни. Варто зауважити, що через складний і специфічний характер кіберзлочинів не існує певної універсальної моделі щодо виявлення усіх можливих категорій загроз та безпосередньо розслідування зазначеного виду кримінальних правопорушень. Аналізуючи доктринальні визначення поняття кіберзлочину, які пропонують як вітчизняні так і зарубіжні науковці, можна дійти висновку, що наразі немає чіткого поняття кіберзлочину яке б характеризувало його через його основні притаманні виключно йому ознаки.

Загалом сучасний стан кіберзлочинності в державі стрімко трансформується і пристосовується до потреб та викликів які наразі ставляться перед суспільством та державою. У сучасному світі проблема кіберзлочинності не може бути вирішена виключно на локальному рівні та без правових заходів та норм щільної міжнародної співпраці.

Література:

1. Закон України «Про основні засади забезпечення кібербезпеки України» від. 05.10.2017 № 2163-VIII.
2. Копан О. В. Словник термінів з кібербезпеки. К. : «Аванпост-Прим», 2012. 214 с.
3. Карчевский Н. В. Киберпреступление или преступление в сфере использование информационных технологий. Кібербезпека в Україні: правові та організаційні питання : матеріали всеукр. наук.-практ. конф., м. Одеса, 21 жовтня 2016 р. С. 10–15.
4. Tropina, T., Self- and Co-regulation in Fighting Cybercrime and Safeguarding Cybersecurity. In: Jähnke at al. (eds.), «Current Issues in ITU Security», Duncker & Humblot, Berlin, 2012. P. 24–31.
5. Бессонов В. А. Виктимологические аспекты предупреждения преступлений в сфере компьютерной информации. URL: https://rusneb.ru/catalog/000200_000018_RU_NLR_bibl_294121/
6. Буяджи С. А. Правове регулювання боротьби з кіберзлочинністю: теоретико-правовий аспект : дис. … канд. юрид. наук. 12.00.01. Київ, 2018. 203 с.

7. Дворецкий М. Ю. Уголовная ответственность за преступления в сфере компьютерной информации в России и зарубежных государствах. URL: https://cyberleninka.ru/article/n/ugolovnaya-otvetstvennost-za-prestupleniya-v-sfere-kompyuternoy-informatsii-v-rossii-i-zarubezhnyh-gosudarstvah/viewer
8. Погорецький М. А. Кіберзлочини: до визначення поняття. *Вісник прокуратури*. 2012. № 8. С. 89–96.
9. Боровиків В. Б. Кримінальне право. 2015 р. URL: https://stud.com.ua/53995/pravo/kriminalne_pravo
10. Кримінальний кодекс України. Закон України від 05.04.2001 № 2341-II. *Верховна Рада України*. URL: http://zakon2.rada.gov.ua/laws/show/2341-14
11. Волеводз А. Г. Противодействие компьютерным преступлениям. М. : Юрлитинформ, 2002. 496 с.
12. Савченко А. В. Кваліфікація кіберзлочинів. Протидія кіберзлочинності в Україні: правові та організаційні засади : навч. посіб. Київ : Видавничий дім «Скіф», 2012. С. 140–210.
13. Дзюндзюк В. Б. Поява і розвиток кіберзлочинності. *Державне будівництво.* 2013. № 1. URL: http://nbuv.gov.ua/UJRN/DeBu_2013_1_3
14. Васильковский І. І. Поняття, класифікація та характеристика окремих видів кіберзлочинів. *Прикарпатський юридичний вісник.* 2017. № 1. ULR: http://www.pjv.nuoua.od.ua/v1-2_2017/44.pdf

Dumchykov M. Criminal – legal characteristics of the concept and types of cybercrime

Summary. Cybercrime is a very important issue today both at the state level and at the level of the individual citizen. Its relevance is evidenced by news from around the world, statistics of criminal proceedings, problems in criminal proceedings, as well as problematic issues in the science of criminal law. All this is due primarily to the fact that cybercrime is a very specific category that is constantly evolving as technology advances.

The article is devoted to the study of doctrinal approaches to defining the concept of cybercrime, and defining the main types of cybercrime. The purpose of the article is to study the phenomenon of cybercrime, to define the concept of cybercrime and the types of these criminal offenses, to provide a general description of cybercrime. The object of research is public relations that arise in cyberspace, as well as the use of computers (computers), systems and computer networks and telecommunications networks.

Various methods of scientific knowledge were used as a methodological basis for writing this article. In particular, the method of comparison and analogy was used to study the legal regulation of different types of cybercrime. The method of observation was used to get acquainted with the nature of cybercrime and the general specifics of this phenomenon. The generalization method was used to study different types of cybercrime.

The article discusses the doctrinal definitions of the concept of cybercrime of both domestic and foreign scientists, in particular, it is observed that most scholars identify the concept of cybercrime and computer crime. The author's definition of cybercrime is given, namely intentional socially dangerous, illegal, guilty acts that encroach on and harm public relations that regulate the order of storage, dissemination, use of information and their protection in cyberspace.

It is emphasized that computer crimes and computer crimes are a type of cybercrime, not identical criminal offenses.

The article analyzes different approaches to the classification of cybercrime at the international and national levels, as well as at the doctrinal level, and proposed an author's classification of cybercrime. In particular, to classify cybercrime, according to the object of harm: criminal offenses in the field of payment systems; computer information fraud; criminal offenses in the field of intellectual property; criminal offenses in the field of information security; crimes against the foundations of national security and defense of the state.

Key words: cybercrime, crimes in the field of computer information, computer crimes, cyberspace, criminal offenses in the field of computer information.