Ярослав Неділько

студент 2 курсу магістратури юридичного факультету
Київського національного університету
імені Тараса Шевченка,
м. Київ, Україна
nedilkoyaroslav@gmail.com

УДК 343.9

ПОНЯТТЯ КІБЕРЗЛОЧИНІВ ТА ЇХ ВИДИ

Анотація. *Перші злочини, вчинені з використанням електронно-обчислювальних машин, були зареєстровані на початку 60-х років минулого століття, і в американській пресі з'явилося поняття "комп'ютерна злочинність". Незважаючи на те, що були відсутні як криміналістичні, так і правові підстави, цей термін стали використовувати в засобах масової інформації, вчені, працівники правоохоронних органів тощо. Визначення поняття "комп'ютерний злочин" вперше було надане у 1983 році в Парижі (Франція) групою експертів Організації економічного співробітництва та розвитку ООН: комп'ютерний злочин – це будь-яке незаконне, неетичне чи недозволене діяння, що стосується автоматизованої обробки даних чи передачі даних. Відтоді й донині поняття кіберзлочину є дискусійним і одним із найбільш обговорюваних у правничих колах.*

Метою статті *є висвітлення сучасних наукових і законодавчих підходів до визначення поняття кіберзлочину та формування на підставі цього авторського бачення змісту вказаного поняття.*

Автор здійснює розмежування понять "кіберзочинність" та "комп'ютерна злочинність". Щодо цього погляди науковців розділились. Одні вважають, що зазначені поняття синонімічні й замість терміна "комп'ютерні злочини" припустимо вживати понятійну категорію "кіберзлочинність (кіберзлочин)". Інші погоджуються, що ці поняття подібні, але все-таки не синонімічні. Термін "кіберзлочинність" (в англомовному варіанті – cybercrime) ширший, ніж "комп'ютерна злочинність" (computer crime), і більш точно відображає природу такого явища, як злочинність в інформаційному просторі. Оксфордський тлумачний словник визначає cyber як компонент складного слова, що стосується інформаційних технологій, мережі Інтернет, віртуальної реальності. Таке визначення дає і Кембриджський словник. Таким чином, cybercrime – це злочинність, пов'язана як з використанням комп'ютерів, так і з використанням інформаційних технологій та глобальних мереж. Разом з тим термін computer

сгіте переважно стосується злочинів у сфері використання комп'ютерів або комп'ютерних даних.

Висвітлені доктринальні та законодавчі підходи до формування поняття кіберзлочину дають змогу трактувати його як кримінальне правопорушення, що вчиняється в кіберпросторі з використанням комп'ютерної техніки (комп'ютерів, пристроїв та іншого обладнання), інформаційних технологій, комп'ютерних систем і мереж з порушенням встановленого законом порядку інформаційної безпеки, незалежно від предмета посягання та сфери застосування. Кіберзлочини поділяються на види залежно від підстави для класифікації та її мети і можуть мати як криміналістичне, так і кримінологічне чи кримінально-правове значення.

Ключові слова: *кіберзлочин; кіберзлочинність; розслідування кіберзлочинів; комп'ютерні злочини; електронно-обчислювальні машини; кіберпростір.*

На початку 60-х років минулого століття, коли були зареєстровані перші злочини, вчинені з використанням електронно-обчислювальних машин, в американській пресі з'явилося поняття "комп'ютерна злочинність". Цей термін використовували в засобах масової інформації, вчені, працівники правоохоронних органів, незважаючи на те, що для цього не було ні криміналістичних, ні правових підстав. Визначення поняття "комп'ютерний злочин" вперше було надане у 1983 році в Парижі (Франція) групою експертів Організації економічної співробітництва та розвитку ООН: комп'ютерний злочин – це будь-яке незаконне, неетичне чи не дозволене діяння, що стосується автоматизованої обробки даних чи передачі даних[1]. Відтоді й застосовується поняття кіберзлочину, яке й сьогодні лишається дискусійним і одним із найбільш обговорюваних у правничих колах.

Метою статті є висвітлення сучасних наукових і законодавчих підходів до визначення поняття кіберзлочину та формування на підставі цього авторського бачення змісту вказаного поняття.

Дослідженнями у сфері протидії кіберзлочинності, формуванням понятійного апарату цього виду злочинності та розробкою криміналістичної тактики і методики розслідування кіберзлочинів займались такі науковці, як Н. Ахтирська, В. Бутузов, С. Буяджи, В. Гавловський, І. Європіна, О. Іванченко, М. Погорецький, Л. Скалозуб, Є. Скулиш та інші.

Як правова категорія злочини, що вчиняються з використанням інформаційних технологій, або коротко – кіберзлочини, стали предметом дослідження вчених порівняно недавно.

Доречно зауважити, що на території колишнього Радянського Союзу перший злочин з використанням комп'ютера був зареєстрований 1979 року у Вільнюсі (Литва), де в результаті розкрадання була завдана шкода розміром 78 584 рублів[2].

В Україні перший комп'ютерний злочин було вчинено у 1990 році. Програма для електронно-обчислювальної машини, що здійснювала перерахунок комсомольських внесків робітників одного з промислових підприємств

[1] Див.: В Вехов и В Голубев, *Расследование компьютерных преступлений в странах СНГ: моногр.* (ВА МВД России 2004) 43–4.

[2] Див.: Ю Батурин, *Проблемы компьютерного права* (Юридическая литература 1991) 271.

Луганська на розрахунковий рахунок районного комітету комсомолу, була складена таким чином, що відрахування відповідних грошових сум здійснювалось із заробітної плати не тільки членів комсомолу, а й усіх інших робітників підприємства[3].

З подальшим розвитком інформаційних технологій поряд з поняттям "комп'ютерна злочинність" поступово починає вживатись поняття "кіберзлочинність (кіберзлочини)". Цей термін є сполученням слів "кібернетика" та "злочин".

Як зазначено у Словнику української мови: 'Кібернетика – наука про загальні закономірності процесів керування та зв'язку в організованих системах (машини, живі організми, суспільні формування тощо)'[4].

Значного поширення термін "кіберзлочини" набуває після підписання державами – членами Ради Європи та іншими державами у 2001 році Конвенції про кіберзлочинність[5]. Згодом, 21 липня 2006 року, було ратифіковано Додатковий протокол до Конвенції, що стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи[6].

Разом з тим у вітчизняній юридичній літературі, дисертаційних дослідженнях і нормативних правових актах надається перевага терміну "комп'ютерна злочинність". Зокрема, у Законі України від 19 червня 2003 року "Про основи національної безпеки України" наводяться терміни "комп'ютерна злочинність", "комп'ютерний тероризм"[7]. Ці поняття застосовуються і в Доктрині інформаційної безпеки України, затвердженій Указом Президента України від 8 липня 2009 року[8]. Натомість у Стратегії національної безпеки України, затвердженій Указом Президента України від 26 травня 2015 року, уже наявний термін "кіберзлочини"[9].

Щодо розмежування понять "кіберзочинність" та "комп'ютерна злочинність" погляди науковців розділились. Одні вважають, що зазначені поняття синонімічні й замість терміна "комп'ютерні злочини" припустимо вживати понятійну категорію "кіберзлочинність (кіберзлочин)"[10].

На думку інших, 'зазначені поняття подібні, але все-таки не синонімічні. Термін "кіберзлочинність" (в англомовному варіанті – *cybercrime*) ширший, ніж "комп'ютерна злочинність" (*computer crime*), і більш точно відображає

[3] Див.: В Вехов и В. Голубев, *Расследование компьютерных преступлений в странах СНГ* (н 1) 46.

[4] І Білодід (укл), *Словник української мови: в 11 т* (Наукова думка 1970–1980) т 4, 158.

[5] Див.: Конвенція про кіберзлочинність: міжнародний документ від 23 листопада 2001 року (2007) 65 *Офіційний вісник України.*

[6] Див.: Про ратифікацію Додаткового протоколу до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи: Закон України від 21 липня 2006 року № 23-V (2006) 39 *Відомості Верховної Ради України* 328.

[7] Див.: Про основи національної безпеки України: Закон України від 19 червня 2003 року № 964-IV (2003) 39 *Відомості Верховної Ради України* 351.

[8] Див.: Про доктрину інформаційної безпеки України: Указ Президента України від 8 липня 2009 року № 514/2009 (2009) 52 *Офіційний вісник України* 1783.

[9] Див.: Стратегія національної безпеки України: Указ Президента України від 26 травня 2015 року № 287/2015 (2015) 43 *Офіційний вісник України* 1353.

[10] Див.: І Європіна, 'Криміналістичне забезпечення протидії комп'ютерній злочинності' (дис канд юрид наук, Академія адвокатури України 2011) 12.

природу такого явища, як злочинність в інформаційному просторі'[11].

Фахівці зазначають:

> <...> Оксфордський тлумачний словник визначає '*cyber*' як компонент складного слова, що стосується інформаційних технологій, мережі Інтернет, віртуальної реальності. Практично таке саме визначення міститься і у Кембриджському словнику. Таким чином, '*cybercrime*' – це злочинність, пов'язана як з використанням комп'ютерів, так і з використанням інформаційних технологій і глобальних мереж. У той же час термін '*computer crime*' переважно стосується злочинів у сфері використання комп'ютерів або комп'ютерних даних[12].

О. Користін вважає, що термін "комп'ютерна злочинність" є вужчим за своїм змістовим навантаженням і зводить сутність явища до злочинів, що вчиняються за допомогою комп'ютера. У той же час з подальшим розвитком інформаційних технологій саме поняття "комп'ютер" стає не чітким. Наприклад, триває процес з'єднання мобільних телефонів з мережею Інтернет, випускаються так звані комунікатори і смартфони, що поєднують в собі властивості мобільних телефонів і комп'ютерів[13].

Слід звернути увагу на те, що у міжнародному праві застосовується саме термін "кіберзлочинність". Зокрема, у Конвенції Ради Європи про кіберзлочинність вживається поняття *cybercrime*, а не *computer crime*. Україна ратифікувала Конвенцію 7 вересня 2005 року[14], а отже, згідно зі ст. 9 Конституції України вона стала частиною національного законодавства, що регулює відносини у сфері боротьби з кіберзлочинністю в Україні[15].

Проте у Конвенції визначення поняття кіберзлочинності не надано. Водночас у преамбулі зазначено, що Конвенція:

> <...> є необхідною для зупинення дій, спрямованих проти конфіденційності, цілісності й доступності комп'ютерних систем, мереж і комп'ютерних даних, а також зловживання такими системами, мережами і даними шляхом встановлення кримінальної відповідальності за таку поведінку[16].

Вітчизняні та зарубіжні фахівці у науковій літературі намагались дати визначення вказаній категорії злочинів.

Так, Т. Тропіна зазначає, що під кіберзлочинністю слід розуміти сукупність злочинів, 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[17].

---

[11] Див.: В Номоконов и Т Тропина, 'Киберпреступность: угрозы, прогнозы, проблемы борьбы' (2013) 1 Information Technology and Security 86–94.

[12] Д Маріц, '"Кібератака" – війна майбутнього' (2015) 3(15) Інформація і право 104–9.

[13] Див.: О Користін та ін, *Протидія кіберзлочинності в Україні: правові та організаційні засади: навч. посіб.* (Скіф 2012) 41–2.

[14] Див.: Про ратифікацію Конвенції про кіберзлочинність: Закон України від 7 вересня 2005 року № 2824-IV (2006) 5–6 *Відомості Верховної Ради України* 71.

[15] Див.: Конституція України: Закон України від 28 червня 1996 року № 257к/96-ВР (1996) 30 *Відомості Верховної Ради України* 141.

[16] Конвенція про кіберзлочинність (н 5).

[17] Див.: Т Тропина, 'Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы' (автореф дис канд юрид наук, Дальневосточный государственный университет 2005) 9.

З таким визначенням кіберзлочинності погоджуються О. Іванченко[18] та інші вітчизняні науковці. Разом з тим С. Буяджи зауважує, що, акцентуючи увагу на специфіці кіберзлочинів та кіберпростору як осередку їх вчинення, автори цього визначення нехтують ознаками злочинності загалом, і пропонує:

> <...> тлумачити 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[19].

На наш погляд, доволі розлоге визначення кіберзлочину дає В. Бєлєнький. Він зазначає:

> Кіберзлочин – це винне, суспільно небезпечне, кримінально каране втручання в сферу безпеки обігу комп'ютерної інформації, роботу комп'ютерів, комп'ютерних програм, комп'ютерних мереж, несанкціонована модифікація комп'ютерних даних, а також інші протиправні суспільно небезпечні діяння, зроблені за допомогою комп'ютерів, комп'ютерних мереж і програм, а також за допомогою інших пристроїв із вбудованими процесорами і контролерами, які можуть мати доступ до інформаційного простору[20].

Своєю чергою, А. Русецький та Д. Куцолабський пропонують таку дефініцію:

> Кіберзлочин – це протиправне винне діяння (дія або бездіяльність), яке передбачає втручання в дані персональних комп'ютерів, комп'ютерних програм і комп'ютерних мереж, або діяння, вчинене за допомогою комп'ютерів та інших сучасних технологій, за яке передбачається кримінальна відповідальність та яке може створити особисту небезпеку для громадян, загрозу національній безпеці держави та світовій безпеці[21].

Важливим кроком на шляху до визначення на національному рівні понять "кіберзлочин" та "кіберзлочинність" стало прийняття 5 жовтня 2017 року Закону України "Про основні засади забезпечення кібербезпеки України", де у п. 8 ч. 1 ст. 1 зазначається, що:

> <...> кіберзлочин (комп'ютерний злочин) – 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[22].

А відповідно до п. 9 зазначеної статті кіберзлочинність – сукупність кіберзлочинів. Також усунуто невизначеність щодо терміна "кіберпростір". У п. 11 Закону визначено:

---

[18] Див.: О Іванченко, 'Кримінологічна характеристика кіберзлочинності, запобігання кіберзлочинності на національному рівні' (2016) 3 Актуальні проблеми вітчизняної юриспруденції 173.

[19] С Буяджи, 'Правове регулювання боротьби з кіберзлочинністю: теоретико-правові аспекти' (дис канд юрид наук, Класичний приватний університет ПВНЗ "Університет короля Данила" 2018) 25.

[20] В Бєлєнький, 'Відповідальність за кіберзлочини за кримінальним правом США, Великобританії та України' (автореф дис канд юрид наук, Академія адвокатури України 2016) 6.

[21] А Русецький та Д Куцолабський, 'Теоретико-правовий аналіз понять кіберзлочин і кіберзлочинність' (2017) 1(64) Право і безпека 75.

[22] Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 року № 2163-VIII (2017) 45 *Відомості Верховної Ради України* 403.

> <…> кіберпростір – 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[23].

Слід звернути увагу на те, що у вказаному Законі після терміна "кіберзлочин" у дужках зазначається "комп'ютерний злочин". Цей Закон був прийнятий з урахуванням зауважень науково-експертного та юридичного управлінь Апарату Верховної Ради України, які не заперечують можливості введення нової термінології у національне правове поле. Проте вона має вводитись комплексно і узгоджуватися з чинним законодавством. Зокрема, наголошувалось на необхідності визначення співвідношення понять "комп'ютерні злочини" і "кіберзлочини". Також поняття "кіберзлочин" має бути узгоджене із термінологією КК України, у якому є окремий розділ XVI "Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку"[24], та з іншими законодавчими актами, де використовується термін "комп'ютерний злочин".

Отже, можна дійти висновку, що, використовуючи конструкцію "кіберзлочин (комп'ютерний злочин)", законодавець з метою уникнення колізії при застосуванні на національному рівні цих термінів узгоджує їх. Однак це не означає, що за змістом ці поняття тотожні.

Ми поділяємо позицію тих науковців, які обґрунтовують доцільність вживання понятійної категорії "кіберзлочинність (кіберзлочин)" і погоджуємося, що термін "кіберзлочинність" є ширшим, оскільки охоплює як традиційні злочини, вчинені за допомогою комп'ютера, наприклад, крадіжки, шахрайства, вимагання тощо, так і злочини, в яких об'єктом є використання електронно-обчислювальних машин (комп'ютерів), систем, комп'ютерних мереж, а також програм та баз даних.

У кримінально-правовому аспекті треба зауважити, що при визначенні кіберзлочинів варто врахувати погляди авторів, які пропонують давати визначення і з криміналістичного погляду, оскільки воно ширше і включає діяння, де інформаційні технології є предметом, знаряддям або засобом вчинення злочину, що має значення для методики розслідування[25].

Саме таким є визначення, яке пропонують М. Погорецький і В. Шеломенцев. На їхню думку, кіберзлочини потрібно розглядати у широкому та вузькому розумінні. 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[26].

[23] Про основні засади забезпечення кібербезпеки України: Закон України (н 22).

[24] Див.: Про основні засади забезпечення кібербезпеки України: проект Закону України від 19 червня 2015 року № 2126а. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc41?pf3511=55657 (дата звернення: 20.12.2018).

[25] Див.: В Вехов, *Компьютерные преступления: способы совершения и раскрытия* (Право и Закон 1996) 24.

[26] М Погорецький та В Шеломенцев, 'Кіберзлочини: до визначення поняття' (2012) 8 Вісник прокуратури 89–96.

У вузькому розумінні під кіберзлочинами пропонується розуміти 'кримінальні посягання з використанням кіберпростору на відносини керування певними процесами, пов'язаними з використанням комп'ютерних систем'[27].

Схвалюючи таке трактування, водночас вважаємо найбільш сучасним і практично значущим визначення, яке надає Н. Ахтирська:

> Кіберзлочини – це кримінальні правопорушення, що вчиняються з використанням комп'ютерної техніки (комп'ютерів, пристроїв та іншого обладнання), інформаційних технологій, комп'ютерних систем та мереж з порушенням встановленого законом порядку інформаційної безпеки, незалежно від предмета посягання та сфери застосування[28].

Разом з тим до зазначеної дефініції пропонуємо додати, що такі кримінальні правопорушення вчиняються в кіберпросторі.

У криміналістичній літературі кіберзлочини поділяють на види здебільшого залежно від об'єкта, предмета посягання, способу вчинення тощо. Загальноприйнятою залишається класифікація за структурою Конвенції про кіберзлочинність. Відповідно до Конвенції фахівці виділяють 4 групи[29]. Першу групу кіберзлочинів становлять правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем:

1) незаконний доступ – доступ до цілої комп'ютерної системи або її частини без права на це з метою отримання комп'ютерних даних або з іншою недобросовісною метою (ст. 2 Конвенції);

2) нелегальне перехоплення – протиправне перехоплення технічними засобами комп'ютерних даних (ст. 3 Конвенції);

3) втручання у дані – навмисне пошкодження, знищення, погіршення, зміна або приховування комп'ютерної інформації (ст. 4 Конвенції);

4) втручання в систему – перешкоджання функціонуванню комп'ютерної системи шляхом введення, передачі, пошкодження, знищення, погіршення, зміни або приховування комп'ютерних даних (ст. 5 Конвенції);

5) зловживання пристроями – навмисне, без права на це, їх виготовлення, продаж, придбання для використання, розповсюдження або надання для використання іншим чином (ст. 6 Конвенції).

До другої групи належать правопорушення, пов'язані з комп'ютерами:

1) підробка, пов'язана з комп'ютерами, – введення, зміна, знищення або приховування комп'ютерних даних, що призводить до створення недійсних даних з метою, щоб вони розглядались наче справжні, незалежно від того, можна чи ні їх прочитати чи зрозуміти (ст. 7 Конвенції);

2) шахрайство з використанням комп'ютерів – позбавлення іншої особи її власності шляхом введення, зміни, знищення чи приховування комп'ютерних даних або втручання у функціонування комп'ютерної системи (ст. 8 Конвенції).

[27] М Погорецький та В Шеломенцев, 'Кіберзлочини: до визначення поняття' (н 26).

[28] Н Ахтирська, *Актуальні проблеми розслідування кіберзлочинів: навч. посіб.* (Київський університет 2018) 12.

[29] Див.: В Болгов та ін, *Організаційно-правове забезпечення протидії кримінальним правопорушенням, що вчиняються з використанням інформаційних технологій: наук.-практ. посіб.* (Національна академія прокуратури України 2015) 27–30.

До третьої групи належать правопорушення, пов'язані зі змістом, зокрема правопорушення, пов'язані з дитячою порнографією, – вироблення, пропонування або надання, розповсюдження або передача, здобуття, володіння (ст. 9 Конвенції).

Четверту групу становлять правопорушення, пов'язані з порушенням авторських та суміжних прав (ст. 10 Конвенції)[30].

Варто зазначити, що у Додатковому протоколі до Конвенції окреслено ще одну групу – акти расизму та ксенофобії, вчинені з використанням комп'ютерних мереж (ст. 3)[31].

За об'єктами посягання наковці виділяють такі групи: 1) злочини проти конфіденційності, цілісності та доступності комп'ютерних даних і комп'ютерних мереж; 2) економічні комп'ютерні злочини; 3) комп'ютерні злочини проти особистих прав і недоторканності приватної сфери; 4) комп'ютерні злочини проти суспільних і державних інтересів[32].

З урахуванням мотивації злочинців О. Пфо пропонує кіберзлочини умовно поділити на категорії:

– кібершахрайство – з метою заволодіння коштами;
– кібершахрайство – з метою заволодіння інформацією (для власного користування або для подальшого продажу);
– втручання в роботу інформаційних систем – з метою отримання доступу до автоматизованих систем управління (для навмисного пошкодження за винагороду або для завдання шкоди конкурентам);
– інші злочини[33].

На наш погляд, сьогодні доволі поширеною і практично прийнятою є класифікація злочинів на:

1) насильницькі чи інші потенційно небезпечні;

2) ненасильницькі.

До першої групи фахівці відносять кібертероризм, погрозу фізичної розправи, кіберпереслідування, кіберсталкінг (протиправне сексуальне домагання та переслідування іншої особи через Інтернет), дитячу порнографію (створення порнографічних матеріалів, виготовлених із зображенням дітей, розповсюдження цих матеріалів, отримання доступу до них).

Другу групу становлять кіберкрадіжки, кібершахрайство, кібершпигунство, кібервандалізм, розповсюдження спаму та вірусних програм. Є також й інші ненасильницькі кіберзлочини, наприклад реклама послуг проституції, азартні ігри в Інтернеті, відмивання грошей за допомогою електронного переміщення тощо[34].

[30] Див.: Конвенція про кіберзлочинність (н 5).

[31] Див.: Додатковий протокол до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи: міжнародний документ від 28 січня 2003 року. URL : http://zakon.rada.gov.ua/laws/show/994_687 (дата звернення: 20.12.2018).

[32] Див.: І Діордіца, 'Поняття та зміст кіберзлочинності' (2017) 3 (2) Науковий вісник Херсонського державного університету. Серія "Юридичні науки" 175.

[33] О Пфо, 'Основні поняття і класифікація кіберзлочинності' *Актуальні задачі та досягнення у галузі кібербезпеки: всеукр. наук.-практ. конф.* (КНТУ 2016) 33–4.

[34] Див.: О Користін та ін, *Протидія кіберзлочинності в Україні: правові та організаційні засади* (н 13).

У чинному Кримінальному кодексі України хоча і не закріплено поняття кіберзлочину, проте в розділі XVI "Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку" виокремлені такі види злочинів:

1) несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку (ст. 361);

2) створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут (ст. 361[1]);

3) 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 (ст. 361[2]);

4) 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 (ст. 362);

5) 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 (ст. 363);

6) перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку (ст. 363[1])[35].

Цілком слушно зазначає Н. Ахтирська, що до цього переліку можна віднести деякі статті КК України, де у диспозиції також міститься вказівка на спосіб вчинення злочину з використанням комп'ютера чи інформаційних (автоматизованих) систем. Зокрема, склади злочинів, передбачені у ч. 3 ст. 190 КК України, – "шахрайство, вчинене у великих розмірах або шляхом незаконних операцій з використанням електронно-обчислювальної техніки"; ч. 4 ст. 301 КК України – "примушування неповнолітніх до участі у створенні творів, зображень або кіно- та відеопродукції, комп'ютерних програм порнографічного характеру"; ст. 200 "Незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, електронними грошима, обладнанням для їх виготовлення", ст. 376[1] "Незаконне втручання в роботу автоматизованої системи документообігу суду". Але наданим переліком не варто обмежуватись, оскільки можуть бути й інші види злочинів, що вчиняються з використанням комп'ютерних технологій[36].

Отже, доходимо висновку, що висвітлені доктринальні та законодавчі підходи до формування поняття кіберзлочину дають змогу розуміти під таким –

[35] Див.: Кримінальний кодекс України: Закон України від 5 квітня 2001 року № 2341-III. URL: http://zakon.rada.gov.ua/laws/show/2341-14 (дата звернення: 20.12.2018).

[36] Н Ахтирська, *Актуальні проблеми розслідування кіберзлочинів: навч. посіб.* (н 28) 17–9.

кримінальне правопорушення, що вчиняється в кіберпросторі з використанням комп'ютерної техніки (комп'ютерів, пристроїв та іншого обладнання), інформаційних технологій, комп'ютерних систем та мереж з порушенням встановленого законом порядку інформаційної безпеки, незалежно від предмета посягання та сфери застосування. А також, що види кіберзлочинів виокремлюються залежно від підстави для класифікації та її мети і можуть мати як криміналістичне, так і кримінологічне чи кримінально-правове значення.

REFERENCES

List of legal dokuments

Legislation

1. Dodatkovyi protokol do Konventsii pro kiberzlochynnist, yakyi stosuietsia kryminalizatsii dii rasystskoho ta ksenofobnoho kharakteru, vchynenykh cherez kompiuterni systemy [The Additional Protocol to the Convention on Cybercrime, Concerning the Criminalization of Racist and Xenophobic Acts Committed through Computer Systems] vid 28 sichnia 2003 roku. URL: http://zakon.rada.gov.ua/laws/show/994_687 (accessed: 20.12.2018) *(in Ukrainian)*.
2. Konstytutsiia Ukrainy [Constitution of Ukraine]: Zakon Ukrainy [Law of Ukraine] vid 28 chervnia 1996 roku № 257k/96-VR (1996) 30 *Vidomosti Verkhovnoi Rady Ukrainy* 141 *(in Ukrainian)*.
3. Konventsiia pro kiberzlochynnist [Convention on Cybercrime]: mizhnarodnyi dokument [international document] vid 23 lystopada 2001 roku (2007) 65 *Ofitsiinyi visnyk Ukrainy (in Ukrainian)*.
4. Kryminalnyi kodeks Ukrainy [Criminal Code of Ukraine]: Zakon Ukrainy [Law of Ukraine] vid 5 kvitnia 2001 roku № 2341-III. URL: http://zakon.rada.gov.ua/laws/show/2341-14 (accessed: 20.12.2018) *(in Ukrainian)*.
5. Pro doktrynu informatsiinoi bezpeky Ukrainy [On Doctrine of Information Security of Ukraine]: Ukaz Prezydenta Ukrainy [Decree of the President of Ukraine] vid 8 lypnia 2009 roku № 514/2009 (2009) 52 *Ofitsiinyi visnyk Ukrainy* 1783 *(in Ukrainian)*.
6. Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy [On Basic Principles of Providing Cyber Security of Ukraine]: proekt Zakonu Ukrainy [draft law of Ukraine] vid 19 chervnia 2015 roku № 2126a. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc41?pf3511=55657 (accessed: 20.12.2018) *(in Ukrainian)*.
7. Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy [On Basic Principles of Providing Cyber Security of Ukraine]: Zakon Ukrainy [Law of Ukraine] vid 5 zhovtnia 2017 roku № 2163-VIII (2017) 45 *Vidomosti Verkhovnoi Rady Ukrainy* 403 *(in Ukrainian)*.
8. Pro osnovy natsionalnoi bezpeky Ukrainy [On the Fundamentals of National Security of Ukraine]: Zakon Ukrainy [Law of Ukraine] vid 19 chervnia 2003 roku № 964-IV (2003) 39 *Vidomosti Verkhovnoi Rady Ukrainy* 351 *(in Ukrainian)*.
9. Pro ratyfikatsiiu Dodatkovoho protokolu do Konventsii pro kiberzlochynnist, yakyi stosuietsia kryminalizatsii dii rasystskoho ta ksenofobnoho kharakteru, vchynenykh cherez kompiuterni systemy [On Ratification of the Additional Protocol to the Convention on Cybercrime, Concerning the Criminalization of Racist and Xenophobic Acts Committed through Computer Systems]: Zakon Ukrainy [Law of Ukraine] vid 21 lypnia 2006 roku № 23-V (2006) 39 *Vidomosti Verkhovnoi Rady Ukrainy* 328 *(in Ukrainian)*.
10. Pro ratyfikatsiiu Konventsii pro kiberzlochynnist [On Ratification of the Convention on Cybercrime]: Zakon Ukrainy [Law of Ukraine] vid 7 veresnia 2005 roku № 2824-IV (2006) 5–6 *Vidomosti Verkhovnoi Rady Ukrainy* 71 *(in Ukrainian)*.
11. Stratehiia natsionalnoi bezpeky Ukrainy [The National Security Strategy of Ukraine]: Ukaz Prezydenta Ukrainy [Decree of the President of Ukraine] vid 26 travnia 2015 roku № 287/2015 (2015) 43 *Ofitsiinyi visnyk Ukrainy* 1353 *(in Ukrainian)*.

Bibliography

Authored books

12. Akhtyrska N, *Aktualni problemy rozsliduvannia kiberzlochyniv: navch. posib. [Actual Problems of Cybercrime Investigation: teach. manual]* (Kyivskyi universytet 2018) 12 *(in Ukrainian)*.
13. Baturin Ju, *Problemy komp'juternogo prava [Computer Law Problems]* (Juridicheskaja literatura 1991) 271 *(in Russian).*

14. Bolhov V ta in, *Orhanizatsiino-pravove zabezpechennia protydii kryminalnym pravoporushenniam, shcho vchyniaiutsia z vykorystanniam informatsiinykh tekhnolohii: nauk.-prakt. posib. [Organizational and Legal Support of Counteraction to a Criminal Offense Committed with the Use of Information Technologies: scen.-pract. manual]* (Natsionalna akademiia prokuratury Ukrainy 2015) 27–30 *(in Ukrainian)*.
15. Korystin O ta in, *Protydiia kiberzlochynnosti v Ukraini: pravovi ta orhanizatsiini zasady: navch. posib. [Countering Cybercrime in Ukraine: Legal and Organizational Foundations: teach. manual]* (Skif 2012) 50–6 *(in Ukrainian)*.
16. Vehov V, *Komp'juternye prestuplenija: sposoby sovershenija i raskrytija [Computer Crimes: Methods of Committing and Disclosing]* (Pravo i Zakon 1996) 24 (*in Russian*).
17. Vehov V i Golubev V, *Rassledovanie komp'juternyh prestuplenij v stranah SNG: monogr. [Investigation of Computer Crimes in the CIS Countries: monogr.]* (VA MVD Rossii 2004) 43–4 *(in Russian).*

Dictionaries

18. Bilodid I (comp), *Slovnyk ukrainskoi movy: v 11 t [Dictionary of the Ukrainian Language: in 11 t]* (Naukova dumka 1970–1980) *(in Ukrainian)*.

Dissertations

19. Buiadzhy S, 'Pravove rehuliuvannia borotby z kiberzlochynnistiu: teoretyko-pravovi aspekty' ['Legal Regulation of the Fight against Cybercrime: Theoretical and Legal Aspects'] (dys kand yuryd nauk, Klasychnyi pryvatnyi universytet PVNZ "Universytet korolia Danyla" 2018) 25 *(in Ukrainian)*.
20. Yevropina I, 'Kryminalistychne zabezpechennia protydii kompiuternii zlochynnosti' ['Forensic Provision against Computer Crime'] (dys kand yuryd nauk, Akademiia advokatury Ukrainy 2011) 12 *(in Ukrainian)*.

Thesis abstracts

21. Bielienkyi V, 'Vidpovidalnist za kiberzlochyny za kryminalnym pravom SShA, Velykobrytanii ta Ukrainy' ['Responsibility for Cybercrime in US, UK and Ukraine Criminal Law'] (avtoref dys kand yuryd nauk, Akademiia advokatury Ukrainy 2016) 6 *(in Ukrainian)*.
22. Tropina T, 'Kiberprestupnost': ponjatie, sostojanie, ugolovno-pravovye mery bor'by' ['Cybercrime: Concept, State, Criminal Law Measures to Combat'] (avtoref diss kand jurid nauk, Dal'nevostochnyj gosudarstvennyj universitet 2005) 9 *(in Russian).*

Conference papers

23. Pfo O, 'Osnovni poniattia i klasyfikatsiia kiberzlochynnosti ['Basic Concepts and Classification of Cybercrime'] *Aktualni zadachi ta dosiahnennia u haluzi kiberbezpeky: vseukr. nauk.-prakt. konf. [Current Tasks and Achievements in the Field of Cyber Security: All-Ukrainian scien.-pract. conf.]* (KNTU 2016) 33–4 *(in Ukrainian)*.

Journal articles

24. Diorditsa I, 'Poniattia ta zmist kiberzlochynnosti' ['The Concept and Content of Cybercrime'] (2017) 3(2) Naukovyi visnyk Khersonskoho derzhavnoho universytetu. Seriia "Yurydychni nauky" 175 *(in Ukrainian)*.
25. Ivanchenko O, 'Kryminolohichna kharakterystyka kiberzlochynnosti, zapobihannia kiberzlochynnosti na natsionalnomu rivni' ['Criminological Characteristics of Cybercrime, Prevention of Cybercrime at the National Level'] (2016) 3 Aktualni problemy vitchyznianoi yurysprudentsii 173 *(in Ukrainian)*.
26. Marits D, '"Kiberataka" – viina maibutnoho' ['"Ciberataka" is the war of the future'] (2015) 3(15) Informatsiia i pravo 104–9 *(in Ukrainian)*.
27. Nomokonov V i Tropina T, 'Kiberprestupnost': ugrozy, prognozy, problemy bor'by' ['Cybercrime: Threats, Predictions, Problems of the Struggle'] (2013) 1 Information Technology and Security 86–94 *(in Russian)*.
28. Pohoretskyi M ta Shelomentsev V, 'Kiberzlochyny: do vyznachennia poniattia' ['Cybercrime: to Define the Concept'] (2012) 8 Visnyk prokuratury 89–96 *(in Ukrainian)*.
29. Rusetskyi A ta Kutsolabskyi D, 'Teoretyko-pravovyi analiz poniat kiberzlochyn i kiberzlochynnist' ['Theoretical and Legal Analysis of the Concepts of Cybercrime and Cybercriminality'] (2017) 1(64) Pravo i bezpeka 75 *(in Ukrainian)*.

Неділько Я. Поняття кіберзлочинів та їх види. *Науковий часопис Національної академії прокуратури України.* 2018. № 4(20). С. 49–60 <http://www.chasopysnapu.gp.gov.ua/ua/pdf/4-2018/nedilko.pdf>

Yaroslav Nedilko
student of 2nd year of law faculty magistracy,
Taras Shevchenko National University of Kyiv,
Kyiv, Ukraine

CONCEPT OF CYBERCRIMES AND THEIR TYPES

Abstract. *The first crimes committed using electronic computing machines were registered in the early 60's of the last century, and the term "computer crime" appeared in the American press. Despite the fact that there were no criminal as well as legal grounds, this term was used in mass media, scientists, law enforcement officers, and others like that. For the first time, the definition of "computer crime" was introduced in 1983 in Paris (France) by a group of experts from the Organization for Economic Cooperation and Development: a computer crime is any unlawful, unethical or unlawful act concerning automated data processing or transmission data. Since then and until now, the concept of cybercrime is debatable and one of the most discussed in the legal circles.*

The purpose of the article *– to highlight the modern scientific and legislative approaches to the definition of the concept of cybercrime and to formulate, on the basis of this author's vision, the content of the concept.*

The author delimits between the concepts of "cybercrime" and "computer crime". In this regard were divided the opinions of scientists. Some believe that these notions are synonymous and instead of the term "computer crimes" it is permissible to use the conceptual category "cybercrime". Others agree that these concepts are very similar, but they are not synonymous. The term "cybercrime" (in the English version – cybercrime) is wider than "computer crime" and more accurately reflects the nature of such phenomenon as crime in the information space. The Oxford Explanatory Dictionary defines cyber as a component of a complex word related to information technology, the Internet, virtual reality. This definition is also given by the Cambridge Dictionary. Thus, cybercrime – is a crime linked both to the use of computers and the use of information technology and global networks. At the same time, the term computer crime predominantly refers to crimes committed against computers or computer data.

The doctrinal and documented approaches to the formation of the concept of cybercrime make it possible to treat it as a criminal offense committed in cyberspace with the use of computer equipment (computers, devices and other equipment), information technology, computer systems and networks in violation of the established law of the order of information security, regardless of the subject of the attack and the scope of application. Cybercrime is divided into types depending on the basis of the classification and its purpose and can have both forensic, and criminological or criminal law significance.

Keywords: *cybercrime; cybercrimes; investigation of cybercrime; computer crimes; electronic computers; cyber space.*