

УДК 342.9

КОМП'ЮТЕРНІ ПРАВОПОРУШЕННЯ ТА ІНФОРМАЦІЙНІ ПРАВОПОРУШЕННЯ: АСПЕКТИ СПІВВІДНОШЕННЯ

**С.А. ПРАВДЮК, здобувач¹,
Національний університет біоресурсів і
природокористування України**

Аналізуються наукові позиції щодо визначення поняття «комп'ютерні правопорушення», досліджується кримінальне законодавство у цій сфері, виокремлюються особливості (риски) комп'ютерних правопорушень, а також визначається співвідношення понять «інформаційні правопорушення» (інформаційні злочини) та «комп'ютерні правопорушення» (комп'ютерні злочини).

Правопорушення, інформаційні правопорушення, комп'ютерні правопорушення, кіберзлочинність, інформаційні злочини, комп'ютерні злочини.

Найбільш розповсюдженим критерієм класифікації правопорушень загалом та інформаційних зокрема є суспільна небезпечність (суспільна шкідливість), згідно з яким вони розподіляються на злочини та проступки. Серед усього різноманіття інформаційних правопорушень найбільшу суспільну небезпеку мають саме інформаційні злочини. Водночас слід констатувати, що, незважаючи на чималу кількість робіт у цьому контексті, дослідження даної проблематики так і знайшло адекватного наукового пізнання. Більше того, доволі часто у наукових розвідках відсутнє розмежування понять «інформаційні правопорушення» (інформаційні злочини) та «комп'ютерні правопорушення» (комп'ютерні злочини).

Зазначене вище і обумовило актуальність написання цієї наукової роботи. **Метою** статті є окреслення співвідношення понять «комп'ютерні правопорушення» та «інформаційні правопорушення». Задля досягнення цього автором поставлено такі завдання:

- проаналізувати наукові позиції щодо визначення поняття «комп'ютерні правопорушення»;
- дослідити кримінальне законодавство у цій сфері;
- виокремити особливості (риски) комп'ютерних правопорушень;
- визначити співвідношення понять «інформаційні правопорушення» (інформаційні злочини) та «комп'ютерні правопорушення» (комп'ютерні злочини).

¹ Науковий керівник – доктор юридичних наук, професор В.І. Курило

Аналіз Кримінального кодексу України з порушеної тематики дає змогу зробити декілька висновків. По-перше, з 447 злочинів, що передбачено Кримінальним кодексом України, сьома частина є інформаційними правопорушеннями, враховуючи широке розуміння інформаційних правопорушень. Кількість складів інформаційних злочинів, що передбачено чинним КК України збільшилась майже 1,5 рази. По-друге, інформаційні злочини розміщуються у 17 розділах Особливої частини КК України з двадцяти. По-третє, найбільша кількість складів інформаційних правопорушень знаходяться в розділі V «Злочини проти виборчих, трудових та інших особистих прав і свобод людини і громадянина» (одинадцять), розділі VII «Злочини у сфері господарської діяльності» (вісім), розділі XVIII «Злочини проти правосуддя» (вісім). По-четверте, у розділі V «Злочини проти виборчих, трудових та інших особистих прав і свобод людини і громадянина» кількість складів інформаційних злочинів превалює над іншими складами інформаційних правопорушень. По-п'яте, Особлива частина КК України передбачає окремий розділ, усі склади злочинів яких є інформаційними. По-шосте, більшість інформаційних злочинів у КК України є такими через особливості діяння як об'єктивної сторони, яке має інформаційний характер. На другому місці є інформаційні злочини, предметом яких є різного роду інформація. Невелика частина злочинів є злочинами, що мають ознаки як перших, так і других. По-сьоме, кількість «звичайних» злочинів можуть бути охарактеризовані також як інформаційні, беручи до уваги конкретні обставини суспільно небезпечного діяння. Наприклад, просто крадіжка не є інформаційним злочином, а є злочином проти власності. У разі скоєння крадіжки електронних збережень слід говорити про інформаційний злочин. До того ж, «до таких злочинів, що перейшли з реального, фізичного світу до кіберпростору, можна назвати тероризм, розповсюдження порнографічної інформації, відмивання грошей тощо» [1]. Особливе занепокоєння у міжнародному товаристві нині займає проблема протидії інформаційному тероризму (кібертероризму). По-восьме, найбільш розповсюдженими видами покарань за скоєння інформаційних злочинів згідно з кримінальним законодавством України є: штраф, позбавлення права обіймати певні посади або займатися певною діяльністю, виправні роботи, обмеження волі.

Особливе місце у КК України відведено таким видам інформаційних правопорушень, як комп'ютерні злочини. Зростання масштабів використання комп'ютерних інформаційних систем у житті суспільства, інтенсивна комп'ютеризація діяльності органів державної влади, популярність глобальних комп'ютерних мереж Інтернету в усіх сферах призвела до появи та перманентної динаміки різноманітних злочинних посягань, пов'язаних з викраденням, перекиданням або знищенням комп'ютерної інформації, неправомірним використанням комп'ютерів, а також умисним порушенням роботи комп'ютерів.

Так, М.В. Рудик зазначає: «якщо протягом 2002–2006 р. підрозділами ДСБЕЗ розкрито 2535 злочинів, що посягали на комп'ютерну інформацію (у 2002 р. було розкрито 311 злочинів (з яких до суду направлено 266), у 2003 – 464 (з яких до суду направлено 290), у 2004 – 562 (з яких до суду направлено 367), то у 2005 р. – 615 (з яких до суду направлено 364), а в 2006 р. – 583 (з яких до суду направлено 415) злочини. Найбільшу питому вагу мають злочини у сфері комп'ютерних та Інтернет-технологій – 29 %, сфері функціонування електронних платежів або платіжних карток – 15 %; сфері телекомунікацій – 24%» [2, с. 4].

Не менш цікавим є також і зарубіжний досвід у цій сфері. Наприклад, аналіз російськими вченими статистичних даних зареєстрованих злочинів у сфері комп'ютерної інформації у Російській Федерації упродовж 2000–2010 рр. дав змогу зробити висновок, що найбільше зростання злочинів було в 2005 та 2009 роках. Але у 2010 р. відбувся спад в реєстрації на 18,6 % [3, с. 31]. Внаслідок цього дослідники зазначають про суперечливу динаміку, причинами якої є не фактичний стан злочинності, так як загальна тенденція – це зростання числа кіберзлочинів, а зміни в правовій політиці держави, відомств, органів, що займаються виявленням, обліком, розслідуванням і розкриттям даної категорії злочинів [3, с. 31]. Інші ж автори стверджують, що це також пов'язано з різними методиками рахування кількості вказаних злочинів правоохоронними органами [4, с. 126].

Перед тим як розкрити специфіку та особливості комп'ютерних злочинів як найбільш суспільно небезпечних інформаційних правопорушень, вважаємо за необхідне визначити співвідношення понять «інформаційні правопорушення» та «комп'ютерні правопорушення», оскільки доволі часто ці поняття абсолютно не розрізняються та навіть ототожнюються. Наприклад, навіть такий знаний спеціаліст цієї тематики як І.Л. Бачило зауважує: «слабка вивченість комп'ютерних правопорушень та інших правопорушень є причиною низького відсотка виявлення інформаційних і комп'ютерних правопорушень...» [5, с. 417].

Як слушно зауважує К.І. Беляков з цього приводу: «З одного боку, вживання наведених понять на побутовому рівні обумовлене, мабуть, використанням дослівного перекладу іншомовних сполучень (калька), що не є чимось небезпечним у разі відсутності визначення таких понять у вітчизняній науці. Щоправда, це надає їм загадкового, екзотичного забарвлення, але лише для пересічних громадян. З іншого боку, з урахуванням лексико-семантичної специфіки наукового стилю ділового мовлення деяких країн світу (наприклад, тяжіння американського варіанта англійської мови до скорочень), ми вважаємо, що пряме їх використання, і тим більше у вітчизняній галузевій юридичній терміносистемі, як мінімум, невиправдане і недоречне, а, як максимум, – неприпустиме» [6, с. 267–268].

Крім того, в наукових джерелах поряд з вищезазначеним поняттям («комп'ютерні правопорушення») дослідники як синонімічні використовують і інші: «е-правопорушення», «правопорушення у сфері високих технологій», «правопорушення, що вчинюються з використанням інформаційних технологій», «правопорушення, що вчиняються в галузі комп'ютерних технологій» т. ін.

Як слушно зауважують А.А. Протасевич, Л.П. Зверянська, на даний момент, на піку зростання кіберзлочинів, не виведено єдиного загальноновизнаного поняття кіберзлочинності [3, с. 33].

Наприклад, у п. 14 Доповіді Комітету II Десятого Конгресу ООН 2000 р. з попередження злочинності і поводження з правопорушниками виокремлено дві категорії злочинів: 1) кіберзлочини у вузькому розумінні («комп'ютерні» злочини) – будь-яке протиправне діяння, здійснюване шляхом електронних операцій, метою якого є подолання захисту комп'ютерних систем і оброблюваних ними даних; 2) кіберзлочини в широкому розумінні (злочини, пов'язані з використанням комп'ютерів) – будь-яке протиправне діяння, що вчинюється шляхом або в зв'язку з комп'ютерною системою або мережею, включаючи такі злочини, як незаконне зберігання, пропонування або розповсюдження інформації через комп'ютерні системи або мережі [7, с. 338].

Дослідження вітчизняного кримінального законодавства дозволяє констатувати, що в Україні передбачено кримінальну відповідальність за комп'ютерні злочини у вузькому розумінні, тобто в розділі XVI «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» Особливої частини Кримінального кодексу України жодна із «шести статей не містить норми, згідно з якою можна було притягти до відповідальності особу, що вчинила, наприклад, шахрайство шляхом незаконних операцій з використанням електронно-обчислювальної техніки (ч. 3 ст. 190 КК), або окремі суспільно-небезпечні дії, передбачені ст. 200 КК» [8].

Як зазначають А.А. Музика та Д.С. Азаров, «застосування комп'ютерів для вчинення названих діянь є лише певним способом вчинення злочину, який зазвичай не включається до обов'язкових ознак об'єктивної сторони складу злочину. За наявності певних фактичних обставин ці злочини можуть кваліфікуватись за сукупністю зі злочинами, передбаченими Розділом XVI Особливої частини КК України [9, с. 234].

Згідно з рекомендаціями експертів ООН термін «кіберзлочинність» охоплює будь-який злочин, який може скоюватись за допомогою комп'ютерної системи чи мережі, в рамках комп'ютерної системи чи мережі [10].

На думку О.В. Суслопарова, під комп'ютерними злочинами слід розуміти суспільно небезпечні протиправні діяння, що мають свій родовий об'єкт суспільні відносини з забезпечення інформаційної безпеки суспільства, які посягають на нормальний режим охорони, обробки і

передачі даних в комп'ютерах (комп'ютерних системах) [4, с. 9]. Тобто комп'ютерним злочином за міркуваннями дослідника є лише такі злочини, що мають своєю метою несанкціоноване отримання даних, що містить комп'ютер. Та чи не буде комп'ютерним злочином злочин, що вчиняється за допомогою комп'ютера?

Саме така позиція міститься у українській науковій літературі, зокрема Юридичній енциклопедії, згідно з якою пропонується таке визначення поняття «комп'ютерна злочинність»: «... вид злочинності, пов'язаний з незаконним використанням сучасних інформаційних технологій і засобів комп'ютерної техніки» [11, с. 197]. Аналіз цього визначення дозволяє констатувати, що це визначення має доволі широке трактування та не відображає сутність і зміст комп'ютерних злочинів. Так, використання сучасних інформаційних технологій є одним із способів скоєння інформаційних злочинів. Комп'ютерні ж злочини скоюються винятково за допомогою комп'ютерів чи інших комп'ютерних систем.

До того ж, дослідження науково-практичних коментарів у цьому контексті дозволило дійти висновку, що предметом злочинів, передбачених розділом 16 КК України є: 1) електронно-обчислювальна машина (далі – ЕОМ) – комп'ютер – комплекс технічних засобів, призначених для автоматичної обробки інформації в процесі вирішення обчислювальних та інформаційних задач; 2) автоматизовані комп'ютерні системи (далі – АКС) – сукупність взаємопов'язаних ЕОМ, периферійного обладнання та програмного забезпечення, призначених для автоматизації прийому, зберігання, обробки, пошуку і видачі інформації споживачам. Комп'ютерні системи можуть бути регіонального та галузевого характеру; 3) комп'ютерні мережі (мережа ЕОМ) – це з'єднання декількох комп'ютерів (ЕОМ) та комп'ютерних систем, що взаємопов'язані і розташовані на фіксованій території та орієнтовані на колективне використання загальномережових ресурсів. Комп'ютерні мережі передбачають спільне використання ресурсів обчислювальних центрів (далі – ОЦ), запуск загальних програм, які входять до комп'ютерних систем; 4) носії комп'ютерної інформації – фізичні об'єкти, машинні носії, призначені для постійного зберігання, перенесення і обробки комп'ютерної інформації. До них відносяться гнучкі магнітні диски (дискети), жорсткі магнітні диски (вінчестери), касетні магнітні стрічки (стримери), магнітні барабани, магнітні карти тощо; 5) комп'ютерна інформація – це текстова, цифрова, графічна чи інша інформація (дані, відомості) про осіб, предмети, події, яка існує в електронному виді, зберігається на відповідних електронних носіях і може використовуватися, оброблятися або змінюватися за допомогою ЕОМ (комп'ютерів).

Таким чином, **комп'ютерними злочинами слід визнати суспільно небезпечні протиправні карані діяння деліктоздатного суб'єкта, що скоюються за допомогою комп'ютера чи інших комп'ютерних систем**

(мереж), а також посягають на нормальний режим охорони, обробки і передачі даних в комп'ютерах (комп'ютерних системах).

Фахівці цієї проблематики стверджують, що кіберзлочини мають низку особливостей. Так, Сьюзанн В. Бреннер виділяє наступні ознаки «кіберзлочинів», що відрізняє їх від «звичайних» злочинних посягань та значно підвищує їх суспільну небезпечність. По-перше, «кіберзлочин» не вимагає фізичного зближення жертви та суб'єкта злочину в момент вчинення такого. По-друге, «кіберзлочин» є «автоматизованим» злочином. Це означає, що суб'єкт злочину за допомогою комп'ютерних технологій протягом короткого періоду часу може збільшити кількість протиправних діянь до декількох тисяч. По-третє, суб'єкт «кіберзлочину» не підвладний обмеженням, які існують у реальному, фізичному світі. Так, «кіберзлочини» можуть бути вчинені миттєво, і тому потребують швидкої реакції у відповідь. І, по-четверте, «кіберзлочинність» і досі залишається новим феноменом, і наука ще не здатна встановлювати моделі розповсюдження різних видів злочинів географічно та демографічно, як це має місце зі злочинами, що вчиняються у реальному, фізичному світі [7].

Аналіз зазначеної вище позиції, дає змогу констатувати, що запропонований дослідницею перелік особливостей кіберзлочинів не відображає їх специфіку, оскільки усі ці особливості є особливостями будь-яких інформаційних правопорушень.

Щодо безпосередньо співвідношення понять «комп'ютерні правопорушення» та «інформаційні правопорушення», то близькою нашому баченню є позиція О.В. Полушкіна, який зауважує: «информационное правонарушение не сводится к правонарушению, связанному только с использованием компьютерной техники, прочих ЭВМ и связанных с ними технологий, как это может показаться на первый взгляд. Так называемые «киберпреступления» и иные правонарушения, совершаемые с использованием ЭВМ и их компонентов, представляют собой относительно меньшую часть информационных правонарушений. ... Так называемая киберпреступность – лишь наиболее современный и ярко выраженный вид информационных правонарушений в целом и, соответственно, компьютерная техника и сеть ЭВМ являются относительно новым предметом преступных посягательств. Следовательно, отождествление компьютерных преступлений со всеми информационными правонарушениями не совсем верно» [12, с. 75–76].

О.В. Суслопаров також зазначає: «Компьютерные преступления являются разновидностью преступлений информационного характера в силу наличия у них предмета в виде информации, а также дополнительного объекта в виде общественных отношений по обеспечению информационной безопасности. Специфическим признаком, отличающим компьютерные преступления от иных преступлений информационного характера, является наличие у них в

качестве предмета преступления особого вида информации – компьютерных данных...» [4, с. 34].

Л.О. Букалєрова, розрізняючи інформаційні та комп'ютерні правопорушення, зауважує: «Преступления, предметом которых является компьютерная информация, являются частью существующих информационных преступлений в сфере информационных технологий» [13, с. 34].

Таким чином, «комп'ютерні правопорушення» є лише частиною інформаційних правопорушень, тобто співвідносяться між собою як частина та загальне. Щодо співвідношення понять «кіберправопорушення» та «комп'ютерні правопорушення», то ці поняття є синонімічними, тобто правопорушення, які вчиняються у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, а їх наявність обумовлена перекладом іншомовних слів та впровадженням їх в наукову літературу.

Список літератури:

1. Юртаєва К.В. Визначення місця вчинення злочинів з використанням комп'ютерних технологій / К.В. Юртаєва : [Електронний ресурс]. – Режим доступу : <http://www.nbun.gov.ua>
2. Рудик М.В. Незаконний збут, розповсюдження комп'ютерної інформації з обмеженим доступом : дис. ... канд. юрид. наук : спец. 12.00.08 / Михайло Вікторович Рудик. – Х., 2007. – 229 с.
3. Протасевич А.А. Борьба с киберпреступностью как актуальная задача современной науки / А.А. Протасевич, Л.П. Зверьянская // Криминологический журнал ГУЭП. – 2011. – № 3. – С. 28–33.
4. Суслопаров А.В. Компьютерные преступления как разновидность преступлений информационного характера : дис. ... канд. юрид. наук : спец. 12.00.08 / Алексей Васильевич Суслопаров. – Красноярск, 2010. – 206 с.
5. Бачило И.Л. Информационное право : [учебник] / И.Л. Бачило. – М. : Издательство Юрайт; ИД Юрайт, 2010. – 454 с.
6. Беляков К.І. «Інформаційна» аксіоматика у праві: проблеми формування / К.І. Беляков // Науковий вісник Юрид. академії МВС України. – 2004. – № 3. – С. 263–268.
7. Brenner S.W. Toward a Criminal Law for Cyberspace A New Model of Law Enforcement? 30 Rutgers Computer & Tech. L.J.1 (2004).
8. Європіна І.В. Види протиправних діянь у сфері новітніх інформаційних технологій / І.В. Європіна // Вісник Академії адвокатури України : [Електронний ресурс]. – Режим доступу : http://archive.nbuv.gov.ua/portal/soc_gum/VAAU/2010_3/text/10eivnit.pdf
9. Музика А.А. Законодавство України про кримінальну відповідальність за комп'ютерні злочини : науково-практичний коментар і шляхи вдосконалення / А.А. Музика, Д.С. Азаров. – К. : Вид-во Паливода А. В., 2005. – 345 с.
10. Рекомендації експертів ООН : [Електронний ресурс]. – Режим доступу : <http://www.un.org/ru>

11. Юридична енциклопедія : в 6 т. / редкол.: Ю.С. Шемшученко (відп. ред.) та ін. – К. : Укр. енцикл., 2001. – Т. 3. : К–М. – 792 с.

12. Полушкин А.В. Информационное правонарушение: понятие и виды : дис. ... канд. юрид. наук : спец. 12.00.14 / Александр Васильевич Полушкин. – Екатеринбург, 2009. – 223 с.

13. Букалерева Л.А. Информационные преступления в сфере государственного и муниципального управления: законотворческие и правоприменительные проблемы : дис. ... д-ра юрид. наук : спец. 12.00.08 / Людмила Александровна Букалерева. – М., 2007. – 574 с.

Анализируются научные позиции относительно определений понятия «компьютерные правонарушения», исследуется уголовное право в этой сфере, выделяются особенности (черты) компьютерных правонарушений, определяется соотношение понятий «информационные правонарушения» (информационные преступления) и «компьютерные правонарушения» (компьютерные преступления).

Правонарушения, информационные правонарушения, компьютерные правонарушения киберпреступность, информационные преступления, компьютерные преступления.

Analyzes the scientific attitude definitions of «computer crime», examines the criminal law in this area are highlighted features (features) of computer crime, the ratio is determined by the terms «information of the offense» (information crimes), and «computer crime» (computer crime).

Offense, offense information, computer crime cyber crime, information crime, computer crime.