УДК 343.3/.7

Ю. Бельський,
ад'юнкт кафедри кримінального права
Національної академії внутрішніх справ

ЩОДО ВИЗНАЧЕННЯ ПОНЯТТЯ КІБЕРЗЛОЧИНУ

23 листопада 2001 року в Будапешті підписана Конвенція Ради Європи про кіберзлочинність (далі – Конвенція), яка була прийнята для протидії комп'ютерним злочинам та для співробітництва й координації діяльності правоохоронних органів різних держав. На сьогодні ратифікована 18 країнами та підписана 25 країнами. Україна ратифікувала Конвенцію 7 вересня 2005 року [8]. Згодом, у липні 2006 року, було ратифіковано додатковий протокол до Конвенції, що стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи (далі – Додатковий протокол) [9].

Терміни, які вживаються в Конвенції та додатковому протоколі до неї, так і не знайшли свого визначення у вітчизняному законодавстві. Так, у Законі України «Про основи національної безпеки України» згадуються терміни «комп'ютерна злочинність» та «комп'ютерний тероризм» [7], проте закон не дає визначення цим поняттям, також ці визначення відсутні в інших нормативних актах. Не визначено й поняття «комп'ютерний тероризм» (кібертероризм) у Законі України «Про боротьбу з тероризмом», а питання, які можуть охоплюватися цим поняттям, частково викладені як складова поняття «технологічний тероризм» [6].

Стратегія національної безпеки від 12 лютого 2007 року № 105/2007 також не містить визначень основних понять, проте є загадка про Конвенцію в контексті застосування інформаційно-комунікаційних технологій, гармонізованих із відповідними європейськими стандартами та Конвенцією про кіберзлочинність [10]. Проте вже в новій редакції Стратегії національної безпеки, затвердженій Указом Президента України від 8 червня 2012 року № 389/2012, вживаються терміни «кіберзлочинність», «кіберзагроза», «кібербезпека» [12]. Слід зазначити, що в «Доктрині інформаційної безпеки України» згадувалися поняття «комп'ютерна злочинність» та «комп'ютерний тероризм», а також питання захисту інформації від «кібернетичних атак» [11].

Проте в жодному із перелічених актів так і не було відображено визначення цих понять.

З огляду на це слід зазначити, що у вітчизняному законодавстві досі відсутнє законодавче визначення понять із префіксом кібер-: «кіберзлочин», «кіберзлочинність», «кібербезпека», «кіберпростір», «кіберзагроза», «кібератака», «кібернетичний захист». Натомість є лише поняття злочинів, які вчиняються з використанням комп'ютерів, комп'ютерних систем та мереж електрозв'язку, закріплених у розділі XVI Кримінального кодексу України. Проте й у самій Конвенції та Додатковому протоколі до неї також не міститься визначення поняття «кіберзлочин» та суміжних понять, а лише надається перелік діянь, за які на національному рівні пропонується встановити кримінальну відповідальність та наводиться їх умовна класифікація, тому, відповідно до Конвенції, до *кіберзлочинів* слід віднести такі посягання:

1) правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем:

– незаконний доступ – навмисний доступ до цілої комп'ютерної системи або її частини без права на це з метою отримання комп'ютерних даних або з іншою недобросовісною метою;

– втручання в дані, навмисне пошкодження, знищення, погіршення, зміну або приховування комп'ютерної інформації без права на це;

– втручання в систему – навмисне серйозне перешкоджання функціонуванню комп'ютерної системи шляхом введення, передачі, пошкодження, знищення, погіршення, заміни або приховування комп'ютерних даних без права на це;

– зловживання пристроями, а саме їх виготовлення, продаж, придбання для використання, розповсюдження або надання для використання іншим чином.

2) правопорушення, пов'язані з комп'ютерами, включаючи підробку й шахрайство, здійснені з використанням комп'ютерів;

3) правопорушення, пов'язані зі змістом інформації, зокрема дитяча порнографія, расизм та ксенофобія;

4) правопорушення, пов'язані з порушенням авторських і суміжних прав, наприклад незаконне відтворення й використання комп'ютерних програм, аудіо/відео й інших видів цифрової продукції, а також баз даних і книг.

Відсутність законодавчо закріплених визначень породжує на теоретичному рівні дискусії. Наприклад М. Погорецький та В. Шеломенцев вбачають загальною ознакою протиправних діянь, передбачених Конвенцією та Додатковим протоколом до неї, те, що їх вчинення на різних стадіях безпосередньо пов'язане з використанням ресурсів комп'ютерних систем (вчинення за допомогою комп'ютерних систем або через комп'ютерні системи), які у свою чергу є середовищем вчинення кіберзлочинів. Комп'ютерні дані при цьому, на їхню думку, слід розглядати як інформаційний ресурс комп'ютерних систем, а комп'ютерні мережі – як різновид комп'ютерних систем [3]. Виходячи із цього, кіберзлочини слід вважати злочинами, які вчиняються за допомогою або через комп'ютерні системи чи пов'язані саме з комп'ютерними системами, тобто із сукупністю пристроїв, із яких один чи більше у відповідності до певної програми виконують автоматичну обробку даних [3, с. 91].

Також автори не погоджуються з позицією інших науковців, які розглядають кіберзлочини як злочини, вчинені в інформаційному середовищі, проти інформаційних ресурсів, тобто у сфері комп'ютерної інформації, або за допомогою інформаційних засобів. На думку М. Погорецького та В. Шеломенцева, терміни «інформаційне середовище», «інформаційні ресурси», «інформаційні засоби» є занадто загальними для сфери використання комп'ютерних систем і не розкривають суті процесів автоматичної обробки інформації [3, с. 92].

Слід розглянути інший погляд на це питання, який відстоює група науковців. А. Музика та Д. Азаров визначають тотожність понять кіберзлочину та злочинів у сфері комп'ютерної інформації [2, с. 5]. Вчені вказують, що визначати кіберзлочин треба як злочини у сфері комп'ютерної інформації.

В. Бутузов обґрунтовує думку, що комп'ютерні злочини та кіберзлочини являють собою різні види злочинів у сфері високих інформаційних технологій, класифікація яких відбувається за такими ознаками:

– ознакою віднесення певних злочинів у сфері високих інформаційних технологій до комп'ютерних є знаряддя вчинення злочину – комп'ютерна техніка. Причому об'єктом посягання є суспільні відносини у сфері автоматизованої обробки інформації;

– ознакою віднесення злочинів у сфері високих інформаційних технологій до кіберзлочинів є специфічне середовище вчинення злочинів – кіберпростір (середовище комп'ютерних систем та мереж). Причому об'єктом злочинного посягання можуть бути відносини будь-якої галузі людської діяльності, що має свій прояв у кіберпросторі. При цьому автор посилається на перелік протиправних діянь, які передбачені в Конвенції та Додатковому протоколі до неї. На його думку, тільки діяння із

цього переліку можуть бути віднесені до кіберзлочинів [1, с. 119].

Таким чином, ми можемо побачити, що на сьогодні законодавча невизначеність понять породила дискусійність питання щодо тлумачення, що насправді являє собою кіберзлочини, та умовно поділило науковців на дві групи.

Перша група науковців відносить до кіберзлочинів дії, у яких комп'ютер є об'єктом або засобом посягання.

Інша група визначає кіберзлочини як злочини, об'єктом посягання в яких є інформація, що обробляється в електронно-обчислювальній машині (комп'ютері) або в комп'ютерній системі, а засобом скоєння є електронно-обчислювальна машина (комп'ютер), тобто протизаконні дії у сфері автоматичної обробки інформації.

Частково питання визначення термінології мав вирішити Закон України «Про кібернетичну безпеку України», проект якого було зареєстровано ще 04 червня 2013 року. Проте він так і не містив визначення кіберзлочину та не був прийнятий. Дещо пізніше Указом Президента України № 449/2014 від 01 травня 2014 року «Про рішення Ради національної безпеки і оборони України від 28 квітня 2014 року "Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України"» було поставлено завдання розробити проект Стратегії кібернетичної безпеки України, а також проект Закону України «Про кібернетичну безпеку України», а також завдання щодо приведення національного законодавства у відповідність до міжнародних стандартів із питань інформаційної та кібернетичної безпеки, удосконалення системи формування та реалізації державної політики у сфері інформаційної безпеки України [13].

У проекті Стратегії забезпечення кібернетичної безпеки України, розробленої Національним інститутом стратегічних досліджень, було запропоновано визначення ключових термінів у сфері кібербезпеки, зокрема визначення кіберзлочину: кібернетичний злочин (кіберзлочин) – передбачене кримінальним законом суспільно небезпечне винне діяння, що полягає в протиправному використанні інформаційних та комунікаційних технологій, відповідальність за яке встановлена законодавством про кримінальну відповідальність [4].

Словник термінів із кібербезпеки за редакцією О. Копана надає два визначення поняттю кіберзлочину.

Кіберзлочин (комп'ютерний злочин) – протиправне втручання в роботу кібернетичних систем, основною управляючою ланкою яких є комп'ютер (наприклад, спотворення інформації про стан об'єкта в каналі зворотного зв'язку, спотворення керуючого сигналу й каналу зв'язку, використання шкідливого програмного забезпечення тощо), створення та використання в злочинних цілях певної кібернетичної (комп'ютерної) системи, використання в злочинних цілях існуючих кібернетичних (комп'ютерних) систем (наприклад комп'ютерних чи телекомунікаційних мереж у шахрайстві, вимаганні тощо) [5, с. 85].

Кіберзлочин (кібернетичний злочин) також визначено таким чином:

1. Кіберзлочин – злочин, пов'язаний із використанням кібернетичних комп'ютерних систем, та злочин в кіберпросторі. На відміну від комп'ютерного злочину, поняття якого пов'язане з використанням будь-якої комп'ютерної техніки, кіберзлочин є більш вузьким поняттям, пов'язаним із функціонуванням саме кібернетичних комп'ютерних систем. До протиправного використання кібернетичних комп'ютерних мереж відносять несанкціоноване отримання прав керування такою системою (наприклад, використання шкідливого програмного забезпечення, спотворення інформації про стан об'єкта в каналі зворотного зв'язку, спотворення керуючого сигналу в каналі прямого зв'язку тощо) та її нерегламентоване використання (наприклад, із метою спричинення аварії на виробництві, дезорганізації

діяльності підприємства тощо), а також створення та використання в злочинних цілях однієї кібернетичної комп'ютерної системи проти інших (наприклад, створення мережі зомбованих комп'ютерів для здійснення атак на веб-сайти, створення несанкціонованого робочого місця в системі електронного переказу коштів тощо) [5, с. 85–86];

2. Кіберзлочин – найбільш небезпечне кіберправопорушення, за яке законодавством встановлюється кримінальна відповідальність [5, с. 85–86].

Також подаються визначення похідних понять від кіберзлочину.

Кіберправопорушення – суспільно небезпечне діяння, що здійснюється з використанням технологій перетворення (створення, зберігання, обміну, обробки знищення) інформації, представленої у вигляді комп'ютерних даних, і тягне за собою юридичну відповідальність. Кіберправопорушення має всі загальні ознаки правопорушення, що виділяються в теорії права та вирізняються лише факультативною частиною юридичного складу, у якому кіберпростір виступає як засіб або мета здійснення правопорушення [5, с. 87].

Кіберпроступки – кіберправопорушення, які не несуть суттєвої суспільної небезпеки, за які законодавством передбачена юридична відповідальність (крім кримінальної) [5, с. 88].

Кіберпростір (кібернетичний простір) – 1) штучне електронне середовище існування інформаційних об'єктів у цифровій формі, що утворене в результаті функціонування кібернетичних комп'ютерних систем управління й обробки інформації та забезпечує користувачам доступ до обчислювальних та інформаційних ресурсів систем, вироблення електронних інформаційних продуктів, обмін електронними повідомленнями, а також можливість за допомогою електронних інформаційних образів у режимі реального часу вступати у відносини щодо спільного використання обчислювальних та інформаційних ресурсів системи (надання послуг, ведення електронної комерції тощо); 2) простір, сформований інформаційно-комунікаційними системами, у якому проходять процеси перетворення (створення, зберігання, обміну та знищення) інформації, представленої у вигляді електронних комп'ютерних даних [5, с. 87–88].

Проаналізувавши теоретичні та практичні дослідження в галузі визначення поняття кіберзлочину, можна дійти висновку, що серед сучасних українських науковців немає єдиного підходу до визначення поняття кіберзлочину. Причому підходи досить суттєво відрізняються, що може бути причиною неправильного трактування, а це у свою чергу може призвести до неправильної кваліфікацію злочинних дій, що створить проблеми не тільки на теоретичному, а й на практичному рівнях.

Розглянувши різні підходи та проаналізувавши положення Конвенції, можна дійти висновку, що кіберзлочини – це злочини, які вчиняються в процесі автоматизованої обробки інформації за допомогою електронно-обчислювальних машин або через комп'ютерні системи, об'єктом посягання яких є суспільні відносини у сфері обігу електронної інформації та інші суспільних відносин, у яких комп'ютер виступає кваліфікуючою ознакою вчинення злочину (наприклад, комп'ютерне шахрайство, або кібертероризм).

Ключові слова: кіберзлочин, комп'ютерний злочин, кіберправопорушення, кіберпроступки, кібертероризм.

Стаття присвячена аналізу наукових підходів до визначення поняття кіберзлочину, розгляду його сутності, а також проблемі його законодавчого закріплення.

Статья посвящена анализу научных подходов к определению понятия киберпреступления, рассмотрению его сущности, а также законодательного закрепления.

The article is devoted to the analysis of the notion of cyber-crime, and problem of its legislative consolidation in Ukraine.

Література

1. Бутузов В. Протидія комп'ютерній злочинності в Україні (системно-структурний аналіз) : [монографія] / В. Бутузов. – К. : КИТ, 2010. – 148 с.

2. Погорецький М. «Кіберзлочини: до визначення поняття» / М. Погорецький, В. Шеломенцев // Вісник прокуратури. – 2012. – № 8. – С. 89–96.

3. Проблеми чинної вітчизняної нормативно-правової бази у сфері боротьби із кіберзлочинністю: основні напрями реформування : Аналітична записка [Електронний ресурс]. – Режим доступу : http://www.niss.gov.ua/articles/454.

4. Словник термінів з кібербезпеки / за заг. ред. О. Копатіна, Є. Скулишина. – К. : ВБ «Аванпост-Прим», 2012. – 214 с.

5. Про боротьбу з тероризмом : Закон України // Відомості Верховної Ради України. – 2003. – № 25. – Ст. 180.

6. Про основи національної безпеки України : Закон України // Відомості Верховної Ради України. – 2003. – № 39. – Ст. 351.

7. Про ратифікацію Конвенції про кіберзлочинність : Закон України від 7 вересня 2005 р. № 2824-IV // Відомості Верховної Ради України. – 2006. – № 5. – С. 128. – Ст. 71.

8. 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 р. № 23-V // Відомості Верховної Ради України. – 2006. – № 39. – С. 1384. – Ст. 328.

9. Про Стратегію національної безпеки України : Указ Президента України // Урядовий кур'єр. – 2007. – № 43.

10. Про Доктрину інформаційної безпеки України : Указ Президента України // Офіційний вісник України. – 2009. – № 52. – С. 7. – Ст. 1783.

11. Про рішення Ради національної безпеки і оборони України від 8 червня 2012 р. «Про нову редакцію Стратегії національної безпеки України» : Указ Президента України // Урядовий кур'єр. – 2012. – № 113.

12. Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України : Указ Президента України Про рішення Ради національної безпеки і оборони України від 28 квітня 2014 р. // Офіційний вісник Президента України. – 2014. – № 16. – С. 6. – Ст. 982.