Орлов Юрій Юрійович – доктор юридичних наук, старший науковий співробітник, проректор Національної академії внутрішніх справ з науково-методичної роботи

РЕАЛІЗАЦІЯ ВИМОГ МІЖНАРОДНОЇ КОНВЕНЦІЇ ПРО КІБЕРЗЛОЧИННІСТЬ* У ЗАКОНОДАВСТВІ УКРАЇНИ

Проаналізовано рівень реалізації вимог Міжнародної конвенції про кіберзлочинність у законодавстві України.

Ключові слова: кіберзлочинність; Конвенція про кіберзлочинність; Кримінальний кодекс України; кримінальна відповідальність.

Проанализирован уровень реализации требований Международной конвенции о киберпреступности в законодательстве Украины.

Ключевые слова: киберпреступность; Конвенция о киберпреступности; Уголовный кодекс Украины; уголовная ответственность.

The level of implementation of the International Convention on Cybercrime in the legislation of Ukraine is analyzed.

Keywords: Cybercrime; Convention on Cybercrime; Criminal Code of Ukraine; criminal liability.

В епоху інформаційного суспільства інформаційні й телекомунікаційні технології охопили майже всі сфери життєдіяльності суспільства й держави. Людство, створивши безпрецедентний технічний проект – глобальну комп'ютерну мережу Інтернет, очевидно, не могло передбачити, які можливості для зловживань створюють ці технології.

Завдяки Інтернету комп'ютерна кримінальна епідемія стрімко розвивається. За оцінками Інтерполу, швидкість зростання рівня злочинності в глобальній комп'ютерній мережі є найбільшою, порівняно з іншими видами злочинів, серед яких торгівля наркотиками та зброєю. За оцінкою голови зовнішньополітичного відомства

* Кіберзлочинність у цій статті розуміють як сукупність злочинів, що вчинюють із застосуванням інформаційних технологій [1].

Великої Британії В. Хейга, глобальна шкода від кіберзлочинів становить понад трильйон доларів США на рік [2]. За даними опитування, проведеного компанією Symantec, майже дві третини користувачів Інтернету хоча б одноразово ставали жертвами кібернетичного злочину [3].

За словами Генерального секретаря Інтерполу Р. Ноубла, анонімність кіберпростору перетворює кіберзлочини в найбільш небезпечні з будь-коли вчинюваних кримінальних діянь [3].

Кіберзлочинність не знає державних кордонів. Її транснаціональний характер спричинює проблему кваліфікації злочинів, яку слід розв'язувати шляхом уніфікації національних кримінальних законодавств. На це спрямовано дію Міжнародної конвенції про кіберзлочинність, яку укладено 23 листопада 2001 р. в м. Будапешті й до якої нещодавно приєдналась Україна [4].

Конвенція стала важливим правовим документом, на базі якого держави, що приєдналися до неї, розбудовують власні системи протидії кіберзлочинам.

Визначаючи перелік кримінальних діянь, що вчинюють із застосуванням інформаційних технологій, та пропонуючи єдині підходи до боротьби з кіберзлочинами, Конвенція має сприяти ефективності протидії цьому виду злочинів. Отже, успішність боротьби з кіберзлочинністю в конкретній країні значною мірою залежить від того, чи відповідає її кримінальне законодавство вимогам Конвенції.

Питанням криміналізації суспільно небезпечних діянь у сфері комп'ютерної інформації присвятили наукові праці П. П. Андрушко, М. В. Карчевський, В. В. Кузнецов, А. А. Музика, С. О. Орлов, Н. А. Розенфельд та ін. На початку 2003 р. Д. С. Азаров запропонував невідкладно гармонізувати чинне кримінальне законодавство України з положеннями щойно укладеної Міжнародної конвенції про кіберзлочинність [5, с. 13].

Уперше стан і проблеми імплементації Україною міжнародно-правових зобов'язань щодо відповідальності за злочини у сфері комп'ютерної інформації докладно дослідив М. В. Плугатир. Відстоюючи необхідність узгодження норм кримінального законодавства України з положеннями Конвенції про кіберзлочинність, автор обмежує своє дослідження пропозиціями щодо імплементації ст. 2–6 Конвенції, що стосуються правопорушень проти конфіденційності, цілісності та доступності комп'ютерних даних та систем і мають охоплюватися розділом XVI Особливої частини Кримінального кодексу (КК) України [6, с. 9–10]. Водночас дослідник не вивчає стан реалізації в Україні вимог Конвенції щодо правопорушень, пов'язаних з використанням комп'ютерних засобів (ст. 7, 8), зі змістом даних (контентом) (ст. 9), а також з порушеннями авторського права та суміжних прав (ст. 10).

Метою цієї статті є комплексне дослідження реалізації вимог Конвенції про кіберзлочинність у кримінальному законодавстві України, виявлення наявних прогалин і формування пропозицій щодо його вдосконалення.

Отже, Конвенція передбачає чотири групи злочинів, пов'язаних з використанням комп'ютерних технологій як інструменту їх учинення. До першої групи віднесено злочини проти конфіденційності, цілісності й доступності комп'ютерних даних і систем (протизаконний доступ, протизаконне перехоплення, вплив на дані, вплив на функціонування системи, а також протизаконне використання пристроїв і комп'ютерних програм). До другої групи – злочини, пов'язані з використанням комп'ютерних засобів (підроблення, шахрайство). До третьої групи віднесено злочини, пов'язані зі змістом даних (дитяча порнографія). До четвертої – злочини, пов'язані з порушенням авторського права та суміжних прав.

Держави, що приєдналися до Конвенції, взяли зобов'язання переглянути своє законодавство, з метою приведення його у відповідність з рекомендаціями, викладеними в цьому міжнародному документі.

Аналіз чинного законодавства України свідчить, що за більшість злочинів, зазначених у Конвенції, у нашій країні передбачено кримінальну відповідальність.

Так, розділ XVI Особливої частини КК України містить низку статей, що передбачають кримінальну відповідальність за злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку:

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

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

ст. 361^2 (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);

ст. 362 (несанкціоновані дії з інформацією, яку опрацьовують в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігають на носіях такої інформації, вчинені особою, яка має право доступу до неї);

ст. 363 (порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яку в них опрацьовують);

ст. 363[1] (перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку) [7].

На виконання вимог Конвенції до розділу XVI Особливої частини КК України Законом України від 5 червня 2003 р. № 908-IV внесено відповідні зміни.

Водночас перелік кіберзлочинів не вичерпується діяннями, визначеними в розділі XVI Особливої частини КК України. Певні злочини, що існували задовго до створення комп'ютерів, також можуть бути вчинені із застосуванням інформаційних технологій. Використання комп'ютерів спрощує вчинення злочину або уможливлює його вчинення в нових формах. Отже, ці злочини можна розглядати як такі, що підпадають під дію Конвенції. Зокрема, ідеться про такі злочинні діяння: різні види підроблення: грошей, цінних паперів, платіжних карток, знаків поштової оплати, марок акцизного збору, контрольних марок, номерів вузлів та агрегатів транспортних засобів, документів на отримання наркотиків, інших документів тощо (ст. 199, 200, 215, 216, 224, 290, 318, 358, 366 КК України); шахрайство з різними предметами (ст. 190, 192, 222, 262, 308, 312, 313, 357, 410 КК України); увезення, виготовлення, збут і розповсюдження порнографічних предметів (ст. 301 КК України); порушення авторського права й суміжних прав (ст. 176 КК України).

Доцільно з'ясувати, чи враховано всі вимоги Конвенції в чинному кримінальному законодавстві України. Необхідно встановити відповідність між статтями Конвенції та КК України на семантичному рівні, що висвітлено в таблиці, аналіз змісту якої дає підстави загалом ствердно відповісти на поставлене питання.

Таблиця

Статті Конвенції	**Зміст статті Конвенції**	**Статті КК України**
Злочини проти конфіденційності, цілісності й доступності комп'ютерних даних і систем		
2	Протизаконний доступ	361, 363
3	Протизаконне перехоплення	362, 363
4	Вплив на дані	361, 362, 363[1]
5	Вплив на функціонування системи	361, 361[1], 362, 363, 363[1]
6	Протизаконне використання пристроїв і комп'ютерних програм	361[1], 362, 363
Злочини, пов'язані з використанням комп'ютерних засобів		
7	Підроблення з використанням комп'ютерних технологій	199, 200, 215, 216, 224, 290, 318, 358, 366

Закінч. таблиці

Статті Конвенції	**Зміст статті Конвенції**	**Статті КК України**
8	Шахрайство з використанням комп'ютерних технологій	190, 192, 222, 262, 308, 312, 313, 357, 410
Злочини, пов'язані зі змістом даних		
9	Злочини, пов'язані з дитячою порнографією	301
Злочини, пов'язані з порушенням авторського права та суміжних прав		
10	Злочини, пов'язані з порушенням авторського права та суміжних прав	176

Слід зробити два зауваження. Перше зауваження стосується того факту, що *в Україні передбачено кримінальну відповідальність також за інші діяння, що можуть бути вчинені шляхом застосування інформаційних технологій, проте їх немає в тексті Конвенції.*

Виокремимо три групи цих діянь. До першої слід віднести злочини, що полягають у незаконному придбанні та (або) збуті предметів, заборонених для вільного обігу, і можуть бути вчинені з використанням мережі Інтернет:

незаконне придбання чи збут наркотичних засобів, психотропних речовин або їх аналогів (ст. 307 КК України);

незаконне придбання чи збут вогнепальної зброї, бойових припасів, вибухових речовин; збут холодної зброї (ст. 263 КК України);

придбання радіоактивних матеріалів (ст. 265 КК України).

До другої групи діянь належать злочини, пов'язані зі змістом даних (контентом). Конвенція розуміє незаконний контент як виключно дитячу порнографію[*]. Законодавство України дає підстави вважати злочином розміщення в Інтернеті також інформації іншого характеру, а саме: відомостей, що становлять державну чи іншу таємницю, яку охороняє закон: незаконне розголошення лікарської таємниці (ст. 145 КК України), порушення таємниці голосування (ст. 159), розголошення таємниці усиновлення (удочеріння) (ст. 168), розголошення комерційної таємниці (ст. 232), розголошення державної таємниці (ст. 328), несанкціоноване розповсюдження інформації з обмеженим доступом, яку зберігають в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації (ст. 361^2), розголошення відомостей про заходи

[*] Окремим протоколом до Конвенції охоплено також расизм і ксенофобію.

безпеки щодо особи, узятої під захист (ст. 381), розголошення даних досудового слідства та дізнання (ст. 387), розголошення відомостей військового характеру, що становлять державну таємницю (ст. 422); завідомо неправдиве повідомлення про загрозу безпеці громадян, знищення чи пошкодження об'єктів власності (ст. 259 КК України); заклики до вчинення дій, що загрожують громадському порядку (ст. 295 КК України); пропаганда расової, національної, релігійної нетерпимості (ст. 161), культу насильства й жорстокості (ст. 300) або війни (ст. 436 КК України); спам, тобто масове розповсюдження повідомлень, з метою перешкоджання роботі комп'ютерів, автоматизованих систем чи комп'ютерних мереж (ст. 363^1 КК України).

До третьої групи діянь слід віднести легалізацію (відмивання) грошових коштів, одержаних злочинним шляхом (ст. 209 КК України). Для цього злочинці застосовують послуги електронних банків, надають рахунки на завищені або занижені суми, беруть участь у кібераукціонах тощо.

Друге зауваження полягає в тому, що *деякі положення Конвенції не знайшли відображення у вітчизняному кримінальному законодавстві*. Так, КК України не передбачає кримінальної відповідальності за: придбання шкідливих комп'ютерних програм і пристроїв, створених чи адаптованих для вчинення комп'ютерних злочинів [4, п. "a I" ч. 1 ст. 6]; виробництво, продаж, придбання для використання, імпорт, оптовий продаж чи інші форми надання в користування комп'ютерних паролів, кодів доступу чи інших аналогічних даних, за допомогою яких може бути отримано доступ до комп'ютерної системи в цілому чи будь-якої її частини з наміром використати їх з метою вчинення комп'ютерних злочинів [4, п. "a II" ч. 1 ст. 6]; володіння зазначеними вище шкідливими комп'ютерними програмами, пристроями, комп'ютерними паролями, кодами доступу чи іншими аналогічними даними [4, п. "b" ч. 1 ст. 6]; придбання дитячої порнографії через комп'ютерну систему [4, п. "d" ч. 1 ст. 9]; володіння дитячою порнографією, що перебуває в комп'ютерній системі чи на носіях комп'ютерних даних [4, п. "e" ч. 1 ст. 9].

Запровадження кримінальної відповідальності за більшість з указаних діянь кожна держава – учасник Конвенції має право визначати самостійно. Тому питання щодо необхідності криміналізації цих діянь залежить від ступеня їх суспільної небезпеки в умовах України та кримінологічних характеристик (рівня, динаміки тощо).

Водночас питання щодо криміналізації діянь, передбачених п. "a II" ч. 1 ст. 6 Конвенції, необхідно вирішувати з урахуванням змісту ч. 3 ст. 6 цього міжнародного документа, що контекстуально зобов'язує всіх держав-учасників передбачити кримінальну відповідальність за продаж, оптовий продаж чи інші форми надання в користування комп'ютерних паролів, кодів доступу чи інших аналогічних даних, за

допомогою яких може бути вчинено комп'ютерний злочин. Відповідальність за ці діяння в Україні не встановлено.

Поширення практики викрадення та продажу злочинцям комп'ютерних паролів і кодів доступу особами, які мають доступ до них у зв'язку з виконанням службових обов'язків, неодмінно призведе до збільшення кількості комп'ютерних злочинів, значно спрощуючи їх учинення. Серед зазначених злочинів – учинення крадіжок з використанням підроблених платіжних карток, несанкціоноване проникнення в корпоративні комп'ютерні мережі, з метою блокування їх роботи, учинення шахрайств, пов'язаних із функціонуванням інтернет-магазинів і наданням послуг мережею Інтернет, отримання доступу до грошових коштів банку, незаконне отримання персональних даних, одержання конфіденційної інформації тощо.

Установлення кримінальної відповідальності за продаж чи інші форми надання в користування комп'ютерних паролів, кодів доступу чи інших даних, за допомогою яких може бути вчинено комп'ютерний злочин, на нашу думку, має стати актуальним завданням подальшої законотворчої роботи у сфері боротьби з кіберзлочинністю.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Преступления в сфере информационных технологий [Электронный ресурс]. – Режим доступа :
http://www.ru.wikipedia.org/wiki.

2. Невидин С. Хейг: ущерб от киберпреступлений превышает $1 трлн [Электронный ресурс]. – Режим доступа :
http://www.newsland.ru/news/detail/id/807021.

3. Интерпол: киберпреступления являются самой опасной криминальной угрозой [Электронный ресурс]. – Режим доступа :
http://www.virusovnet.org/main/309.

4. Конвенция о борьбе с киберпреступностью [Электронный ресурс]. – Режим доступа :
http://194.8.63.186/portals.

5. Азаров Д. С. Кримінальна відповідальність за злочини у сфері комп'ютерної інформації : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.08 / Д. С. Азаров. – К. : Ін-т держави і права НАН України, 2003. – 18 с.

6. Плугатир М. В. Імплементація Україною міжнародно-правових зобов'язань щодо відповідальності за злочини у сфері комп'ютерної інформації : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.08 / М. В. Плугатир. – К. : Держ. наук.-дослід. ін-т МВС України, 2010. – 16 с.

7. Кримінальний кодекс України : Закон України від 5 квіт. 2001 р. № 2341-III [Електронний ресурс]. – Режим доступу :
http://www.liga.net.