Питання оптимізації зобов'язань, зумовлених ратифікацією Конвенції про кіберзлочинність

Доводиться теза про необхідність ширшого використання механізму застережень при ратифікації Конвенції про кіберзлочинність.
Ключові слова: *суспільна небезпечність, кіберзлочини, конвенція, ратифікація.*

Доказывается тезис о необходимости более широкого использования механизма предостережений при ратификации Конвенции о киберпреступности.
Ключевые слова: *общественная опасность, киберпреступления, конвенция, ратификация.*

There is a thesis about the necessity of more deployment of mechanism of reserve during ratification of Convention on Cybercrime.
Keywords: *public danger, cybercrime, convention, ratification.*

М. В. Карчевський
кандидат юридичних наук, докторант Національної академії внутрішніх справ України

Прийняте рішення щодо ратифікації Конвенції про кіберзлочини [1] не відповідає соціальним потребам у кримінально-правовому впливі на інформаційні суспільні відносини та засадам формування національного кримінального законодавства. Україною взяті на себе

зобов'язання щодо криміналізації діянь, які не характеризуються достатньою для злочинів суспільною небезпечністю. Мета статті полягає в аргументації висловленої тези та формулюванні пропозицій щодо виправлення ситуації.

Суспільна небезпечність злочинів в сфері використання комп'ютерної техніки головним чином визначається соціальною значущістю тієї діяльності, для інтенсифікації якої використовуються інформаційні технології. Знищення або перекручення інформації призводить до порушення певної діяльності, для здійснення якої вона необхідна. Саме це і визначає суспільну небезпечність конкретного посягання в сфері використання інформаційних технологій. Однак для настання кримінальної відповідальності за більшість злочинів, передбачених у розділі XVI Кримінального кодексу України (далі – КК України), встановлення таких характеристик суспільно небезпечних наслідків не є обов'язковим. Судячи з прийнятого законодавцем рішення, витік, втрата, підробка, блокування інформації, порушення встановленого порядку її маршрутизації або спотворення процесу її обробки (ст. ст. 361, 362) визнаються суспільно небезпечними. Так само суспільно небезпечними, на думку законодавця, є просте розповсюдження або збут шкідливого програмного або технічного забезпечення (ст. 361-1), розповсюдження або збут комп'ютерної інформації з обмеженим доступом (ст. 361-2) тощо. Лише на рівні кваліфікуючих ознак зустрічаємо залежність кримінальної відповідальності від настання «істотної шкоди».

Проведене дослідження масиву національних судових рішень, пов'язаних з засудженням за злочини в сфері використання комп'ютерної техніки та мереж електрозв'язку, свідчить про те, що неповна відповідність чинного законодавства означеній специфіці суспільної небезпечності комп'ютерних злочинів зумовлює появу негативних тенденцій правозастосовчої практиці. Їх зміст полягає ось у чому: через відсутність у законодавчих визначеннях даних злочинів чітких критеріїв суспільної небезпечності під кримінально-правову заборону та, відповідно, до сфери впливу кримінальної юстиції потрапляють не тільки діяння, що дійсно суспільно небезпечні, а й ті, які такими не є. Саме це і призводить до істотного зниження ефективності кримінально-правової протидії досліджуваним злочинам. Виправлення ситуації передусім передбачає включення до диспозицій відповідних кримінально-правових норм чітких положень щодо критеріїв суспільної небезпечності посягань [4, 3].

Це актуальне завдання кореспондує з проблемою гармонізації положень національного закону з міжнародними нормами, що стосуються протидії кіберзлочинності. Розвиток сучасних систем телекомунікації та комп'ютерних мереж призвів до такої ситуації, коли протидія цим злочинам не може бути достатньо ефективною, якщо здійснюється в межах однієї країни. Так званий кіберпростір не має державних кордонів: наприклад, особа, що вчиняє несанкціонований доступ до комп'ютерної інформації, необов'язково має перебувати в тій країні, де фізично розташований носій цієї інформації; автор комп'ютерного вірусу може розмістити його на популярному сайті в мережі Інтернет, що призведе до його поширення у багатьох країнах. Все це вимагає узгодження національних кримінальних законодавств та створення єдиного правового простору для забезпечення ефективного захисту від злочинних посягань, пов'язаних з використанням комп'ютерної техніки.

Одним із основних міжнародних нормативних документів в цій сфері є Конвенція про кіберзлочинність (далі – Конвенція), прийнята в рамках Ради Європи 23 листопада 2001 р. (підписана Україною 23.11.2001 р., ратифікована 7 вересня 2005 р.), з Додатковим протоколом, який

стосується криміналізації дій расистського та ксенофобського характеру, вчинених через комп'ютерні системи. Нами досліджувалося питання відповідності чинного кримінального законодавства означеним нормативно-правовим актам [5; 2]. Зупинимося лише на головному висновку: порівняльний аналіз Конвенції та КК України дає можливість встановити, що більша частина діянь, передбачених у Конвенції, визнається злочинами в українському законодавстві. До таких діянь відносяться нелегальне перехоплення (ст. ст. 163, 361, 362 КК України), втручання у дані (ст. ст. 361, 362 КК України), втручання у систему (ст. 361 КК України), злочини, пов'язані з дитячою порнографією (ст. 301 КК України), підробка, пов'язана з комп'ютерами (ст. ст. 358, 366 КК України), шахрайство, пов'язане з комп'ютерами (ч. 3 ст. 190 КК України). Діяння, передбачені Додатковим протоколом до Конвенції, охоплюються ст. 161 КК України, яка встановлює відповідальність за порушення рівноправності громадян залежно від їх расової, національної належності або ставлення до релігії, та загальними нормами Особливої частини КК України, що передбачають злочини проти свободи совісті (ст. ст. 178-181 КК України).

Але національне кримінальне законодавство не передбачає відповідальності за таке діяння, передбачене Конвенцією, як навмисний доступ до цілої комп'ютерної системи або її частини без права на це. З урахуванням положень конвенції, норм зарубіжного законодавства та практики здійснення заходів щодо захисту інформації незаконний доступ можна було б визначити так: одержання винним можливості ознайомлюватися, знищувати, перекручувати або блокувати комп'ютерні дані, що мають специфічні організаційні, технічні або програмні засоби захисту. Зауважимо, що як і решта злочинів в сфері використання комп'ютерної техніки, незаконний доступ не може вважатися таким посяганням, що має самостійну суспільну небезпечність. Це з очевидністю випливає з наведених раніше положень щодо формулювання законодавчих визначень комп'ютерних злочинів з урахуванням специфіки суспільної небезпечності таких посягань [4, 3]. Небезпечність незаконного доступу, як і будь якого іншого злочину в сфері використання комп'ютерної техніки, визначається інтенсивністю шкоди, заподіяної тим суспільним відносинам, для забезпечення яких використовується певна інформаційна система. Тому криміналізацію незаконного доступу доцільно здійснювати в межах передбачення відповідної кваліфікуючої ознаки злочинів в сфері використання комп'ютерної техніки.

Подальше дослідження Конвенції вимагає також зазначення того, що національне кримінальне законодавство прямо не передбачає відповідальності за такі дії, як:

навмисний продаж, розповсюдження або надання для використання іншим чином комп'ютерних паролів, кодів доступу або подібних даних, за допомогою яких можна здобути доступ до всієї або частини комп'ютерної системи з наміром використання її для вчинення будь-якого зі злочинів, перерахованих у ст. ст. 2-5 Конвенції;

володіння пристроями, включаючи комп'ютерні програми, створені або адаптовані, в першу чергу, з метою вчинення будь-якого зі злочинів, перерахованих у ст. ст. 2-5 Конвенції або комп'ютерними паролями, кодами доступу або подібними даними, за допомогою яких можна здобути доступ до усієї або частини комп'ютерної системи з наміром використання її для вчинення будь-якого зі злочинів, перерахованих у ст. ст. 2-5 Конвенції, з наміром використання означених предметів для вчинення будь-якого зі злочинів, перерахованих у ст. ст. 2-5.

Однак видається, що наявних у кримінальному законодавстві засобів кримінально-правової охорони від посягань, що вчиняються у співучасті, а також засобів про-

тидії попередній злочинній діяльності, цілком достатньо. Так, навмисний продаж, розповсюдження або надання для використання іншим чином комп'ютерних паролів, кодів доступу або подібних даних, з урахуванням визначень Конвенції, конститутивною ознакою яких є мета подальшого вчинення злочинів, є пособництвом у вчиненні відповідних злочинів. У свою чергу, володіння шкідливими засобами з метою подальшого вчинення злочинів необхідно, відповідно до національного законодавства, слід рахувати готуванням. Як бачимо з наведених вище визначень, Конвенція пропонує встановлювати кримінальну відповідальність не просто за володіння, розповсюдження чи придбання шкідливих програмних чи технічних засобів, кодів доступу чи іншої подібної інформації, а лише в тому випадку, коли ці дії вчиняються з метою подальшого вчинення комп'ютерного злочину. Таким чином, Конвенція, як видається, містить достатньо вдале формулювання, що чітко відображає суспільну небезпечність діянь, пов'язаних зі шкідливими програмними чи технічними даними.

Значний інтерес становить також дослідження Закону України «Про ратифікацію Конвенції про кіберзлочинність» від 7 вересня 2005 р. Як видається, в цьому законі також містяться недоліки, пов'язані з неадекватним відображенням реального змісту суспільної небезпечності досліджуваних посягань. Конвенція формулює типові ознаки складів комп'ютерних злочинів та пропонує механізм т. зв. застережень, який дозволяє максимально враховувати особливості національного розуміння понять «злочин» і «суспільна небезпечність» на рівні законодавств окремих держав. Україна використовує цей механізм для того, щоб відмовитись від криміналізації:

1) виготовлення, придбання для використання, надання для використання іншим чином пристроїв, включаючи комп'ютерні програми, створені або адаптовані, в першу чергу, з метою вчинення будь-якого зі злочинів, перерахованих у ст. ст. 2-5 Конвенції;

2) виготовлення і придбання для використання комп'ютерних паролів, кодів доступу або подібних даних, за допомогою яких можна здобути доступ до усієї або частини комп'ютерної системи з наміром використання її для вчинення будь-якого зі злочинів, перерахованих у ст. ст. 2-5 Конвенції;

3) здобуття дитячої порнографії за допомогою комп'ютерних систем для себе чи іншої особи; володіння дитячою порнографією у комп'ютерній системі чи на комп'ютерному носії інформації.

На цьому перелік застережень закінчується, це фактично призводить до того, що Україна бере на себе зобов'язання визнавати злочинами діяння, які не можна вважати суспільно небезпечними в контексті національного правового поля. Наприклад, у пункті 1 статті 4 Конвенції пропонується встановлювати відповідальність за навмисне пошкодження, знищення, погіршення, зміну або приховування комп'ютерної інформації без права на це. Україною ця норма ратифікована без застережень. Раніше наводилися аргументи недоцільності визнання злочином незаконних дій з інформацією без вказівки на наслідки таких дій [4, 3]. Тому доцільніше було б ратифікувати цю норму з застереженням, яке у п. 2 ст. 4 Конвенції сформульовано таким чином: «Сторона може залишити за собою право вимагати, щоб поведінка, описана у пункті 1, завдавала серйозну шкоду». Ратифікація цієї норми з вказаним застереженням означала б, що Україна зобов'язується криміналізувати лише ті незаконні дії з інформацією, які завдають «серйозну шкоду». Таке рішення більше відповідало б визначеній вище специфіці суспільної небезпечності комп'ютерних злочинів.

Подібні зауваження стосуються й невикористання Україною можливостей ра-

тифікації з застереженнями, що містяться у ст. ст. 2, 3, 7 Конвенції. Їх використання є необхідним для приведення зобов'язань, взятих на себе Україною у сфері гармонізації кримінального законодавства, відповідно до реальних потреб суспільства та національних особливостей кримінальної правотворчості.

Окремо зазначимо, що наукові дослідження питань імплементації положень Конвенції характеризуються іншими результатами. Так, як можна судити з автореферату дисертації М. В. Плугатиря по темі: «Імплементація Україною міжнародно-правових зобов'язань щодо відповідальності за злочини у сфері комп'ютерної інформації», питання зміни об'єму зобов'язань, що виникли при ратифікації Конвенції та можливостей використання системи застережень, не розглядалися. Більше того, автор наполягає на криміналізації несанкціонованого втручання (доступу) як формального складу злочину, вказуючи на те, що «настання наслідків має бути визначене як кваліфікований склад несанкціонованого втручання» [6, с.12], а також зазначає, що «несанкціоноване перехоплення або копіювання, передбачене у ч. 2 ст. 362 КК України, слід визначити як злочин з формальним складом» [6, с.12]. Такі висновки знову повертають нас до питання інфляції закону про кримінальну відповідальність та необхідності врахування дійсної суспільної небезпечності посягань при формулюванні законотворчих пропозицій.

Таким чином, маємо констатувати: 1) загалом національне законодавство відповідає ратифікованій Конвенції про кіберзлочинність, виняток складає лише некриміналізований чинним законодавством незаконний доступ; 2) має місце надлишкова ратифікація, яка зобов'язує на рівні національного законодавства визнавати злочинами діяння, які не характеризуються суспільною небезпечністю; 3) подальша робота щодо вдосконалення чинного законодавства потребує внесення нових застережень до Закону України «Про ратифікацію Конвенції про кіберзлочинність».

Список використаної літератури

1. Закон України «Про ратифікацію Конвенції про кіберзлочинність» від 07.09.2005 року [Електронний ресурс] // Управління комп'ютеризованих систем Апарату Верховної Ради України. – Режим доступу: http://zakon1.rada.gov.ua
2. *Карчевский Н. В.* Проблемы гармонизации украинского и международного законодательства о компьютерных преступлениях / Н. В. Карчевский [Электронный ресурс] // Официальный сайт Центра исследования компьютерной преступности. – Режим доступа: http://www.crime-research.ru
3. *Карчевський М. В.* Дослідження практики використання національними судами норм про кримінальну відповідальність за злочини в сфері використання комп'ютерної техніки та мереж електрозв'язку / М. В. Карчевський [Електронний ресурс] // Злочини в сфері використання ІТ. – Режим доступу: http//www.it-crime.at.ua
4. *Карчевський М. В.* Чи відповідає КК України потребам протидії злочинам у сфері використання комп'ютерної техніки? / М. В. Карчевський // Право України. – № 7. – 2011. – С. 203 – 209.
5. *Карчевський М. В.* Проблеми гармонізації українського та міжнародного законодавства про комп'ютерні злочини / М. В. Карчевський // Вісник Луганського державного університету внутрішніх справ. – 2005. – № 4. – С. 122–133.
6. *Плугатир М. В.* Імплементація Україною міжнародно-правових зобов'язань щодо відповідальності за злочини у сфері комп'ютерної інформації: автореф. дис. ... канд. юрид. наук: 12.00.08 / Плугатир Максим Віталійович; Державний науково-дослідний інститут МВС України. – К., 2010. – 18 с.