УДК 343.985:343.14

ХЛЕВИЦЬКИЙ Віталій Борисович

ПРОБЛЕМНІ ПИТАННЯ ІМПЛЕМЕНТАЦІЇ В УКРАЇНІ НОРМ МІЖНАРОДНОГО ЗАКОНОДАВСТВА ЩОДО ЗАХИСТУ ПРАВ ЛЮДИНИ У ПРОЦЕСІ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ

Постановка проблеми. Бурхливий розвиток інформаційно-комунікаційних технологій докорінно змінив світ навколо нас за якісь десятиріччя. Уявити життя сучасної людини без технологічних надбань цивілізації неможливо. Бездротовий зв'язок, широкополосний доступ до глобальних мереж та власне сама мережа Інтернет, електронні платіжні системи, системи електронного врядування та надання адміністративних послуг, дистанційної освіти та телемедицини, навіть такі "традиційні" речі, як управління комунальними послугами, продаж побутових товарів чи сплата за паркування – ось далеко не весь перелік позитивних зрушень, що надає пересічній людині стрімка інформатизація, яка охопила усі без винятку сфери життєдіяльності та економіки.

Ці очевидні переваги дозволяють людині максимально повно реалізовувати права та свободи, гарантовані міжнародними договорами та Конституцією України: право на вільний розвиток особистості, невід'ємне право на життя, право брати участь в управлінні державними справами, право володіти, користуватись і розпоряджатись своєю власністю, право на підприємницьку діяльність, право на працю, право на соціальний захист, достатній рівень життя, охорону здоров'я та медичну допомогу, право на освіту. У цьому контексті не варто також забувати про право на безпеку, яке включає право безпечно користуватись сучасними інформаційно-комунікаційними технологіями.

Разом із тим, з огляду на глибинну трансформацію усіх вимірів суспільних відносин перегляду потребують підходи до забезпечення інших невід'ємних прав людини – права володіти, користуватись і розпоряджатись своєю інтелектуальною власністю, права на таємницю листування, телефонних розмов телеграфної та іншої кореспонденції.

Інтернет і, у більш широкому розумінні, кіберпростір несе людині та суспільству переваги, водночас породжуючи нові загрози. Зокрема, блокування роботи веб-сторінок державних органів, із якою б метою воно не здійснювалось, обмежує можливість інших осіб користуватись послугами держави та реалізовувати свої особисті політичні й економічні права. А кіберзлочинність, попри певну віртуальність, на відміну від традиційної злочинності, завдає цілком вимірюваної матеріальної шкоди.

Аналіз останніх досліджень і публікацій. У наукових роботах, предмет яких пов'язаний із кіберзлочинністю, переважно досліджувалися: загальна характеристика злочинів цього типу (Д.С.Азаров [1], В.М.Бутузов [2], В.А.Кудінов та В.М.Смаглюк [3]), питання удосконалення кримінального законодавства в частині відповідальності за злочини (І.О.Чернухін [4]), особливості розслідування комп'ютерних

злочинів (І.В.Гора та В.А.Колесник [5], А.В.Тарасюк [6], К.В.Тітуніна [7], В.П.Шеломенцев [8]) та інші.

Разом із тим, дослідження правових засад забезпечення прав людини у процесі боротьби з кіберзлочинністю раніше не проводились. Низка правових колізій, пов'язаних із захистом прав людини у цій сфері, виникла також після прийняття нового Кримінального процесуального кодексу України.

Отже, **метою статті** є визначення шляхів удосконалення норм вітчизняного законодавства, спрямованих на захист прав людини у процесі боротьби з кіберзлочинністю.

Виклад основного матеріалу. Станом на 2012 рік щонайменше 2,3 мільярди людей або більше однієї третини загальної чисельності населення планети мають доступ до інтернету. Більше 60 % із них знаходяться у країнах, що розвиваються, причому 45 % усіх користувачів мають вік до 25 років. За оцінками експертів, до 2017 року доступ до мобільного широкосмугового інтернету одержать до 70 % населення світу. До 2020 року кількість мережевих пристроїв у шість разів перевершить чисельність населення, що повністю змінить сучасне уявлення про інтернет.

Позаяк слід мати на увазі, що кожний власник або користувач комп'ютера, телефону, радіотелефону, модему, пластикової картки може стати жертвою кіберзлочинців, які стають дедалі винахідливішими та користуються все більш досконалими технологіями.

Власне, кіберзлочинність давно стала транснаціональною, а для угруповань хакерів у віртуальному просторі немає ані державних кордонів, ані океанів та континентів. Злочинцям уже не обов'язково знати одне одного особисто чи хоча б імена, а одноразові хакерські оборудки подекуди сягають сотень мільйонів доларів США. При цьому відбувається розподілення рольової участі: злочинець може знаходитись в одній країні, знаряддя злочину, як-то бот-мережа, ще в кількох країнах, об'єкт посягань, наприклад, банківській рахунок, – у третій країні, а потерпілий – у четвертій, власне банк – у п'ятій, а гроші виводяться ще через кілька транзитних країн. І ця схема ще не найскладніша.

Наведений цілком реальний приклад свідчить, що без широкого міжнародного співробітництва боротьба з кіберзлочинністю є неефективною.

Позитивним уважаємо те, що за останнє десятиліття спостерігається значна активність в ухваленні міжнародних і регіональних документів, спрямованих на протидію кіберзлочинності та створення відповідних міжнародних юридичних механізмів.

Серед найбільш визначних нормативно-правових документів із правового регулювання міжнародних відносин у такій сфері слід згадати зокрема Конвенцію ООН проти транснаціональної організованої злочинності, Віденську декларацію про злочинність і правосуддя: відповіді на виклики XXI століття (ООН), Конвенцію Ради Європи про кіберзлочинність, Конвенцію Європейського Союзу про взаємну правову допомогу з кримінальних справ, Договір про співробітництво держав – учасниць СНД у боротьбі зі злочинами у сфері комп'ютерної інформації. Застосуванню підлягають і положення інших правових документів, наприклад, Конвенції про правову допомогу і правові відносини по цивільних, сімейних і кримінальних справах (держав – учасниць СНД).

Усі ці документи значною мірою доповнюють та вдосконалюють один одного, зокрема в частині, що стосується концепцій і підходів, розроблених у Конвенції Ради Європи про кіберзлочинність.

Більше 40 країн світу вважають Конвенцію Ради Європи про кіберзлочинність (далі – Конвенція) найбільш використовуваним багатостороннім документом при розробленні законодавства у сфері протидії кіберзлочинності. На нашу думку, це комплексний документ, який базуючись на основних принципах міжнародного права, сприяє забезпеченню належного балансу між правоохоронними інтересами й повагою до основних прав і свобод людини.

При цьому серед основних прав, які вимагають адекватного захисту, визначаються право кожного безперешкодно дотримуватись поглядів, право на свободу слова

(включаючи право на пошук, отримання й передачу будь-якої інформації та ідей, незважаючи на кордони), а також право на повагу до приватного життя.

З огляду на зазначене норми Конвенції спрямовані на регулювання трьох основних груп питань, які передбачають:

– зближення кримінально-правової оцінки злочинів у сфері комп'ютерної інформації (ст. 2–13);

– зближення національних кримінально-процесуальних заходів, спрямованих на розслідування таких злочинів (ст. 14–22);

– принципи і форми міжнародного співробітництва у кримінально-процесуальній діяльності, спрямованій на збирання доказів учинення таких злочинів за кордоном (ст. 23–35).

Одна з особливостей Конвенції – вихідний принцип пріоритетності у регулюванні процесу розслідування комп'ютерних злочинів саме національного законодавства. На нашу думку, позитивним кроком є перетворення Конвенції з регіонального механізму співробітництва правоохоронців на справді універсальний механізм, про що свідчить приєднання до неї нових членів, які не входять до Ради Європи. Насправді, чим більше країн будуть сповідувати однакову ідеологію, стандарти правоохоронної діяльності та використовувати уніфіковані механізми взаємної допомоги, тим менше буде "цифрових офшорів" і "безпечних гаваней" для кіберзлочинців.

Україна ратифікувала Конвенцію ще у 2005 році. Досвід практичної реалізації її положень в українських реаліях виявив окремі недоліки цього акта міжнародного права.

Фактично залишаються відкритими такі питання:

– можливість доступу до даних без отримання згоди користувача чи власника, але з подальшим обов'язковим повідомленням останніх чи компетентних органів держави, де знаходиться комп'ютерна система або дані;

– відсутність регулювання механізму відмови у транскордонному доступі особі, яка володіє законним правом на управління комп'ютерною системою і даними, що в ній зберігаються;

– порядок оскарження рішення про збирання комп'ютерних даних при транскордонному доступі;

– захист конфіденційності інформації, отриманої вказаним вище способом;

– судовий та відомчий контроль національних судів і компетентних органів за законністю дій іноземних органів.

Також на сьогодні залишається актуальним питання повноти імплементації положень Конвенції у вітчизняне законодавство.

Аналіз свідчить, що подальшого удосконалення потребують зокрема Цивільний кодекс України, закони України "Про телекомунікації", "Про банки та банківську діяльність", "Про захист інформації в інформаційно-телекомунікаційних системах" у частині, що стосується:

– надання повноважень правоохоронним органам щодо видачі обов'язкових до виконання володільцями комп'ютерних даних (провайдерами й операторами телекомунікацій, іншими юридичними та фізичними особами) приписів про термінове фіксування та подальше зберігання комп'ютерних даних, які потрібні для розкриття злочину, на термін до 90 днів із можливістю продовження терміну до 3 років;

– установлення вимог із надання провайдером телекомунікацій правоохоронним органам інформації для ідентифікації постачальників послуг і маршруту, яким було передано інформацію.

Занепокоєння викликає і стан імплементації Конвенції з огляду на реформування процесуального законодавства України.

Конвенція передбачає такі механізми документування кіберзлочинів, як термінове збереження і часткове розкриття даних про рух інформації (ст. 17), обшук і арешт комп'ютерних даних, які зберігаються (ст. 19), збирання даних про рух інформації в реальному масштабі часу (ст. 20), перехоплення даних змісту інформації (ст. 21) та термінове розкриття збережених даних про рух інформації (ст. 30).

У новому Кримінальному процесуальному кодексі України негласні слідчі дії, які

відповідають зазначеним статтям Конвенції, визначені ст. 263 "Зняття інформації з транспортних телекомунікаційних мереж", а також ст. 264 "Зняття інформації з електронних інформаційних систем" і є різновидом втручання у приватне спілкування.

Відповідно до ст. 246 того ж Кодексу втручання у приватне спілкування проводиться винятково у кримінальному провадженні щодо тяжких або особливо тяжких злочинів. При цьому практично усі злочини, передбачені розділом XVI Кримінального кодексу, не є тяжкими.

Таким чином, склалась ситуація, коли прийняття нового Кримінального процесуального кодексу, який, зауважимо, був розроблений на виконання вимог Ради Європи та пройшов її експертизу, створило передумови для унеможливлення виконання зобов'язань, узятих Україною в рамках Конвенції про кіберзлочинність.

У цьому контексті слід зазначити, що досвід багатьох країн – учасниць Конвенції свідчить про можливість запровадження норм, які установлюють особливий порядок перехоплення та розкриття інформації про рух даних у комп'ютерній системі під час розслідування кіберзлочинів, навіть якщо вони не є тяжкими. Слід усвідомлювати, що кіберзлочинність – особливе явище за своєю природою, а кіберзлочини вчиняються в телекомунікаційних системах, тому зняття інформації з них є не забаганкою правоохоронних органів, а часто єдиним способом встановити істину та задокументувати й припинити протиправну діяльність. Тому, в цьому випадку слід виходити із здорового балансу інтересів особи, суспільства та держави.

Висновки. Конвенція Ради Європи про кіберзлочинність є базовим нормативно-правовим актом для формування національних законодавств, зокрема вітчизняного, у сфері боротьби з кібернетичними злочинами. Україною ратифіковано зазначену Конвенцію, водночас багато її положень у вітчизняному правовому полі залишаються неімплементованими. Крім того, новий Кримінальний процесуальний кодекс України містить норми, які в частині захисту прав людини суперечать положенням Конвенції Ради Європи про кіберзлочинність.

Вирішення зазначених суперечностей можливе шляхом удосконалення вітчизняного законодавства, зокрема Цивільного кодексу України, законів України "Про телекомунікації", "Про банки та банківську діяльність", "Про захист інформації в інформаційно-телекомунікаційних системах". Думка фахівців у сфері протидії кіберзлочинності щодо уведення норм, які б передбачали певне обмеження прав людини в інтересах припинення протиправної діяльності в кіберпросторі, також вбачається слушною.

Список використаних джерел

1. Бутузов В.М. Протидія комп'ютерній злочинності в Україні (системно-структурний аналіз) : моногр. / В.М.Бутузов. – К. : КИТ, 2010. – 408 с.

2. Азаров Д.С. Злочини у сфері комп'ютерної інформації (кримінально-правове дослідження) : моногр. / Д.С.Азаров. – К. : Атіка, 2007. – 304 с.

3. Кудінов В.А. Динаміка злочинів у сфері високих технологій в Україні у 2002–2010 роках за даними МВС України / В.А.Кудінов, В.М.Смаглюк // Актуальні проблеми управління інформаційною безпекою держави : зб. матер. наук.-практ. конф., 22 березня 2011 р. – К. : Наук.-вид. відділ НА СБ України, 2011. – Ч. 2. – 107 с.

4. Чернухін І.О. Співвідношення понять, які визначають об'єкт посягання комп'ютерних злочинів / І.О.Чернухін // Інформаційна безпека людини, суспільства, держави. – 2012. – № 3 (10). – С. 64–70.

5. Гора І.В. Вчинення злочинів у сфері інформаційних технологій та їх криміналістичний аналіз / І.В.Гора, В.А.Колесник // Інформаційна безпека людини, суспільства, держави. – 2012. – № 2 (9). – С. 129–136.

6. Тарасюк А.В. Актуальні питання тактики проведення окремих слідчих дій при розсліду-

вання комп'ютерних злочинів / А.В.Тарасюк, І.В.Гора, В.А.Колесник // Інформаційна безпека людини, суспільства, держави. – 2011. – № 3 (7). – С. 64–69.

7. Тітуніна К.В. До питання розслідування комп'ютерних злочинів, що вчинені з використанням мережі Інтернет / К.В.Тітуніна // Актуальні проблеми управління інформаційною безпекою держави : зб. матер. наук.-практ. конф., 22 березня 2011 р. – К. : Наук.-вид. відділ НА СБ України, 2011. – Ч. 2. – С. 72–74.

8. Шеломенцев В.П. Особливості структури оперативно-розшукових заходів у кіберпросторі / В.П.Шеломенцев // Актуальні проблеми управління інформаційною безпекою держави : зб. матер. наук.-практ. конф., 22 березня 2011 р. – К. : Наук.-вид. відділ НА СБ України, 2011. – Ч. 2. – С. 98–101.

Аннотация: В статье исследуются противоречия в законодательстве Украины, направленном на обеспечение прав человека в процессе борьбы с киберпреступностью. Отмечается необходимость соблюдения надлежащего баланса между защитой прав человека и вынужденными мерами по доступу к личной информации в особых случаях, связанных с документированием и прекращением противоправной деятельности в киберпространстве.

Ключевые слова: Конвенция Совета Европы про киберпреступность, Уголовный процессуальный кодекс Украины, защита прав человека.

Abstract: The article examines contradictions in Ukrainian leoislation, which is aimed of safeguarding human rights in the process of fighting against cybercrime The necessity to stick to the appropriate balance between human rights protection & coercive measures concerning the access to private information in particular cases, related to documenting & halting illegal activity in cyberspace.

Key words: The Convention of the Council of Europe on cybercrime, Criminal procedural code of Ukraine, protection of human rights.