ПРАВОВІ АСПЕКТИ ЗАХИСТУ ІНФОРМАЦІЇ ТА ПЕРСОНАЛЬНИХ ДАНИХ

УДК [343.533+347.77/.78](477)

О. М. Тихоненко, В. С. Тихоненко

НОРМАТИВНО-ПРАВОВІ ОСНОВИ БОРОТЬБИ З КІБЕРЗЛОЧИННІСТЮ В УКРАЇНІ

У ряді узагальнених характеристик розвитку людства третього тисячоліття, заслуговує на увагу такий феномен, як поява інформаційно-комунікаційних технологій (ІКТ) та створення на їх основі мережі Інтернет.

У зв'язку з цим ІКТ відіграють глобальну роль; на рух інформаційних потоків істотно не впливають державні кордони і бар'єри; значно зросли можливості збору, обробки, зберігання, передачі інформації та доступу до неї; підвищується вплив інформації на розвиток різних сфер людської діяльності; заглиблюється процес децентралізації суспільства; відбувається перехід до нових форм зайнятості, що прискорює процес формування нових трудових ресурсів за рахунок збільшення кількості кадрів, зайнятих у інформаційній індустрії.

Тотальна доступність створює широкі технічні можливості для осіб, що використовують ІКТ з протиправною метою. Нові види правопорушень та злочинів об'єднуються під загальними назвами «комп'ютерних», «кібернетичних», «інформаційних», а проблеми боротьби з такими злочинами на сучасному етапі розвитку людства набули особливої актуальності.

Так, за даними голови Служби безпеки України І. Калініна наразі «статистичні дані свідчать про те, що збиток, який завдає кіберзлочинність, сьогодні значно перевищує розмір збитків від традиційних видів злочинів» [1].

Наукові розвідки, присвячені даній проблематиці, вже започатковані такими авторами, як Д. Азаров, П. Андрушко, Ю. Батурін, О. Бойцов, В. Волженкін, В. Гавловський, В. Голубєв, М. Гуцалюк, А. Калюжний, В. Максимов, М. Панов, В. Цимбалюк;

– проблеми правової кібернетики розглядають В. Андріанова, В. Бабін, В. Герасимов, І. Дворянський, В. Кринський, Л. Литвинова, О. Сасорова, Г. Собко;

– загальнотеоретичні положення кримінального права розробляються такими авторами, як М. Бажановим, Ю. Бауліним, В. Борисовим, Ю. Голіком, В. Комісаровим, П. Матишевським, П. Михайленком, В. Навродським, В. Тацій, Є. Фесенком;

– теоретичні основи кіберзлочинності у сфері економіки активно досліджуються А. Базилюк, С. Головнін, А. Шохіна, О. Осіпенко, П. Пушкаренко.

В цілому аналіз наукових джерел показує, що питання кіберзлочинності вивчаються науковцями дуже активно. У публікаціях, монографіях, дисертаційних дослідженнях озвучені провідні ідеї організаційних питань запобігання злочинам, що вчиняються у сфері використання інформаційно-комунікаційних технологій, але недостатньо досліджені саме нормативно-правові основи боротьби з кіберзлочинністю в Україні.

Метою даної роботи є аналіз нормативно-правових основ боротьби з кіберзлочинністю в Україні.

Історично термін «комп'ютерна злочинність» вперше з'явився в американській літературі на початку 60-х років XX століття, коли були виявлені перші випадки злочинів, заподіяних з використанням ЕОМ.

Американська асоціація адвокатів висунула основні ознаки таких злочинів, серед яких:

а) використання або спроба використання комп'ютера, мережі комп'ютерів або обчислювальної системи з метою одержання грошей, власності або послуг, під прикриттям фальшивих приводів або помилкових обіцянок, або видаючи себе за іншу особу;

б) навмисна несанкціонована дія, що має на меті зміну, ушкодження, знищення або викрадання комп'ютера, мережі комп'ютерів або обчислювальної системи, що мають системи математичного забезпечення програм або інформації;

в) навмисне несанкціоноване порушення зв'язку між комп'ютерами, мережами комп'ютерів або обчислювальними системами

У 1986 році в Парижі групою експертів Організації економічного співробітництва і розвитку вперше було подано кримінологічне визначення комп'ютерного злочину, під яким розумілася будь-яка незаконна, неетична або недозволена поведінка, що стосувалася автоматизованої обробки і/або передачі даних [2].

В одному з документів ООН вказано, що існує дві категорії кіберзлочинів: у вузькому розумінні («комп'ютерний злочин» чи «computer crime») – будь-яке противоправне діяння, що здійснюється за допомогою електронних операцій, метою якого є подолання захисту комп'ютерних систем та даних, що ними обробляються; в широкому розумінні («злочини, пов'язані з використанням комп'ютера» чи «computer-related crime») – будь-яке противоправне діяння, що здійснюється за допомогою або у зв'язку з комп'ютерною системою чи мережею [3].

Також становить цікавість Європейська конвенція про кіберзлочинність – комплексний документ, який містить норми, покликані впливати на різні галузі права: кримінальне, кримінально-процесуальне, авторське, громадянське, інформаційне.

Конвенцією запропоновано включити в національне законодавство країн-учасниць норми кримінальної відповідальності за злочини в сфері комп'ютерної інформації.

У даному документі термін «злочини в сфері комп'ютерної інформації» конкретно не визначається, а замінено на «кіберзлочини», що розкривається переліком: діяння, спрямовані проти комп'ютерної інформації (як предмета злочинного замаху) та використовуючи її у якості унікального знаряддя злочину; діяння предметом замаху яких є інші, охороняючи законом блага, а інформація, комп'ютери тощо є лише одним із елементів об'єктивної сторони злочину у якості, наприклад, знаряддя його здійснення, складовою частиною способу здійснення чи приховування.

Об'єктом кіберзлочинів, згідно Конвенції, є широкий спектр суспільних відносин, що виникають при виконанні інформаційних процесів з приводу виробництва, збору, обробки, накопичення, зберігання, пошуку, передачі, розповсюдження та споживання комп'ютерної інформації, а також в інших галузях, де використовуються комп'ютери, комп'ютерні системи та мережі. Серед них, враховуючи підвищену суспільну значимість виділяють правовідносини, що виникають у сфері забезпечення конфіденційності, цілісності та доступності комп'ютерних даних і систем, законного використання комп'ютерів та комп'ютерної інформації, авторських та суміжних прав [4].

Зрозуміло, що об'єктивна сторона кіберзлочинів передусім характеризується виділенням чотирьох груп суспільно небезпечних діянь, що пов'язані з:

– конфіденційністю, цілісністю та доступністю комп'ютерних даних і систем (протизаконний доступ та перехват даних, порушення цілісності даних, втручання в функціонування системи);

– використанням комп'ютерів (підробка та шахрайство з використанням комп'ютера);

– порушенням у галузі авторських та суміжних прав;

– змістом даних (правопорушення, пов'язані, наприклад, з дитячою порнографією).

Суб'єктом кіберзлочинів може бути фізична особа, що здійснила вказані вище діяння.

До недавнього часу законодавство більшості зарубіжних країн покликано було забезпечити захист законних прав та інтересів як особистості так і суспільства у матеріальному світі.

З поступовим розвитком інформаційних технологій та засобів телекомунікації, які стали незамінною складовою життя людини, діяльності суспільства та механізмів держави виникла необхідність нормативно-правової підтримки нових відносин, що виникають при використанні інформаційно-комунікаційних технологій, формування

правової середи з чітким колом категорій та понять – важливих елементів ефективного розвитку нових явищ.

Зазначена проблематика знаходиться у полі зору міжнародної спільноти, оскільки міждержавні нормативно-правові акти резюмують, що кіберзлочинність становить загрозу головним чином національній безпеці окремих держав, загрожує людству, а вивчення міжнародного досвіду активізує міжнародне співробітництво.

У той же час, зважаючи на те, що в сучасних умовах значна частка засобів боротьби з кіберзлочинами належить до внутрішньої компетенції кожної окремої держави, необхідно паралельно розвивати й національне законодавство, спрямоване на боротьбу з даними злочинами, узгоджуючи його з міжнародними нормами права та спираючись на існуючий позитивний досвід.

Внаслідок цього окреслені проблеми перебувають під пильним наглядом Президента України, Верховної Ради та Уряду України, що актуалізує проблематику інтеграції України у світове та європейське співтовариство.

Так, 10 грудня 2010 року Указом Президента України № 1119/2010 набуло чинності Рішення Ради національної безпеки і оборони України від 17 листопада 2010 року «Про виклики та загрози національній безпеці України у 2011 році». Відповідно до цього рішення було поставлене завдання «розробити за участю та подати у двомісячний строк на розгляд Ради національної безпеки і оборони України пропозиції щодо створення єдиної загальної системи протидії кіберзлочинності» [5].

Враховуючи викладене слід відмітити, що як у юридичній літературі, так і в кримінальному законодавстві різних держав не розроблене єдине поняття таких злочинів, відсутня термінологічна єдність та система теоретичних понять, яка повною мірою описує та відображає діяння, а також наслідки, що виникають у результаті неправомірного використання комп'ютерів, їх систем, локальних та глобальних комп'ютерних мереж.

Нормативно-правові основи боротьби з кіберзлочинністю базуються на засадах інформаційного законодавства – комплексної галузі законодавства України та ґрунтується на Конституції України, яка покликана забезпечити правову основу державної політики України щодо боротьби з комп'ютерною злочинністю, у тому числі, положення, визначені Статтею 17 – захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього українського народу; Статтею 31 гарантується кожному таємниця листування, телефонних розмов, телеграфної та іншої кореспонденції за винятками, встановленими лише судом у випадках, передбачених законом, з метою запобігання злочину чи з'ясування істини під час розслідування кримінальної справи, якщо іншими способами одержати інформацію

неможливо; Стаття 32 відзначає, що ніхто не може зазнавати втручання в особисте і сімейне життя, крім випадків, передбачених Конституцією України, не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини [6].

Розвиток положень Конституції України знаходить відображення у законодавстві України:

– Закон України «Про інформацію» (1992 р.), який регулює відносини щодо створення, збирання, одержання, зберігання, використання, поширення, охорони, захисту інформації [7];

– Закон України «Про науково-технічну інформацію» (1993 р.) визначає основи державної політики в галузі науково-технічної інформації, порядок її формування і реалізації в інтересах науково-технічного, економічного і соціального прогресу країни. Метою Закону є створення в Україні правової бази для одержання та використання науково-технічної інформації [8];

– Закон України «Про захист інформації в автоматизованих системах» (1994 р.) регулює відносини у сфері захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах [9];

– Закон України «Про охорону прав на топографії інтегральних мікросистем» регулює відносини, що виникають у зв'язку з набуттям і здійсненням права власності на топографії інтегральних мікросистем в Україні (1997 р.) [10];

– Закон України «Про Концепцію Національної програми інформатизації» (1998 р.) включає характеристику сучасного стану інформатизації, стратегічні цілі та основні принципи інформатизації, очікувані наслідки її реалізації [11];

– Закон України «Про Національну програму інформатизації» (1998 р.) визначає загальні засади формування, виконання та коригування Національної програми інформатизації [12];

– Кримінального кодексу України, що має своїм завданням правове забезпечення охорони прав і свобод людини і громадянина, власності, громадського порядку та громадської безпеки, забезпечення миру і безпеки людства, а також запобігання злочинам. Для здійснення цього завдання Кримінальний кодекс України визначає які суспільно-небезпечні діяння є злочинами та які покарання застосовуються до осіб, що їх вчинили.

Кримінальним кодексом України встановлена відповідальність за злочини, родовим об'єктом замахів, згідно назви розділу XVI, визначена сфера використання електронно-обчислювальних машин (комп'ютерів), систем і комп'ютерних мереж. Даний розділ містить:

– Ст. 361 «Незаконне втручання в роботу електронно-обчислювальних машин, систем та комп'ютерних мереж». Згідно з нею

склад злочину утворює умисне втручання в роботу автоматизованих ЕОМ, їх систем та мереж, що спричинило перекручування або знищення інформації чи носіїв інформації або розповсюдження комп'ютерного вірусу шляхом використання програмних та технічних засобів, призначених для незаконного проникнення в автоматизовані системи тощо.

Кваліфікованим змістом таких злочинів є ті дії, що спричинили шкоду в великих розмірах, здійснені удруге або за попередньою змовою групою осіб.

– Ст. 362 «Викрадення, привласнення, вимагання комп'ютерної інформації або привласнення її шляхом шахрайства або зловживання службовим становищем».

– Ст. 363 «Порушення правил експлуатації автоматичних електронно-обчислювальних систем», встановлює відповідальність за порушення правил експлуатації ЕОМ, системи ЕОМ або їх мереж особою, що відповідає за їх експлуатацію, що спричинило розкрадання, знищення, перекручування комп'ютерної інформації, обладнання її захисту або незаконне копіювання інформації [13];

– Кримінально-процесуального кодексу України призначенням якого є визначення порядку провадження кримінальних справ. Завданням кримінального судочинства є охорона прав та законних інтересів фізичних і юридичних осіб, які беруть в ньому участь, а також швидке і повне розкриття злочинів, викриття винних та забезпечення правильного застосування Закону з тим, щоб кожний хто вчинив злочин, був притягнутий до відповідальності [14];

– Цивільного кодексу України, що регулює особисті немайнові та майнові відносини, засвоєні на юридичній рівності, вільному волевиявленню, майновій самостійності їх учасників [15];

– Кодексу України про адміністративні правопорушення завданням якого є охорона прав і свобод, власності, конституційного ладу України, прав і законних інтересів підприємств, установ і організацій, встановленого правопорядку, зміцнення законності, запобігання правопорушенням, виховання громадян у дусі точного і неухильного додержання Конституції і законів України, поваги до прав, честі і гідності інших громадян, до правил співжиття, сумлінного виконання своїх обов'язків, відповідальності перед суспільством [16];

– Закону України «Про внесення змін до деяких законодавчих актів України щодо протидії розповсюдженню дитячої порнографії», яким посилено кримінальну відповідальність за розповсюдження, виготовлення творів, зображень або інших предметів порнографічного характеру, що містять дитячу порнографію, та встановлено додатковий контроль за діяльністю операторів телекомунікацій [17].

Деякі положення щодо регулювання інформаційних правовідносин в умовах становлення та розвитку інформаційного суспільства в Україні закріплені у Постановах Верховної Ради України

про затвердження Концепції (основ державної політики) національної безпеки України; про організацію роботи по формуванню єдиної системи правової інформації в Україні; про Консультативну раду з питань інформатизації при Верховній Раді України тощо.

Державна політика України щодо боротьби з кіберзлочинністю знаходить вираз у нормативно-правових актах органів державної влади у межах їх компетенції, функцій, прав і обов'язків – Укази Президента України, нормативно-правові акти Уряду України, міністерств і відомств, таких, як: Положення Указу Президента України №1193/2001 «Про рішення Ради національної безпеки і оборони України від 31 жовтня 2001 р.» «Про заходи щодо вдосконалення державної інформаційної політики за забезпечення інформаційної безпеки України» від 6 грудня 2001 р. [18].

Аналіз дозволяє стверджувати, що в Україні сформовано специфічні національні нормативно-правові основи боротьби з кіберзлочинністю, серед недоліків та прогалин яких є:

1. правотворчий процес на рівні органів державної влади здійснюється нерідко без узгодження з чинним законодавством, без урахування специфіки національної ментальності, правової культури та особливостей соціального та державного життя;

2. проаналізовані закони приймалися у різні часи без узгодження понятійного апарату, тому низка термінів розуміються неоднозначно, деякі категорії не мають чіткого визначення свого змісту, що призводить до їх неоднозначного застосування, що в свою чергу створює умови для уникнення відповідальності правопорушників;

3. значна кількість юридичних норм міститься у різних законах та підзаконних нормативних актах, що ускладнює пошук, аналіз та узгодження для практичного застосування;

4. досвід багатьох країн свідчить, що розслідуванням кіберзлочинів повинні займатися не лише співробітники правоохоронних органів. Це пов'язано з тим, що робота вимагає спеціальних знань. Існує потреба у створенні спеціалізованих підрозділів у системі правоохоронних органів України та у підготовці кваліфікованих кадрів не тільки у юридичних, а й економічних та технічних аспектах;

5. формування юридичної деліктології (вчення про правопорушення) у сфері інформаційно-комунікаційних відносин на принципі гармонізації норм з галузевими деліктологіями – конституційного, адміністративного, цивільного, кримінального, трудового. Невизначеність законодавства знайшла відображення у проаналізованих законах, де визначені диспозиції правопорушень, але чітко не визначена, а в деяких і зовсім відсутня відповідальність за них;

6. сьогодні законодавство має значний масив законів та підзаконних актів, які прямо чи опосередковано регулюють суспільні інформаційні відносини в Україні. Це ставить першочергове завдання визначення статусу суспільних відносин та шляхів їх публічно-правового

регулювання з метою уникнення, зменшення, запобігання та подолання негативних проявів інформаційного суспільства та стимулювання бажаних для людини, держави та суспільства правил поведінки його суб'єктів.

Список використаної літератури

1. СБУ: Головні проблеми для України – тероризм і кіберзлочинність // http://www.pravda.com.ua/news/2012/03/23/6961285/ **2. Волеводз А.Г.** Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. – М. : ООО Издательство «Юрлитинформ», 2002. – 496 с. **3. Преступления**, связанные с использованием компьютерной сети. Справочный документ для семинара-практикума по использованию компьютерной сети. / Документ ООН A/CONF. 187/10 – с. 6. – Режим доступа: http://zakon3.rada.gov.ua **4. Конвенція** про кіберзлочинність // http://zakon2.rada.gov.ua/laws/ show/994_575 **5. Указ** Президента «Про Рішення Ради національної безпеки і оборони України» (№ 1119/2010 від 10.12.2010) // http://zakon2.rada.gov.ua/laws/show/n0008525-10 **6. Конституція** України http://zakon2.rada.gov.ua/laws/show/ **7. Закон** України «Про інформацію» // http://zakon2.rada.gov.ua/laws/show/2657-12 **8. Закон** України «Про науково-технічну інформацію» // http://zakon2.rada.gov.ua /laws/show/ **9. Закон** України «Про захист інформації в автоматизованих системах» // http://zakon1.rada.gov.ua/laws/show/2594-15 **10. Закон** України «Про охорону прав на топографії інтегральних мікросистем» // http://zakon.nau.ua/doc/?code=621/97-%C2%D0 **11. Закон** України «Про Концепцію Національної програми інформатизації» // http://zakon2.rada.gov.ua/laws/show/75/98 **12. Закон** України «Про Національну програму інформатизації» // http://zakon3.rada.gov.ua/laws/ show/74/98 **13. Кримінальний** кодекс України // http://zakon2.rada.gov.ua/ laws/show/2341-14 **14. Кримінально-**процесуальний кодекс України // http://zakon2.rada.gov.ua/laws/show/1001-05 **15. Цивільний** кодекс України // http://zakon.nau.ua/doc/?uid=1011.25.77&nobreak=1 **16. Кодекс** України про адміністративні правопорушення // http://search.ligazakon.ua/ l_doc2.nsf/link1/KD0005.html **17. Закон** України «Про внесення змін до деяких законодавчих актів України щодо протидії розповсюдженню дитячої порнографії» http://khpg.org/index.php?id=1264077929 **18. Положення** Указу Президента України №1193/2001 «Про рішення Ради національної безпеки і оборони України від 31 жовтня 2001 р.» «Про заходи щодо вдосконалення державної інформаційної політики за забезпечення інформаційної безпеки України» від 6 грудня 2001 р. // zakon.rada.gov.ua/laws/show/1193/2001

Тихоненко О. М., Тихоненко В. С. Нормативно-правові основи боротьби з кіберзлочинністю в Україні

У статті проаналізовано нормативно-правові основи боротьби з кіберзлочинністю в Україні, виявлено прогалини та колізії регулювання відносин у сфері кіберзлочинності.

Ключові слова: інформаційно-комунікаційні технології, інформаційне законодавство, кіберзлочин, кіберзлочинність.

Тихоненко Е. Н., Тихоненко В. С. Нормативно-правовые основы борьбы с киберпреступностью в Украине

В статье проанализированы нормативно-правовые основы борьбы с киберпреступностью в Украине, выявлены пробелы и колизии регулирования отношений в сфере киберпреступности.

Ключевые слова: информационно-комуникационные технологи, информационное законодательство, киберпреступление, киберпреступность.

Tyhonenko O. M., Tyhonenko V. S. The Normative and Legal Bases of Fighting Cyber Crime in Ukraine

In the article were analyzed the normative and legal bases of fighting cyber crime in Ukraine; were determined gaps and impacts in relations regulation in the sphere of cyber crime.

Key words: information and communication technologies, information legislation, cyber crime, cyber criminality.

Стаття надійшла до редакції 05.09.2012 р.
Прийнято до друку 28.09.2012 р.