УДК 340.13

Буяджи С.А.,
Президент благодійного фонду «Ангели Доброти»

ТЕНДЕНЦІЇ РОЗВИТКУ ПРАВОВОГО РЕГУЛЮВАННЯ БОРОТЬБИ З КІБЕРЗЛОЧИННІСТЮ В УКРАЇНІ

У статті наведено перелік тенденцій розвитку правового регулювання боротьби з кіберзлочинністю в Україні. Охарактеризовано зміст і значення кожної з них. Автор доходить висновку те, що сьогодні Україною ведеться активна діяльність щодо покращення існуючої ситуації з кібербезпекою. Вітчизняне законодавство все ще перебуває на недостатньому рівні для вирішення поточних проблем, а співробітництво з іншими державами у даному напрямку потребує активізації.

Ключові слова: тенденція, правове регулювання, боротьба з кіберзлочинністю, законодавство, кібербезпека.

В статье приведен перечень тенденций развития правового регулирования борьбы с киберпреступностью в Украине. Охарактеризовано содержание и значение каждой из них. Автор приходит к выводу о том, что сегодня Украиной ведется активная деятельность по улучшению существующей ситуации с кибербезопасностью. Отечественное законодательство все еще находится на недостаточном уровне для решения текущих проблем, а сотрудничество с другими государствами в данном направлении требует активизации.

Ключевые слова: тенденция, правовое регулирование, борьба с киберпреступностью, законодательство, кибербезопасность.

In the article examined list of the trends of legal regulation of combating cybercrime in Ukraine. Characterized the meaning and significance of each of them. The author comes to the conclusion that, today, the active work is, in order to improve the existing situation of cybersecurity by Ukraine. Domestic legislation is still at

low level to solve current problems, and cooperation requires an activation with other countries in this direction.

Keywords: trend, legal regulation, cybercrime combating, legislation, cybersecurity.

Постановка проблеми. У контексті підвищення актуальності питань, пов'язаних з боротьбою із кіберзлочинністю, в Україні важливими були останні декілька років, коли почали спостерігатися тенденція підвищення ролі та значення кібербезпеки в суспільному житті. Ключовими факторами розвитку правового регулювання боротьби з кіберзлочинністю в Україні є збільшення активності громадян в Інтернет-просторі, активізація діяльності кіберзлочинців та необхідність імплементації міжнародних правових норм у вітчизняне законодавство для боротьби з цим негативним явищем. В той же час, звертаючись до наукової доктрини, варто відзначити недостатню увагу до даного питання з боку саме вчених-правознавців. Переважна більшість робіт з цієї тематики охоплюють тенденції поширення кіберзлочинів, або ж не є вже актуальними сьогодні. Це є проблемою, оскільки досліджуване питання у цілому постійно перебуває в сфері наукових інтересів вітчизняних дослідників і ніколи не втрачає доцільності дослідження.

Аналіз дослідження даної проблеми. Розробкою питань, пов'язаних з визначенням тенденцій розвитку правового регулювання боротьби з кіберзлочинністю в Україні займались вчені різноманітних сфер вітчизняної науки, зокрема правової та економічної. Серед них виділимо таких як Ю.М. Батурин, В.Л. Бурячок, В.Б. Вєхов, В.О. Голубєв, Н.Ф. Казакова, О.Ф. Мельников, Ю.М. Онищенко, О. В. Орлов, Б.В. Романюк, Ю.Є. Якубівська та багато інших. Водночас, в проаналізованих роботах не завжди присутній правовий аспект досліджуваних проблем. При цьому, важливість аналізу тенденцій розвитку правового регулювання боротьби з кіберзлочинністю в Україні на сучасному етапі її розвитку обумовлюється постійним розвитком інформаційних технологій та нормативно-правової бази їх реалізації.

Виклад основного матеріалу. Аналіз української наукової доктрини дозволив виділити три основних тенденції розвитку правового регулювання боротьби з кіберзлочинністю: 1) тенденція розвитку вітчизняної нормативно-правової та термінологічної бази у сфері боротьби з кіберзлочинністю; 2) тенденція посилення міжнародного співробітництва у сфері боротьби з кіберзлочинністю в Україні; 3) тенденція збільшення рівня контролю за користувачами мережі Інтернет.

Окрім проаналізованих позицій, вважаємо за необхідне доповнити перелік основних тенденцій розвитку правового регулювання боротьби з кіберзлочинністю в Україні підтенденціями, які деталізуватимуть їх зміст. Так, у рамках тенденції розвитку вітчизняної нормативно-правової та термінологічної бази у сфері боротьби з кіберзлочинністю пропонуємо виокремити наступні підтенденції: 1) розширення меж розуміння поняття «кіберзлочинність»; 2) посилення кримінальної відповідальності за вчинення кіберзлочинів; 3) термінологічне узгодження усіх нормативно-правових актів, що регламентують це питання, запровадження єдиного термінологічного апарату.

Щодо тенденції посилення міжнародного співробітництва у сфері боротьби з кіберзлочинністю в Україні основними підтенденціями є: 1) ратифікація тих міжнародних нормативно-правових актів у сфері боротьби з кіберзлочинністю, які на сьогодні ще не є джерелом вітчизняного права; 2) укладення міжнародних дво- чи багатосторонніх угод з іншими державами; 3) правова допомога іншим державам з питань боротьби з кіберзлочинністю; 4) втілення міжнародних стандартів у нормах вітчизняного законодавства.

В тенденції збільшення рівня контролю за користувачами мережі Інтернет виділимо наступні підтенденції: 1) встановлення правил користування громадянами кіберпростором; 2) створення спеціальних органів контролю, покликаних спостерігати та виявляти порушників встановлених правил користування кіберпростором.

Для розуміння того, які заходи є необхідними для розвитку правового регулювання боротьби з кіберзлочинністю в Україні, варто належним чином розкрити кожну із названих тенденцій.

Тенденція розвитку вітчизняної нормативно-правової та термінологічної бази у сфері боротьби з кіберзлочинністю в Україні полягає у прямій залежності наших успіхів та розвитку від тієї законодавчої бази, яка врегульовує питання кіберзлочинності. Будь-які суспільні відносини, як у реальному, так і у віртуальному світі мають бути належним чином регламентовані та захищені нормами законодавства.

Контроль та запобігання негативних явищ вимагає від держави інтенсивніших дій щодо вдосконалення нормативно-правової та термінологічної бази у сфері боротьби з кіберзлочинністю. Зокрема, було б доцільним здійснення централізованої діяльності у наступних напрямках:
1) розширення меж розуміння поняття «кіберзлочинність»;
2) посилення відповідальності за вчинення кіберзлочинів;
3) встановлення єдиного термінологічного апарату у вітчизняному законодавстві тощо.

Наша держава залишається вразливою до кібервпливу. Причину цьому варто шукати у тому, що вітчизняні закони, які врегульовують питання кіберпростору та злочинних посягань у ньому, є недостатньо розробленими. У Кримінальному кодексі України (далі – КК України) передбачено Розділ XVI «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку». Проте станом на сьогодні він містить лише шість статей: 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, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається 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, яка в них оброблюється», 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 або порядку чи правил захисту інформації, яка в них оброблюється» [1]. Очевидно, що розвиток комп'ютерних технологій дозволяє зловмисникам здійснювати кіберзлочини фактично безкарно, оскільки кримінальне законодавство у такому вигляді є неадаптованим до нових форм злочинів у сфері інформаційних технологій. Наведемо актуальний приклад: в умовах гібридної війни Україна щодня отримує атаки на інформаційний простір. Поширення неправдивої інформації, створення ситуацій, що викликають паніку, провокування ненависті тощо. Це далеко не повний перелік заходів, що є елементами негативного інформаційного впливу на кіберпростір України. Сьогодні інформація є одним із видів зброї, що застосовується проти громадян України. Проте КК України жодним чином не регламентує цю протиправну діяльність у інформаційному просторі.

Для вирішення даної проблеми в першу чергу варто розширити зміст Розділу XVI КК України. Безліч сучасних кіберзлочинів на сьогодні залишаються поза правового врегулювання. Наприклад, поширення неправдивої інформації, створення ситуацій, що викликають паніку за допомогою комп'ютерних мереж, провокування ненависті за допомогою комп'ютерних мереж, використання спеціальних шкідливих комп'ютерних програм тощо. Їх регламентація у нормах КК України дозволить, по-перше, осучаснити розуміння поняття «кіберзлочинність», оскільки з розвитком сучасних технологій, кіберзлочинці постійно знаходять нові шляхи для здійснення протиправної діяльності. По-друге, дасть змогу врегулювати вже наявні на сьогодні загрози та продемонструє готовність держави адекватно реагувати на небезпеки. По-третє, при розширенні змісту Розділу XVI КК України необхідним є

звернення до збільшення санкцій за вчинення відповідних злочинів. Аналіз статей 361-363[1] КК України засвідчив, що санкції, передбачені ними, є в цілому схожими: мінімальне покарання за вчинення злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку встановлено на рівні від п'ятисот до тисячі неоподатковуваних мінімумів доходів громадян, а максимальне – позбавлення волі на строк від двох до п'яти років. Розвиток даного виду злочинності свідчить про те, що таких санкцій на сьогодні недостатньо. В сучасних умовах кіберзлочинність несе загрозу не просто окремим суб'єктам, а державі в цілому.

Наступною проблемою є відсутність єдиного понятійного апарату, що має вияв у вільному трактуванні ключових понять: «кіберзлочини», «кібербезпека», «кіберпростір» тощо у нормах вітчизняного законодавства. Наприклад, у КК України законодавець оперує такими поняттями, як «злочини у сфері використання електронно-обчислювальних машин», «комп'ютерні системи», «комп'ютерні мережі», «мережі електрозв'язку» тощо. Водночас, Законом України від 20.03.2003 р. № 638-IV «Про боротьбу з тероризмом» подібна до кіберзлочинності термінологія не використовується взагалі. Кіберзлочини роз'яснюються як складова частина технологічного тероризму, оскільки ними є у т.ч. злочини, які «вчиняються з терористичною метою із застосуванням комп'ютерних систем та комунікаційних мереж» [2]. Тобто, в даному випадку законодавцем взагалі проігноровано використання загальноприйнятої на міжнародному рівні та у вітчизняній науці термінології. В Законі України від 19.06.2003 р. № 964-IV «Про основи національної безпеки України» містяться терміни «комп'ютерна злочинність» та «комп'ютерний тероризм». Тобто, у трьох проаналізованих нами нормативно-правових актах одні й ті самі явища позначені трьома різноманітними варіантами термінів. Враховуючи наведене, варто зробити наступні висновки:

1) в нормах вітчизняного законодавства відсутній єдиний термінологічний апарат. Для подолання даної прогалини варто внести зміни до усіх нормативно-правових актів, якими

врегулювано боротьбу з кіберзлочинністю в Україні. Найбільш доцільним вбачається саме використання термінології із частиною «кібер-», яка на сьогодні ще не отримала сформованого визначення на нормативно-правовому рівні. Проте в міжнародних нормативно-правових актах даний вид злочинності позначається саме так, свідченням чому є прийняття Конвенції про кіберзлочинність від 23.11.2001 року [3];

2) законодавець оперує термінами, визначення яким не надано взагалі, а чинні терміни є численними та неузгодженими між собою. Це стосується тих визначень, які закріплено в діючому законодавстві: «комп'ютерні системи», «комп'ютерні мережі», «мережі електрозв'язку», «комп'ютерна злочинність», «комп'ютерний тероризм» тощо. Проте, більш доцільним є прийняття єдиного термінологічного апарату із його подальшим роз'ясненням в правових нормах. На науковому рівні розуміння цієї проблеми сформувалось вже давно, оскільки розробка необхідної термінології постійно перебуває у сфері наукових інтересів вітчизняних дослідників.

Здійснений аналіз дає підстави узагальнити наявні сьогодні проблеми вітчизняної нормативно-правової та термінологічної бази у сфері боротьби з кіберзлочинністю в Україні: 1) вузький спектр злочинних діянь, за які передбачено покарання у нормах КК України; 2) проблеми понятійного апарату, пов'язані із вільним використанням великої кількості термінів, які не узгоджуються між собою; 3) чинне законодавство про боротьбу з кіберзлочинністю в Україні не повною мірою відповідає вимогам часу.

А отже, в рамках даної тенденції вбачаємо доцільним у майбутньому проведення наступних дій:

1) формування єдиної системи нормативного забезпечення протидії кіберзлочинності на загальнодержавному рівні. Це можна здійснити шляхом прийняття нормативно-правових актів, які стосуватимуться виключно кібербезпеки нашої держави. Наприклад, таку систему може сформувати Закон України «Про боротьбу із кіберзлочинністю», який закріпить та узагальнить усі ключові поняття досліджуваного інституту, та низка

підзаконних нормативно-правових актів, які передбачатимуть механізми реалізації його норм;

2) розширення Розділу XVI «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» КК України статтями «Поширення неправдивої інформації», «Провокування ненависті і нетерпимості за допомогою комп'ютерних мереж» тощо. Пропонуємо сформулювати дані статті наступним чином (при встановленні міри покарань ми орієнтувались на орієнтовні розміри санкцій статей Розділу XVI КК України):

- «Поширення неправдивої інформації.

1. Поширення у мережі Інтернет неправдивої інформації, що спричиняє паніку серед населення, – карається штрафом від п'ятисот до тисячі неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років.

2. Дії, передбачені частиною першою цієї статті, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду, – караються позбавленням волі на строк до шести років»;

- «Провокування ненависті і нетерпимості за допомогою комп'ютерних мереж.

1. Поширення у мережі Інтернет інформації, що провокує ненависть і нетерпимість серед населення, – карається штрафом від шестисот до тисячі неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років.

2. Дії, передбачені частиною першою цієї статті, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду, – караються позбавленням волі на строк до шести років»;

3) створення необхідного понятійного апарату, термінологічне узгодження у нормах усіх нормативно-правових актах, що регламентують дане питання: у нормах КК України, Закону України від 19.06.2003 № 964-IV «Про основи національної безпеки України», Закону України від 20.03.2003 № 638-IV «Про боротьбу з тероризмом» тощо, а також в новоприйнятих нормативно-правових актах закріпити єдиний термінологічний апарат (визначення понять «кіберпростір»,

«кібермережі», «кібербезпека», «кіберзлочинність», «кібертероризм», «кіберзлочинець», «кібертерорист» тощо):

- КК України: Розділ XVI «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» запропонуємо перейменувати на «Злочини у сфері кібербезпеки», в статтях даного розділу терміни «злочини у сфері використання електронно-обчислювальних машин», «комп'ютерні системи», «комп'ютерні мережі», «мережі електрозв'язку» замінити на «злочини у кіберпросторі», «кіберпростір», «кібермережі» тощо;

- Закон України від 20.03.2003 № 638-IV «Про боротьбу з тероризмом»: у ст. 1 визначити поняття кібертероризму як «суспільно небезпечної діяльності, яка полягає у вчиненні злочинів з терористичною метою із застосуванням кібермереж»;

- Закон України від 19.06.2003 № 964-IV «Про основи національної безпеки України»: у ст. 7 терміни «комп'ютерна злочинність» та «комп'ютерний тероризм» замінити на «кіберзлочинність» та «кібертероризм».

Наступною виділеною нами тенденцією є посилення міжнародного співробітництва у сфері боротьби з кіберзлочинністю в Україні. Потреба міжнародного співробітництва стосовно нашої держави має трьохаспектний характер. По-перше, в умовах формування інституту правового регулювання боротьби з кіберзлочинністю в Україні важливим є звернення до досвіду тих держав, які його успішно втілили у вітчизняних правових системах, із урахуванням сильних сторін та проблем, які супроводжували даний процес. По-друге, потреба у міжнародному співробітництві з'явилась, передусім, внаслідок масової появи транснаціональних комп'ютерних злочинів, складність яких свідчить про те, що жодна держава не здатна їх подолати, покладаючись виключно на власні сили. По-третє, прагнення України до євроінтеграції неможливо втілити без встановлення міцних зв'язків із європейськими державами, в т.ч. і у питанні кібербезпеки.

Втілення тенденції посилення міжнародного співробітництва у сфері боротьби з кіберзлочинністю в Україні вбачаємо у наступних діях:

1) ратифікація низки міжнародних нормативно-правових актів у сфері боротьби з кіберзлочинністю, наприклад, Віденської декларації про злочинність і правосуддя: відповіді на виклики XXI століття (ООН) від 17.04.2000 року [4]. У разі завершення процесу євроінтеграції, важливим кроком є ратифікація Конвенції про взаємодопомогу в кримінальних справах між державами-членами ЄС [5];

2) укладення міжнародних дво- чи багатосторонніх угод, зокрема із державами-сусідами України, а враховуючи євроінтеграційне прагнення нашої держави – з європейськими країнами;

3) надання правової допомоги іншим державам у кримінальних справах, обмін відомостями оперативно-розшукового характеру з іншими державами у справах про кіберзлочини, виїзд членів слідчо-оперативних груп за кордон та прийняття працівників правоохоронних органів іноземних держав в Україні для проведення слідчих і оперативно-розшукових дій, адже такі дії можуть здійснюватись лише за умови укладення угод з іншими державами;

4) здійснення детального наукового аналізу міжнародного законодавства та аналіз досвіду інших країн у сфері боротьби з кіберзлочинністю.

Тенденція збільшення рівня контролю за користувачами мережі Інтернет полягає у зміні балансу між правоохоронними інтересами та повагою до основних прав і свобод людини й громадянина в інтересах держави. Дана тенденція у цілому є вкрай негативним явищем, проте за умови досягнення кіберзлочинністю катастрофічних масштабів, подібне рішення може виступити у якості основного вирішення поставлених перед державою завдань.

Впродовж останніх десятиліть було сформовано концептуальне розуміння боротьби з кіберзлочинами та захистом інтересів держави в інформаційній сфері як забезпечення належного і стійкого балансу між правоохоронними інтересами та повагою до основних прав і свобод людини й громадянина. При цьому, звичайно і на сьогодні існує можливість використання інформаційних технологій на шкоду основним правам і свободам людини.

До проблем втілення такої тенденції варто віднести: 1) необхідність переосмислення сутності конституційних прав та свобод людини і громадянина; 2) проникнення держави у приватне життя громадян; 3) посилення контролю, що негативним чином відіб'ється на суспільстві; 4) обмеження можливостей людини вільно розпоряджатись благами науково-технічного прогресу.

Сама ж тенденція збільшення рівня контролю за користувачами мережі Інтернет повинна втілюватись наступним чином:

1) встановлення правил користування громадянами кіберпростором, наприклад як і у випадку з прийняттям Указу Президента України №133/2017, яким введено в дію рішення Ради національної безпеки і оборони України від 28 квітня 2017 р. «Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)» [6], яким заборонено доступ до окремих Інтернет-ресурсів. Схожим чином буде здійснюватись регулювання й інших питань, пов'язаних із контролем за користувачами мережі Інтернет;

2) створення спеціальних органів контролю, покликаних спостерігати та виявляти порушників встановлених правил користування кіберпростором. Сьогодні таким органом є Департамент кіберполіції Національної поліції України, проте збільшення обсягу контролю потребуватиме розширення такої мережі.

Висновки. Тенденції є явищем, що представляє собою сукупність напрямів розвитку правового регулювання боротьби з кіберзлочинністю в Україні. Дослідження засвідчило, що сьогодні нашою державою ведеться активна діяльність щодо покращення існуючої ситуації з кібербезпекою. В умовах курсу на євроінтеграцію та реальних кіберзагроз, вітчизняному законодавцю варто все ж посилити діяльність у даному напрямку. Як засвідчило дослідження, законодавство все ще перебуває на недостатньому рівні для вирішення поточних проблем, а співробітництво з іншими державами у даному напрямку потребує посилення. Окрім того, стратегічним напрямком є встановлення часткового контролю над кіберпростором. Всесвітня мережа характеризується

відсутністю кордонів та анонімністю, проте окремі напрямки очікуваних загроз можливо передбачити, що і може бути віднесено до об'єктів державного регламентування користування Інтернетом. Більше того, подібні процеси уже розпочато.

Література:

1. Кримінальний кодекс України, 2001 // Відомості Верховної Ради України. 2001. № 25-26. Ст. 131.

2. Про боротьбу з тероризмом: Закон України від 20.03.2003 р. № 638-IV // Відомості Верховної Ради України. 2003. № 25. Ст. 180.

3. Конвенція про кіберзлочинність, 2001 // Офіційний вісник України. 2007. № 65. Ст. 2535.

4. Віденська декларація про злочинність та правосуддя: відповіді на виклики XXI століття. Міжнародний документ від 17.04.2000 року. – URL: http://zakon5.rada.gov.ua/laws/show/995_443

5. Конвенція про взаємодопомогу в кримінальних справах між державами-членами Європейського Союзу, 2000. URL: http://zakon3.rada.gov.ua/laws/show/994_238?test=Up9Mf3o6frtCt4d2ZiIViVNwHI4Uks80msh8Ie6

6. Про рішення Ради національної безпеки і оборони України від 28 квітня 2017 року "Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)": Указ Президента України від 15.05.2017 р. №133/2017. URL: http://www.president.gov.ua/documents/1332017-21850

УДК 342.5:37.014

Дронов В.Ю.,
викладач Міжнародного гуманітарного університету

ПРОЗОРІСТЬ ТА ВІДКРИТІСТЬ ЯК ВИХІДНІ ЗАСАДИ РЕАЛІЗАЦІЇ ОСВІТНЬОЇ ФУНКЦІЇ СУЧАСНОЇ ДЕРЖАВИ: ТЕОРІЯ ТА ЗАКОНОДАВЧЕ РЕГУЛЮВАННЯ

В статті досліджується формування та розміщення державного замовлення на підготовку фахівців, наукових, науково-педагогічних та робітничих кадрів, підвищення