УГОЛОВНОЕ ПРАВО, УГОЛОВНО-ИСПОЛНИТЕЛЬНОЕ ПРАВО

УДК 342.95:004:343. 3/ 7

ЩОДО ПИТАННЯ СТОСОВНО ЗАРУБІЖНОГО ДОСВІДУ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ

В'ячеслав МАРКОВ,
кандидат юридичних наук, старший науковий співробітник,
начальник факультету підготовки фахівців для підрозділів боротьби з кіберзлочинністю та торгівлею людьми
Харківського національного університету внутрішніх справ

SUMMARY

The article is devoted to the foreign experience in combating cyber crime in the leading countries of the currently world. There was analyzed the experience of the police from many countries in the field of combating cybercrime; it was also pointed out that this kind of activity provides through the following ways: the introduction of additional features to the existing police units (or the creation of special units); the interrelations with the various executive and administrative bodies; with community organizations and citizens. The author concluded that the improvement of the law support of the struggle against cybercrime in Ukraine should occur in accordance with its national cultural, historical, socio-economic features.

Key words: information, foreign experience, protection of information, combating cybercrime.

АНОТАЦІЯ

Стаття присвячена питанню зарубіжного досвіду протидії кіберзлочинності провідних країн світу в сучасних умовах. Проаналізовано досвід роботи поліції багатьох країн світу у сфері протидії кіберзлочинності; зазначено, що цей напрям забезпечується такими основними шляхами, як покладення додаткових функцій на чинні підрозділи поліції або створення спеціальних підрозділів, взаємовідносини з різноманітними органами влади й управління, громадськими організаціями, окремими громадянами. Зроблено висновок про те, що вдосконалення правового забезпечення протидії кіберзлочинності в Україні має відбуватись з урахуванням національних культурно-історичних, соціально-економічних особливостей країни.

Ключові слова: інформація, зарубіжний досвід, захист інформації, протидія кіберзлочинності.

Постановка проблеми. Загальна інформатизація є основною ознакою переходу цивілізованого світу до технологічно нового виробництва інформаційних відносин. Невпинно зростають темпи розвитку цифрової економіки, які в кілька разів перевищують показники всіх інших галузей виробництва [1, с. 167]. Водночас серйозне занепокоєння викликає поширення фактів протизаконного збирання й використання інформації, несанкціонованого доступу до інформаційних ресурсів тощо. Варто зазначити, що в період глобалізації швидкий розвиток інформаційних технологій, нових систем комунікацій і комп'ютерних мереж супроводжується зловживанням цими технологіями зі злочинною метою. Становлення інформаційного суспільства в Україні певною мірою стримується низкою проблем нормативно-правового та організаційного вектора [2, с. 5–6; 3, с. 39–41].

Актуальність теми. З огляду на відсутність у вітчизняній юридичній науці (зокрема науці адміністративного права) комплексного дослідження зарубіжного досвіду провідних країн світу у сфері протидії кіберзлочинності, державної діяльності щодо адміністративно-правових механізмів регулювання захисту інформації у сучасних умовах автором опрацьовувались наявні матеріали з указаної проблеми, відображені, зокрема, у працях М.О. Будакова, В.М. Бутузова, М.М. Галамби, Р.А. Калюжного, В.В. Коваленко, Я.Ю. Кондратьєва, Б.А. Кормича, Ю.М. Максименко, А.І. Марущака, Г.В. Новицького та інших.

Під час дослідження було використано наукові доробки таких іноземних дослідників: А. Роберта, К. Осакве, Т. Блентана, Д. Банісара та інших.

Метою статті є дослідження проблеми вивчення та запозичення міжнародного досвіду провідних країн світу у сфері державної діяльності щодо адміністративно-правових механізмів регулювання захисту інформації в сучасних умовах, протидії кіберзлочинності певною мірою для забезпечення стратегічних намірів України щодо європейської та євроатлантичної інтеграції.

Виклад основного матеріалу дослідження. Серед основних сучасних тенденцій розвитку суспільства варто відзначити глобальну інформатизацію практично всіх сфер життєдіяльності людини, включаючи економіку, державне управління, науку, мистецтво.

Потрібно акцентувати увагу на тому, що в умовах глобальної інформатизації змінюється характер формування сучасних правовідносин у сфері розповсюдження інформації; сутність, зміст, роль і місце організаційно-правових основ захисту інформації, у т. ч. з обмеженим доступом до певних видів інформації, зокрема правоохоронної діяльності й забезпечення суспільного порядку [2, с. 5–6].

Треба зазначити, що становлення інформаційного суспільства має безсумнівні як позитивні, так і певні негативні наслідки. З одного боку, пришвидшилася передання інформації значного обсягу, прискорилась її обробка та впровадження. З іншого – серйозне занепокоєння викликає поширення фактів протизаконного збирання та використання інформації, несанкціонованого доступу до інформаційних ресурсів, незаконного копіювання інформації в електронних системах, викрадення інформації з бібліотек, архівів, банків і баз даних, порушення технологій обробки інформації, запуску програм-вірусів,

знищення та модифікації даних в інформаційних системах, перехоплення інформації в технічних каналах її витоку, маніпулювання суспільною й індивідуальною свідомістю тощо.

Перехід суспільства до інформаційного змінив статус інформації. Наразі вона може бути як засобом забезпечення безпеки, так, у свою чергу, і загрозою та небезпекою [4, с. 1], так як містить різноманітні дані щодо як громадян відповідної держави, так і стратегічних державних програм. Використання інформаційних технологій на основі персональних комп'ютерів, інформаційно-обчислювальних мереж і комп'ютеризованих комунікаційних систем забезпечило людству вихід на новий етап свого розвитку – етап інформаційного суспільства. Саме це спричинило появу нового виду злочинності – «комп'ютерної» або кіберзлочинності.

Зазначимо, що одним із можливих підходів до боротьби з кіберзлочинністю в транснаціональному аспекті й розвитку міжнародної співпраці є вироблення і стандартизація відповідної нормативно-правової бази. На міжнародному рівні першим документом у цій сфері стала Конвенція про кіберзлочинність, прийнята Радою Європи 23 листопада 2001 р. [5], і Додатковий протокол до Конвенції від 28 січня 2003 р., направлений на боротьбу з розповсюдженням через комп'ютерні мережі інформації расистського й ксенофобського характеру [6]. Прийняття цих актів ознаменувало закладення правового фундаменту у сфері захисту свободи, безпеки і прав людини в мережі Інтернет не тільки на регіональному рівні, оскільки Конвенція відкрита для підписання для держав, які не є членами Ради Європи [7]. Відповідно до Конвенції «Про кіберзлочинність», держави-учасники (у т. ч. й Україна) повинні здійснити організаційні заходи щодо розробки необхідних умов (зокрема організація контактних пунктів) на національному рівні, приєднатися до мережі щоденного цілодобового доступу (міжнародне позначення «24/7 Network» або «доступ 24 години 7 діб на тиждень»), що спрямована на співпрацю та надання допомоги під час розкриття й розслідуванні кіберзлочинів. Значна увага приділяється визначенню загальних і конкретних принципів міжнародного співробітництва в цій сфері. Конвенцією встановлено такі обов'язкові вимоги для врахування в законодавстві країн, що приєднались:

– надання органам дізнання та слідства повноважень щодо видання обов'язкових до виконання приписів про термінове фіксування й подальше зберігання комп'ютерних даних, які необхідні для розкриття злочину (ч. 1 ст. 16 ст. 17 Конвенції про кіберзлочинність);

– збереження провайдерськими установами даних про трафік інформації на термін 90 днів із можливістю подальшого продовження цього строку (ч. 2 ст. 16 Конвенції про кіберзлочинність);

– установлення для суб'єктів, які зберігають комп'ютерні дані, зобов'язання не розголошувати факт проведення оперативно-розшукових і процесуальних дій протягом періоду, який визначається законодавством держави (ч. 3 ст. 16, ч. 3 ст. 20, ч. 3 ст. 21 Конвенції про кіберзлочинність) [5].

Відмітимо, що укладення міжнародних угод, приєднання до різних програм у сфері боротьби з кіберзлочинністю тільки сприяє боротьбі з такого роду злочинами.

Необхідно акцентувати увагу на тому, що для багатьох країн, зокрема для України, кіберзлочинність є достатньо актуальним явищем, породженим широким упровадженням в економічні процеси сучасних інформаційних і телекомунікаційних технологій. Так, з'являються нові вияви комп'ютерної злочинності, які отримують поширення під час використання нових технологій – Bluetooth, бездротових систем зв'язку WI-FI та WIMAX, піринговых мереж (P2P), спаму тощо. Зокрема, крадіжки грошей із банківських карток, виготовлення та поширення шкідливих програм, пропаганда насильства й расової, релігійної, етнічної ненависті, кібератаки на комп'ютерні мережі державних установ тощо.

Зазначимо, що на сьогодні законодавством України термін «кіберзлочинність» безпосередньо не визначено. Європейська конвенція про кіберзлочинність також не надає конкретизованого визначення, хоча й окреслює коло суспільно-небезпечних діянь, які можуть підпасти під поняття «кіберзлочин» на національному рівні, серед них незаконний доступ до комп'ютерної системи, нелегальне перехоплення даних, втручання в систему, зловживання пристроями, підробка та шахрайство, пов'язані з комп'ютерами; правопорушення, пов'язані з дитячою порнографією; правопорушення, пов'язані з порушенням авторського й суміжних прав.

Відмітимо, що характерними особливостями злочинів у сфері інформаційно-телекомунікаційних технологій є такі:

– необхідність широкого застосування спеціальних знань під час виявлення та фіксації слідів злочину в електронній формі;

– організованість і транснаціональний характер, оскільки для цього явища національні кордони не є перешкодою;

– висока латентність, спричинена небажанням постраждалих інформувати про такі злочини через недовіру до потенційних можливостей правоохоронних органів і небажанням визнати слабкі місця своїх систем безпеки;

– високий рівень технічного забезпечення правопорушників;

– великий ступінь анонімності;

– інформація, що зберігається в комп'ютерних системах, має короткостроковий характер;

– можливість знищення або зміни комп'ютерної інформації;

– виявлення, фіксація й вилучення доказової інформації є складним процесом;

– широке використання комп'ютерної техніки в повсякденному житті;

– відсутність сталості явища кіберзлочинності, оскільки комп'ютерні технології постійно вдосконалюються.

Ураховуючи особливості злочинів у сфері інформаційно-комунікаційних технологій, можемо констатувати, що велике значення для результативності їх оперативного документування має взаємодія різних підрозділів поліції на всіх рівнях, у тому числі із представниками правоохоронних органів інших країн [8, с. 518–519]. Для покращення співпраці Конвенцією передбачено створення сторонами на національному рівні органу для здійснення контактів цілодобово з метою надання негайної допомоги для розслідування або переслідування стосовно кримінальних правопорушень, пов'язаних із комп'ютерними системами й даними, або з метою збирання доказів у електронній формі, що стосуються кримінального правопорушення. Така допомога включає сприяння або, якщо це дозволяється її внутрішньодержавним законодавством і практикою, пряме а) надання технічних порад; б) збереження даних відповідно до ст. ст. 29 («Термінове збереження комп'ютерних даних, які зберігаються») і 30 («Термінове розкриття збережених даних про рух інформації»); с) збирання доказів, надання юридичної інформації й установлення місцезнаходження підозрюваних (ст. 35) [5].

Питання боротьби з кіберзлочинністю знаходиться й у центрі уваги органів та інституцій Організації Об'єднаних Націй, зокрема Генеральної Асамблеї (док. A/RES 63/195),

Економічної і Соціальної Ради (рез. 2009/22), Комісії із запобігання злочинності і кримінального правосуддя (док. E/ CN.15/2009/15), конгресів ООН із запобігання злочинності і кримінального правосуддя, потребує розробки шляхів і засобів його вирішення [7, с. 195].

У низці міждержавних нормативно-правових актів [6; 9; 10] визнано, що кіберзлочинність сьогодні становить загрозу не тільки національній безпеці окремої держави, а загрожує людству загалом. Саме тому зазначеній проблемі приділяється значна увага в багатьох державах.

Проаналізувавши досвід роботи поліції багатьох країн світу у сфері протидії кіберзлочинності, варто відмітити, що цей напрям забезпечується такими основними шляхами, як покладення додаткових функцій на чинні підрозділи поліції або створення спеціальних підрозділів.

Створення спеціальних підрозділів поліції у сфері протидії кіберзлочинності практикується в багатьох країнах світу, зокрема в Австралії, Бельгії, Білорусі, Великобританії, Данії, Естонії, Індії, Канаді, Малайзії, Нідерландах, Німеччині, Норвегії, Польщі, США, Швейцарії, Швеції та ін.

Серед основних функцій цих підрозділів виділяють такі:

– моніторинг кіберпростору з метою виявлення кіберзлочинів, вірусів або шкідливого програмного забезпечення;

– здійснення оперативно-розшукових і розвідувальних заходів з метою фіксування протиправної діяльності кіберзлочинців;

– розслідування кіберзлочинів і надання методичної та практичної допомоги іншим галузевим службам і правоохоронним органам у межах своєї компетенції;

– накопичення, узагальнення й аналіз інформації про кіберзлочинність;

– профілактика цих злочинів за допомогою громадськості й засобів масової інформації;

– навчання працівників поліції.

Деякі зі спеціальних підрозділів поліції у сфері протидії кіберзлочинності (їх ще називають спеціальними підрозділами щодо протидії злочинам із використанням інформаційних технологій) виконують ще й додаткові функції:

– розкриття кіберзлочинів;

– профілактика та нагляд за телекомунікаційними послугами;

– експертне дослідження доказів на електронних носіях;

– створення відповідної бази даних щодо злочинів у сфері кіберпростору й постійне її оновлення;

– надання послуг банкам у захисті персональної інформації клієнтів тощо.

Наприклад, в Індії підрозділи щодо розслідування кіберзлочинів для розкриття цих злочинів можуть залучати професійних хакерів у ході реалізації своїх функцій.

Варто зазначити, що під час розслідування кіберзлочинів значна увага приділяється допомозі постраждалому у відновленні пошкодженої або втраченої інформації, уживаються всі необхідні заходи щодо збереження доказів по справі [11, с. 193].

Крім того, останніми роками в різних регіонах світу було застосовано низку підходів щодо боротьби з кіберзлочинністю. Так, у 2002 р. Співдружністю націй був розроблений типовий закон про комп'ютерні й пов'язані з комп'ютерами злочини, який має на меті вдосконалення законодавчих норм держав-членів Співдружності в галузі боротьби з кіберзлочинністю і поглиблення міжнародної співпраці. За відсутності цього договору для розвитку транскордонної співпраці в цій галузі членам Співтовариства націй необхідно було б укласти між собою низку двосторонніх договорів, які б набагато ускладнили процедуру співпраці. Типовий закон містить, зокрема, положення про міжнародну співпрацю. Оскільки він має регіональний характер, положення закону стосуються тільки держав-членів Співдружності (п. 20).

Європейським Союзом докладено зусиль щодо узгодження законодавства стосовно кіберзлочинності, яке діє на території держав-членів організації. Для цього були прийняті, зокрема, директива № 2000/31/ЄС Європейського парламенту і Ради про деякі правові аспекти послуг інформаційного співтовариства, такі як електронна торгівля на внутрішньому ринку; рамочне рішення Ради Європейського Союзу 2000/41/ЈНА про боротьбу з шахрайством і фальсифікацією безготівкових платіжних засобів; рамочне рішення Ради Європейського Союзу 204/68/ЈНА про боротьбу з сексуальною експлуатацією тощо (п. п. 20–21) [2].

Необхідно зазначити, що на шляху вдосконалення адміністративно-правового забезпечення протидії кіберзлочинності в Україні ми маємо вивчати позитивний досвід діяльності правоохоронних органів інших країн у цьому напрямі.

Зокрема, одним із важливих напрямів діяльності поліції Канади є боротьба з комп'ютерними і телекомунікаційними злочинами, розслідуванням яких займається підрозділ Королівської канадської кінної поліції (далі – КККП) (федеральної поліції) із боротьби з комп'ютерною злочинністю, опираючись на дані канадського поліцейського інформаційного центру та співпрацюючи з іншими країнами.

Діяльність підрозділу направлена на розслідування й розкриття злочинів, пов'язаних із комп'ютерами і телекомунікаціями. Секція захисту інформаційних технологій забезпечує захист федеральних державних комп'ютерних центрів, приватного сектора; надає консультації, готує персонал для роботи зі здійснення комп'ютерного захисту. Співробітники підрозділу допомагають поліцейським у проведенні розслідувань злочинів, пов'язаних із комп'ютерними системами.

Ураховуючи ту обставину, що інформаційна система дає змогу передавати повідомлення від одного терміналу до іншого майже негайно, у Канаді діє близько 2 500 точок доступу, до яких уходять близько 1 285 федеральних і провінційних поліцейських відділень. 1 180 підрозділів спеціалізованих відділів КККП підключені до ліній системи [13].

Безперечно, цей напрям діяльності поліції є важливим, оскільки економічні втрати досягли широких масштабів, деякі злочинці діють на міжнародному рівні, організованою групою.

Варто визнати, що канадське законодавство щодо визначення комп'ютерної злочинності потребує вдосконалення. Так як завдання, які стоять перед підрозділами поліції щодо боротьби з комп'ютерною злочинністю, мають міжнародний характер і не специфічні для Канади, вони активно співпрацюють з іншими країнами, Інтерполом з метою вдосконалення законодавства в цьому напрямі.

Розкриття комп'ютерних злочинів являє собою складне завдання насамперед через фактор часу, оскільки передання даних може бути виконане майже миттєво, часто буває даремно шукати які-небудь докази, що підтверджують порушення міжнародного законодавства. За даними КККП, на сьогодні безліч комп'ютерних злочинів здійснюється дітьми, котрі не досягли дванадцятирічного віку. Згідно з кримінальним кодексом Канади, для встановлення кримінальної відповідальності необхідно довести несанкціоноване використання комп'ютерної системи та

намір особи заподіяти своїми діями шкоду. Такий підхід потребує чіткого встановлення параметрів доступу до комп'ютерної техніки з метою запобігання порушенням. Необхідно враховувати дані щодо осіб, параметри доступу з урахуванням обмежень, можливість службовцями «експериментувати» з програмами. Кваліфіковану консультацію щодо можливої неправомірної поведінки в цьому напрямі може надати міністерство юстиції чи відповідний підрозділ КККП [14].

Варто зазначити, що методика розслідування випадків несанкціонованого дистанційного доступу до комп'ютерних мереж технічно складна, ними займаються спеціалізовані поліцейські підрозділи. З огляду на небезпеку комп'ютерної злочинності, тенденцію її розвитку, впливу на світове співтовариство в межах ООН регулярно проводяться симпозіуми з профілактики та припинення комп'ютерної злочинності. Як один із напрямів фахівці відзначають програмні методи захисту інформації в комп'ютерних системах колективного користування шляхом удосконалення системи автоматичного контролю. На запобігання й зменшення злочинів щодо незаконного використання телекомунікаційних систем на міжпровінційному, державному й міжнародному рівнях спрямовано дії й управління із боротьби з економічними злочинами. Допомагає поліцейським підрозділам Інформаційний центр.

Поліцейська діяльність щодо запобігання та розкриття діянь, пов'язаних із кіберзлочинністю, спрямована й на різнобічний розвиток відносин із якомога більшим суспільним колом через засоби масової інформації, консультативні зустрічі з представниками громадськості, взаємовідносини з різноманітними органами влади та управління, громадськими організаціями, окремими громадянами.

Отже, поліція є важливим партнером у співтоваристві відомств, що займаються боротьбою зі злочинністю, у тому числі кіберзлочинністю, забезпеченням дотримання прав людини, забезпеченням захисту федеральних державних комп'ютерних центрів, приватного сектора [14]. Оскільки ефективність діяльності поліції щодо розкриття кіберзлочинів стримується низкою чинників технікотехнологічного, фінансово-економічного, нормативно-правового, адміністративно-організаційного характеру, потрібні скоординовані дії правоохоронців різних держав, у т. ч. в межах Інтерполу.

Погоджуємось із думкою В.В. Коряк, В.Р. Сливенко щодо визначення взаємодії різних підрозділів поліції як узгодженої в часі, методах і засобах діяльності підрозділів (або працівників), не пов'язаних між собою прямим підпорядкуванням, для реалізації загальних цілей і вирішення завдань.

Ураховуючи особливості злочинів у сфері інформаційно-комунікаційних технологій, можемо зазначити, що велике значення для результативності їх оперативного документування має взаємодія оперативного підрозділу поліції на всіх рівнях:

1) внутрішньовідомчому – з іншими оперативними підрозділами поліції, науково-дослідними, експертно-криміналістичними центрами та слідчими підрозділами;

2) внутрішньодержавному – з іншими правоохоронними органами України, трудовими колективами, громадськими організаціями й населенням;

3) міжнародному – із правоохоронними органами інших країн.

Так, основними видами співробітництва поліції України з правоохоронними органами іноземних держав є такі:

– обмін відомостями оперативно-розшукового характеру;

– надання правової допомоги в кримінальних справах;

– виїзд членів слідчо-оперативних груп за кордон для присутності під час виконання слідчих дій і оперативно-розшукових заходів;

– виїзд для обміну інформацією оперативно-розшукового характеру;

– виїзд за кордон для присутності під час проведення слідчих та інших дій у межах надання правової допомоги;

– виїзд для конвоювання розшуканих і затриманих за кордоном осіб;

– виїзд працівників прикордонних правоохоронних органів у сусідні регіони суміжних держав в оперативно-розшукових справах;

– прибуття працівників правоохоронних органів іноземних держав в Україну для проведення слідчих і оперативно-розшукових дій [8, с. 523–535].

Підсумовуючи вищевикладене, можемо дійти таких висновків:

– поширеність і суспільна небезпечність кіберзлочинів останніми роками набула загрозливих масштабів, що диктує необхідність формування адекватної відповіді з боку держави на інноваційні безпекові виклики;

– сучасний етап становлення громадянського суспільства визначається входженням України до глобального інформаційного простору. Саме тому ми маємо використовувати досвід тих країн, що вже мають досить серйозні напрацювання у сфері забезпечення інформаційної безпеки [15, с. 225], оскільки інформаційна безпека є невід'ємним напрямом розбудови інформаційного суспільства, розвиток якого повинен іти не тільки через нарощування технологічних можливостей здійснення інформаційного обміну, а й через глибоке усвідомлення всіма суб'єктами інформаційних відносин – власниками інформації та її користувачами, виробниками інформаційних технологій і засобів, постачальниками послуг, державою – необхідності здійснення всіх заходів щодо захисту інформаційних ресурсів і забезпечення безпеки держави;

– необхідним напрямом діяльності правоохоронних органів є вдосконалення заходів взаємодії з підприємствами, установами, організаціями, незалежно від форм власності, діяльністю яких є розробка комп'ютерної техніки та програмного забезпечення, з метою виявлення осіб, схильних до скоєння протиправних діянь, отримання відповідних знань у сфері розвитку комп'ютерних технологій, удосконалення програмного забезпечення власних систем через перейняття відповідного досвіду, не забуваючи про інформаційну безпеку держави, окремих громадян;

– вивчення зарубіжного досвіду протидії кіберзлочинності в окремо взятих країнах і надбань міжнародної спільноти, удосконалення механізму міжнародної взаємодії є важливим, адже більшість кіберзлочинів мають транснаціональний характер;

– кіберзлочинність сьогодні становить загрозу не тільки національній безпеці окремої держави, а загрожує людству загалом, саме тому зазначеній проблемі приділяється значна увага в багатьох державах;

– виходячи з аналізу організації діяльності роботи поліції багатьох країн світу у сфері протидії кіберзлочинності, можемо відмітити, що цей напрям забезпечується такими основними шляхами, як покладення додаткових функцій на чинні підрозділи поліції або створення спеціальних підрозділів;

– необхідно внести зміни та доповнення до чинного законодавства України в частині захисту національного інформаційного простору від протиправного контенту, надання додаткових повноважень правоохоронним органам з оперативного припинення окремих видів злочинів тощо;

– удосконалення адміністративно-правового забезпечення протидії кіберзлочинності в Україні має відбуватись з урахуванням національних культурно-історичних,

соціально-економічних особливостей країни на підставі детального наукового аналізу міжнародного законодавства й досвіду інших країн у сфері боротьби з кіберзлочинністю з метою оптимального входження в європейське та світове правове поле за взаємодії між різними правоохоронними органами на рівні держави та міжнародному рівні;

– з огляду на сучасну ситуацію в державі та світі Україна має постійно вдосконалювати методи боротьби з кіберзлочинністю, удосконалюючи чинне законодавство, у т. ч. в галузі адміністративного права, ураховуючи надбання окремих зарубіжних держав, міжнародної спільноти загалом, спрямовані на забезпечення кібербезпеки країни.

Вивчення й запозичення міжнародного досвіду провідних країн світу у сфері адміністративно-правових механізмів регулювання захисту інформації в сучасних умовах, протидії кіберзлочинності є важливим певною мірою для забезпечення стратегічних намірів України щодо європейської та євроатлантичної інтеграції. Саме тому до найбільш перспективних напрямів подальших досліджень зарубіжного досвіду щодо боротьби з кіберзлочинністю можемо зарахувати питання адміністративно-правової регламентації діяльності спеціальних підрозділів поліції щодо боротьби з кіберзлочинністю окремих держав.

Список використаної літератури:

1. Бойченко О.В. Інформаційна безпека в органах внутрішніх справ України (організаційно-правові засади) : [монографія] / О.В. Бойченко ; Кримський юридичний інститут ОДУВС. – Сімферополь : ВАТ «Сімферопольська міська друкарня» (СГТ), 2009. – 288 с.

2. Сідак В.С. Забезпечення інформаційної безпеки в країнах НАТО та ЄС : [навч. посіб.] / В.С. Сідак, В.Ю. Артемов. – К. : КНТ, 2007. – 160 с.

3. Бойченко О.В. Угрозы информационных ресурсов государственного самоуправления / О.А. Бойченко // Материалы Международной научно-практической конференции «Проблемы и особенности влияния международной информации на экономические и общественно-политические процессы». – Симферополь : ИСВА МСУ, 2007. – С. 39–41.

4. Максименко Ю.Є. Теоретико-правові засади забезпечення інформаційної безпеки України : автореф. дис. … канд. юрид. наук : спец. 12.00.01 «Теорія та історія держави і права, історія політичних і правових учень» / Ю.Є. Максименко. – К., 2007. – 20 с.

5. Конвенція про кіберзлочинність [Електронний ресурс]. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/994_575.

6. Дополнительный протокол к Конвенции о киберпреступности относительно криминализации деяний расистского и ксенофобского характера, совершаемых при помощи информационных систем [Электронный ресурс]. – Режим доступа : http://zakon4.rada.gov.ua/laws/show/994_687.

7. Сироїд Т.Л. Правова основа міжнародної співпраці у сфері боротьби з кіберзлочинністю / Т.Л. Сироїд // Актуальні питання діяльності правоохоронних органів у сфері протидії кіберзлочинності : матеріали Міжнар. наук.– практ. конф., м. Харків, 12 листопада 2014 р. / МВС України, Харків. нац. ун-т внутр. справ. – Х. : Права людини, 2014. – 200 с.

8. Протидія кіберзлочинності в Україні: правові та організаційні засади : [навч. посіб.] / [О.Є. Користін, В.М. Бутузов, В.В. Василевич та ін.]. – К. : Видавничий дім «Скіф», 2012. – 728 с.

9. Конвенція ООН проти транснаціональної організованої злочинності, прийнята резолюцією 55/25 Генеральної Асамблеї від 15 листопада 2000 р., ратифікована із застереженнями і заявами Законом України від 04 лютого 2004 р. № 1433 [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/995_789.

10. Конвенция об информационном и правовом сотрудничестве, касающемся «Информационных общественных услуг» (ETS N 180) от 04 октября 2001 г. [Электронный ресурс]. – Режим доступа : http://zakon4.rada.gov.ua/laws/show/994_559.

11. Сень Р.Ю. Досвід іноземних країн у сфері розслідування кіберзлочинів / Р.Ю. Сень // Актуальні питання діяльності правоохоронних органів у сфері протидії кіберзлочинності : матеріали Міжнар. наук.– практ. конф., м. Харків, 12 листопада 2014 р. / МВС України, Харків. нац. ун-т внутр. справ. – Х. : Права людини, 2014. – 200 с.

12. Двенадцатый Конгресс Организации Объединенных Наций по предупреждению преступности и уголовному правосудию (Сальвадор, Бразилия, 12–19 апр. 2010 г.) A/CJNF.213/1 [Электронный ресурс]. – Режим доступа : http://www.un.org/ru/conf/crimecongress2010/.

13. RCMP Fact sheets 1995. // Minister of Supply and Services Canada. – 1995. – P. 25.

14. Варунц Л.Д. Досвід організації діяльності Королівської канадської кінної поліції та шляхи його використання в Україні : дис. … канд. юрид наук : 12.00.07 «Адміністративне право і процес; фінансове право; інформаційне право» / Л.Д. Варунц. – Дніпропетровськ, 2012. – 203 с.

15. Ліпкан В.А. Інформаційна безпека України в умовах євроінтеграції : [навч. посіб.] / В.А. Ліпкан, Ю.Є Максименко, В.М. Желіховський. – К. : КНТ, 2006. – 280 с.