К., 1998. – Т. 1. – С. 639.

6. Про затвердження Інструкції щодо порядку обліку злочинів, вчинених у громадських місцях, на вулицях в стані алкогольного сп'яніння: Наказ МВС України від 21 червня 1996 р. № 438.

7. Про затвердження Інструкції з обліку злочинів, вчинених у громадських місцях: Наказ МВС № 1394 від 19.12.2003 р.

8. Про заходи про попередження та зменшення вживання тютюнових виробів і їх шкідливого впливу на здоров'я населення: Закон України // ВВР. – 2005. – № 52. – Ст. 565.

9. Конституція України. – К., 1996.

10. Міжнародна поліцейська енциклопедія: У 10 т. / Відп. ред. Ю.І. Римаренко, Я.Ю. Кондратьєв, В.Я. Таційй, Ю.С. Шемшученко. – К., 2004. – Т. 1.

11. *Курінний Є.В.* Відносини громадської безпеки: окремі проблеми адміністративно-правового забезпечення // Науковий вісник Юридичної академії Міністерства внутрішніх справ. – 2005. – № 2. – С. 286-290.

12. Про Національну гвардію Міністерства внутрішніх справ України: Проект Закону України. – К., 2006.

13. *Гусаров С.М.* Адміністративно-правові засади державного управління безпекою дорожнього руху в Україні: Автореф. дис. ... канд. юрид. наук. – Х., 2001.

14. *Долгополова М.М.* Деякі аспекти застосування судами України законодавства про адміністративні правопорушення, пов'язані із забезпеченням безпеки дорожнього руху // Запорізькі правові читання: Тези доповідей щорічної Міжнародної наук.-практ. конф. / За заг. ред. С.М. Тимченка і Т.О. Коломоєць. – Запоріжжя, 2006.

15. *Лукьянов В.В.* Безопасность дорожного движения. – М., 1983.

16. *Ярмакі Х.П.* Адміністративно-наглядова діяльність міліції в Україні. – Одеса, 2006.

17. *Жульов В.И.* Водитель и безопасность дорожного движения. – М., 1984.

18. *Лукьянов В.И.* Обеспечение безопасности дорожного движения. – М., 1979.

19. *Долгополова М.М.* Управління загальнодержавною системою забезпечення безпеки дорожнього руху: Автореф. дис. ... канд.. юрид. наук. – Х., 2003.

20. *Бельский К.С.* Полицейское право: Лекционный курс / Под ред. канд. юрид. наук А.В. Куракина. – М., 2004.

21. *Новиков В.В.* Адміністративно-правові основи профілактики порушень правил дорожнього руху: Автореф. дис. ... канд. юрид. наук. – К., 1997.

22. *Развадовський В.Й.* Адміністративно-правове регулювання правовідносин у транспортній сфері України: Монографія. – Х., 2004.

Надійшла до редакції 28.11.2011

Є.В. Зозуля
кандидат історичних наук, доцент
(Донецький юридичний інститут МВС України)

УДК 343.96 : 341

МІЖНАРОДНЕ СПІВРОБІТНИЦТВО МВС УКРАЇНИ ЩОДО ПРОТИДІЇ ЗЛОЧИННОСТІ У СФЕРІ ВИСОКИХ ТЕХНОЛОГІЙ

Розглянуто питання діяльності МВС України щодо нормативно-правового та організаційного забезпечення міжнародного співробітництва щодо протидії злочинності у сфері високих технологій. Проаналізовано формування нормативно-правової бази, особливості організаційно-правового забезпечення та форми мі-

жнародного співробітництва спецпідрозділів МВС у боротьбі з кіберзлочинністю.

Ключові слова: *злочини у сфері високих технологій, кіберзлочинність, міжнародне співробітництво, правоохоронні органи.*

В статье рассмотрены вопросы деятельности МВД Украины относительно нормативно-правового и организационного обеспечения международного сотрудничества в деле противодействия преступности в сфере высоких технологий. Анализируются формирование нормативно-правовой базы, особенности организационно-правового обеспечения и формы международного сотрудничества спецподразделений МВД в борьбе с киберпреступностью.

Ключевые слова: *преступления в сфере высоких технологий, киберпреступность, международное сотрудничество, правоохранительные органы.*

Questions of activity the Ministry of Internal Affairs of Ukraine concerning legal and organizational support for international cooperation in combat against crime in the sphere of high technologies are considered in the article. The formation of the regulatory framework, peculiarities of organizational and legal support state policy peculiarities in the organizational and legal support and forms of MIA international cooperation in the fight against cybercrime are analyzed.

Keywords: *crime in the sphere of high technologies, cyber crime, international cooperation, law enforcement agencies.*

Постановка проблеми. Останнім часом в усьому світі спостерігається значне зростання чисельності злочинів, скоєних у сфері високих технологій, а надто інформаційних систем. Цей вид злочинів становить усе більшу загрозу як окремим установам, організаціям і фізичним особам, так і економічним системам кожної держави. Широке ж упровадження в економічні процеси сучасних інформаційно-телекомунікаційних технологій спричиняє появу і поширення нових видів правопорушень.

В Україні, як і в інших державах світу, невпинно розвиваються якісно нові галузі економіки, що базуються передусім на використанні сучасних інформаційних технологій, локальних та глобальних комп'ютерних мереж, зокрема мережі Інтернет. Темпи розвитку української складової «Світової павутини» сьогодні випереджають як європейські, так і загальносвітові показники. За даними міжнародних організацій за 2010 р., Україна входить до першої десятки країн Європи за кількістю Інтернет-користувачів – доступ до всесвітньої мережі мають до 15 млн. українців [1].

Водночас наслідком розбудови інформаційного суспільства є те, що злочинні групи та співтовариства все частіше використовують у своїй діяльності новітні досягнення науки й техніки. Зокрема, комп'ютерні технології застосовують для створення систем конспіративного зв'язку, проникнення в бази даних приватних організацій та державних відомств; комп'ютери й мережні технології стали інструментами вчинення

злочинів, а інформаційні ресурси – об'єктами злочинних зазіхань.

Аналіз публікацій, в яких започатковано розв'язання даної проблеми. Проблеми запобігання та протидії злочинам у сфері високих технологій розглянуто в роботах Н.М. Ахтирської, П.Д. Біленчука, В.М. Бутузова, В.Д. Гавловського, В.Д. Гвоздецького, В.О. Голубєва, М.В. Гуцалюка, В.Є. Козлова, В.В. Крилова, В.Г. Лукашевича, Г.А. Матусовського, В.А. Мінаєва, Р.А. Калюжного, М.В. Салтевського, О.П. Снігерьова, В.С. Цимбалюка, О.М. Юрченка та ін.

Аналізуючи стан вивчення цієї проблеми в сучасній історико-правовій науці, необхідно зазначити, що рівень науково-теоретичної розробленості всіх аспектів цієї проблеми та потреб практики є недостатнім. Відсутність належної теоретичної бази не сприяє ефективній боротьбі з такого роду посяганнями. Актуальність розглянутих у статті питань зумовлена потребами правоохоронної практики в науково обґрунтованих рекомендаціях щодо протидії транснаціональній комп'ютерній злочинності.

Отже, **метою** статті слід вважати дослідження історії розвитку цього напрямку діяльності органів внутрішніх справ, аналіз досвіду й напрямів міжнародного співробітництва МВС щодо протидії злочинності у сфері високих технологій.

Виклад основного матеріалу дослідження. Розпочинаючи безпосереднє висвітлення проблеми, зазначимо, що розвиток та впровадження комп'ютерних технологій у всіх сферах суспільного життя потребує розв'язання питань забезпечення безпеки використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, у числі іншого й кримінально-правовими засобами. У багатьох країнах, у тому числі в Україні, ці посягання одержали умовну назву «комп'ютерні злочини» [2]. Нині вчені пропонують також інші назви означеної категорії злочинів – найчастіше вживаними є терміни «кіберзлочинність» чи «кіберзлочини», що вповні узгоджується з нормами міжнародних актів.

Комп'ютерна злочинність – це сукупність комп'ютерних злочинів, де комп'ютерна інформація становить предмет злочинних посягань. Ці діяння чинять замах на безпеку сфери комп'ютерної інформації, постаючи одним із найбільш небезпечних і шкідливих явищ сучасного світу [3]. Зокрема, якщо, згідно із дослідженням міжнародної компанії McAfee (МакАфі), у 2004 р. прибутки від кіберзлочинності сягали 104 млрд. доларів США, то відповідно до бюлетеня, опублікованого ФБР у 2009 р., вони перевищили 1 трильйон доларів, що в десятки разів випереджає за прибутковістю торгівлю зброєю і наркобізнес [4]. Тому боротьба з комп'ютерною злочинністю є одним із найважливіших завдань сучасності.

Зазначимо, що ефективна боротьба проти транснаціональної комп'ютерної злочинності та кібертероризму вимагає тісного, швидкого, ефективного й функціонального міжнародного співробітництва усіх державних структур (і щонайперше правоохоронних органів) у

розслідуванні такого роду злочинів.

Перші значущі кроки на шляху налагодження міжнародного співробітництва у протидії кіберзлочинності Україна зробила на початку XXI ст., коли 23 листопада 2001 р. в Будапешті наша держава разом із 30-ма іншими державами підписала Європейську конвенцію «Про кіберзлочинність». Представники країн, які підписали зазначену конвенцію, усвідомлюючи глибокі зміни, викликані переходом на цифрові технології та глобалізацією комп'ютерних мереж, стурбовані ризиком того, що комп'ютерні мережі й електронна інформація можуть бути використані для вчинення злочинів, вважаючи, що ефективна боротьба проти кіберзлочинності вимагає тісного, швидкого та ефективного, функціонального міжнародного співробітництва у розслідуванні таких злочинів, погодилися з необхідністю вжиття конкретних заходів у кожній країні [5].

Означеною конвенцією передбачається надання повноважень, достатніх для ефективної боротьби зі злочинами у сфері інформаційно-телекомунікаційних технологій як на внутрішньому, так і міжнародному рівнях. Згідно з цим документом, сторони співпрацюють шляхом застосування відповідних міжнародних угод із кримінальних питань, укладених на основі єдиного або взаємного законодавства, а також внутрішнього законодавства з метою розслідування правопорушень, пов'язаних із комп'ютерними системами та даними і збиранням доказів у електронній формі.

Наступним важливим кроком України на шляху до налагодження міждержавної співпраці у розглядуваній сфері є ратифікація 7 вересня 2005 р. зазначеної Конвенції із Додатковим протоколом до неї від 28 січня 2003 р., якою передбачене надання повноважень, достатніх для ефективної боротьби зі злочинами у сфері інформаційно-телекомунікаційних технологій як на внутрішньодержавному, так і міжнародному рівнях; укладення домовленостей щодо дієвого міжнародного співробітництва. У зв'язку з цим одним із нагальних завдань органів державної влади і управління нашої держави варто вважати приведення чинних механізмів міжнародної взаємодії у відповідність до положень вищезгаданої Конвенції.

Принагідно зазначимо, що в Україні створена і діє досить розгалужена система забезпечення безпеки інформації, її захисту. Наявна певна законодавча база, яка складається із Законів України «Про інформацію», «Про захист інформації в автоматизованих інформаційних системах», «Про державну таємницю» тощо. Є чинними низка указів Президента та постанов Кабінету Міністрів України, якими регульовано конкретні напрями діяльності в галузі захисту інформації.

Одним із останніх кроків на цьому шляху стало ухвалення Президентом України 21 вересня 2010 р. закону «Про внесення змін до Закону України «Про ратифікацію Конвенції кіберзлочинності». За цим законом Міністерство внутрішніх справ України стає єдиним органом, який має повноваження щодо створення цілодобової контакт-

ної мережі для надання невідкладної допомоги в розслідуванні справ, пов'язаних із кіберзлочинністю, а також у виявленні осіб, звинувачуваних у цьому, та зборі доказів для цих справ [6].

Суттєвим внеском у справу розвитку міжнародної співпраці є діяльність міжнародних правоохоронних структур. До прикладу, Генеральний Секретаріат Інтерполу ще 1994 р. задля того, щоб інформація з інших держав мобільно і в доступній формі (мова спілкування, специфічні терміни, коди злочинів тощо) надходила до національних спецпідрозділів, а також із метою оперативного обміну такими даними між країнами рекомендував державам-членам цієї організації створити Національний центральний консультативний пункт із проблем комп'ютерної злочинності. В Україні такий підрозділ з'явився 1996 р. на базі НЦБ Інтерполу.

Аналіз практики викриття та розслідування кримінальних справ у сфері високих технологій свідчить, що найбільш поширеними видами злочинів, пов'язаних із використанням комп'ютерних технологій на території сучасної України, є: злочини у сфері комп'ютерних та Інтернет-технологій – 26 %, злочини у сфері функціонування електронних платежів чи платіжних карток – 16 %, злочини у сфері телекомунікацій – 11 %, злочини у сфері використання комп'ютерних технологій при скоєнні традиційних злочинів – 47 %. До того ж самостійним видом злочинного промислу стало викрадення ідентифікаційних даних інших осіб, використовуючи які, правопорушники набувають доступ до чужих банківських рахунків, безоплатно отримуючи послуги Інтернет-провайдерів та операторів зв'язку. Такі злочини характеризуються високим рівнем технічного забезпечення, латентністю, організованістю, наявністю міжрегіональних та міжнародних зв'язків [7].

У сучасних умовах комп'ютерна злочинність має здебільшого організований і міжнародний характер, базується на стрімкому розвитку і використанні телекомунікаційних засобів повідомлень. Близько 62 % комп'ютерних злочинів вчинюються в складі організованих груп, часто на території декількох країн. Комп'ютерна злочинність також характеризується невпинним нарощуванням і вдосконаленням способів учинення злочинів, кожен із них має безліч способів реалізації [3, с. 49-50].

Безперечно, що розкрити такого роду злочини і викрити осіб, котрі їх скоїли, без допомоги правоохоронних органів держав-партнерів практично неможливо. З метою забезпечення ефективної протидії злочинності у сфері високих технологій МВС України впродовж усього періоду незалежного розвитку нашої держави повсякчас уживало організаційних і практичних заходів щодо забезпечення ефективної протидії цьому сучасному виду транснаціональної злочинності.

Основні зусилля були спрямовані передусім на законодавче забезпечення боротьби з комп'ютерними злочинами і створення відповідної нормативно-правової бази; профілактику, супроводження розслідування і розкриття резонансних правопорушень у сфері

комп'ютерних технологій; напрацювання методик документування і розкриття злочинів означеної категорії, проведення семінарів і тренінгів для працівників спецпідрозділів; налагодження ефективної взаємодії з міжбанківськими установами, телекомунікаційними компаніями, зацікавленими центральними державними і правоохоронними органами інших країн із метою документування злочинних груп, що мають міжнародні зв'язки.

Необхідно зазначити, що перші спроби на шляху протидії цьому виду злочинності були започатковані МВС ще наприкінці 1990-х рр. У цей історичний період, коли змінювалися стереотипи та методи боротьби зі злочинністю, зародилася ідея створення підрозділу боротьби з кіберзлочинністю. Зазначений підрозділ було створено в структурі головного управління боротьби з економічною злочинністю МВС України. Його діяльність була орієнтована за двома основними напрямками – захист інтелектуальної власності та боротьба з кіберзлочинністю.

Основною причиною зосередження зусиль у боротьбі з таким новим видом злочинності в означеному напрямку стало те, що в другій половині 1990-х рр. Україну критикували з приводу значної кількості контрафактної продукції на її території. Саме тому робота цього управління здебільшого була зосереджена на захисті прав інтелектуальної власності та боротьбі з незаконним поширенням контрафактної продукції.

Практика діяльності новоствореного підрозділу мала результатом усвідомлення того, що необхідно приділяти більше часу, засобів та уваги справі боротьби з кіберзлочинністю. Тому в липні 2009 р. у структурі Департаменту боротьби зі злочинами, пов'язаними з торгівлею людьми, було створено окремий відділ боротьби з кіберзлочинністю. Обов'язками підрозділу є формування та реалізація державної політики в розглядуваній сфері правоохоронної діяльності, виробленя методичних рекомендацій щодо протидії злочинам такої категорії, організація міжнародного співробітництва у справах про комп'ютерні правопорушення, розроблення та внесення відповідних змін до чинного законодавства.

Також до переліку завдань цього відділу належить виявлення та документування організованих груп транснаціонального й регіонального характеру, учасники яких спеціалізуються на вчиненні злочинів із використанням високих технологій і телекомунікаційних систем. У перспективних планах – створення в системі МВС України самостійного підрозділу боротьби зі кіберзлочинністю.

Аналіз тенденцій і динаміки комп'ютерної злочинності в Україні дозволяє дійти висновку, що найбільш ураженими цим явищем слід вважати регіони з розвинутою інформаційною інфраструктурою, де населення широко застосовує телекомунікаційні технології (Автономна Республіка Крим, Донецьк, Дніпропетровськ, Одеса, Львів, Харків). Лідером у цій сфері є місто Київ, де перебуває майже 60 % усієї української Інтернет-аудиторії [4].

Характерною рисою злочинів, учинених за допомогою

комп'ютерних систем і телекомунікаційних мереж, є їх транскордонність, тому в основі розкриття та документування таких протиправних посягань, як нами вже зазначено вище, лежить ефективне співробітництво з правоохоронними органами інших держав і міжнародними організаціями, які спеціалізуються на протидії кіберзлочинності.

У сучасних реаліях ці завдання покладені на Департамент боротьби з кіберзлочинністю і торгівлею людьми, створений у липні 2010 р. Новостворений підрозділ зосередив основні зусилля на боротьбі з комп'ютерними злочинами проти конституційних прав і свобод людини й громадянина (комп'ютерне піратство, різноманітні способи порушення таємниці електронних повідомлень і неправомірний доступ до автоматизованих систем підрахунків голосів тощо); на боротьбі з комп'ютерними злочинами у сфері економіки (різні форми розкрадання шляхом неправомірного доступу до автоматизованих систем забезпечення діяльності, передусім, фінансових установ, розкрадання коштів у міжнародній міжбанківській системі електронних платежів, дії, спрямовані на виготовлення кредитних або розрахункових карток, тощо); з комп'ютерними злочинами проти державної безпеки (наприклад, такі суспільно небезпечні діяння, як неправомірний доступ до державної таємниці на електронному носії, незаконний збір різного роду інформації тощо).

До актуальних питань сьогодення належить і поширення шахрайських дій, пов'язаних із рекламою так званих програм-шпигунів, «телефонних сканерів», перехоплювачів коротких текстових повідомлень, програм для виявлення місцеперебування терміналів стільникового зв'язку, що набуває популярності у зловмисників завдяки відносній нескладності вчинення таких посягань. Департамент, попри нетривалий час своєї діяльності, вже має позитивну практику припинення функціонування таких ресурсів у випадках причетності громадян України до використання коротких сервісних номерів із метою розповсюдження протиправного контенту.

Протидія злочинам у сфері високих інформаційних технологій неможлива без забезпечення належного рівня співпраці з Інтернет-провайдерами як основним витоком оперативної та доказової інформації. Отже, першочерговим завданням підрозділу боротьби з кіберзлочинністю в сучасних умовах уповні небезпідставно вважаємо залучення суб'єктів ринку телекомунікації до виявлення, документування та припинення злочинів. Із метою вдосконалення такої діяльності працівники служби беруть участь у функціонуванні робочої групи з питань взаємодії громадських організацій і державних структур у протидії кіберзлочинності, яку створено при Інтернет-асоціації України.

У перспективі досягнення згоди з суб'єктами ринку телекомунікації щодо впровадження позитивного зарубіжного досвіду, а саме створення системи добровільного обмеження доступу користувачів (абонентів) до інформаційних ресурсів із забороненим контентом, зокрема, з дитячою порнографією. У зв'язку з цим Департамент прова-

дить відповідну системну роз'яснювальну роботу з провідними операторами стільникового зв'язку, контент-провайдерами, хостінговими компаніями, реєстраторами доменних імен.

Міжнародне співробітництво у сфері запобігання та протидії кіберзлочинності не обмежується контактами з іноземними правоохоронними органами. У напрямку впровадження міжнародних стандартів у цій сфері Департамент наразі активно розвиває співпрацю з представниками Ради Європи та Європейського Союзу, іншими державними та неурядовими організаціями.

Ще одним пріоритетним напрямком роботи Департаменту є боротьба з комп'ютерними злочинами у сфері економіки. Серед основних завдань на цьому напрямку діяльності необхідно назвати протидію легалізації тіньових доходів. Аналіз схем відмивання коштів свідчить про значну зацікавленість організованої злочинності у використанні можливостей електронних платіжних систем, які дозволяють здійснювати миттєві перекази коштів із забезпеченням практично повної анонімності контрагентів. Особливий інтерес у світлі проблеми становить і те, що електронні платіжні системи не належать до розряду суб'єктів первинного фінансового моніторингу, а тому не зобов'язані інформувати наглядові органи про виявлення підозрілих транзакцій, зберігати відомості про транзакції, а також дані, що дозволяють ідентифікувати клієнта.

З метою протидії легалізації коштів, одержаних від злочинної діяльності, Департамент налагодив співпрацю з представництвами найбільш поширених в українському Інтернет-просторі електронних платіжних систем та кредитно-фінансовими установами, які надають послуги з обслуговування суб'єктів електронної комерції та мають дані про факти шахрайств, втручань у роботу комп'ютерних систем та інших протиправних посягань, учинених із використанням високих технологій.

Не менш важливим напрямком діяльності підрозділу боротьби з кіберзлочинністю є протидія обігу дитячої порнографії та сексуальному розбещенню дітей, учинюваним із використанням телекомунікаційних мереж. Доречно зазначити, що на цьому напрямку діяльності зусилля оперативного складу зосереджені не лише на виявленні осіб, причетних до вчинення злочину, але й на ідентифікації жертв сексуальної експлуатації.

Позитивним прикладом такої роботи слугує співпраця з Агентством боротьби з організованою злочинністю Великобританії (SOCA) щодо причетності підданих Об'єднаного Королівства до вчинення розпусних дій стосовно українських неповнолітніх. З метою ідентифікації дітей, потерпілих від сексуальної експлуатації, поліцією Об'єднаного Королівства було надано копію вилучених у злочинців порноматеріалів. У ході аналізу отриманої інформації та подальшої перевірки вдалося встановити, що протизаконний контент виготовлено на території Київської області. У подальшому оперативні працівники ідентифікували та опитали шістьох неповнолітніх, залучених до

зйомок порнографічного характеру й розпусних дій, які підтвердили факти сексуальної експлуатації, вчинені фігурантами. За цими фактами порушено кримінальну справу.

З метою превенції таких протиправних посягань спільно з правозахисними організаціями «Ла-Страда» та «ЕСРАТ» реалізуються ініціативи щодо просвітницької діяльності, спрямованої на запобігання комерційній сексуальній експлуатації дітей в Інтернеті, створено «гарячу лінію» з питань безпеки дітей в глобальній комп'ютерній мережі. Плідна співпраця триває і в рамках меморандуму «Про взаєморозуміння», підписаного між Міністерством внутрішніх справ та компанією «Майкрософт Україна» щодо інтенсифікації заходів, спрямованих на боротьбу з розповсюдженням «дитячої порнографії» в мережі Інтернет.

Доречним буде зазначити, що цей відділ у складі силового відомства МВС України є надзвичайно молодим. Тому проблема номер один, яка постала перед Департаментом боротьби з кіберзлочинністю і торгівлею людьми МВС України, – проблема формування кадрів. Це пов'язано з тим, що фахівці, які працюватимуть у цій сфері, повинні бути як оперативниками, так і фахівцями з комп'ютерної техніки. Вочевидь, що підготовка кваліфікованих кадрів для зазначеного підрозділу – одне з нагальних завдань вищих навчальних закладів МВС України. Принагідно зазначимо, що ця проблема є досить ефективно вирішуваною. Позитивний досвід підготовки фахівців для підрозділів боротьби з правопорушеннями у сфері інтелектуальної власності та високих технологій накопичений у Донецькому юридичному інституті Луганського державного університету внутрішніх справ, де підготовка фахівців зазначеного профілю провадиться з 2003 р.

Безумовно, специфіка протидії таким протиправним посяганням у сучасних умовах вимагає особливого підходу до комплектування підрозділу боротьби з кіберзлочинністю. Зокрема, такі працівники, на додаток до знань у сфері високих інформаційних технологій, навичок отримання інформації та збору доказів у електронній формі, повинні на достатньому рівні володіти іноземними мовами.

Висновок. Аналіз викладеного матеріалу дає підстави дійти висновків, що попри певні успіхи відповідних спецпідрозділів МВС України в боротьбі з кіберзлочинністю за доволі нетривалий час їх існування існує ціла низка проблем, вирішення яких дозволило би суттєво підвищити ефективність на цьому напрямку їх діяльності.

Головними проблемами, що існують у зазначеній сфері, є такі. Насамперед, це недосконаліть нормативно-правової бази щодо окремих напрямів діяльності з боротьби з комп'ютерною злочинністю. Чинне кримінальне та кримінально-процесуальне законодавство України наразі не забезпечує надійного захисту від кіберзлочинності. Його неузгодженість із міжнародно-правовими актами, а надто в частині того, які види діянь необхідно вважати злочинами, пов'язаними з використанням комп'ютерів і яку відповідальність повинен нести винний у їх учиненні, спричиняє труднощі в притягненні відповідних

осіб до кримінальної відповідальності. По-друге, потребує вдосконалення і механізм оперативного обміну інформацією стосовно громадян, затримуваних на території інших держав за скоєння злочинів, пов'язаних із використанням підроблених або викрадених платіжних пластикових карток банківських установ, за шахрайство у мережі Інтернет, незаконне проникнення до комп'ютерних баз даних різних міністерств і відомств, для перевірки на причетність до скоєння злочинів у сфері банківської діяльності й високих технологій.

Зрештою, враховуючи те, що кіберзлочинність невпинно вдосконалює способи вчинення протиправних посягань та має тенденцію до зростання організованості, нагальним завданням є систематичне підвищення кваліфікації оперативних працівників шляхом ознайомлення з передовим зарубіжним досвідом та нововведеннями щодо методології розкриття й розслідування таких злочинів.

Зазначені проблеми потребують розроблення відповідної стратегії щодо боротьби з кіберзлочинністю всіма правоохоронними органами України, зважаючи на те, що боротьба з цим найсучаснішим видом злочинності повинна стати однією з найважливіших їх функцій.

Бібліографічні посилання

1. Топ-10 країн Європи за кількістю Інтернет-користувачів [Електронний ресурс]. – Режим доступу: www.internetworldsstats.com /stats4.

2. *Бабанін С.В.* Комп'ютерні злочини за кримінальним законодавством України, США та Польщі // Співпраця поліції/міліції зі службами безпеки Інтернет-сайтів (аукціонів, соціальних мереж тощо) у боротьбі з Інтернет-злочинністю на підставі національного законодавства та законодавства, яке діє у Європейському Союзі: Тези доповідей міжнар. наук.-практ. конф. – Хмельницький, 2010.

3. *Стеблинська О.С.* Актуальні проблеми комп'ютерної злочинності в Україні // Співпраця поліції/міліції зі службами безпеки Інтернет-сайтів (аукціонів, соціальних мереж тощо) у боротьбі з Інтернет-злочинністю на підставі національного законодавства та законодавства, яке діє у Європейському Союзі: Тези доповідей міжнар. наук.-практ. конф. – Хмельницький, 2010.

4. Матеріали брифінгу в МВС України щодо новітніх напрацювань органів внутрішніх справ у боротьбі з кіберзлочинністю [Електронний ресурс]. – Режим доступу: mvs.gov.ua

5. Конвенція про кіберзлочинність [Електронний ресурс]. – Режим доступу: zakon.rada.gov.ua.

6. Про внесення змін до Закону України «Про ратифікацію Конвенції про кіберзлочинність»: Закон України // ВВР. – 2011. – № 5. – Ст. 32.

7. *Гвоздецький В.* Проблеми міжнародного співробітництва в протидії злочинності у сфері високих технологій // Вісник Академії управління МВС. – 2007. – № 2-3. – С. 6.

Надійшла до редакції 13.10.2011