ТЕОРІЯ ТА ІСТОРІЯ ДЕРЖАВИ І ПРАВА

УДК 340.15 (477) «1991/2015»

О. В. Барановський
адвокат, аспірант заочної форми навчання
кафедри загальноправових дисциплін
Донецького юридичного інституту
Міністерства внутрішніх справ України

ІСТОРИКО-ПРАВОВИЙ АНАЛІЗ ДІЯЛЬНОСТІ МІЛІЦІЇ УКРАЇНИ У СФЕРІ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ (1991–2015 РР.)

У статті із застосуванням історико-правового методу пізнання явищ державної і правової дійсності здійснено аналіз процесу формування та розвитку нормативно-правового та організаційно-штатного забезпечення діяльності спецпідрозділів міліції України щодо боротьби з кіберзлочинністю. Охарактеризовано основні види кіберзлочинності, які набули поширення в незалежній державі. Розкрито завдання, функції та основні форми й методи діяльності спецпідрозділів міліції щодо боротьби з кіберзлочинністю. Проаналізовано напрями та форми міжнародного співробітництва з Інтерполом та Європолом, правоохоронними органами європейських держав і США у сфері боротьби з кіберзлочинністю. З урахуванням історичного досвіду діяльності спецпідрозділів міліції сформовано окремі пропозиції з удосконалення діяльності підрозділів Департаменту кіберполіції Національної поліції України.

Ключові слова: *злочини у сфері високих технологій, боротьба з кіберзлочинністю, міліція України, нормативно-правова база, організаційно-штатне забезпечення, міжнародне співробітництво.*

Постановка проблеми. Стрімкий розвиток інформаційно-телекомунікаційних технологій та їх упровадження у всі сфери життєдіяльності суспільства, особливо в економічну, спричинили появу абсолютно нового виду протиправної поведінки – кіберзлочинності. Після здобуття незалежності кіберзлочинність дуже швидко посіла в Україні одне з перших місць поряд із наркобізнесом, торгівлею зброєю та людьми. Для органів і підрозділів української міліції протидія цьому новітньому виду злочинності стало одним із пріоритетних напрямів оперативно-службової діяльності.

Протягом усього періоду існування спецпідрозділів міліції України з протидії кіберзлочинності ними був накопичений значний досвід боротьби з цим якісно новим видом злочинності, який потребує комплексного історико-правового дослідження та узагальнення. Його важливість зумовлена необхідністю врахування зазначеного досвіду з метою вдосконалення діяльності підрозділів Департаменту кіберполіції новоствореного правоохоронного відомства – Національної поліції України. Отже, зазначене свідчить про **актуальність** досліджуваної проблеми.

Аналіз останніх досліджень і публікацій свідчить про те, що 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, О.Є. Користіна, В.В. Крилова, В.Г. Лукашевича, Г.А. Матусовського, В.А. Мінаєва, К.М. Рудоя, О.П. Снігерьова, В.Г. Хахановського, В.С. Цимбалюка, О.М. Юрченка та інших учених.

Водночас вважаємо за необхідне систематизувати історико-правовий досвід становлення та діяльності спецпідрозділів міліції України у протидії злочинності у сфері інформаційних технологій, забезпечення кібербезпеки та кіберзахисту держави.

Метою статті є дослідження історії формування та розвитку нормативно-правової бази, основних етапів організаційно-штатного забезпечення, форм і методів діяльності спецпідроз-

ділів міліції України з протидії кіберзлочинності, формування науково обґрунтованих рекомендацій для підвищення ефективності діяльності Департаменту кіберполіції Національної поліції України.

Виклад основного матеріалу. Розпочинаючи безпосереднє висвітлення проблеми, зазначимо, що в основу формування нормативно-правової бази діяльності спецпідрозділів української щодо протидії кіберзлочинності були покладені положення Конституції України, стаття 17 якої зазначає, що забезпечення інформаційної безпеки України є найважливішою функцією держави, справою всього Українського народу [1].

При цьому необхідно зазначити, що за роки незалежності в Україні була сформована досить розгалужена нормативно-правова база різних рівнів, яка дала змогу забезпечити діяльність правоохоронних органів із запобігання та протидії кримінальним правопорушенням у сфері інформаційно-телекомунікаційних технологій.

Це, зокрема, закони України «Про Державну службу спеціального зв'язку та захисту інформації України», «Про інформацію», «Про державну таємницю», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про основи національної безпеки України», «Про внесення змін до Закону України «Про платіжні системи та переказ грошей в Україні», «Про внесення змін до Кримінального та Кримінально-процесуального кодексів України» (щодо відповідальності за комп'ютерні злочини)», «Про внесення змін до Закону України «Про захист інформації в автоматизованих системах», «Про ратифікацію Конвенції про кіберзлочинність», «Про ратифікацію Додаткового протоколу до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи».

Зазначена система нормативно-правових актів була доповнена документами стратегічного характеру, а саме – Доктриною інформаційної безпеки, затвердженою Указом Президента України від 8 липня 2009 року [2], та Стратегією національної безпеки України, затвердженою Указом Президента України від 26 травня 2015 року [3]. Крім того, чинний Кримінальний кодекс України встановлює (відповідно до розділу XVI відповідальність за «злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» (статті 361–363) [4].

Складником системи нормативно-правової бази також стали відомчі накази, розпорядження, вказівки, інструкції та настанови МВС України, якими упорядковувалися організаційно-штатні питання, основні завдання і функції підрозділів міліції з боротьби з кіберзлочинністю за основними напрямами їх оперативно-службової діяльності, міжнародні міжвідомчі угоди про співробітництво МВС України з відповідними компетентними органами інших країн у зазначеній сфері.

До системи нормативно-правових актів у цій сфері, на наш погляд, належать також міжнародні договори у сфері забезпечення інформаційної безпеки, згода на обов'язковість яких надана Верховною Радою України.

Окрім того, на сучасному етапі державотворення основні засади формування та реалізації державної інформаційної політики, насамперед щодо протидії руйнівному інформаційному впливу Російської Федерації в умовах розв'язаної нею гібридної війни визначені Доктриною інформаційної безпеки України, затвердженою Указом Президента України від 25 лютого 2017 року [5]. До цього загалу необхідно додати Закон України «Про основні засади забезпечення кібербезпеки України» від п'ятого жовтня 2017 року, який визначає правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки [6].

Органи внутрішніх справ України, міліція, як основна їх складова, протягом усього періоду своєї діяльності, безумовно, були одним із ключових спеціалізованих суб'єктів протидії кіберзлочинності. Аналіз даних офіційної статистичної звітності за період 2002–2015 років свідчить про тенденцію стабільного та стрімкого зростання рівня кіберзлочинів. Їх середньорічний рівень в інтервалі 2002–2015 років становив 205 злочинів. Середньорічний темп приросту протягом 2002–2015 років становив 107,5%. [7, с. 7].

Характеризуючи процес організаційно-штатного забезпечення, необхідно зазначити, що перші спроби на шляху протидії цьому виду

злочинності були започатковані МВС ще наприкінці 90-тих років минулого століття. У цей історичний період, коли змінювалися стереотипи та методи боротьби зі злочинністю, зародилася ідея створення підрозділу боротьби з кіберзлочинністю.

Отже, перший підрозділ із протидії кіберзлочинності був створений у структурі головного управління боротьби з економічною злочинністю МВС України в травні 2001 року. Його діяльність була орієнтована за двома основними напрямами – захист інтелектуальної власності та боротьба з кіберзлочинністю.

Необхідно зазначити, що основною причиною зосередження зусиль у боротьбі з таким новим видом злочинності в зазначеному напрямі стало те, що в другій половині 90-х років Україну критикували з приводу значної кількості контрафактної продукції на її території. Саме тому робота цього управління переважно була зосереджена на захисті прав інтелектуальної власності та боротьбі з незаконним поширенням контрафактної продукції.

У листопаді 2003 року відділення, групи боротьби з правопорушеннями у сфері інтелектуальної власності та високих технологій були реорганізовані у відповідні відділи (відділення) при ГУМВС (УМВС, УМВСТ) в регіонах нашої держави та на транспорті [8, арк. 54].

Наступними кроками на шляху організаційно-штатних перетворень стало створення в липні 2009 року в структурі Департаменту боротьби зі злочинами, пов'язаними з торгівлею людьми, окремого відділу боротьби з кіберзлочинністю, а через рік, у липні 2010 року, – Департаменту боротьби з кіберзлочинністю і торгівлею людьми. Надалі з метою оптимізації структури кримінальної міліції апарату Міністерства внутрішніх справ, забезпечення належного виконання оперативно-службових завдань, відповідно до Наказу МВС України від 26 грудня 2011 року було створено Управління боротьби з кіберзлочинністю (далі – УБК) та його структурні підрозділи в регіонах країни [9].

Згідно з Положенням Управління боротьби з кіберзлочинністю МВС України стало самостійним структурним підрозділом у складі кримінальної міліції МВС України, який відповідно до законодавства України забезпечує реалізацію державної політики у сфері боротьби з кіберзлочинністю, зокрема організовує та здійснює в межах компетенції та відповідно до законодавства оперативно-розшукову діяльність.

Серед основних завдань УБК МВС України такі: участь у формуванні та забезпеченні реалізації державної політики щодо запобігання та протидії кримінальним правопорушенням, механізм підготовки, вчинення або приховування яких передбачає використання електронно-обчислювальних машин (комп'ютерів), систем і комп'ютерних мереж і мереж електрозв'язку, а також іншим кримінальним правопорушенням, учиненим з їх використанням (далі – сфера боротьби з кіберзлочинністю). Також на УБК МВС України було покладено завдання зі сприяння в порядку, передбаченому чинним законодавством, іншим підрозділам МВС України у попереджені, виявлені та припиненні кримінальних правопорушень, а також у проведенні досудового розслідування [10].

До цього необхідно додати, що за Законом «Про внесення зміни до Закону України «Про ратифікацію Конвенції про кіберзлочинність» від 21 вересня 2010 року в Україні органом, на який покладаються повноваження щодо створення та функціонування цілодобової контактної мережі для надання невідкладної допомоги під час розслідування злочинів, пов'язаних із комп'ютерними системами та даними, переслідування осіб, що обвинувачуються у вчиненні таких злочинів, а також збирання доказів в електронній формі, є Міністерство внутрішніх справ України [11].

Цифри міліцейської статистики свідчать про такі показники зростання цього виду злочинності: за 2009 рік було зареєстровано 96 злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів) в автоматизованих системах (комп'ютерних мережах), у 2010 році – 87, у 2011 році – 67, у 2012 році – 83, у 2013 році – 408, у 2014 році – 140 злочинів відповідно. Водночас лише у 2015 році абсолютна кількість зареєстрованих кіберзлочинів сягнула 556, що на 1753,3% більш ніж у 2002 році та на 33% більше ніж у 2014 [7, с. 7]. Вони свідчать про поширення злочинності у цій сфері та її високу латентність.

Найбільш поширеним видом кіберзлочинів, з яким повело боротьбу новостворене УБК МВС України у сфері економіки держави, було списання коштів із рахунків фізичних і юридичних осіб із використанням систем дистанційного банківського обслуговування та подальшою легалізацією незаконно отриманих доходів. Наприклад, за 2012 рік правоохоронними органами було зафіксовано 270 спроб злому систем на суму понад 100 млн грн. Із загальної суми

зареєстрованих списань – понад 67 млн грн. – власникам повернуто близько 47 млн грн. Крім того, упродовж 2011–2013 років спостерігалось значне зростання кількості випадків застосування скіммінгових пристроїв. Співробітниками УБК МВС України у 2011 році було виявлено 45 таких пристроїв, у 2012 році – 73, у 2013 році – 160. Серед інших специфічних видів кіберзлочинів, яким протидіяли підрозділи міліції з боротьби з кіберзлочинністю, – підробка банківських карток, крадіжка конфіденційних даних банківських карт, шахрайство з банкоматами, злочинні дії в банківській системі онлайн та інші [12, с. 16].

За територіальним розподілом найбільша кількість цього виду злочинів за період 2009–2012 роках була зареєстрована в Дніпропетровській, Донецькій, Запорізькій областях, а у 2013–2014 роках – у містах Київ, Одеса, Дніпропетровськ [13, с. 179].

Необхідно зазначити, що за період своєї діяльності спецпідрозділи міліції відбудували певну систему форм і методів із протидії кіберзлочинності. Серед найбільш ефективних – оперативне супроводження підприємств, установ та організацій, основна діяльність яких пов'язана з використанням комп'ютерних технологій або наданням інформаційних послуг і забезпечення заходів безпеки на об'єктах, що призначені для передачі інформації; організація превентивної діяльності щодо виявлення осіб, схильних до вчинення кіберзлочинів, запобігання й припинення їх кримінальної активності. Також важливими аспектами вдосконалення запобіжної діяльності є впровадження передового досвіду діяльності зарубіжних правоохоронних органів у цій сфері; активізація міжнародного співробітництва щодо розкриття, розслідування та запобігання кіберзлочинам; формування сучасних комплексних механізмів захисту від кібератак мережевих ресурсів органів державної влади та інше [7, с. 11].

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

Підрозділи української міліції з боротьби з кіберзлочинністю протягом усього періоду своєї діяльності активно нарощували рівень міжнародного співробітництва на цьому напрямі їх оперативно-службової діяльності. Одним із найбільш ефективних було співробітництво з компетентними органами країн-учасників СНД для забезпечення ефективного запобігання, виявлення, припинення, розкриття й розслідування злочинів у сфері комп'ютерної інформації.

Нормативно-правовою базою зі забезпечення міжнародної взаємодії правоохоронних органів на цьому напрямі став прийнятий 17 лютого 1996 року на VII пленарному засіданні Міжпарламентської Асамблеї Модельний кримінальний кодекс, в якому регламентується відповідальність за комп'ютерні злочини, Угода про співробітництво держав-учасників СНД у боротьбі зі злочинами у сфері комп'ютерної інформації, Концепція співпраці держав-учасників СНД у сфері забезпечення інформаційної безпеки й Комплексний план заходів щодо її реалізації, відповідні Програми співробітництва держав-учасників СНД.

Наявність комплексу нормативно-правових актів дала змогу визначити основні форми співпраці спецпідрозділів міліції України у цій сфері міжнародної взаємодії, серед яких такі: обмін інформацією різноманітного змісту, виконання запитів про проведення оперативно-розшукових заходів і слідчих дій; планування і проведення скоординованих заходів і операцій із запобігання, виявлення, припинення, розкриття і розслідування злочинів у сфері комп'ютерної інформації; надання допомоги в підготовці й підвищенні кваліфікації кадрів; створення інформаційних систем, які забезпечують виконання завдань із запобігання, виявлення, припинення, розкриття і розслідування злочинів у сфері комп'ютерної інформації; проведення спільних наукових досліджень із відповідних проблем; обміну нормативними правовими актами, науково-технічною літературою з боротьби зі злочинами у сфері комп'ютерної інформації [14, с. 508–509].

Наступним напрямом міжнародної взаємодії стала співпраця з компетентними органами європейських країн і США. Характеризуючи співпрацю в зазначеній сфері зі США, необхідно зазначити, що вона була регламентована підписаним у 2002 році між урядами України і США Меморандумом про взаєморозуміння між Урядами обох держав щодо допомоги з правоохоронних питань, який був підписаний [15], та протоколами № № 1–11 до цього Меморан-

думу, підписаними протягом 2006–2014 років. Крім того, для ще більш тісної співпраці в цьому напрямі був підписаний меморандум про взаємини між ФБР США і МВС України.

Завдяки дії зазначених нормативно-правових актів спецпідрозділам української міліції з протидії кіберзлочинності вдалося здійснити низку практичних заходів, які суттєво поліпшили результативність їх дій на цьому напрямі оперативно-службової діяльності. Серед них такі: надання іноземному представнику робочого місця на території міністерства для забезпечення максимально ефективного та оперативного процесу з працівниками УБК; створення програмно-технічної інфраструктури для забезпечення оперативно-розшукової діяльності підрозділів МВС; упровадження досвіду застосування правоохоронними підрозділами США програмного забезпечення для онлайн-розслідувань, яке може бути адаптоване до аналогічних потреб українських правоохоронців.

На європейському напрямі однією з ефективних форм міжнародної взаємодії підрозділів української міліції з протидії кіберзлочинності стало співробітництво в рамках окремих європейських регіональних стратегій. Серед таких прикладів ефективного співробітництва можна виділити участь МВС України у реалізації програм протидії кіберзлочинності в межах стратегії ЄС для Дунайського регіону, у реалізації проекту «Cybercrime@EAP» у рамах механізму Східного партнерства та інше.

Також важливим складником міжнародного співробітництва на зазначеному напрямі оперативно-службової діяльності підрозділів міліції України була взаємодія з Інтерполом та Європолом.

Важливим практичним кроком на шляху розбудови міжнародної співпраці з Інтерполом на зазначеному напрямі стало створення за ініціативи МВС на виконання статті 35 Конвенції про кіберзлочинність Національного контактного пункту формату 24/7 щодо реагування та обміну терміновою інформацією про вчинені комп'ютерні злочини в Україні. НКП зарахували до міжнародної мережі таких пунктів, і він успішно пройшов необхідні тестування та акредитацію [14, с. 514]. НКП здійснював свою діяльність у структурі Управління боротьби з кіберзлочинністю МВС України цілодобово впродовж тижня з метою надання негайної допомоги для розслідування або переслідування стосовно кримінальних правопорушень, пов'язаних із комп'ютерними системами і даними, або з метою збирання доказів в електронній формі, що стосуються кримінального правопорушення [16, с. 132].

Взаємодія МВС України з Європолом визначена Законом України від 5жовтня 2010 року № 2576-VI «Про ратифікацію Угоди між Україною та Європейським поліцейським офісом про стратегічне співробітництво». Ефективність співпраці на цьому напрямі значною мірою посилилась із початком діяльності із січня 2013 року створеного під егідою Європолу нового Європейського центру боротьби з кіберзлочинністю. Серед пріоритетів Центру – розслідування шахрайства через онлайн-мережі, зокрема в системі електронного банкінгу та інших видах фінансової діяльності, протидія сексуальній експлуатації дітей через Інтернет, а також розслідування інших злочинів, що посягають на безпеку важливої інфраструктури та інформаційних систем ЄС.

Основними формами співпраці підрозділів із боротьби з кіберзлочинністю з цією європейською правоохоронною структурою стали обмін оперативною інформацією в рамках кримінальних проваджень і створення можливостей для спільних заходів із розслідування злочинів і пошуку осіб, причетних до скоєння злочинів.

Висновки і пропозиції. Підсумовуючи, варто зазначити, що протидія кіберзлочинності, яка має транснаціональний характер, стала абсолютно новим напрямом діяльності міліції незалежної України. Цей вид злочинності тісно пов'язаний із транснаціональними злочинними організаціями. У структурі МВС України були створені відповідні спеціальні структурні підрозділи міліції, головним завданням яких була організація боротьби з вказаною категорією злочинів.

Діяльність зазначених підрозділів дала змогу певною мірою вплинути на поліпшення стану боротьби з кіберзлочинністю на території держави. Водночас зупинити зростання цього виду злочинності українська міліція не змогла. Основними причинами такого стану справ стали такі: недостатній досвід практичних підрозділів міліції щодо протидії кіберзлочинності; недосконалість нормативно-правового забезпечення на цьому напрямі їх оперативно-службової діяльності; відсутність єдиної системи підготовки, перепідготовки кадрів – працівників ОВС, які спеціалізувались би на розслідуванні цих видів транснаціональних злочинів у рамках

міжнародної співпраці; недоліки у використанні сучасних інформаційних і комунікаційних технологій у сфері боротьби з кіберзлочинністю. Крім того, тодішні форми міжнародної співпраці правоохоронних органів у боротьбі із транснаціональною злочинністю мали суттєві недоліки у зв'язку з відсутністю єдиного підходу у процедурі формування, використання доказової бази у справах про такі злочини, а також у встановленні, розшуку і притягненні винних до відповідальності.

Аналіз досвіду діяльності спеціальних підрозділів міліції України з боротьби з кіберзлочинністю дає змогу висновувати, що на сучасному етапі діяльності підрозділів Департаменту кіберполіції Національної поліції України основними умовами ефективності їх діяльності є такі: подальше вдосконалення нормативно-правового забезпечення їх роботи; інтеграція правоохоронної системи України в єдиний європейський правоохоронний простір; активний розвиток регіонального співробітництва з правоохоронними органами ближнього та дальнього зарубіжжя на цьому напрямі оперативно-службової діяльності; вирішення проблем кадрового забезпечення діяльності підрозділів із боротьби з кіберзлочинністю; розроблення програм спільного спеціалізованого навчання працівників правоохоронних органів ЄС та України, основним призначенням яких має стати обмін передовим досвідом, посилення співробітництва та вдосконалення співпраці між підрозділами з боротьби з кіберзлочинністю.

Список використаної літератури:

1. Конституція України від 28 червня 1996 р. *Відомості Верховної Ради України.* 1996. № 30. Ст. 141.
2. Про Доктрину інформаційної безпеки України: Указ Президента України від 8 липня 2009 р. № 514/2009. *Офіційний вісник України*. 2009. № 52. С. 7. Ст. 1783.
3. Про Стратегію національної безпеки України: Указ Президента України від 26 травня 2015 р. № 287/2015. URL: https://www.president.gov.ua/documents/2872015-19070.
4. Кримінальний кодекс України: редакція від 11 січня 2019 р., підстава – 2227-VIII. URL: https://zakon.rada.gov.ua/laws/show/2341-14.
5. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 р. «Про Доктрину інформаційної безпеки України»: Указ Президента України від 25 лютого 2017 р. № 47/2017 URL: https://zakon.rada.gov.ua/laws/show/47/2017.
6. Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 р. № 2163-VIII. *Відомості Верховної Ради (ВВР).* 2017. № 45. Ст. 403.
7. Кравцова М.О. Кіберзлочинність: кримінологічна характеристика та запобігання органами внутрішніх справ: автореф. дис. ... канд. юрид. наук: спец. 12.00.08; Харк. нац. ун-т внутр. справ. Харків, 2016. 16 с.
8. Про зміцнення підрозділів боротьби з правопорушеннями у сфері інтелектуальної власності та високих технологій при ГУМВС, УМВС УМВСТ: Наказ МВС України від 30 листопада 2003 р. № 1463. Архів ГУМВС України в Донецькій області за 2013 рік. Арх. 193. Ф. 20. Д. 1. Т. 9. Арк. 54–56.
9. Про зміни структури кримінальної міліції апарату Міністерства: Наказ МВС України від 26 грудня 2011 р. № 941. Поточний архів Донецького юридичного інституту МВС України, справа з наказами, розпорядженнями, вказівками МВС України за 2011 рік. Арк. 71–72.
10. Про організацію діяльності Управління боротьби з кіберзлочинністю МВС України та підрозділів боротьби з кіберзлочинністю ГУМВС, УМВС: наказ МВС України від 30 жовтня 2012 р. № 988. URL: http://zakon.rada.gov.ua/rada/show/v0988320-12.
11. Про внесення зміни до Закону України «Про ратифікацію Конвенції про кіберзлочинність»: Закон України 21 вересня 2010 р. № 2532-VI. *Відомості Верховної Ради України*. 2011. № 5. Ст. 32.
12. Кобилянська Л.М. Кіберзлочинність як глобальна загроза економічній безпеці сучасної держави. *Науковий вісник Херсонського державного університету. Серія: «Економічні науки».* 2014. Вип. 8 (5). С. 14–17.
13. Пивоваров В.В. Кіберзлочинність: кримінологічний погляд на генезис явища та шляхи запобігання. *Право і суспільство*. 2016. № 3. Ч. 2. С. 177–182.
14. Зозуля Є.В. Міжнародне співробітництво органів внутрішніх справ України: історико-правове дослідження: монографія. Х.: «Ніка Нова», 2014. 782 с.
15. Меморандум про взаєморозуміння між Урядом України та Урядом Сполучених Штатів Америки щодо допомоги з правоохоронних питань. Підписаний 9 грудня 2002 р. URL: http://zakon.rada.gov.ua/laws/show/840_103.
16. Лєшукова І.В. Проблемні питання міжнародного співробітництва у сфері протидії кіберзлочинності. *Актуальні питання розслідування кіберзлочинів*: матер. Міжнар. наук.-практ. конф. (м. Харків, 10 грудня 2013 р.). МВС України, Харк. нац. ун-т внутр. справ. Х.: ХНУВС, 2013. 272 с.

Барановский А. В. Историко-правовой анализ деятельности милиции Украины в сфере противодействия киберпреступности (1991–2015 гг.)

В статье с применением историко-правового метода познания явлений государственной и правовой действительности осуществлен анализ процесса формирования и развития нормативно-правового и организационно-штатного обеспечения деятельности спецподразделений милиции Украины по борьбе с киберпреступностью. Охарактеризованы основные виды киберпреступности, получившие распространение в независимом государстве. Раскрыты задачи, функции, основные формы и методы деятельности спецподразделений милиции по борьбе с киберпреступностью. Проанализированы направления и формы международного сотрудничества с Интерполом и Европолом, правоохранительными органами европейских государств и США в сфере борьбы с киберпреступностью. С учетом исторического опыта деятельности спецподразделений милиции сформированы отдельные предложения по совершенствованию деятельности подразделений Департамента киберполиции Национальной полиции Украины.

Ключевые слова: *преступления в сфере высоких технологий, борьба с киберпреступностью, милиция Украины, нормативно-правовая база, организационно-штатное обеспечение, международное сотрудничество.*

Baranovskyi O. V. Historical and legal analysis of the activities of the police of Ukraine in the field of countering cybercrime (1991–2015)

Using of the historical and legal method of knowledge of the phenomena of state and legal reality in the article it is carried out the analysis of the process of formation and development of the regulatory and organizational staff support of the activities of the special police units of Ukraine in the fight against cybercrime. The main types of cybercrime, which became widespread in an independent state are characterized. The tasks, functions, basic forms and methods of the activities of special police units for combating cybercrime are discovered. It is analyzed the directions and forms of international cooperation with Interpol and Europol, law enforcement agencies of European countries and the United States in the fight against cybercrime. Taking into account the historical experience of the activities of the special police units, separate proposals have been formed for improving the activities of the units of the Cyber Police Department of the National Police of Ukraine.

Key words: *crimes in the field of high technologies, fight against cybercrime, police of Ukraine, regulatory framework, organizational and staffing, international cooperation.*