УДК 343.96:341

Зозуля Євген Вікторович, доктор юридичних наук, доцент (Донецький юридичний інститут МВС України)

НОРМАТИВНО-ПРАВОВЕ ТА ОРГАНІЗАЦІЙНЕ ЗАБЕЗПЕЧЕННЯ ДІЯЛЬНОСТІ МВС УКРАЇНИ ЩОДО ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ (ІСТОРИКО-ПРАВОВИЙ АСПЕКТ)

У статті досліджуються питання нормативно-правового та організаційного забезпечення діяльності МВС України щодо протидії злочинності у сфері високих технологій. Проаналізовано формування нормативно-правової бази протидії кіберзлочинності як на внутрішньонаціональному, так і міжнародному рівнях. Визначена важливість приєднання України до основоположних міжнародних конвенцій у протидії кіберзлочинності, їхній вплив на формування національної нормативно-правової бази у цій сфері. Досліджено ґенезу становлення і розвитку організаційно-правового забезпечення та форми міжнародного співробітництва спецпідрозділів МВС у боротьбі з кіберзлочинністю. На основі проведеного дослідження визначено коло проблем, вирішення яких дозволить суттєво підвищити ефективність діяльності підрозділів кіберполіції Національної поліції України.

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

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 результатами всеукраїнського дослідження, проведеного на початку 2016 року Київським міжнародним інститутом соціології (КМІС), 62% дорослого населення України користуються мережею Інтернет. Частка користувачів мережі Інтернет серед людей 18-39 років в Україні сягнула 91% [1].

Водночас наслідком розбудови інформаційного суспільства є те, що злочинні групи та співтовариства усе 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.

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. 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. Розпочинаючи безпосереднє висвітлення проблеми, зазначимо, що розвиток та впровадження комп'ютерних технологій у всіх сферах суспільного життя потребує розв'язання питань забезпечення безпеки використання електроннообчислювальних машин (комп'ютерів), систем, комп'ютерних мереж, мереж електрозв'язку, у тому числі й кримінально-правовими засобами. У багатьох країнах, зокрема і в Україні, ці посягання отримали 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, за деякими оцінками, через кіберзлочинців щорічно світова економіка втрачає 114 млрд. доларів. А США оцінили свої збитки за всі роки існування глобальної мережі у 400 млрд. доларів [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 насамперед правоохоронних органів) у розслідуванні такого роду злочинів.

Перші значущі кроки на шляху налагодження міжнародного співробітництва у протидії кіберзлочинності Україна зробила на початку XXI століття, коли 23 листопада 2001 року 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 використаними 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 на 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, даними, зі збиранням доказів в електронній формі.

Наступним важливим кроком України на шляху до налагодження міждержавної співпраці у розглядуваній сфері є ратифікація 7 вересня 2005 року зазначеної Конвенції із Додатковим протоколом від 28 січня 2003 року до неї, якою передбачене надання повноважень, достатніх для ефективної боротьби зі злочинами у сфері інформаційнотелекомунікаційних 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 й управління нашої

держави варто вважати приведення чинних механізмів міжнародної взаємодії у відповідність до положень вищезгаданої Конвенції.

Згодом, у липні 2006 року, було ратифіковано Додатковий протокол до Конвенції, що стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи [6]. У зв'язку з цим одним із нагальних завдань органів державної влади й 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. Це перш за все Конституція України, яка стала гарантом побудови демократичної правової держави і яка не могла не врахувати загальносвітових тенденцій інформатизації суспільства. Тому ряд її статей (зокрема ст. 17, 32, 34) визначають забезпечення інформаційної безпеки як одну з найважливіших функцій держави і мають стати основою розвитку інформаційного законодавства. Наявна певна законодавча база, яка складається із Законів України «Про інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про захист персональних даних», «Про державну таємницю» тощо. Є чинними низка указів Президента та постанов Кабінету Міністрів України, якими врегульовано конкретні напрями діяльності в галузі захисту інформації.

Одним із важливих кроків на шляху створення нормативно-правової бази діяльності правоохоронних органів щодо протидії кіберзлочинності є закон України «Про внесення змін до Закону України «Про ратифікацію Конвенції кіберзлочинності». Згідно з цим законом, Міністерство внутрішніх справ України стає єдиним органом, який має повноваження щодо створення цілодобової контактної 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 [7].

У сучасних умовах розбудова дієвої системи кібернетичної безпеки є одним із найважливіших завдань забезпечення національної безпеки України.

Відтак нагальним завданням є необхідність визначення основних засад державної політики, спрямованої на захист життєво важливих інтересів особи, суспільства і держави, реалізація яких залежить від належного функціонування інформаційних, телекомунікаційних та інформаційнотелекомунікаційних систем.

Це потребує невідкладного прийняття Закону України «Про кібернетичну безпеку України», проект якого було зареєстровано ще 04 червня 2013 року. Прийняття зазначеного законопроекту сприятиме вдосконаленню нормативно-правової бази у сфері забезпечення кібернетичної безпеки України, дозволить закласти необхідну юридичну базу для формування й подальшого вдосконалення системи кібернетичної безпеки України.

Серед важливих кроків на цьому шляху є Указ Президента України № 449/2014 від 01 травня 2014 року «Про рішення Ради національної безпеки і оборони України від 28 квітня 2014 року «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України». У ньому було поставлено завдання розробити проект Стратегії кібернетичної безпеки України, проект Закону України «Про кібернетичну безпеку України», а також завдання щодо приведення національного законодавства у відповідність до міжнародних стандартів із питань інформаційної та кібернетичної безпеки, удосконалення системи формування та реалізації державної політики у сфері інформаційної безпеки України [8].

Принагідно зазначимо, що у 2016 році відбувся значний прогрес у цій сфері, зокрема на інституційно-організаційному рівні, а саме: 15 березня 2016 року Указом Президента затверджена Стратегія кібербезпеки України, яка має на меті створення національної системи кібербезпеки [9]; у червні 2016 року Президент України підписав Указ про створення Національного координаційного центру кібербезпеки [10]. Першим етапом його роботи є здійснення аналізу та розроблення галузевих індикаторів стану кібербезпеки. Також у вересні 2016 року Верховна Рада у першому читанні прийняла Закон про основні засади забезпечення кібербезпеки України [11].

Суттєвим внеском у справу розвитку міжнародної співпраці є діяльність міжнародних правоохоронних структур. Наприклад, Генеральний Секретаріат Інтерполу ще у 1994 році 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 задля 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 у 1996 році 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 отримують 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 [12].

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 є учинюваними 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 90-тих років минулого століття. 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 90-х років Україну критикували з приводу значної кількості контрафактної продукції на її території. Саме тому робота цього управління переважним

чином була зосереджена на захисті прав інтелектуальної власності та боротьбі з незаконним поширенням контрафактної продукції.

Практика діяльності новоствореного підрозділу мала за результат усвідомлення того, що необхідно приділяти більше часу, засобів та уваги справі боротьби з кіберзлочинністю. Тому в липні 2009 року в структурі Департаменту боротьби зі злочинами, пов'язаними з торгівлею людьми, було створено окремий відділ боротьби з кіберзлочинністю. Обов'язками підрозділу стало формування та реалізація державної політики в розглядуваній сфері правоохоронної діяльності, вироблення 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 належало виявлення та документування організованих груп транснаціонального й регіонального характеру, учасники яких спеціалізуються на вчиненні злочинів із використанням високих технологій і телекомунікаційних систем.

У сучасних умовах протидія злочинності у сфері високих технологій покладена на Департамент кіберполіції Національної поліції України, основним завданням якого є участь у формуванні та забезпеченні реалізації державної політики щодо попередження та протидії кримінальним правопорушенням, механізм підготовки, учинення або приховування яких передбачає використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.

Відповідно до Закону України «Про ратифікацію Конвенції про кіберзлочинність» та з метою забезпечення міжнародної діяльності кіберполіції, у штатній структурі Департаменту кіберполіції створено сектор Національного контактного пункту з реагування на кіберзлочини.

Сьогодні відбувається перетворення колишньої моделі підрозділів боротьби з кіберзлочинністю у новітній орган правозахисного призначення, який за своїми технічними та професійними можливостями матиме змогу

миттєво реагувати на кіберзагрози, а також відповідно до кращих європейських та світових стандартів проводитиме міжнародну співпрацю щодо знешкодження транснаціональних злочинних угрупувань у даній сфері [13].

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.

Міжнародне співробітництво у сфері запобігання та протидії кіберзлочинності не обмежується контактами з іноземними правоохоронними органами. У напрямку впровадження міжнародних стандартів у цій сфері Департамент кіберполіції Національної поліції України 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. З метою протидії легалізації коштів, одержаних від злочинної діяльності, Департамент налагоджує 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 у цьому напрямку діяльності зусилля оперативного складу зосереджені не лише на виявленні осіб, причетних до вчинення злочину, але й на ідентифікації жертв сексуальної експлуатації.

Варто зазначити, що наразі проблема номер один, яка постала перед Департаментом кіберполіції Національної поліції 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.

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

Висновки та перспективи подальших досліджень. Аналіз викладеного матеріалу дає підстави дійти висновків, що, попри певні успіхи відповідних спецпідрозділів МВС України в боротьбі з кіберзлочинністю за доволі нетривалий час їхнього існування, існує ціла низка проблем, вирішення яких дозволило б суттєво підвищити ефективність у цьому напрямку їхньої діяльності.

У зазначеній сфері проблемними залишаються такі питання. 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 спричиняє труднощі в притягненні відповідних осіб до кримінальної відповідальності. По-друге, потребує вдосконалення механізм оперативного

обміну інформацією стосовно осіб, затриманих 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.

Серед першочергових завдань є вирішення проблем, котрі виникають у процесі розслідування і кримінального провадження злочинів, пов'язаних з електронними доказами. Відтак однією з найбільш важливих умов для забезпечення ефективності заходів щодо боротьби з кіберзлочинністю та іншими злочинами, пов'язаними з електронними доказами, є ефективне міжнародне співробітництво між судовими органами та поліцією.

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 кіберполіції шляхом вивчення та впровадження у практичну діяльність передового зарубіжного досвіду та новацій щодо методології розкриття й розслідування злочинів у цій сфері.

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

Список використаних джерел:

1. Динаміка використання Інтернет в Україні: лютий-березень 2016 [Електронний ресурс]. – Режим доступу: http://kiis.com.ua/?lang=ukr&cat=reports&id=621&page=1.

2. Бабанін С.В. Комп'ютерні злочини за кримінальним законодавством України, США та Польщі / С.В. Бабанін / Співпраця поліції/міліції зі службами безпеки Інтернетсайтів (аукціонів, соціальних мереж тощо) у боротьбі з

інтернет-злочинністю на підставі національного законодавства та законодавства, яке діє у Європейському Союзі: тези доповідей міжнародної науково-практичної конференції (м. Хмельницький, 16–17 листопада 2010 року) / МВС України; УМВС України в Хмельницькій області. – Хмельницький: УМВС, 2010. – 100 с.

3. Стеблинська О.С. Актуальні проблеми комп'ютерної злочинності в Україні / О.С. Стеблинська / 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 міжнародної науково-практичної конференції (м. Хмельницький, 16–17 листопада 2010 року) / МВС України; УМВС України в Хмельницькій області. – Хмельницький: УМВС, 2010. – 100 с.

4. Довбиш М. Кіберзлочинність в Україні / Микита Довбиш Електронний ресурс]. – Режим доступу: https://www.science-community.org/ru/node/16132.

5. Конвенція про кіберзлочинність : міжнар. докум. від 23 лист.2001 р. [Електронний ресурс]. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/994_575.

6. Про ратифікацію Додаткового протоколу до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи : Закон України від 21 липня 2006 р. № 23-V // Відомості Верховної Ради України. – 2006. – № 39. – С. 1384. – Ст. 328.

7. Про внесення змін до Закону України «Про ратифікацію Конвенції про кіберзлочинність»: закон України // Відомості Верховної Ради України. – 2011. – № 5. – Ст.32.

8. Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України : Указ Президента України Про рішення Ради національної безпеки і оборони України від 28 квітня 2014 р // Офіційний вісник Президента України. – 2014. – № 16. – С. 6. – Ст. 982.

9. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» : Указ Президента України від 15.03.2016 № 96/2016 [Електронний ресурс]. – Режим доступу: http://zakon2.rada.gov.ua/laws/show/96/2016.

10. Про Національний координаційний центр кібербезпеки : Указ Президента України від 07.06.2016 № 242/2016 / Офіційне інтернет-представництво Президента України [Електронний ресурс]. – Режим доступу: http://www.president.gov.ua/documents/2422016- 20141.

11. Проект Закону про основні засади забезпечення кібербезпеки України / Офіційний сайт Верховної Ради України [Електронний ресурс]. – Режим доступу: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=55657.

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

13. Офіційний сайт Національної поліції України. Департамент кіберполіції Національної поліції України [Електронний ресурс]. – Режим доступу: https://www.npu.gov.ua/uk/publish/article/1816252.

Зозуля Евгений Викторович, доктор юридических наук, доцент (Донецкий юридический институт МВД Украины)

НОРМАТИВНО-ПРАВОВОЕ И ОРГАНИЗАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДЕЯТЕЛЬНОСТИ МВД УКРАИНЫ ПО ПРОТИВОДЕЙСТВИЮ КИБЕРПРЕСТУПНОСТИ (ИСТОРИКО-ПРАВОВОЙ АСПЕКТ)

В статье исследуются вопросы нормативно-правового и организационного обеспечения деятельности МВД Украины по противодействию преступности в сфере высоких технологий. Проанализировано формирование нормативно-правовой базы противодействия киберпреступности как на внутринациональном, так и международном уровнях. Подчеркнута важность присоединения Украины к основополагающим

международным конвенциям в противодействии киберпреступности, их влияние на формирование национальной нормативно-правовой базы в этой сфере.

Акцентировано внимание на том, что в современных условиях развитие действенной системы кибернетической безопасности является одной из неотложных задач обеспечения национальной безопасности Украины.

Определено, что МВД Украины в течение всего периода независимого развития государства постоянно предпринимает организационные и практические мероприятия по обеспечению эффективного противодействия этому современному виду транснациональной преступности.

Исследован генезис становления и развития организационно-правового обеспечения и формы международного сотрудничества спецподразделений МВД по борьбе с киберпреступностью. На основе проведенного исследования обозначены некоторые проблемы, решение которых позволит существенно повысить эффективность деятельности подразделений киберполиции Национальной полиции Украины.

Среди них: необходимость совершенствования нормативно-правовой базы по отдельным направлениям деятельности по борьбе с киберпреступностью; приведение его в соответствие с международно-правовыми актами в этой сфере; совершенствование механизма оперативного обмена информацией в отношении лиц, задерживаемых на территории других государств за совершение компьютерных преступлений; налаживание эффективного международного сотрудничества между судебными органами и полицией в расследовании киберпреступлений; систематическое повышение квалификации оперативных работников киберполиции путем изучения и внедрения в практическую деятельность передового зарубежного опыта и новаций по методологии раскрытия и расследования преступлений в этой сфере.

Сделан вывод о том, что насущной задачей является разработка соответствующей «дорожной карты» по борьбе с киберпреступностью всеми

правоохранительными органами Украины, исходя из того, что борьба с этим современным видом преступности должна стать одной из важнейших их функций.

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

Evgeniy Zozulya, doctor of legal sciences, associate professor (Donetsk law Institute of the MIA of Ukraine)

LEGAL AND ORGANIZATIONAL SUPPORT OF THE MINISTRY OF INTERNAL AFFAIRS OF UKRAINE ON CYBERCRIME RESISTANCE (HISTORICAL AND LEGAL ASPECT)

The article it is examined the issues of legal and organizational support of the activities of the Ukrainian Interior Ministry concerning the combat crime in the sphere of high technologies. It is analyzed the formation of the legal framework to counter cybercrime on intra-national and international levels. It is emphasized the importance of Ukraine's accession to fundamental international conventions in combating cybercrime, its influence on the formation of a national legal framework in this area.

It is paid great attention to the fact that in modern conditions, the development of effective cyber security system is one of the urgent tasks of national security of Ukraine. It was determined that the Ministry of Internal Affairs of Ukraine during the whole period of independent development of the state had been constantly taking organizational and practical measures to ensure an effective response to this modern type of transnational crime.

It was investigated the genesis of the formation and development of organizational and legal support and forms of international cooperation of special divisions of the Ministry of Interior to combat cybercrime. On the basis of the study it is indicated some of the problems the solution of which will greatly increase the activity efficiency of Ukrainian cyberpolice departments of the National Police.

Among them: the need to improve the regulatory framework in certain areas of the fight against cybercrime activities; bringing it in line with international legal instruments in this field; improving the mechanism for rapid exchange of information in respect of persons detained on the territory of other countries for committing computer crimes; the establishment of effective international cooperation between the judicial authorities and the police in the investigation of cybercrime; systematic training of cyberpolice operatives by analysis and implement in practical activities the foreign experience and innovation on the methodology of detection and investigation of crimes in this area;

It is concluded that the urgent task is to develop a corresponding «road map» for the fight against cybercrime by all law enforcement agencies in Ukraine, based on the fact that the fight against this modern form of crime should be one of their most important functions.

Keywords: crimes in the sphere of high technologies, cybercrime, international cooperation and law enforcement agencies.

Надійшла до редколегії 15.09.2016