КІБЕРПОЛІЦІЯ УКРАЇНИ

ДЕМЕДЮК Сергій Васильович - начальник Управління боротьби з кіберзлочинністю МВС України

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

УДК ***351.749***

В данной статье рассмотрены концептуальные аспекты создания киберполиции Украины, главной целью которой является организация эффективного противодействия проявлениям киберпреступности и обеспечение действенного влияния на оперативную обстановку в сфере общественных информационных отношений. Изложены предложения о принципах неотложного реформирования соответствующих подразделений органов внутренних дел, функций центрального и региональных офисов киберполиции, организации подготовки квалифицированных кадров, способных результативно предотвращать, пресекать и расследовать киберпреступления.

Ключові слова: міліція, поліція, органи внутрішніх справ, кіберзлочини, кіберполіція, концепція реформування.

Вступ

Необхідність реформування системи Міністерства внутрішніх справ України вже давно ні в кого не викликає сумнівів. Про необхідність створення поліції в Україні давно і багато говориться, дискутують усі – і політики, і громадські діячі, й пересічні громадяни. Але як це зробити?

Частина людей вважає, що необхідні кардинальні зміни – звільнити усіх, хто знехтував честю міліціонера, а на їхнє місце взяти нових людей, які будуватимуть в Україні нову поліцію. Інші вважають, що практично неможливо знайти 172 тисячі нових правоохоронців, які зможуть докорінно змінити існуючу систему.

На думку експертів, до основних шляхів здійснення реформування української міліції в поліцію відносяться:

– розробка критеріїв оцінки працівників;

– зміна системи підготовки кадрів;

– створення мобільних груп поліції;

– підняття зарплат правоохоронцям [1].

Для подолання негативних явищ, що існують в органах внутрішніх справ України, і досягнення оптимальної та ефективної моделі їхньої побудови Концепцією першочергових заходів реформування системи Міністерства внутрішніх справ (далі – Концепція), що була затверджена 22.10.2014 Кабінетом Міністрів України, передбачено здійснити комплекс організаційних і практичних заходів, спрямованих на розбудову Міністерства внутрішніх справ як цивільного органу європейського зразка та формування в найближчій перспективі поліції як основного виконавця заходів забезпечення безпеки населення [2].

Проблеми реформування органів внутрішніх справ розглядалися у наукових роботах С. М. Алфьорова, В. С. Березняка, В. В. Єфімова, Н. В. Камінської, В. О. Криволапчука, С. В. Кушнарьова, В. В. Криж-

ної, А. В. Самотуги, М. О. Свіріна, Ю. М. Коцюбинської, О. О. Титаренко, Д. В. Гопфалова, М. І. Македона, О. В. Юхимчука та інших.

На сучасному етапі розвитку людства, у час переходу суспільства на нову стадію розвитку – від індустріального до інформаційного, однією з найважливіших соціальних проблем, обумовленої негативними факторами інформатизації, є протидія правопорушенням у сфері суспільних інформаційних відносин. У науково-популярній літературі такі правопорушення одержали узагальнюючі визначення – «комп'ютерна злочинність» або «кіберзлочинність» [3].

Кіберзлочинність є новітнім соціальним явищем, що активно поширюється по всьому світу. Під кіберзлочинністю розуміються кримінальні правопорушення, механізм підготовки, вчинення або приховування яких передбачає використання електронно-обчислювальних машин (комп'ютерів), телекомунікаційних систем, комп'ютерних мереж і мереж електрозв'язку, а також інші кримінальні правопорушення, учинені з їх використанням.

Характерним для кіберзлочинності є те, що організовані злочинні угруповання дедалі частіше прагнуть використовувати Інтернет і новітні інформаційно-комп'ютерні технології для досягнення своїх кримінальних цілей. В умовах зовнішньої агресії на сході та півдні України, відкритості кордонів та єдиного світового інформаційного простору виникає потенційна загроза поширення в Україні таких небезпечних явищ, як кіберекстремізм та кібертероризм.

Протягом останнього десятиліття спостерігаються загальносвітові тенденції до глобалізації соціально-економічних, політичних та інформаційних процесів, а також конвергенції в телекомунікаційних мережах, яка обумовила глибоке проникнення високих інформаційних технологій у життєдіяльність суспільства.

З метою забезпечення ефективної протидії таким негативним проявам більшість розвинутих держав світу побудували свою політику в правоохоронній сфері шляхом створення окремих відомств чи служб, що спеціалізуються на протидії міжнародній кіберзлочинності (США – (Federal Bureau of Investigation), Великобританія – (National Crime Agency), Китай – (People's Police), Японія – (National Police Agency), Франція – (Office central de lutte contre la criminalite liee aux technologies de l'information et de la communication) [4].

У силу свого географічного розташування (транзитний пункт між цивілізованою та більш заможною Західною Європою і менш розвинутими та цивілізованими Східною Європою й Азією) Україна в усі часи привертала увагу до себе як плацдарм для розгортання тієї чи іншої діяльності, в тому числі й протиправної.

Зокрема, лише за вісім місяців 2015 р. правоохоронними органами України було зафіксовано понад 20 тис. незаконних операцій з платіжними картками фізичних осіб, що спричинило збитків на суму близько 500 млн. грн. Це лише ті факти, які вдалося зафіксувати і встановити [6]

Саме тому важко переоцінити актуальність питання боротьби з кіберзлочинністю для нашої держави. Створення нових механізмів з протидії даним правопорушенням сьогодні, як ніколи, є виправданим кроком.

Слід відзначити, що в Стратегії національної безпеки України до основних напрямів державної політики національної безпеки України у сфері забезпечення кібербезпеки і безпеки інформаційних ресурсів відноситься розвиток спроможностей правоохоронних органів щодо розслідування кіберзлочинів [7, п. 4.12].

У затвердженій 22.10.2015 розпорядженням Кабінету Міністрів України «Стратегії розвитку органів внутрішніх справ України» до переліку довгострокових заходів, спрямованих на реформування МВС та органів внутрішніх справ, відноситься також реформування підрозділу по боротьбі з кіберзлочинністю, зазначивши основним напрямком діяльності попередження та протидію кримінальним правопорушенням, пов'язаним з кібератаками та втручання в роботу інформаційних систем, виключивши такі напрямки

роботи підрозділу, як протидія гральному бізнесу, протидія шахрайствам і легалізації (відмиванню) доходів, одержаних від зазначених вище кримінальних правопорушень, протидія злочинам у сфері інтелектуальної власності [7]

У цих умовах постає завдання швидкого та якісного реформування підрозділів МВС України, задіяних у протидії кіберзлочинності та підготовки для них кваліфікованих кадрів, здатних на належному рівні забезпечити правопорядок у сфері використання інформаційно-телекомунікаційних систем, попереджувати та оперативно виявляти хакерські атаки на сервери державних установ, забезпечувати безпеку функціонування державних і відомчих електронних обліків та баз даних тощо.

Враховуючи зазначене вище, можна говорити про нагальну потребу створення в Україні так званої кіберполіції.

Метою створення кіберполіції є організація ефективної протидії проявам кіберзлочинності та забезпечення дієвого впливу на оперативну обстановку в зазначеній сфері. Для цього є доцільним створення в структурі кримінальної поліції Національної поліції України окремого міжрегіонального підрозділу, орієнтованого на виявлення та припинення найбільш небезпечних і резонансних форм транснаціональної організованої кіберзлочинності.

Кіберполіція повинна стати складовою частиною кримінальної поліції Національної поліції України, що складається з Департаменту кіберполіції (центральний офіс кіберполіції) – структурного міжрегіонального підрозділу та його територіальних управлінь із широкими аналітичними та оперативно-тактичними повноваженнями, котрий спеціалізується на попередженні, виявленні, припиненні та розкритті кримінальних правопорушень, механізм підготовки, вчинення або приховування яких передбачає використання електронно-обчислювальних машин (комп'ютерів), телекомунікаційних систем, комп'ютерних мереж і мереж електрозв'язку, а також інших кримінальних правопорушень, учинених з їх використанням.

При цьому компетенція кіберполіції має бути обмежена виявленням та документуванням протиправної діяльності як національних регіональних, міжрегіональних, так і транснаціональних організованих злочинних груп (далі – ОЗГ).

Слід зазначити, що виокремлення кіберзлочинності в окрему категорію правопорушень є настільки ж закономірним і виправданим як і необхідність формування особливого підходу до протидії цим напрямам протиправної діяльності, адже виявлення та документування всіх цих злочинів вимагає відповідної кваліфікації працівників Національної поліції, розуміння ними механізмів учинення правопорушень з міжнародною складовою, джерел доказової інформації, напрямів та способів документування таких протиправних дій, налагодження та підтримання міжнародного співробітництва з іноземними правоохоронцями, здатність і навички в проведенні комплексу комп'ютерно-технічних досліджень та кваліфікованих технічних заходів.

Організація ефективної протидії злочинам міжнародного характеру вимагає й окремого підходу до формування інфраструктури та оцінки результатів діяльності спеціалізованого підрозділу в цій сфері.

Водночас суттєвого реформування потребує і підхід до розгортання діяльності служби в регіонах держави, особливо в контексті адміністративної реформи, скорочення кількості особового складу, обмежених людських та матеріальних ресурсів, а також труднощів з фінансуванням.

Очевидним є той факт, що в рамках існуючої структури та компетенції регіональних органів однакового підходу до розподілу службових завдань, оцінювання роботи, а також з урахуванням динаміки розвитку транснаціональної кіберзлочинності, географії протиправної діяльності, регіонального розподілу злочинних елементів, їх міжрегіональних та міжнародних злочинних зв'язків боротьба з таким масштабним і складним явищем не буде ефективною. В означеному (такому) випадку головна мета створення цих підрозділів – знешкодження міжрегіональних органі-

зованих злочинних груп та національних осередків міжнародних ОЗГ залишиться без реалізації. Натомість, матиме місце (як це надзвичайно часто буває сьогодні в роботі територіальних підрозділів боротьби з кіберзлочинністю) так званий ефект «биття по хвостах», що виявляється в документуванні не цілісних злочинних мереж, а лише їх окремих учасників, і майже ніяк не впливає на оперативну обстановку в цілому.

Концепція створення кіберполіції — це розробка арсеналу сучасних інструментів удосконалення роботи системи Національної поліції України взагалі. Створення кіберполіції передбачає таке реформування та розвиток підрозділів МВС, що забезпечить підготовку та функціонування висококваліфікованих працівників в експертних, оперативних та слідчих підрозділах поліції, задіяних у протидії кіберзлочинності, та здатних застосовувати на високому професійному рівні новітні технології в оперативно-службовій діяльності.

При створенні кіберполіції доцільне синхронне, поетапне перетворення існуючої моделі підрозділу до новітнього державного органу правозахисного призначення на прикладі сучасного європейського типу, який за своїми функціями забезпечуватиме охорону прав, свобод і законних інтересів особи та держави; за технічними та професійними можливостями матиме змогу миттєвого реагування на кіберзлочини та кіберзагрози, а також, відповідно до кращих світових стандартів, здійснюватиме міжнародну співпрацю зі знешкодження транснаціональних злочинних угруповань в означеній (у цій) сфері.

У процесі реформування необхідно вирішити наступні завдання:

1) у структурі кримінальної поліції Національної поліції України створити Департамент кіберполіції (центральний офіс кіберполіції), до складу якого входитимуть територіальні управління (регіональні офіси кіберполіції), що забезпечуватимуть захист та охорону прав і свобод особи та держави, а також надаватимуть якісні правоохоронні та правозахисні функції;

2) створити механізм координації та взаємодії діяльності кіберполіції з іншими підрозділами Національної поліції та правоохоронними органами держави;

3) удосконалити та модернізувати професійну підготовку фахівців у вищих навчальних закладах та науково-дослідних установах МВС з метою отримання висококваліфікованих спеціалістів, здатних виконувати свої професійні обов'язки в умовах нового етапу розвитку органів внутрішніх справ та у сфері протидії сучасним високотехнологічним кіберзлочинам;

4) упровадити в діяльність Національної поліції України функціонування програмно-технічних комплексів (терміналів) зворотного зв'язку для прийому звернень та заяв про кіберзлочини, що дозволить у режимі реального часу здійснювати оперативне реагування для їх запобігання, припинення або розкриття;

5) передбачити участь фахівців кіберполіції у формуванні та реалізації державної політики щодо попередження та протидії кримінальним правопорушенням, механізм підготовки, вчинення або приховування яких передбачає використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, а також іншим кримінальним правопорушенням, учиненим з їх використанням;

Запропонований далі підхід до концепції створення кіберполіції засновано на принципах всезагального управління якістю, що представляє собою систему управління, засновану на отриманні позитивного результату з погляду суспільства при реагуванні на ту чи іншу подію, та визначається як зосереджений на якості, сфокусований на громадськості, заснований на фактах, керований командний процес, спрямований на планомірне досягнення стратегічної мети організації шляхом постійного покращення якості її діяльності.

Основними принципами такої концепції є:

1) постійність мети (удосконалення матеріально-технічної бази лабораторії експертно-технічних досліджень та підбір висококваліфікованих експертів, у тому чис-

лі із спеціальною освітою в області такого роду досліджень);

2) нова філософія впровадження в діяльність поліції заходів, що здійснюватиме кіберполіція (здійснення на базі підрозділу повного циклу оперативно-розшукових та оперативно-технічних заходів, що входять до компетенції служби — комп'ютерна розвідка, зняття та розшифровка трафіка, перехоплення мережевих з'єднань, відновлення даних);

3) адекватне реагування комплектування кіберполіції у регіонах відповідно викликам сьогодення (виключно регіональні офіси кіберполіції із штатним розкладом, який відповідатиме місцевій криміногенній обстановці).

Головним завданням кіберполіції є забезпечення реалізації державної політики у сфері боротьби з кіберзлочинністю.

Функції центрального та регіональних офісів кіберполіції:

1) визначення, розроблення та забезпечення реалізації комплексу організаційних і практичних заходів, спрямованих на попередження та протидію кримінальним правопорушенням, які віднесені до компетенції центрального та регіональних офісів;

2) у межах своїх повноважень, відповідно до законів, що становлять правову основу діяльності Національної поліції, вживання необхідних оперативно-розшукових заходів щодо викриття причин і умов, які сприяють вчиненню кримінальних правопорушень, віднесених до компетенції кіберполіції;

3) здійснення попередження правопорушень у сфері високих технологій, а також інформування населення стосовно новітніх видів кіберзлочинів;

4) організація та контроль діяльності регіональних офісів кіберполіції щодо виконання вимог національного законодавства і нормативних актів Національної поліції та МВС з питань розслідування кримінальних правопорушень, а також дотримання вимог дисципліни та законності, режиму секретності;

5) створення та розробка організаційно-методичних рекомендацій для підвищення професійного рівня та поінформованості діяльності підрозділів Національної поліції та населення;

6) забезпечення спільно з приватним сектором створення автоматизованих інформаційних систем та масивів даних для потреб оперативного реагування та розслідування кримінальних правопорушень;

7) організація виконання доручень прокуратури та слідчих органів щодо проведення слідчих (розшукових) дій та негласних слідчих (розшукових) дій у кримінальних провадженнях, які належать до компетенції кримінальної поліції;

8) здійснення контролю у межах компетенції та відповідно до законодавства за виконанням відповідних доручень кіберполіцією, координація їх діяльності в цій сфері;

9) здійснення поточного і перспективного планування роботи кіберполіції та проведення комплексних і цільових оперативно-профілактичних заходів на території держави чи окремих регіонів, у тому числі за участю правоохоронних органів інших країн;

10) розроблення проектів нових законодавчих та інших нормативних актів, а також надання пропозицій щодо вдосконалення існуючої законодавчої бази у сфері протидії кіберзлочинам;

11) впровадження програмних засобів для систематизації та аналізу інформації про криміногенні процеси та стан боротьби з кримінальними правопорушеннями за пріоритетними напрямами діяльності кіберполіції на загальнодержавному та регіональному рівнях, оцінка результатів за окремими показниками оперативно-службової діяльності кіберполіції;

12) адміністрування програмно-технічних комплексів, аналіз та систематизація даних про кримінальні правопорушення, учинені у сфері та з використанням високих технологій, що надходитимуть від громадян каналами call-центрів, електронними листами та терміналами зворотнього зв'язку;

13) обробка запитів та оперативної інформації від закордонних правоохоронних органів, що надходитиме каналами

Національної цілодобової мережі контактних пунктів з реагування на кіберзлочини;

14) у рамках міжнародної співпраці та на виконання міжнародно-правових доручень здійснення належного, висококваліфікованого надання допомоги закордонним колегам за визначеними напрямками роботи, у тому числі в рамках функціонування цілодобової контактної мережі для надання невідкладної допомоги при провадженні кримінальних правопорушень, пов'язаних з комп'ютерними системами та даними, переслідуванні осіб, які підозрюються або обвинувачуються в їх учиненні, а також збирання доказів в електронній формі;

14) забезпечення функціонування локальних експертних лабораторій та мобільних груп швидкого реагування, призначених для залучення до місць вчинення кримінальних правопорушень, з метою зняття даних з носіїв інформації.

Кіберполіція в межах компетенції здійснюватиме взаємодію з:

1) уповноваженим Верховної Ради України з прав людини;

2) органами і підрозділами Генеральної прокуратури, Служби безпеки, Державної прикордонної служби, Службою фінансового моніторингу, Національним антикорупційним бюро України та іншими державними органами та установами, а також органами місцевого самоврядування;

3) підрозділами центрального органу та територіальними підрозділами Національної поліції, науково-дослідними установами Національної поліції;

4) іншими правоохоронними органами та приватним сектором у сфері боротьби з кіберзлочинністю;

5) правоохоронними органами іноземних держав, а також міжнародними установами та організаціями, до компетенції яких віднесені питання попередження та протидії кіберзлочинам.

З урахуванням міжрегіонального характеру діяльності кіберзлочинців територію держави доцільно створити регіональні офіси кіберполіції.

Керівники регіональних офісів кіберполіції та їх заступники будуть призначатися, а структура та штатна чисельність – затверджуватися наказом керівника Національної поліції за поданням керівника кримінальної поліції.

Соціальний та правовий захист працівників кіберполіції, як вид державного захисту, повинний передбачити систему правових, матеріальних, фінансових та соціальних заходів щодо забезпечення належних умов проходження служби в органах внутрішніх справ, забезпечення гідних умов життя працівників кіберполіції та членів їх родин, запобігання та захисту від несприятливих умов здійснення професійної діяльності.

Реалізацію концепції потрібно проводити за наступними етапами:

1) утворення в складі кримінальної поліції Національної поліції Департаменту кіберполіції;

2) розроблення та затвердження Положення про Департамент кіберполіції;

3) вивчення та впровадження позитивного досвіду розвинутих європейських держав на напрямку протидії кіберзлочинам;

4) створення нової моделі регіональних офісів кіберполіції;

5) забезпечення сталого функціонування Департаменту та регіональних офісів кіберполіції в співробітництві з відповідними міжнародними інституціями та національними органами протидії кіберзлочинності розвинутих держав світу.

Висновки

Підсумовуючи, зазначимо, що загальне керівництво та контроль за процесом виконання концепції повинно здійснюватися Міністром внутрішніх справ України. Основою даля контролю є концепція про створення кіберполіції та програма її реалізації.

Література

1. Реформа міліції: розігнати чи перевчити? [Електронний ресурс] // UA: Перший. – 15 квітня 2015. – Режим доступу: http://1tv.com.ua/news/channel/67750.

АНОТАЦІЯ

У даній статті розглянуті концептуальні аспекти створення кіберполіції України, головною метою якої є організація ефективної протидії проявам кіберзлочинності та забезпечення дієвого впливу на оперативну обстановку в сфері суспільних інформаційних відносин. Викладено пропозиції щодо принципів невідкладного реформування відповідних підрозділів органів внутрішніх справ, функцій центрального та регіональних офісів кіберполіції, організації підготовки кваліфікованих кадрів, здатних результативно запобігати, припиняти та розслідувати кіберзлочини.

SUMMARY

The present article deals with conceptual aspects of formation of Cyber police of Ukraine, which main purpose is to organize effective cybercrime counteraction and to ensure effective influence on the background in the area of information relations in the society. The article provides propositions as to the principles of the immediate reformation of the correspondent law enforcement subdivisions, functions of the central and regional offices of the cyber police and the organization of training of qualified personnel who will be able to prevent, counteract and investigate cybercrimes successfully.

2. Концепція першочергових заходів реформування системи Міністерства внутрішніх справ [Електронний ресурс] // МВС України: офіційний веб-сайт. – Режим доступу: http://www.mvs.gov.ua/mvs/control/main/uk/publish/article/1221414.

3. Бєляков К. І. Питання визначення правопорушень, що вчинюються з використанням інформаційних технологій: аксіоматичний підхід // Боротьба з організованою злочинністю і корупцією (теорія і практика). – К., 2004. – № 9. – С. 179–186.

4. Бандурка О. М. Оперативно-розшукова компаративістика: монографія / О. М. Бандурка, М. М. Перепелиця, О. В. Манжай та ін. – Х. : Золота миля, 2013. – 352 с.: іл.

6. Брифінг начальника Управління боротьби з кіберзлочинністю МВС України Сергія Демедюка [Електронний ресурс] // МВС України: офіційний веб-сайт. – 10.09.2015. – Режим доступу: http://www.mvs.gov.ua/mvs/control/main/uk/publish/article/1628496.

7. Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України» : указ Президента України від 26.05.2015 № 287/2015 [Електронний ресурс]. – Режим доступу: http://zakon5.rada.gov.ua/laws/show/287/2015