Список використаних джерел:

1. Про імплементацію Угоди про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським Співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони : Розпорядження Кабінету Міністрів України від 17.09.2014 р. № 847-р. *Урядовий кур'єр*. 2014. № 185.
2. Концепція публічного управління у сфері містобудівної діяльності : аналітична записка. Київ, 2019. 369 с.
3. Стукаленко О.В. Адміністративно-правове забезпечення будівельної галузі: теоретико-правові та праксеологічні засади : дис. ... докт. юрид. наук : 12.00.07. Дніпропетровськ, 2016. 500 с.
4. APEC Building Codes, Regulations, and Standards. Minimum, Mandatory and Green. APEC Sub-committee on Standards and Conformance, 2013. 227 s.
5. Савіцький Р.Є. Зарубіжний досвід здійснення архітектурно-будівельного контролю та можливості його впровадження в Україні. *Visegrad journal on human rights*. 2015. 3/2. С. 106–110.
6. Слончак В.В. Нагляд та контроль за виконанням законодавства у будівельній галузі: міжнародний досвід. *Порівняльно-аналітичне право*. 2017. № 3. С. 154–156.
7. Visscher H. BUILDING CONTROL IN FIVE EUROPEAN COUNTRIES. Delft University Press. 1993. URL: file:///C:/Users/Jetro/Downloads/8501_467_G.pdf. Ст. 52.
8. Code de la construction et de l'habitation. Article L151-1. Modifié par LOI n°2018–1021 du 23 novembre 2018. URL: <https://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT00006074096&idArticle=LEGIARTI000006824360&dateTexte=&categorieLien=cid>.
9. Інформаційна сторінка з сайту уряду Великобританії. URL: <https://www.gov.uk/government/collections/approved-documents>.
10. Довідник для членів Консультативного комітету будівельних правил. 23 р. URL: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/721530/180629_BRAC_membershandbook_2018.pdf.
11. Інформаційна сторінка Консультативного комітету з питань будівельних правил Великобританії. URL: <https://www.gov.uk/government/organisations/building-regulations-advisory-committee/about>.
12. Building control. Department for Communities and Local Government. 2019. URL: https://www.planningportal.co.uk/info/200128/building_control.

УДК [351.741:004] (477)
DOI <https://doi.org/10.32844/2618-1258.2019.3-1.42>

ШЕВЧУК Г.В.

**ОСОБЛИВОСТІ ДІЯЛЬНОСТІ ДЕПАРТАМЕНТУ КІБЕРПОЛІЦІЇ
НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ**

У статті проаналізовано особливості Департаменту кіберполіції Національної поліції України. Визначено, що Департамент кіберполіції Національної поліції України є міжрегіональним територіальним органом Національної поліції України, що входить до складу кримінальної міліції Національної поліції та відповідно до законодавства України забезпечує здійснення державної політики у сфері протидії кіберзлочинності, організовує та здійснює оперативно-розшукову діяльність. Підкреслюється, що особливістю кіберполіції є здійснення заходів щодо боротьби з кіберзлочинністю. Визначено, що остання в узагальненій формі є злочином у так званому віртуальному просторі. Специфіка цього виду злочину полягає в тому,

© ШЕВЧУК Г.В. – кандидат юридичних наук, доцент кафедри поліцейського права (Національна академія внутрішніх справ)

що підготовка та вчинення злочину здійснюється, коли злочинець практично не віддаляється від робочого місця за комп'ютером, а вчинення таких злочинів є доступним широкому колу осіб, оскільки комп'ютерна техніка постійно дешевшає. Такі злочини можуть бути вчинені з будь-якого місця і в будь-якому населеному пункті, а предмети злочинного нападу можуть бути за тисячі миль від винного. Крім того, під час здійснення слідчих дій досить важко виявити, зафіксувати та вилучити криміналістичну інформацію, щоб використовувати її надалі як доказ. Все це, звісно, є перевагою для кіберзлочинців. Підкреслюється, що особливість кіберполіційної діяльності пов'язана з визначенням її основних завдань та функцій. Зокрема, до завдань кіберполіції належать такі: реалізація державної політики у сфері протидії кіберзлочинності; інформування населення заздалегідь про появу новітніх кіберзлочинів; впровадження програмних засобів для систематизації та аналізу інформації про кіберінциденти, кіберзагрози та кіберзлочинність; протидія кіберзлочинності. Зроблено висновок, що діяльність Департаменту кіберполіції Національної поліції України потребує вдосконалення законодавства та врегулювання конфліктів у законі. Також доцільно визначити правову основу діяльності, принципи, повноваження, компетенцію, виявити особливості моніторингу кіберзагроз, визначити механізми взаємодії з приватним сектором у створенні автоматизованих інформаційних систем та масивів даних для потреб оперативного реагування та розслідування кіберзлочинів.

Ключові слова: діяльність, Департамент, кіберполіція, Національна поліція, Україна.

The article analyzes the features of the Department of Cyberpolicies of the National Police of Ukraine. It is determined that the Department of Cyberpolicies of the National Police of Ukraine is an interregional territorial body of the National Police of Ukraine, which is part of the structure of the criminal police of the National Police and, in accordance with Ukrainian legislation, ensures the implementation of state policy in the field of combating cybercrime, organizes and carries out operative-search activities in accordance with the legislation. It is emphasized that the peculiarity of cyberpolice activities is the implementation of measures to combat cybercrime. It is determined that the latter in a generalized form is a crime in the so-called virtual space. The specificity of this type of crime lies in the fact that the preparation and commission of a crime is carried out, practically moving away from the workplace, crimes are available; since computer technology is constantly cheaper; Crimes can be committed from anywhere in any locality, and objects of criminal assault may be thousands of miles away from the perpetrator. In addition, it is rather difficult to detect, capture and remove forensic-meaningful information when performing investigative actions to use it as evidence. All this, of course, is an advantage for cybercriminals. It is emphasized that the peculiarity of cyberpolice activity is related to the definition of its main tasks and functions. In particular, the tasks of the cyberpolice include: implementation of state policy in the field of countering cybercrime; advance informing the population about the emergence of the latest cybercrime; Implementation of software tools for the systematization and analysis of information on cyber incidents, cyber threats and cybercrime; counteracting cybercrime. It is concluded that the activities of the Department of Cyberpolicies of the National Police of Ukraine require legislative improvement and conflict resolution of law. It is also expedient to define: the legal basis of activity, principles, powers, competence, to determine the features of monitoring cyber threats, to determine the mechanisms of interaction with the private sector to create automated information systems and data sets for the needs of rapid response and investigation of cybercrime.

Key words: activity, Department, cyber police, National Police, Ukraine.

Вступ. Події, що відбулися 2014 року, стали переломним етапом не лише для правоохоронної системи, але й у цілому для органів державної влади. Складна фінансова та економічна криза, низький рівень ефективності державних органів та неефективність діяльності колишньої

міліції – усе це стало потужним каталізатором суттєвих змін та державних перетворень в країні. Особливу роль у вказаному процесі змін відігравали саме органи внутрішніх справ, оскільки від рівня їхньої діяльності залежав стан внутрішнього правопорядку та стабільності.

Початок реформування правоохоронної системи – це початок функціонування принципово нових органів та підрозділів із оновленими завданнями та функціями. Водночас з огляду на стан злочинності у період 2014–2015 рр. маємо змогу спостерігати появу нових небезпек та загроз, що прийшли у суспільне життя із мережі «Інтернет». Варто пригадати досить негативні наслідки від славнозвісних ігор смерті – «Синій Кит» тощо. Через нерациональне використання інформаційних технологій та мережі «Інтернет» все частіше почали з'являтися нові шкідливі наслідки, що значною мірою порушували права та законні інтереси громадян. На противагу викладеному перед новоствореною Національною поліцією України постало завдання – створити новий орган, що буде боротися з кіберзлочинністю.

XXI століття – це ера інтенсивного розвитку та активного використання інформаційних технологій і комп'ютерних систем. Інформаційні технології сьогодні пронизують майже усі сфери суспільного життя, а діяльність органів публічного права все більшою мірою залежить від їх дієвості. Активне використання інформаційних технологій ми спостерігаємо кожного дня. Це здійснення платіжних операцій, перегляд стрічки новин, комп'ютерні ігри, активність у соціальних мережах тощо. Але майже ніколи ми не замислюємося над тим, які загрози можуть нести в собі ті чи інші вебсайти та ресурси, оскільки останні сьогодні стали невід'ємною складовою частиною життя сучасної людини.

Потенційні та реальні загрози кіберпростору, правопорушення в мережі «Інтернет» прийнято йменувати кіберзлочинністю, що є досить новим для сучасності явищем та правовою категорією. Саме тому з метою запобігання та протидії кіберзлочинності як новітньому віртуальному явищу в Україні був створений спеціалізований орган – кіберполіція.

Діяльність кіберполіції в Україні подекуди має колізійний характер. Це пов'язано із законодавчою неврегульованістю діяльності кіберполіції. Сьогодні у зв'язку з приведенням вітчизняного законодавства України у відповідність до законодавства країн Європейського Союзу питання вдосконалення правового регулювання діяльності органів та підрозділів Національної поліції України є найбільш актуальним, що зумовлено реформуванням правоохоронної системи в Україні.

Постановка завдання. Метою статті є дослідження особливостей діяльності Департаменту кіберполіції Національної поліції України.

Питання діяльності Національної поліції України неодноразово ставали предметами наукових досліджень та дискусій. До числа науковців, що висвітлювали це питання у своїх працях, можна віднести О.М. Бандурку, В.В. Березу, Е.А. Гетьмана, С.М. Гусарова, Д.В. Демедюка, І.В. Клименка, О.М. Ключова, В.К. Колпакова, А.Т. Комзюка, В.В. Маркова, О.М. Музичука, Т.О. Проценко, О.Ю. Салманова, В.В. Сокурена, А.А. Стародубцева, В.О. Тімашова, В.В. Чумака, О.А. Шевчук та деяких інших.

Дослідження вказаних науковців мають важливе наукове та практичне значення, а їх висновки та рекомендації сприяли та сприятимуть подальшому вдосконаленню законодавства в адміністративно-правовій сфері, а також у правозастосовній практиці підрозділів кіберполіції. Однак вимоги сьогодення потребують проведення більш детального адміністративно-правового дослідження особливостей діяльності кіберполіції в Україні.

Результати дослідження. Через інтенсивний розвиток інформаційних технологій все частіше починають з'являтися нові загрози кіберпростору, що потребують своєчасного реагування з боку відповідних спеціалізованих органів. У даному контексті стан кібербезпеки України далекий від оптимального, про що свідчить вітчизняна статистика та ті негативні наслідки, які ми маємо змогу спостерігати у засобах масової інформації. На противагу негативним тенденціям, що розгортаються у кіберпросторі, у складі Національної поліції України був створений міжрегіональний територіальний орган зі статусом юридичної особи публічного права – кіберполіція України.

Департамент кіберполіції Національної поліції України є міжрегіональним територіальним органом Національної поліції України, який входить до структури кримінальної поліції Національної поліції та відповідно до законодавства України забезпечує реалізацію державної політики у сфері боротьби з кіберзлочинністю, організовує та здійснює оперативно-розшукову діяльність [1]. Визначальним фактором, що характеризує кіберполіцію, є боротьба з кіберзлочинністю. Тому вважаємо за доцільне дослідити сутність даної категорії.

Категорія «кіберзлочинність» відображена у вітчизняному офіційному нормативному обігу, зокрема й у підписаній Україною Конвенції про кіберзлочинність. Проте вказана Конвенція не містить визначення категорії «кіберзлочинність», а лише окреслює її обсяг, надаючи перелік видів правопорушень, які туди входять. Законодавство України також не містить визначення такого виду злочинів.

Взагалі «кібер» (“cyber”, що походить від “cybernetics”) – префікс, який додають до повсякденних слів, щоб показати їхню причетність до інтернету, комп’ютерів тощо. А кібернетику (cybernetics, від грец. “cybernos” – «кермовий») зараз розглядають як науку про зв’язки, керування й організацію об’єктів різноманітної природи. У сучасних умовах інформаційно-телекомунікаційні технології (далі – ІТТ) є основними засобами забезпечення вказаних процесів.

Кіберзлочинність – це злочинність у так званому віртуальному просторі. Віртуальний простір можна визначити як інформаційний простір, що моделюється за допомогою комп’ютера, у якому перебувають відомості про особу, предмети, факти, події, явища і процеси, представлені в математичному, символічному або будь-якому іншому виді, а також рухи, що перебувають у процесі, у локальних і глобальних комп’ютерних мережах, або відомості, що зберігаються в пам’яті будь-якого фізичного або віртуального пристрою, а також іншого носія, спеціально призначеного для їхнього зберігання, обробки й передачі [2, с. 32].

Отже, семантичний аналіз поняття «кіберзлочинність» вказує на те, що інтегруючим елементом складових частин даного явища є ІТТ, які різним чином задіяні при вчиненні відповідних діянь. Основною сутнісною ознакою кіберзлочину є те, що це є діяння, сама можливість вчинення якого витікає із особливих можливостей інформаційних технологій, які використовуються з метою завдання шкоди суспільним відносинам.

Специфіка даного виду злочинності полягає у тому, що готування та скоєння злочину здійснюється, коли злочинець практично не відходить від робочого місця, а вчинення злочинів є доступним для широкого кола осіб, оскільки комп’ютерна техніка постійно дешевшає. Такі злочини можна скоювати з будь-якої точки земної кулі і в будь-якому населеному пункті, а об’єкти злочинних зазіхань можуть перебувати за тисячі кілометрів від злочинця. Крім того, доволі складно виявити, зафіксувати і вилучити криміналістично значущу інформацію при виконанні слідчих дій для використання її як речового доказу. Усе це, безумовно, є перевагами для кіберзлочинців [3]. З огляду на це було створено кіберполіцію України як центральний орган, що покликаний здійснювати заходи боротьби із кіберзлочинністю.

Ведучи мову про здійснення заходів боротьби зі злочинністю, ми говоримо про особливості діяльності кіберполіції, оскільки остання є спеціально уповноваженим органом для здійснення особливого виду діяльності. Зазначимо, що поняття «діяльність» розуміється як свідомий, вольовий процес активних дій певного суб’єкта, що спрямовані на досягнення певної мети. Комплекс таких дій в рамках певної діяльності йменуються завданнями. Тобто завдання діяльності кіберполіції в Україні – це конкретизація та інтеграція способів вирішення певних ситуацій. З огляду на специфіку діяльності кіберполіції до основних завдань Департаменту кіберполіції віднесено:

- 1) реалізацію державної політики у сфері протидії кіберзлочинності;
- 2) завчасне інформування населення про появу новітніх кіберзлочинів;
- 3) впровадження програмних засобів для систематизації та аналізу інформації про кіберінциденти, кіберзагрози та кіберзлочини;
- 4) реагування на запити закордонних партнерів, що надходять каналами Національної цілодобової мережі контактних пунктів;
- 5) участь у підвищенні кваліфікації працівників поліції щодо застосування комп’ютерних технологій у протидії злочинності;
- 6) участь у міжнародних операціях та співпраця в режимі реального часу;
- 7) протидію кіберзлочинам:
 - а) у сфері використання платіжних систем:
 - скімінгу (шімінгу) – незаконному копіюванню вмісту треків магнітної смуги (чіпів) банківських карток;
 - кеш-трепінгу – викраденню готівки з банкомату шляхом встановлення на шатер банкомату спеціальної утримуючої накладки;
 - кардінгу – незаконним фінансовим операціям з використанням платіжної картки або її реквізитів, не ініційованим або не підтвердженим її держателем;
 - несанкціонованому списанню коштів з банківських рахунків за допомогою систем дистанційного банківського обслуговування;

- б) у сфері електронної комерції та господарської діяльності:
 - фішингу – виманюванню у користувачів інтернету їхніх логінів та паролів до електронних гаманців, сервісів онлайн-аукціонів для переказування або обміну валюти тощо;
 - онлайн-шахрайству – заволодінню коштами громадян через інтернет-аукціони, інтернет-магазини, сайти та телекомунікаційні засоби зв'язку;
- в) у сфері інтелектуальної власності:
 - піратству – незаконному розповсюдженню інтелектуальної власності в інтернеті;
 - кардшарінгу – наданню незаконного доступу до перегляду супутникового та кабельного TV;

- г) у сфері інформаційної безпеки:
 - соціальній інженерії – технології управління людьми в інтернет-просторі;
 - шкідливому програмному забезпеченню (англ. “malware”) – створенню та розповсюдженню вірусів і шкідливого програмного забезпечення;
 - протиправному контенту – контенту, який пропагує екстремізм, тероризм, наркоманію, порнографію, культ жорстокості і насильства;
 - рефайлінгу – незаконній підміні телефонного трафіку [4].

Із завданнями, у яких конкретизується мета діяльності кіберполіції, у нерозривному взаємозв'язку перебувають функції, що є відображенням завдань у реальній дійсності. Дослідники визначають функції як окремий вид виконавчо-розпорядчої діяльності. Функції відображають зміст діяльності суб'єкта, значною мірою визначаючи його сутність і соціальне призначення. Дослідження функцій має прикладне значення. Це зумовлено їх визначальним впливом на структуру та повноваження кожного конкретного органу виконавчої влади [5].

Отже, функції охоплюють комплекс способів, методів, прийомів і дій, які забезпечують виконання певних завдань і досягнення цілі. Функції поліції реалізують уповноважені суб'єкти (посадові особи), які несуть юридичну відповідальність за обґрунтованість і законність конкретних дій [6, с. 125].

Департамент кіберполіції України виконує такі основні функції:

- визначає, розробляє та забезпечує реалізацію комплексу заходів, спрямованих на попередження та протидію кримінальним правопорушенням у сфері протидії кіберзлочинності;
- у межах своїх повноважень уживає необхідних оперативно-розшукових заходів щодо викриття причин і умов, які призводять до вчинення кримінальних правопорушень у сфері протидії кіберзлочинності;
- уживає передбачених чинним законодавством заходів зі збирання й узагальнення інформації стосовно об'єктів сфери телекомунікацій, інтернет-послуг, банківських установ і платіжних систем з метою попередження, виявлення та припинення кримінальних правопорушень;
- організовує та контролює діяльність підпорядкованих підрозділів кіберполіції щодо виконання вимог законодавства України у сфері протидії кіберзлочинності;
- проводить серед населення роз'яснювальну роботу з питань дотримання законодавства України у сфері використання новітніх технологій, а також захисту та протидії кіберзагрозам у повсякденному житті;
- забезпечує формування й наповнення інформаційних масивів даних, автоматизованих інформаційних систем відповідно до потреб службової діяльності;
- організовує виконання у межах компетенції доручень слідчого, прокурора щодо проведення слідчих (розшукових) дій та негласних слідчих (розшукових) дій у кримінальних провадженнях [7].

На нашу думку, вказані функції не втратили своєї актуальності. З огляду на це важливо визначити такі функції за напрямками діяльності: адміністративну, профілактичну, функцію боротьби з кіберзлочинністю, оперативно-розшукову, кримінальну та кримінально-процесуальну, а також деякі інші. Це зумовлено відсутністю законодавчого врегулювання питань, що стосуються завдань та функцій кіберполіції й особливостей її діяльності.

Також вважаємо слушною позицію С.В. Демедюка і В.В. Маркова, які до основних функцій кіберполіції відносять здійснення попередження правопорушень у сфері високих технологій, а також інформування населення стосовно новітніх видів кіберзлочинів; створення та розробку організаційно-методичних рекомендацій для підвищення професійного рівня та поінформованості діяльності підрозділів Національної поліції та населення; забезпечення спільно з приватним сектором створення автоматизованих інформаційних систем та масивів даних для потреб оперативного реагування та розслідування кримінальних правопорушень; організацію 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; здійснення контролю у межах компетенції та відповідно до законодавства за виконанням відповідних доручень кіберполіцією, координацію їх діяльності в цій сфері; 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, переслідування осіб, які підозрюються або обвинувачуються в їх учиненні, а також збирання доказів в електронній формі; 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) [8, с. 91–92].

Висновки. Таким чином, сучасний стан суспільних відносин, що складаються в мережі «Інтернет», характеризується інтенсивним розвитком з дещо негативними наслідками та появою нових видів злочинів. У вказаних процесах особливе місце повинні зайняти заходи із протидії кіберзлочинності як новому віртуальному явищу, що завдає шкоди охоронюваному законом правам, свободам та інтересам громадян.

Заходи боротьби з кіберзлочинністю повинні мати сьогодні комплексний характер та бути спрямованими на мінімізацію ризиків віртуальних загроз та на підвищення засобів і способів захисту у віртуальному просторі. У вказаних процесах кіберполіція стає центральним суб'єктом боротьби з кіберзлочинністю. Водночас практика реалізації завдань та функцій кіберполіції показує неефективність деяких законодавчих норм. Спостерігаються прогалини у праві, що мають своїм наслідком неспроможність кіберполіції якісно та ефективно виконувати покладені на неї законом повноваження.

Враховуючи викладене, зазначимо, що сьогодні головним завданням є розробка та затвердження основного закону, який би регулював діяльність кіберполіції в Україні – Закону України «Про кіберполіцію України». Вказаний нормативно-правовий акт повинен відображати основні положення органу поліції та висвітлювати його особливості.

Отже, слід чітко визначити основні завдання кіберполіції України, серед яких можна виділити захист прав, свобод та законних інтересів осіб, протидію кіберзлочинності, а також подолання негативних тенденцій віртуального простору. Поряд із завданнями слід визначити функції кіберполіції, які умовно можна було б поділити на зовнішні та внутрішні, оскільки кіберзлочинність не обмежується територіальними межами країни, адже вона займає дещо іншу площину.

Також вважаємо за доцільне визначити правову основу діяльності, принципи, повноваження, компетенцію, особливості моніторингу кіберзагроз, механізми взаємодії з приватним сектором у створенні автоматизованих інформаційних систем та масивів даних для потреб оперативного реагування та розслідування кіберзлочинів.

Підкреслимо, що в сучасних умовах проведення на території України Операції Об'єднаних Сил вважаємо вказаний напрям наукових досліджень перспективним з урахуванням досвіду діяльності кіберполіції в інших країнах Європи.

Список використаних джерел:

1. Про підрозділ. Кіберполіція в Україні / сайт. URL: <https://cyberpolice.gov.ua/contacts/>.
2. Біленчук Д.П. Кібершахраї – хто вони? *Міліція України*, 1999. № 7–8. С. 32–34.
3. Кіберзлочинність в Україні. Science-Community / сайт. URL: <https://www.science-community.org/ru/node/16132>.
4. Кіберполіція (Україна) / Вікіпедія : матеріали із Вільної Енциклопедії / сайт. URL: [https://uk.wikipedia.org/wiki/%D0%9A%D1%96%D0%B1%D0%B5%D1%80%D0%BF%D0%BE%D0%BB%D1%96%D1%86%D1%96%D1%8F\(%D0%A3%D0%BA%D1%80%D0%B0%D1%97%D0%BD%D0%B0\)](https://uk.wikipedia.org/wiki/%D0%9A%D1%96%D0%B1%D0%B5%D1%80%D0%BF%D0%BE%D0%BB%D1%96%D1%86%D1%96%D1%8F(%D0%A3%D0%BA%D1%80%D0%B0%D1%97%D0%BD%D0%B0)).
5. Проневич О.С. Функції поліції (міліції): нормативно-доктринальна інтерпретація. URL: <http://radnuk.info/statti/565-pranoohor/14779-2011-01-19-02-35-05.html>.
6. Крищенко А.Є. Завдання та функції національної поліції як учасника адміністративно-правових відносин у сфері забезпечення публічної безпеки і порядку. *Науковий вісник Національної академії внутрішніх справ*. 2017. № 2 (103). С. 121–128.
7. Департамент кіберполіції Національної поліції. Головне управління. База знань / сайт. URL: <http://wiki.1551.gov.ua/pages/viewpage.action?pageId=18842098>.
8. Демедюк С.В., Марков В.В. Кіберполіція України. Наше право. *Кримінальне право, кримінальний процес та криміналістика*. 2015. № 6. С. 87–93.