- суспільний розголос корупційних справ та притягнення до відповідальності корупціонерів, справи яких і досі залишаються без вироку;
- застосування та повноцінне введення в дію антикорупційної реформи «Україна-2020».

Список використаних джерел:

1. Мельник М.І. Корупція: загальна характеристика, проблеми кваліфікації, удосконалення законодавства. Київ : Парлам. вид-во, 2015. 256 с.
2. Невмержицький Є.В. Корупція в Україні: причини, наслідки, механізми протидії : монографія. Київ : КНТ, 2014. 368 с.
3. Про запобігання корупції : Закон України від 14.10.2014 р. № 1700-VII. База даних «Законодавство України» / ВР України. URL: <https://zakon.rada.gov.ua/laws/show/1700-18> (дата оновлення 18.02.2020)
4. Мовчан А.В. Актуальні проблеми протидії корупції. *Вісник кримінального судочинства*. 2018. № 1. С. 116–119.
5. Знизити рівень корупції. Київ : Річний звіт Трансперенсі Інтернешнл Україна, 2018. С. 7–10.
6. Костецький М. Залучення до боротьби з Корупцією. Робота з викривачами. Київ : Розбудова спроможності громадських організацій у регіонах, 2019. С. 37–39.
7. Ефективність запобігання та протидії корупції в Україні: проблеми та перспективи. URL: <http://www.vidkryti-ochi.org.ua/2015/02/blog-post.html> (дата звернення 18.02.2020).
8. Про стратегію сталого розвитку «Україна 2020» : Указ Президента України від 2015. URL: <https://zakon1.rada.gov.ua/laws/show/5/2015> (дата звернення 18.02.2020).
9. Литвиненко В.І., Пригунов П.Я. Концепція адміністративно-правового забезпечення протидії корупції в Україні: наук.-аналіт. доп. Київ : ДП «Вид. дім «Персонал», 2016. 89 с.

УДК 340.113:004.056

DOI <https://doi.org/10.32844/2618-1258.2019.5-1.24>

ВЕСЕЛОВА Л.Ю.

**ПОНЯТІЙНО-ТЕРМІНОЛОГІЧНИЙ АПАРАТ У СИСТЕМІ
АДМІНІСТРАТИВНО-ПРАВОВОГО ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ**

У статті розкривається проблема понятійно-термінологічного апарату у системі адміністративно-правового забезпечення кібербезпеки. Розглядаються різні підходи та погляди на досліджувану тематику різних вітчизняних вчених. Аналізується зміст нормативно-правових актів, які стосуються сфери забезпечення кібербезпеки, в аспекті їх понятійно-термінологічного наповнення та узгодження між собою. Акцентується увага на тому, що законодавча неврегульованість кібернетичного простору викликає занепокоєність багатьох вчених і практиків. Особливо це стосується відсутності правових норм, що сприяють підвищенню відповідальності провайдерів і власників сайтів за розміщення недостовірної та свідомо шкідливої інформації (у вигляді встановлення відповідних заходів відповідальності), а також закріплюють механізм впливу на недобросовісних суб'єктів правовідносин у кіберсфері. З аналізу наукових праць фахівців з означеної проблематики, вивчення правової регламентації забезпечення кібербезпеки робиться висновок, що національна безпека України істотно залежить від забезпечення кібербезпеки. Зазначається, що у сфері кібербезпеки є низка проблем, які не можуть бути повноцінно вирішені традиційними засобами та на які слід звернути увагу суспільству та відповідним державним органам. Масштабні кіберзлочини, що зачіпають усі сторони життя суспільства, в основі яких лежать новітні методи здійснення кібератак, а

© ВЕСЕЛОВА Л.Ю. – кандидат юридичних наук, доцент кафедри адміністративної діяльності поліції (Одеський державний університет внутрішніх справ)

також управління суспільною свідомістю, вимагають системного підходу до створення комплексної національної системи кібербезпеки, здатної протистояти цим загрозам. Процес формування механізму адміністративно-правового регулювання забезпечення та організації кібербезпеки стикається з низкою проблем, зумовлених інноваційним характером кібербезпекової проблематики. Зокрема, сутнісними проблемами стають термінологічна невизначеність і неготовність чинної правової бази протистояти новим загрозам. У таких умовах важливим є системний підхід до формування понятійно-термінологічного апарату адміністративно-правового регулювання забезпечення та організації кібербезпеки, який забезпечить адекватне його змістовне наповнення, відповідність вимогам, що висувуються до правової термінології, а також погодження з термінологією діючого українського законодавства та міжнародних актів.

Ключові слова: кіберсистема, об'єкт захисту, кіберзагроза, технологічні можливості.

The article focuses on the problem of the conceptual apparatus in the system of administrative-legal support of cybersecurity. Different approaches and views on the researched subject of different national scientists are considered. The content of regulatory acts related to the field of cybersecurity is analyzed in terms of their conceptual and terminological content and harmonization with each other. Attention is drawn to the fact that the legislative unsettling of cyber space is a concern many scholars and practitioners. This concerns the absence of legal rules that increase the responsibility of providers and site owners for providing inaccurate and deliberately harmful information (in the form of appropriate liability measures), as well as for establishing a mechanism for influencing unscrupulous cyberspace entities. From the analysis of the scientific works in this field, the study of the legal regulation of cybersecurity and the aforementioned research, it is concluded that Ukraine's national security depends significantly on the provision of cybersecurity. It is noted that in the field of cybersecurity there are a number of problems that cannot be fully addressed by traditional means and which should be brought to the attention of the public and relevant state bodies. Large-scale cybercrimes that affect all aspects of society, are based on the latest methods of implementation of cyberattacks, as well as public awareness management, require a systematic approach to creation a comprehensive national cybersecurity system capable of countering these threats. The process of forming a mechanism for administrative and legal regulation of cybersecurity provision and organization faces a number of problems caused by the innovative nature of cybersecurity issues. In particular, terminological uncertainty and the unwillingness of the current legal framework to withstand new threats become essential problems. In such circumstances, a systematic approach to formation of the conceptual and terminological apparatus of administrative-legal regulation of providing and organizing cybersecurity is important, which will ensure its adequate substantive content, compliance with the requirements for legal terminology, as well as compliance with the terminology of the current Ukrainian legislation and international legislation.

Key words: cybersystem, object of protection, cybernetic threat, technological capabilities.

Вступ. Сучасні інформаційні технології, локальні та глобальні комп'ютерні мережі надають можливість доступу до великої кількості інформації не лише органам державної влади, але й пересічним громадянам. Разом з тим щоденне збільшення обсягів даних та інформації, що обробляються, спонукає до необхідності їх захисту від протизаконних посягань, що своєю чергою ставить першочерговим завданням перед правоохоронними органами ефективно та професійно діяти щодо забезпечення кібербезпеки. У цьому напрямі надзвичайно важливо розуміти загрози кіберпростору, серед яких центральне місце посідає кіберзлочинність, і дослідження яких здійснюють провідні світові експерти та міжнародні організації.

Проблемам кіберзлочинності приділили багато уваги такі вітчизняні та зарубіжні вчені, як О.А. Баранов, М.М. Безкоровайний, В. Голубев, О.Є. Користні, С.В. Мельник, Ю.М. Оніщенко, А.Л. Татузов, А.В. Тонконогий, О.О. Тихомиров, І.Г. Чекунов, О.О. Черноног, А. Щетилов та інші. Заслугують на увагу дослідження вітчизняних вчених щодо питання протидії гібридним

загрозам, зокрема інформаційним та кібернетичним, які достатньо широко та комплексно охоплюють проблеми національної безпеки [1; 2]. Разом з тим наукові праці містять різні підходи та погляди на досліджувану тематику, що, звичайно, є позитивним моментом для розвитку науки, але не зовсім зрозумілим для здійснення практичної діяльності, зокрема, в аспекті адміністративно-правового регулювання забезпечення та організації кібербезпеки в Україні, а також у частині формування понятійно-термінологічного апарату кібербезпеки.

Постановка завдання. Метою статті є здійснення аналізу наявного понятійно-термінологічного апарату у системі адміністративно-правового забезпечення кібербезпеки та проблем, які виникають у зв'язку з термінологічною невизначеністю в кібернетичній сфері.

Результати дослідження. Загалом в Україні термін «кібербезпека кіберпростору» з'явився зовсім нещодавно, хоча питання усвідомлення небезпеки кіберзлочинності ставилося вже тоді, коли наша держава приєдналася до міжнародної «Конвенції про кіберзлочинність». Але термінологічне визначення понять у цій сфері викликало суперечність не лише серед науковців, але й серед практиків. Багато хто з фахівців у терміни «інформаційна безпека» та «кібербезпека» вкладає дуже схоже трактування та формально відрізняють додаванням понять «кіберпростір», як об'єкту захисту, «кіберзагрози» тощо. Кібербезпека розглядається як безпека специфічного виду інформації – управлінської інформації. Приставка «кібер» виділяє «клас кіберсистем, які використовуються для вирішення задач управлінського характеру». «В кіберсистемах на перше місце виділяється вимоги неперервності й стійкості управління. А ці вимоги можуть бути виконані лише за умови забезпечення доступності, цілісності та конфіденційності вхідної інформації [3]». Для остаточного розуміння цих термінів ще потрібні додаткові дослідження.

Сьогодні актуальною є класифікація кібернетичних загроз, яка наведена за результатами досліджень “ENISA Threat Landscape 2013” у Річному звіті Cisco щодо безпеки за 2014 р. [4; 5]: “Drive-By” експлойти; хробаки (worms)/трояни; ін'єкція коду; kits: exploit kits; ботнет; відмова в обслуговуванні (denial-of-service (DoS) атака); фішинг і фармінг; компрометація конфіденційної інформації; rogware (шахрайське програмне забезпечення)/scareware (псевдоантивірусні програми); спам; цільові атаки; фізична крадіжка / втрата / пошкодження; крадіжка особистих даних (Identity Theft); abuse of information leakage (зловживання витоком інформації); search engine poisoning (отруєння пошукових систем); система доменних імен Domain Name system (DNS); rogue certificates (підробні сертифікати).

Під кібернетичною загрозою розуміють дестабілізуючий фактор (чинник) негативного впливу на об'єкт безпеки, що здійснюється шляхом використання технологічних можливостей кіберпростору. До кіберзагроз належать загрози порушення конфіденційності, цілісності, авторства, спостережності та доступності інформації, також загрози деструктивних інформаційно-психологічних впливів на свідомість, психологічний та психічний стан людини [6, с. 43]. А отже, кібернетичні загрози є сукупністю умов та факторів, що створюють небезпеку життєво важливим інтересам особистості, суспільства, держави в кібернетичному просторі. Реалізація загроз свідчить про неефективність функціонування системи управління всією національною безпекою і навпаки [7, с. 235].

Закон України «Про національну безпеку України» під загрозами національній безпеці визначає явища, тенденції і чинники, що унеможливають чи ускладнюють або можуть унеможливити чи ускладнити реалізацію національних інтересів та збереження національних цінностей України [6]. Відповідно до норм п. 3.7 Стратегії національної безпеки України, затвердженої Указом Президента України «Про рішення Ради національної безпеки і оборони України від 26 травня 2015 р. «Про Стратегію національної безпеки України» від 26 травня 2015 р. [8] загрозами кібербезпеці визначено: уразливість об'єктів критичної інфраструктури, державних інформаційних ресурсів до кібератак; фізична і моральна застарілість системи охорони державної таємниці та інших видів інформації з обмеженим доступом. Цікавим вбачається перелік загроз кібербезпеці, який визначено Стратегією забезпечення кібернетичної безпеки України [9]. Зокрема, нормами Указу Президента України «Про рішення Ради національної безпеки і оборони України від 20 травня 2016 року «Про Стратегічний оборонний бюлетень України»» визначено низку проблем функціонування сил оборони в умовах наявних та потенційних загроз, серед яких визначено неспроможність ефективно реагувати на зростаючу кількість та потужність кібератак та протистояти кіберзлочинності [10].-

Поняття «кіберзлочин» з'явилося досить недавно завдяки сполученню двох слів: «кібер» і «злочин» [11]. Термін «кібер» означає поняття кіберпростору (у літературі частіше зустрічаються терміни «віртуальний простір», «віртуальний світ») та інформаційний простір, що моделюється

за допомогою комп'ютера. Ми поділяємо думку О. Щетилова, який вважає, що кіберзлочини включають в себе «не тільки діяння, учинені в глобальній мережі Інтернет, а й в інформаційно-телекомунікаційній сфері, де інформація, інформаційні ресурси, техніка можуть виступати предметом злочинних посягань, середовищем, в якому скоєно правопорушення, і засобом або знаряддям злочину» [12]. На нашу думку, такий підхід є більш вдалим, оскільки він відповідає суті кібернетичного простору, утвореного на базі всіх можливих (локальних, глобальних) ІТМ, мережа Інтернет серед яких просто є переважною.

У Законі України «Про основні засади забезпечення кібербезпеки України» під кіберзлочином (комп'ютерним злочином) розуміється як суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України [13].

Заслугоює на увагу думка В.М. Бабакіна, який зазначає, що поняття «кіберзлочину» є поки незвичним для правоохоронних органів, проте злочинні дії, в яких використовується глобальна комп'ютерна мережа Internet, містять в собі велику суспільну небезпеку. Автор наголошує, що транснаціональний характер злочинності з використанням комп'ютерної мережі дає підстави вважати, що розробка спільної політики по основних питаннях повинна бути частиною будь-якої стратегії боротьби з кіберзлочинністю. Також певною мірою чинником, що сприяє зростанню цього нового виду злочинів, можна вважати відсутність належної взаємодії національних правоохоронних органів у питаннях попередження та розслідування таких видів злочинів [11].

Ураховуючи складність реальних проблем щодо боротьби з кіберзлочинністю на національному і міждержавному рівні однією з перших міжнародних угод з юридичних і процедурних аспектів розслідування кіберзлочинів стало прийняття Радою Європи 23 листопада 2001 р. Конвенції Ради Європи про кіберзлочинність [14]. Варто зазначити, що нормами Конвенції про кіберзлочинність передбачено координацію дій на національному та міждержавному рівнях щодо припинення несанкціонованого втручання в роботу комп'ютерних систем, незаконного перехоплення даних і втручання в комп'ютерні системи. Зокрема, важливим є те, що, сьогодні на структурі зазначеного документа ґрунтується найбільш поширена класифікація кіберзлочинів, яка є «еталоном» для наявних міжнародних та регіональних нормативно-правових актів, а також наукової практики. Відповідно, кіберзлочини поділено на п'ять груп: 1) кіберзлочини проти конфіденційності, цілісності та доступності комп'ютерних даних і систем, такі як незаконний доступ, незаконне перехоплення, втручання в дані, втручання в систему; 2) кіберзлочини, пов'язані з використанням комп'ютера як засобу скоєння злочинів, а саме як засобу маніпуляцій з інформацією (наприклад, комп'ютерне шахрайство та комп'ютерне підроблення); 3) кіберзлочини, пов'язані з контентом (змістом даних), тобто з вмістом даних, розміщених у комп'ютерних мережах (наприклад, кіберзлочини, пов'язані з дитячою порнографією); 4) злочини, пов'язані з порушенням авторського права і суміжних прав, при цьому встановлення таких правопорушень віднесено документом до компетенції національних законодавств держав; 5) кіберзлочини як акти расизму та ксенофобії, вчинені за допомогою комп'ютерних мереж, входять до п'ятої групи кіберзлочинів і зафіксовані в окремому протоколі [15, с. 4–5].

Варто звернути увагу на те, що деякі кіберзлочини нормами Конвенції про кіберзлочинність не виділено в окремі групи. В наукових колах ведуться дискусії щодо таких кіберзлочинів, які до цього часу викликають суперечки щодо необхідності гармонізації законодавства на міжнародному рівні з погляду техніки їх криміналізації. Це «кібертероризм» та використання кіберпростору в терористичних цілях. Державами та міжнародними організаціями вживаються зусилля щодо боротьби з терористичними організаціями, які використовують кіберпростір. Як приклад можна навести проект Clean IT, який існує на рівні Європейського Союзу та метою якого є боротьба з кібертероризмом. Але у зв'язку з відсутністю узгодженого визначення тероризму на міжнародному рівні у даному напрямку ускладняється, хоча і не заважає, боротьба з кібертероризмом. Тому нагальною та необхідною для всього міжнародного співтовариства є криміналізація кібертероризму як явища. Не можна поза увагою залишити ще одну категорію кіберзлочинів, а саме крадіжку, передачу і використання персональних даних з метою вчинення злочинів (identity theft), яка, хоча і не включена окремо в Конвенцію про кіберзлочинність, але отримала поширення після прийняття міжнародного документа. Деякі країни виділяють ці злочини в окрему категорію, інші вважають, що ці діяння підпадають під кілька статей кримінального законодавства [16, с. 33], що своєю чергою спонукає до виділення цього злочину в окрему групу та гармонізації міжнародного законодавства у цій сфері. 7 вересня 2005 року Україною ратифікована Конвенція

про кіберзлочинність, нормами якої передбачено поділ кіберзлочинів на категорії. Таким чином, вважається за доцільне вживати саме термін «кіберзлочини».

Дослідження у цій сфері дає підстави стверджувати, що правове та організаційне забезпечення кібербезпеки тісно пов'язано з проблемами нейтралізації негативних інформаційних впливів, протидія яким має здійснюватися не тільки на контентному, а й на технологічному рівнях. Одним із проявів негативних інформаційних впливів є намагання маніпулювати суспільною свідомістю, зокрема, шляхом поширення недостовірної інформації або упередженої інформації. Також відмічається використання ІКТ у цілях, не сумісних з завданнями підтримки міжнародної стабільності та безпеки: для придушення і підпорядкування інших держав [17, с. 37; 18, с. 110].

Особливої актуальності такі кіберзагрози набувають у сучасний період використання нових інформаційно-пропагандистських технологій, що може призводити до досить швидких змін режимів у різних країнах. Значної уваги потребує астротерфінг – штучне створення, формування громадської думки, фальшивих масових компаній, що створюють видимість вимоги великою кількістю громадян проведення певного політичного курсу або виступаючих проти нього.

З'являються нові види посягання не лише на державу, але й на добропорядних громадян. Одним з таких явищ, яке насамперед потребує адміністративно-правового регулювання, є кібердифамація (від латинського «порочити») – поширення за допомогою ЗМІ в мережі Інтернет-відомостей, що не відповідають дійсності, ганьблять честь, гідність, ділову репутацію, добре ім'я. Кіберзлочинами також є правопорушення економічного, політичного і етнодискримінаційного характеру, що виражаються у формі незаконної політичної боротьби (кібертероризмі, кіберекстремізмі), скоєнні шахрайських операцій у всіх сферах суспільної життєдіяльності, у тому числі у вигляді розміщення в Інтернеті, інших засобах електронної комунікації матеріалів, які пропагують радикальні ідеї національної та іншої переваги; інформації, що має свідомо шкідливий характер і стосується незаконної торгівлі зброєю, вибуховими речовинами, вибуховими пристроями, їх виготовлення; торгівлі людьми, людськими органами, наркотичними засобами, психотропними та сильнодіючими речовинами, рецептами з їх виробництва [19, с. 38]. У цьому контексті як нові види можливих внутрішніх і зовнішніх загроз у кібернетичній сфері можна назвати: ініціювання кібернетичних революцій; розповсюдження електронних вірусів, спаму, нелицензійних софт-програм, що не відповідає дійсності інформації; несанкціоноване проникнення на сайти; безконтрольність інформації кримінального характеру.

Законодавча неврегульованість кібернетичного простору викликає занепокоєність багатьох вчених та практиків. Особливо це стосується відсутності правових норм, що сприяють підвищенню відповідальності провайдерів і власників сайтів за розміщення недостовірної та свідомо шкідливої інформації (у вигляді встановлення відповідних заходів відповідальності), а також закріплюють механізм впливу на недобросовісних суб'єктів правовідносин у кіберсфері. З аналізу наукових праць фахівців з означеної проблематики, вивчення правової регламентації забезпечення кібербезпеки та зазначеного вище дослідження можна зробити висновок, що національна безпека України істотно залежить від забезпечення кібербезпеки. В процесі еволюції технічного та кібернетичного прогресу ця залежність дедалі зростатиме. Крім того, законодавче регулювання відносин у кіберпросторі не може ні випередити розвиток зростання кіберзлочинності, ні навіть йти з ним у ногу, що є неминучим процесом. Разом з тим національна законодавча база у сфері забезпечення кібербезпеки має правові колізії та прогалини, що тягне за собою несвоєчасне реагування правоохоронних органів на факти заподіяння шкоди інформації, інформаційно-телекомунікаційних мереж, репутації громадян тощо.

Висновки. Таким чином, у сфері кібербезпеки існує низка проблем, які не можуть бути повноцінно вирішені традиційними засобами та на які слід звернути увагу суспільству та відповідним державним органам. Масштабні кіберзлочини, що зачіпають усі сторони життя суспільства, в основі яких лежать новітні методи здійснення кібератак, а також управління суспільною свідомістю, вимагають системного підходу до створення комплексної національної системи кібербезпеки, здатної протистояти цим загрозам. Процес формування механізму адміністративно-правового регулювання забезпечення та організації кібербезпеки стикається з низкою проблем, зумовлених інноваційним характером кібербезпекової проблематики. Зокрема, сутнісними проблемами стають термінологічна невизначеність і неготовність чинної правової бази протистояти новим загрозам. У таких умовах важливим є системний підхід до формування понятійно-термінологічного апарату адміністративно-правового регулювання забезпечення та організації кібербезпеки, який забезпечить адекватне його змістовне наповнення, відповідність вимогам, що висуваються до правової термінології, а також погодження з термінологією діючого українського законодавства та міжнародних актів.

Список використаних джерел:

1. Ковальчук Т.І., Користін О.Є., Свиридчук Н.П. Гібридні загрози у секторі цивільної безпеки в Україні. *Наука і правоохоронна*. 2019. № 3 (45). С. 69–79.
2. Kovalchuk T. I., Korystin O. Y., Sviridyuk N. P. Hybrid threats in the civil security sector in Ukraine. *Проблеми законності*. 2019. Вип. 147. С. 163–175.
3. Архипов А. Приставка кибер-: все ли очевидно? *Захист інформації*. 2016. Том 18, №3. С. 203–209.
4. Годовой отчет Cisco по безопасности за 2014 год. URL: http://www.cisco.com/assets/global/RU/pdfs/executive_security/sc-1casr2014_cte_lig_ru_35330.pdf.
5. ENISA Threat Landscape. URL: <https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape/enisa-threat-landscape-mid-year-2013>.
6. Мельник С.В. До проблеми формування понятійно-термінологічного апарату кібербезпеки. *Актуальні проблеми управління інформаційною безпекою держави*: зб. матер. наук.-практ. конф. (Київ, 22 березня 2011 р.). Київ: Вид-во НА СБ України, 2011. Ч. 2. С. 43–48.
7. Семенов В.М., Гиркіна О.О. Сучасні аспекти забезпечення інформаційної безпеки України. *Науковий вісник Херсонського державного університету: Серія: Юридичні науки*. Вип. 5., Т. 2. С. 234–240.
8. Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України»: Указ Президента України від 26 травня 2015 р. № 287/2015. URL: <https://zakon.rada.gov.ua/laws/show/287/2015>.
9. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України»: Указ Президента України від 15 берез. 2016 р. № 96/2016. URL: <https://zakon5.rada.gov.ua/laws/show/96/2016>.
10. Про рішення Ради національної безпеки і оборони України від 20 травня 2016 року «Про Стратегію оборонний бюлетень України»: Указ Президента України від 06 червня 2016 року № 240/2016. URL: <https://zakon.rada.gov.ua/laws/show/240/2016#n10>.
11. Бабакін В.М. Особливості міжнародного співробітництва при розслідуванні кіберзлочинів. *Форум права*. 2011. № 4. С. 27–30. URL: <http://Avww.nbuv.gov.ua/e-journals/FP/2011-4/11bvmpk.pdf>
12. Щетилов А.Б. Некоторые проблемы борьбы с киберпреступностью и кибертерроризмом. *Информатизация и информационная безопасность правоохранительных органов*: материалы XI межд. конф. Москва, 2002. С. 132–136.
13. Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 року № 2163-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2163-19>.
14. Конвенція Ради Європи про кіберзлочинність: Міжнародний документ від 23 листоп. 2001 р. URL: https://zakon.rada.gov.ua/laws/show/ru/994_575/ed20161217.
15. Албул С.В., Туляков В.О., Підгородинський В.М. Кваліфікація комп'ютерних злочинів: навчально-методичний посібник. ОНЮА. Одеса : Фенікс, 2007. 28 с.
16. Баранов О.А. Про тлумачення та визначення поняття «кібербезпека». *Правова інформатика*. 2014. № 2 (42). С. 132–138.
17. Цехан Д.М. Використання високих інформаційних технологій в оперативно-розшуковій діяльності органів внутрішніх справ : монографія. Одеса : Юридична література, 2011. 216 с.
18. Протидія відмиванню коштів: міжнародні стандарти, зарубіжний досвід, адміністративно-правові, кримінологічні, кримінально-правові, криміналістичні засади та система фінансового моніторингу в Україні. Підручник. За ред. Користіна О.Є. Київ : Скіф, 2015. 984 с.
19. Чекунов И.Г. Киберпреступность: понятие и классификация. *Российский следователь*. 2012. № 2. С. 37–43.