УДК 342.9
DOI https://doi.org/10.32850/2414-4207.2019.11-2.15

ОРГАНИ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ В НАЦІОНАЛЬНІЙ СИСТЕМІ КІБЕРБЕЗПЕКИ

Ткач Тетяна Віталіївна,
аспірант кафедри поліцейського права
(Національна академія внутрішніх
справ, м. Київ, Україна)

Метою статті є визначення поняття національної системи кібербезпеки й установлення ролі в цій системі Національної поліції. Так, в статті визначено поняття національної системи кібербезпеки на основі його відмежування від поняття системи забезпечення кібербезпеки; встановлено роль Національної поліції в національній системі кібербезпеки. Визначено, що національну систему кібербезпеки доцільно розуміти як сукупність усіх компонентів, за допомогою яких досягається стан захищеності життєво важливих інтересів людини й громадянина, суспільства й держави під час використання кіберпростору, за якого забезпечуються сталий розвиток інформаційного суспільства й цифрового комунікативного середовища, своєчасне виявлення та нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі та запобігання виникненню таких – тобто кібербезпека. Зроблено висновок, що Національну систему кібербезпеки доцільно розуміти як сукупність усіх компонентів, за допомогою яких досягається кібербезпека, а саме: 1) суб'єктів і здійснюваних ними заходів (система забезпечення кібербезпеки); 2) об'єктів кібербезпеки й кіберзахисту як частини системи, які зазнають впливу з боку суб'єктів; 3) норм права, що є основою для забезпечення кібербезпеки через установлення зв'язків між суб'єктом та об'єктом (прямих і зворотних). Водночас підхід до обмеження основних суб'єктів національної системи кібербезпеки й суб'єкта їх координації виключно інституціями держави доцільний для перегляду з точки зору необхідності врахування потреб всіх суб'єктів забезпечення кібербезпеки в Україні. Доцільним для організації є центр взаємодії й координації, що об'єднував би всіх суб'єктів забезпечення кібербезпеки на засадах партнерства. Роль Національної поліції в забезпеченні кібербезпеки визначається поняттям кіберзлочинності, що є новим видом правопорушень, виявлення, припинення й розкриття яких, а також запобігання й протидія вчиненню яких визначає адміністративно-правовий статус Національної поліції як суб'єкта забезпечення кібербезпеки. Однак не обмежує, оскільки найголовнішим є уповноваження на інформування громадян про безпеку в кіберпросторі.

Ключові слова: кібербезпека, національна система кібербезпеки, забезпечення кібербезпеки, кіберпростір, кіберзахист.

BODIES OF THE NATIONAL POLICE OF UKRAINE IN THE DOMESTIC CYBERSECURITY SYSTEM

Tkach Tetiana Vitaliivna,
Postgraduate Student at the Department
of Police Law
(National Academy of Internal Affairs,
Kyiv, Ukraine)

The purpose of the article is to define the concept of the national cybersecurity system and to establish the role of the National Police in this system. Thus, the article defines

the concept of national cybersecurity system on the basis of its separation from the concept of cybersecurity system; the role of the National Police in the national cybersecurity system has been established. It is determined that the national cybersecurity system should be understood as a set of all components through which the state of protection of vital interests of man and citizen, society and the state during the use of cyberspace, which ensures sustainable development of information society and digital communication environment, timely detection, prevention and neutralizing real and potential threats to Ukraine's national security in cyberspace – that is, cybersecurity. It is concluded that the National Cyber Security System should be understood as a set of all components through which cybersecurity is achieved: 1) subjects and measures taken by them (cybersecurity system); 2) objects of cybersecurity and cybersecurity as part of the system affected on the part of the subjects; 3) the rules of law that are the basis for cybersecurity through the establishment of links between the subject and the object: direct and reverse. At the same time, the approach to limiting the main actors of the national cybersecurity system and the subject of their coordination exclusively by state institutions is appropriate for revision in terms of the need to take into account the needs of all actors in cybersecurity in Ukraine. It is appropriate for the organization to have a center of interaction and coordination, which would unite all actors of cybersecurity on a partnership basis. The role of the National Police in cybersecurity is defined by the concept of cybercrime, which is a new type of crime, detection, prevention, termination, counteraction and disclosure of which determines the administrative and legal status of the National Police as a cybersecurity entity. However, it is not limiting, as the authority to inform citizens about cyber security is paramount.

Key words: cybersecurity, national cybersecurity system, cyberspace, cybersecurity.

Постановка проблеми. Розвиток інформаційно-комунікаційних технологій та інформаційно-телекомунікаційних систем створив передумови для формування кіберпростору як якісно нового середовища для встановлення зв'язків суб'єктів правовідносин. Це середовище відрізняється від фізичного простору низкою специфічних ознак, які забезпечують ряд переваг порівняно з комунікацією в просторі фізичному (швидкість комунікації без затрат часу на фізичний контакт, можливість з будь-якої точки планети стати учасником певних відносин, оперативність вирішення питань тощо). Однак попри велику кількість переваг перенесення відносин у кіберпростір має й негативні наслідки. Стрімкий розвиток віртуального середовища, новизна його властивостей є основою для порушення прав суб'єктів правовідносин, які з фізичного простору перенесли свої комунікації в простір віртуальний. А тому поряд з поняттям кіберпростору з'являється поняття кібербезпеки, забезпеченням якої займаються не лише суб'єкти, які безпосередньо користуються кіберпростором, але й спеціально уповноважені.

Аналіз останніх досліджень і публікацій. Проблеми формування й розвитку системи кібербезпеки, як і запобігання й протидія кіберзлочинам неодноразово ставали приводом для наукових досліджень, з-поміж яких для написання статті взято праці таких учених, як В.Л. Бурячок, С.А. Буяджи, І.О. Валюшко, І.В. Діордіца, С.В. Демедюк, В.В. Марков, В.Б. Толубко, С.В. Толюпа, В.О. Хорошко, та інших.

Метою статті є визначення поняття національної системи кібербезпеки й установлення ролі Національної поліції в цій системі.

Виклад основного матеріалу. Органи Національної поліції України згідно з нормами Закону України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 р. № 2163-VIII [1] є одними з основних елементів національної системи кібербезпеки, яку Україна наразі активно формує відповідно до світових тенденцій організації кіберзахисту. Від визначення до втілення на практиці функціонування

система кібербезпеки є тим вирішальним фактором, діяльність якого є передумовою досягнення стану захищеності життєво важливих інтересів людини й громадянина, суспільства й держави під час використання кіберпростору. Як указують М.М. Присяжнюк і Є.І. Цифра, Україна потребує створення адекватної системи безпеки у світі, де виклики національній безпеці все частіше набувають рис, відмінних від традиційних загроз. Активність з боку провідних держав світу в кіберпросторі, глибинні зміни у ставленні до внутрішньої інформаційної політики, формування потужних транснаціональних злочинних груп, що спеціалізуються на злочинах у кіберпросторі, обумовлюють необхідність вироблення рекомендацій щодо коротко- й довгострокових пріоритетів трансформації вітчизняного безпекового сектора [2, с. 65].

Враховуючи той факт, що система національної безпеки є багатокомпонентною, В.А. Ліпкан й І.В. Діордіца вбачають необхідність існування спеціальної підсистеми, мета функціонування якої полягала б у забезпеченні функціонування й розвитку цієї системи, тобто в забезпеченні життєздатності її системотвірних елементів, зокрема національних інтересів людини, суспільства, держави. Науковці ведуть мову про систему забезпечення національної безпеки й національну систему кібербезпеки [3, с. 174]. І одразу звертаємо увагу на розбіжність у підходах до формування категорій.

Система забезпечення національної безпеки ставиться поряд з національною системою кібербезпеки, під якою законодавець розуміє сукупність суб'єктів забезпечення кібербезпеки та взаємопов'язаних заходів різної спрямованості щодо регулювання кіберпростору, про що йдеться в ч. 1 ст. 8 Закону України «Про основні засади забезпечення кібербезпеки України» від 5 жовтня 2017 р. № 2163-VIII [1]. Однак аналіз останнього визначення з точки зору тих складових частин, які визначаються структурними елементами національної системи кібербезпеки, вказує на доцільність використання конструкції «національна система забезпечення кібербезпеки» для позначення тієї структури, яка наведена в указаній статті. Певні суб'єкти й здійснювані ними заходи характеризують діяльнісний підхід до формування поняття, а тому доцільно використовувати й дефініцію (конструкцію), яка б позначала певні дії з боку визначеної системи.

Якщо змінити підхід до поняття, закріпленого у ч. 1 ст. 8 Закону України «Про основні засади забезпечення кібербезпеки України» [1], то постає питання категорії національної системи кібербезпеки. Відповідне визначення можливо надати, виходячи з поняття системи управління, де суб'єкт управління пов'язується зв'язками впливу на об'єкт управління, отримуючи від останнього зворотний зв'язок. Суб'єкт державного управління не може існувати без відповідних керованих об'єктів, і тільки разом вони утворюють систему управління, доводить І.П. Ковалевич. Така система, як вважає науковець, повинна охоплювати організацію й функціонування керівної системи; зв'язки керівної системи з керованими об'єктами; структуру керованої системи, елементи якої безпосередньо сприймають державно-управлінський вплив або беруть участь у його формуванні [4].

Таким чином, національну систему кібербезпеки, як нам видається, доцільно розуміти як сукупність усіх компонентів, за допомогою яких досягається стан захищеності життєво важливих інтересів людини й громадянина, суспільства й держави під час використання кіберпростору, за якого забезпечуються сталий розвиток інформаційного суспільства й цифрового комунікативного середовища, своєчасне виявлення й нейтралізація реальних і потенційних загроз національній безпеці України в кіберпросторі та запобігання виникненню таких, – тобто кібербезпека (п. 5 ч. 1 ст. 1 Закону України «Про основні засади забезпечення кібербезпеки України» [1]). До таких компонентів доцільно, на наш погляд, віднести: 1) суб'єктів і здійснювані ними заходи

(система забезпечення кібербезпеки); 2) об'єкти кібербезпеки й кіберзахисту як частини системи, які зазнають впливу з боку суб'єктів; 3) норми права, що є основою для забезпечення кібербезпеки через установлення зв'язків між суб'єктом й об'єктом (прямих і зворотних).

Повертаючись до складових національної системи кібербезпеки України, які на сьогодні визначені в Законі України «Про основні засади забезпечення кібербезпеки України», звертаємо увагу на належність усіх перерахованих основних суб'єктів до числа органів держави: Державна служба спеціального зв'язку та захисту інформації України, Національна поліція України, Служба безпеки України, Міністерство оборони України й Генеральний штаб Збройних Сил України, розвідувальні органи, Національний банк України [1]. Відведення ролі координатора дій національної системи кібербезпеки з усіма суб'єктами, які безпосередньо здійснюють у межах своєї компетенції заходи з забезпечення кібербезпеки (ч. 4 ст. 5 Закону України «Про основні засади забезпечення кібербезпеки України» [1]), Раді національної безпеки й оборони України, що також є органом держави при Президенті України (ч. 1 ст. 1 Закону України «Про Раду національної безпеки і оборони України» від 5 березня 1998 р. № 183/98-ВР [5]). Така позиція законодавця не повною мірою відповідає викликам і загрозам, які сьогодні постають перед системою забезпечення кібербезпеки; не повною мірою враховує потреби всіх учасників відносин у кіберпросторі; не забезпечує ефективну взаємодію та співпрацю законодавчо виділених основних суб'єктів забезпечення кібербезпеки (які в підсумку представляють державу) з іншими суб'єктами забезпечення кібербезпеки, до числа яких входять численні громадські структури, основною метою діяльності яких є забезпечення кібербезпеки, і ті суб'єкти, що через здійснювану ними діяльність забезпечують кібербезпеку, хоча проголошують інші основні завдання й мету свого утворення (наприклад, отримання прибутку, надання адміністративних послуг тощо).

І от роль указаних суб'єктів у забезпеченні кібербезпеки зростає, а про ефективність взаємодії наразі не йдеться. Здійснивши ґрунтовне дослідження адміністративно-правового регулювання кібербезпеки України І.В. Діордіца обґрунтовує, що кібернетична функція держави через власну іманентну організаційну природу має реалізовуватися в межах сформованої й ефективної національної системи кібербезпеки з залученням усіх центральних органів виконавчої влади, недержавних, у тому числі волонтерських, організацій кожного окремого суб'єкта кібербезпекових правовідносин [6, с. 11]. Одним із ключових питань організації ефективної роботи національних систем кібербезпеки науковець визначає налагодження взаємодії між компетентними державними органами, які є суб'єктами кібернетичної безпеки, та здійснення координації такої діяльності [3, с. 178–179].

Для цього одним із принципів забезпечення кібербезпеки в Україні підп. 4 ч. 1 ст. 7 Закону України «Про основні засади забезпечення кібербезпеки України» визначено державно-приватну взаємодію, широку співпрацю з громадянським суспільством у сфері кібербезпеки та кіберзахисту, зокрема шляхом обміну інформацією про інциденти кібербезпеки, реалізації спільних наукових і дослідницьких проєктів, навчання й підвищення кваліфікації кадрів у цій сфері [1]. Як вказує І.О. Валюшко, «наявність ефективної мережі громадських структур стає за сучасних умов однією з умов забезпечення національної безпеки. Однак наука в Україні до цього часу комплексно не досліджувала недержавну систему безпеки як громадський механізм, а громадські об'єднання – як суб'єкти забезпечення національної безпеки держави <…> сама державна система та бюрократія не дозволяють державним структурам бути настільки мобільними, оперативними й використовувати соціальні мережі як патріотичні хакерські організації <…>

у сучасних умовах громадські об'єднання, як невід'ємний елемент громадянського суспільства, є повноцінним учасником процесу забезпечення інформаційної безпеки України. Взаємодія між громадським сектором і державними інститутами є важливим аспектом безпекової політики…» [7, с. 118, 123].

Однак закріплення певного принципу ще не означає його реалізації. І на сьогодні до числа головних проблем забезпечення кібернетичної безпеки в Україні науковці відносять відсутність належної координації діяльності відповідних відомств, а отже й неузгодженості дій зі створення окремих елементів системи кібербезпеки, відсутність загальнонаціонального координаційного центру, здатного узгоджувати й координувати діяльність правоохоронних органів, силових структур і відомств щодо протидії реальним загрозам інформаційного й кіберпростору України та керувати проведенням комплексних навчань із забезпечення кібернетичної безпеки держави в інфосфері на кшталт навчань Cyber Storm, які проводяться в США, і/або Cyber Europe, що проводяться в ЄС» [8, с. 23]. Отже, необхідним є забезпечення належної координації дій усіх зацікавлених суб'єктів під час запровадження інструментів забезпечення й організації кібербезпеки; удосконалення інституціонального механізму формування, координації та здійснення контролю за виконанням завдань розбудови кібернетичного суспільства [9, с. 122]. У цьому аспекті цілком справедливо до числа напрямів розвитку кібербезпеки відносять реалізацію механізмів партнерства держави, бізнесу й громадян у сфері кібербезпеки. До таких механізмів належать упровадження механізмів обміну інформацією державних ситуаційних центрів і центрів реагування на прояви стороннього кібервпливу з представниками бізнесу та громадського суспільства, підвищення ефективності взаємодії провайдерів інтернет-послуг і користувачів в аспекті інформування про кібервтручання й загрози, потенційні вразливості ІТ-систем і мереж, а також організація співпраці державних і бізнесових інституцій, окремих громадян у питаннях розроблення сучасних програмно-апаратних засобів забезпечення кібербезпеки [8, с. 20–21]. Для виконання вказаного доцільним для організації є центр взаємодії та координації, що об'єднував би всіх указаних суб'єктів.

Враховуючи викладене, поняття національної системи кібербезпеки з точки зору закріпленого в законодавстві підходу до його формування потребує критичної оцінки, а обмеження основних суб'єктів забезпечення кібербезпеки й суб'єкта координації виключно інституціями держави доцільний для перегляду з точки зору необхідності врахування потреб всіх суб'єктів забезпечення кібербезпеки в Україні (згідно зі ст. 5 Закону України «Про основні засади забезпечення кібербезпеки України» це міністерства та інші центральні органи виконавчої влади; місцеві державні адміністрації; органи місцевого самоврядування; правоохоронні, розвідувальні й контррозвідувальні органи, суб'єкти оперативно-розшукової діяльності; Збройні Сили України, інші військові формування, утворені відповідно до закону; Національний банк України; підприємства, установи й організації, віднесені до об'єктів критичної інфраструктури; суб'єкти господарювання, громадяни України та об'єднання громадян, інші особи, які провадять діяльність та/або надають послуги, пов'язані з національними інформаційними ресурсами, інформаційними електронними послугами, здійсненням електронних правочинів, електронними комунікаціями, захистом інформації та кіберзахистом [1]). У сучасному варіанті організації структури системи існує проблема ефективності координації та взаємодії не тільки щодо основних суб'єктів забезпечення кібербезпеки національної системи кібербезпеки з іншими суб'єктами, які реалізують відносини у кіберпросторі, але й між собою.

Як вважає І.В. Діордіца, розв'язання основних завдань кібербезпеки неможливе без створення «міжвідомчого структурного органу, який на постійній основі забезпечував

би координацію діяльності певних відомств, правоохоронних і силових структур України з питань забезпечення кібернетичної безпеки. Кібератака на Україну 27 червня 2017 р. довела неефективність діяльності Національного координаційного центру кібербезпеки, поставила питання не про демагогічні й популістські формування неді-єздатних центрів/органів, а про формування відповідно до національних інтересів національної системи кібербезпеки, власне, як на те вказується безпосередньо в Стратегії кібербезпеки України» [10, с. 111]. Додамо, що забезпечення координації на постійній основі потребують не тільки вказані науковцем органи. Питання забезпечення безпеки знаходить прояв у діяльності як державних структур, так і недержавного сектору.

Отже, вирішенням проблеми може стати, з одного боку, центр координації та взаємодії національного рівня, що охоплював би представників усіх зацікавлених сторін (включаючи «недержавних» суб'єктів), з іншого – створення на рівні кожного суб'єкта забезпечення кібербезпеки одиниці, що відповідатиме за координацію та взаємодію.

Запропоновані напрями досліджень задля розвитку національної системи кібербезпеки України не впливають на вже визначене місце Національної поліції України як основного суб'єкта забезпечення кібербезпеки, яке залишиться незмінним. Вони розроблені як перспективи підвищення ефективності діяльності кожного суб'єкта забезпечення кібербезпеки окремо й водночас у взаємодії між собою як єдиної системи, мета якої – кібербезпека в Україні та за її межами. І останнє уточнення має важливе значення для розуміння ролі Національної поліції для забезпечення кібербезпеки як одного з основних елементів національної системи кібербезпеки. Адже адміністративно-правовий статус указаного суб'єкта забезпечення кібербезпеки пов'язується з поняттям кіберзлочинності.

Як указує Г.В. Шевчук, заходи боротьби з кіберзлочинністю повинні мати сьогодні комплексний характер і бути спрямованими на мінімізацію ризиків віртуальних загроз і на підвищення ефективності засобів і способів захисту у віртуальному просторі. В указаних процесах кіберполіція стає центральним суб'єктом боротьби з кіберзлочинністю [11, с. 249]. Значення Національній поліції у цьому аспекті полягає у створенні умов розвитку безпечного середовища життєдіяльності як основи безпеки на території України [12] шляхом захисту прав і свобод людини й громадянина, інтересів суспільства й держави від злочинних посягань у кіберпросторі. Це означає, що метою створення кіберполіції є організація ефективної протидії проявам кіберзлочинності й забезпечення дієвого впливу на оперативну обстановку в зазначеній сфері [13, с. 89].

Кіберзлочинність не є традиційним злочином, а відносно молодим явищем, яке пов'язується з появою та поширенням глобальної мережі Інтернет, – доходить висновку С.А. Буяджи. З самого моменту виникнення цей вид злочинності проявив себе як зручний для зловмисників. Особлива природа Всесвітньої мережі забезпечила глобальність й анонімність для її користувачів, що, безсумнівно, постало передумовою для появи цього виду злочинності [14, с. 13]. Під кіберзлочинністю розуміють 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 [13, с. 88].

С.В. Демедюк зазначає, що «за своєю сутністю кіберзлочини є транскордонними, і тому міжнародні організації закликають держави до співпраці з іншими зацікавленими сторонами з метою розробляти дієві механізми адміністративно-правового регулювання у сфері кібербезпеки, що передбачає не лише розроблення та прийняття необхідного законодавства, а й проведення спільних розслідувань зазначених діянь з використанням чинного міжнародного права [15, с. 144]. Вказана мета обумовлює

завдання всіх структурних елементів національної системи кібербезпеки, до числа основних якої віднесено Національну поліцію.

Для протидії кіберзлочинності та здійснення інших функцій для виконання поставлених завдань Національну поліцію уповноважено вживати заходи з виявлення, припинення й розкриття кіберзлочинів, запобігання таким злочинам, підвищення поінформованості громадян про безпеку в кіберпросторі (підп. 2 ч. 2 ст. 8 Закону України «Про основні засади забезпечення кібербезпеки України»[1]).

Реалізацію означених функцій покладено насамперед на спеціально створений з огляду на динаміку поширення комп'ютерних інцидентів теренами України структурний підрозділ. Зокрема, в липні 2010 р. в структурі МВС України на базі Департаменту боротьби зі злочинами, пов'язаними з торгівлею людьми, утворено новий структурний підрозділ – Департамент боротьби з кіберзлочинністю та торгівлею людьми [8, с. 4] як структурний міжрегіональний територіальний орган поліції з широкими аналітичними й оперативно-тактичними повноваженнями, котрий спеціалізується на запобіганні, виявленні, припиненні й 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 [13, с. 89].

Висновок. Органи Національної поліції – це один з основних суб'єктів національної системи кібербезпеки, яку на сьогодні визначено як сукупність заходів і їх здійснювачів. Таке визначення потребує вдосконалення в аспекті розмежування поняття системи кібербезпеки як системи управління й системи забезпечення кібербезпеки, структури яких відрізняються. Національну систему кібербезпеки доцільно розуміти як сукупність всіх компонентів, за допомогою яких досягається кібербезпека, а саме: 1) суб'єктів і здійснюваних ними заходів (система забезпечення кібербезпеки); 2) об'єктів кібербезпеки й кіберзахисту як частини системи, які зазнають впливу з боку суб'єктів; 3) норм права, що є основою для забезпечення кібербезпеки через установлення зв'язків між суб'єктом й об'єктом (прямих і зворотних).

Водночас доцільний для перегляду з точки зору необхідності врахування потреб усіх суб'єктів забезпечення кібербезпеки в Україні підхід до обмеження основних суб'єктів національної системи кібербезпеки й суб'єкту їх координації виключно інституціями держави. Має сенс організація центру взаємодії й координації, що об'єднував би всіх суб'єктів забезпечення кібербезпеки на засадах партнерства.

Роль Національної поліції в забезпеченні кібербезпеки визначається поняттям кіберзлочинності, що є новим видом правопорушень. Виявлення, припинення, протидія й розкриття таких злочинів, а також запобігання скоєнню їх визначає адміністративно-правовий статус Національної поліції як суб'єкта забезпечення кібербезпеки. Однак не обмежує, оскільки найбільше значення має уповноваження на інформування громадян про безпеку в кіберпросторі.

Список використаних джерел:

1. Про основні засади забезпечення кібербезпеки України : Закон України від 5 жовтня 2017 р. № 2163-VIII / *Верховна Рада України*. *Офіційний вісник України*. 2017 р. № 91. С. 31.

2. Присяжнюк М.М., Цифра Є.І. Особливості забезпечення кібербезпеки. *Реєстрація, зберігання і обробка даних.* 2017. Т. 19. № 2. С. 61–68.

3. Ліпкан В.А., Діордіца І.В. Національна система кібербезпеки як складова частина системи забезпечення національної безпеки України. *Підприємництво, господарство і право.* 2017. № 5. С. 174–180.

4. Ковалевіч І.П. Теоретичні засади забезпечення зворотного зв'язку в державному управлінні. *Державне будівництво*. 2008. № 2. URL: http://www.kbuapa.kharkov.ua/e-book/db/2008-2/doc/1/15.pdf.

5. Про Раду національної безпеки і оборони України : Закон України від 5 березня 1998 р. № 183/98-ВР / *Верховна Рада України*. *Офіційний вісник України*. 1998 р. № 13. С. 18.

6. Діордіца І.В. Адміністративно-правове регулювання кібербезпеки України : автореф. дис. ... д-ра юрид. наук : 12.00.0; Запорізький нац. ун-т. Запоріжжя, 2018. 32 с.

7. Валюшко І.О. Кібербезпека України: наукові та практичні виміри сучасності. *Вісник Національного технічного університету України «Київський політехнічний інститут». Серія «Політологія. Соціологія. Право»*. 2016. № 3–4. С. 117–124.

8. Бурячок, В.Л. Інформаційна та кібербезпека: соціотехнічний аспект : підручник / за заг. ред. В.Б. Толубка. Київ : ДУТ, 2015. 288 с.

9. Демедюк С.В. Адміністративно-правове регулювання відносин у сфері забезпечення кібербезпеки в Україні. Південноукраїнський правничий часопис. 2015. № 3. С. 119–123.

10. Діордіца І.В. Система забезпечення кібербезпеки: сутність та призначення. *Підприємництво, господарство і право.* 2017. № 7. С. 109–116.

11. Шевчук Г.В. Особливості діяльності департаменту кіберполіції національної поліції України. *Науковий вісник публічного і приватного права.* Вип. 3. Том 1. 2019. С. 244–249.

12. Береза В.В. Принципи діяльності Департаменту кіберполіції Національної поліції України: теоретико-правові аспекти. *Форум права*. 2017. № 5. С. 44–48.

13. Демедюк С.В., Марков В.В. Кіберполіція України. *Наше право.* 2015. № 6. С. 87–93.

14. Буяджи С.А**.** Правове регулювання боротьби з кіберзлочинністю: теоретико-правовий аспект : дис. ... канд. юрид. наук : 12.00.01; Приват. ВНЗ Ун-т Короля Данила. Івано-Франківськ, 2018. 203 с.

15. Демедюк С.В. Окремі питання адміністративно-правового й організаційного забезпечення кібербезпеки. *Південноукраїнський правничий часопис*. 2015. № 2. С. 144–147.