УДК 67.401
DOI https://doi.org/10.32844/2618-1258.2025.2.11

БІЛОБРОВ Т.В.

ПОНЯТТЯ ТА СУЧАСНИЙ СТАН КІБЕРБЕЗПЕКИ В УКРАЇНІ

THE CONCEPT AND CURRENT STATE OF CYBERSECURITY IN UKRAINE

Поняття кібербезпеки нещодавно було введено до законодавства України як відповідь на зміни відносин в аспекті комунікації суб'єктів поза фізичним простором. Розвиток кіберпростору як окремого виду простору став закономірним наслідком взаємопроникнення суспільних та природничих наук, використання математичного апарату. Тож метою статті є розгляд наукових підходів до поняття кібербезпеки та аналіз її сучасного стану в Україні. Кіберпростір пропонується розглядати як середовище, що виникає в результаті функціонування на основі єдиних принципів і за загальними правилами інформаційних (автоматизованих), телекомунікаційних та інформаційно-телекомунікаційних систем. Відкритий кіберпростір розширює свободу та можливості людей, збагачує суспільство, створює новий глобальний інтерактивний ринок ідей, досліджень та інновацій, стимулює відповідальну й ефективну роботу влади і активне залучення громадян до управління державою та вирішення питань місцевого значення, забезпечує публічність і прозорість влади, сприяє запобіганню корупції. Водночас переваги сучасного кіберпростору обумовили виникнення нових загроз національній і міжнародній безпеці. Поряд з інцидентами природного (ненавмисного) походження зростає кількість і потужність кібератак, вмотивованих інтересами окремих держав, груп та осіб. У той же час, кібербезпека - це захищеність від наявних та потенційно небезпечних проявів інформаційного впливу, що створюють небезпеку для функціонування інформаційних ресурсів, систем, мереж, програмних і апаратних засобів, а також свідомості, підсвідомості, морально-психологічного стану людини, соціальних груп та суспільства в цілому. Обґрунтовано, що більш точним є розмежування понять кібербезпеки як певного стану та поняття її забезпечення як діяльності. Така позиція знаходить свої підтвердження в законодавстві України. Практика забезпечення ними кібербезпеки в Україні викриває ряд проблем, які за напрямками вирішення обєднані автором у певні групи.

Ключові слова: *кібезбезпека, кіберпростір, поняття, сучасний стан, проблеми.*

The concept of cybersecurity has recently been introduced into Ukrainian legislation as a response to changes in relations in terms of communication between entities outside of physical space. The development of cyberspace as a separate type of space has become a natural consequence of the interpenetration of social and natural sciences and the use of mathematical tools. Therefore, the purpose of the article is to consider scientific approaches to the concept of cybersecurity and to analyze its current state in Ukraine. It is proposed to consider cyberspace as an environment arising from the functioning of information (automated), telecommunication and information and telecommunication systems on the basis of common principles and according to common rules. Open cyberspace expands people's freedom and opportunities, enriches society, creates a new global interactive marketplace for ideas, research and innovation, stimulates responsible and effective work of the authorities and active involvement of citizens in government and local issues, ensures publicity and transparency of the authorities, and helps prevent corruption. At the same time, the advantages of modern cyberspace have led to the emergence of new threats to national and international security. Along

© БІЛОБРОВ Т.В. – кандидат юридичних наук, старший науковий співробітник (Науково-дослідний інститут публічного права) https://orcid.org/0009-0009-4439-4404

with incidents of natural (unintentional) origin, the number and power of cyberattacks motivated by the interests of individual states, groups and individuals is growing.At the same time, cybersecurity is the protection against existing and potentially dangerous manifestations of information influence that pose a threat to the functioning of information resources, systems, networks, software and hardware, as well as to the consciousness, subconsciousness, moral and psychological state of a person, social groups and society as a whole. It is substantiated that it is more accurate to distinguish between the concepts of cybersecurity as a certain state and the concept of its provision as an activity. This position is confirmed by Ukrainian legislation. The practice of ensuring cybersecurity in Ukraine reveals a number of problems which are grouped by the author into certain groups according to the areas of solution.

Key words: *cybersecurity, cyberspace, concept, current state, problems.*

Вступ.Поняття кібербезпеки нещодавно було введено до законодавства України як відповідь на зміни відносин в аспекті комунікації суб'єктів поза фізичним простором. Як вказують М. М. Присяжнюк та Є. І Цифра, «стрімкий розвиток інформаційних технологій, інформатизація та комп'ютеризація, створення глобального інформаційного простору сформували принципово нові субстанції – інформаційне суспільство, інформаційний і кібернетичний простори, які мають невичерпний потенціал і відіграють головну роль в економічному та соціальному розвитку країн світу. Науково-технічна революція початку XXI ст. спричинила в усьому світі глибокі системні перетворення. Поєднання досягнень у сфері новітніх інформаційно-комунікаційних технологій та стрімкого розвитку інформаційно-телекомунікаційних систем викликало появу так званого віртуального простору, який ще отримав назву «кіберпростір» [1, с. 61] або інформаційний простір – глобальне інформаційне середовище, яке в реальному масштабі часу забезпечує комплексну обробку відомостей [2, с. 7]. Розвиток кіберпростору, вважає І. В. Діордіца, як окремого виду простору став закономірним наслідком взаємопроникнення суспільних та природничих наук, використання математичного апарату [3, с. 87]. І на сьогодні у всьому світі відбувається глобальне перенесення соціальної й економічної активності індивідів у кіберпростір, який стає невід'ємною складовою сучасного суспільства, частиною сучасного навколишнього середовища [4, с. 119] являючи собою нове середовище для встановлення зв'язків суб'єктів правовідносин, який відрізняється від фізичного рядом специфічних ознак.

Тож **метою статті** є розгляд наукових підходів до поняття кібербезпеки та аналіз її сучасного стану в Україні.

Аналіз останніх досліджень та публікацій. Дослідженню природи кібербезпеки та присвятили свої праці В. Л. Бурячок, І. В. Діордіца, М. В. Камчатний, В. А. Ліпкан, М. М. Присяжнюк, С. В. Толюпа, Є. І Цифра та інші.

Виклад основного матеріалу. Що найперше, кіберпростір пропонується розглядати як середовище, що виникає в результаті функціонування на основі єдиних принципів і за загальними правилами інформаційних (автоматизованих), телекомунікаційних та інформаційно-телекомунікаційних систем [5, с. 23]. Кіберпростір не має чітко визначених територіальних меж та кордонів, і взагалі не може вважатися територією. Завдяки цій властивості кіберпростір вважають глобальним середовищем для комунікації суб'єктів правовідносин. Кіберпростір не передбачає фізичного контакту суб'єктів правовідносин, які можуть бути і не ідентифікованими при здійсненні комунікації за допомогою цифровізації їх зв'язків. Такі зв'язки здійснюються через програмне забезпечення на основі спеціальних протоколів. Кіберпростір характеризують «неперевершені можливості зі створення незлічених зв'язків між окремими індивідами і соціальними групами та з надання різнопланових інформаційних послуг» [2, с. 9]. Як вважає В. В. Бухарєв, кіберпростір являє собою високорозвинену модель об'єктивної реальності, в якій відомості щодо осіб, предметів, фактів, подій, явищ і процесів подаються в математичному, символічному або в будь-якому іншому вигляді, розміщуються в пам'яті фізичних пристроїв, спеціально призначених для зберігання, обробки й передавання інформації [6, с. 31]. Всі виділені особливості кіберпростору як якісно нового середовища для реалізації та охорони правовідносин забезпечують суб'єктам правовідносин ряд переваг порівняно з комунікацією у просторі фізичному.

До таких переваг доцільно віднести і швидкість комунікації без затрат часу на фізичний контакт, і можливість з будь-якої точки планети стати учасником певних відносин, і оперативність вирішення питань тощо. Як обґрунтовано стверджують В. А. Ліпкан та І. В. Діордіца, відкритий та вільний кіберпростір розширює свободу і можливості людей, збагачує суспільство, створює

новий глобальний інтерактивний ринок ідей, досліджень та інновацій, стимулює відповідальну та ефективну роботу влади й активне залучення громадян до управління державою та вирішення питань місцевого значення, забезпечує публічність та прозорість влади, сприяє запобіганню корупції [7, с. 176]. Однак, при наявності ряду переваг, перенесення відносин у кіберпростір має і негативні наслідки.

Стрімкий розвиток віртуального середовища, новизна його властивостей є основою для порушення прав суб'єктів правовідносин, які з фізичного простору перенесли свої комунікації у простір віртуальний. На сьогодні, доходить висновку М. В. Камчатний, розвиток технологій досяг такого рівня, що замість первинної мети – полегшення комунікації, пришвидшення інформаційних та виробничих процесів – створюється нова загроза для користувачів таких технологій. Умовно, ще вчора протиправними діями із використанням Інтернету були крадіжки персональних даних, шахрайство, промисловий шпіонаж. На сьогодні ж можливості використання Мережі, як і масштаби її розповсюдження світом, значно підвищилися. Уже абсолютно реальними є такі поняття, як шпигунство із використанням Інтернету, кібернетичний тероризм і навіть кібервійна [8, с. 12]. М. М. Присяжнюк та Є. І. Цифра з цього приводу вказують, що відкритий кіберпростір розширює свободу та можливості людей, збагачує суспільство, створює новий глобальний інтерактивний ринок ідей, досліджень та інновацій, стимулює відповідальну й ефективну роботу влади і активне залучення громадян до управління державою та вирішення питань місцевого значення, забезпечує публічність і прозорість влади, сприяє запобіганню корупції. Водночас переваги сучасного кіберпростору обумовили виникнення нових загроз національній і міжнародній безпеці. Поряд з інцидентами природного (ненавмисного) походження зростає кількість і потужність кібератак, вмотивованих інтересами окремих держав, груп та осіб [1, с. 64].

Отже, не можна заперечувати, що через небачене досі поширення інформаційно-комунікаційних технологій та інформаційно-телекомунікаційних систем світова спільнота отримала не лише численні переваги, а й цілу низку проблем, зумовлених дедалі більшою вразливістю інфосфери щодо стороннього кібернетичного впливу [6, с. 4] Як вважає А. В. Вінаков, вияви кіберзлочинності у вигляді хакерських атак на комп'ютерні системи банківських та інших фінансових установ, крадіжок електронних коштів, широкого використання мережі Інтернет для наркоторгівлі, торгівлі людьми, інших протиправних дій стають реальною загрозою національній безпеці [9, с. 34]. Від так поряд з поняттям кіберпростору з'являється поняття кібербезпеки, забезпечення якої на сьогодні є одним з пріоритетів як внутрішньої, так і зовнішньої політики не тільки України, але і всіх держав світу.

Дослідники В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа вважають, що цілком природно постала необхідність контролю та подальшого врегулювання відповідних взаємовідносин, а отже, і невідкладного створення надійної системи кібернетичної безпеки. Натомість відсутність такої системи може призвести до втрати політичної незалежності будь-якої держави світу, бо йтиметься про фактичний програш нею змагання невійськовими засобами та підпорядкування її національних інтересів інтересам протиборчої сторони. Оскільки саме ці обставини відіграють останнім часом важливу роль у геополітичній конкуренції більшості країн світу, то забезпечення кібербезпеки та злагоди в кіберпросторі стає головним завданням нашої інформаційної епохи [6, с. 4]. Створення інформаційного суспільства, підсумовують автори М. М. Присяжнюк та Є. І Цифра, призвело до виникнення багатьох інформаційних загроз, а одним із головних завдань сучасної інформаційної епохи є забезпечення інформаційної та кібернетичної безпеки [1, с. 61]. На зв'язку таких категорій як «глобальне інформаційне суспільство» та «кібербезпека» наголошується ще в Окінавській хартії глобального інформаційного суспільства, де вперше з'являється поняття кіберпростору «безпечного» і «вільного від злочинності» як мети співпраці міжнародного співтовариства [10]. Дане завдання не втрачає актуальності й до сьогодні.

Автор В. А. Світличний стверджує, що на сучасному етапі розвитку науки і техніки кібербезпека перетворюється на одну з найактуальніших задач високотехнологічного суспільства. Внаслідок надзвичайно широкого використання сучасних інформаційних технологій в усіх сферах свого існування суспільство стало вразливим від незначних кібернетичних впливів, які все частіше стають ефективним інструментом на шляху досягнення мети щодо несилового контролю та управління як об'єктами критичної інфраструктури держави, підприємств, так і окремо взятими громадянами, їх об'єднаннями [11, с. 352]. Широких масштабів проблема кібербезпеки набула тоді, коли держави усвідомили усі можливі наслідки від реалізації загроз у сферах, де використовувались комп'ютерні системи. При незначному обсязі ресурсів для реалізації цих загроз досягаються значні результати, здатні паралізувати цілі компанії та держави [12, с. 118].

При цьому, як вказують В. А.Ліпкан та І. В. Діордіца, останнім часом проблема забезпечення національної безпеки зміщується у бік не стільки декларованої, скільки реально розглядуваної. Передусім, це обумовлено активізацією зовнішніх загроз безпечного розвитку України: посиленням мілітаризації держав у регіоні, використанням положення енергетичної та торговельно-економічної залежності нашої країни, посиленням економічного та інформаційного тиску на неї тощо. Разом із тим, зовнішні загрози посилюються наявністю внутрішніх викликів національній безпеці, зокрема, йдеться про розбалансованість та незавершеність системних реформ, зниження обороноздатності держави, боєздатності Збройних Сил України, незадовільний стан фінансування, складне економічне становище [7, с. 174].

Формуючи поняття кібербезпеки, В. А. Світличний доходить висновку про можливість трактування поняття одночасно у діяльнісному та статичному вимірах. Як вважає науковець, кібербезпека – це захищеність від наявних та потенційно небезпечних проявів інформаційного впливу, що створюють небезпеку для функціонування інформаційних ресурсів, систем, мереж, програмних і апаратних засобів, а також свідомості, підсвідомості, морально-психологічного стану людини, соціальних груп та суспільства в цілому. З іншого, кібербезпека – це комплекс заходів та засобів, що спрямовані на захист комп'ютерів, цифрових даних і мереж їх передачі від несанкціонованого доступу та інших дій, пов'язаних з маніпулюваннями або крадіжкою, блокуванням, пошкодженням, руйнуванням та знищенням як випадкового, так і цілеспрямованого впливу. Тому об'єктом діяльності фахівця з кібербезпеки є процеси захисту інформації у всіх її видах [11, с. 352]. На наш погляд, більш точним є розмежування понять кібербезпеки як певного стану та поняття її забезпечення як діяльності.

Така позиція знаходить свої підтвердження в законодавстві України. Зокрема, в Законі України «Про основні засади забезпечення кібербезпеки України» [13] визначено не тільки поняття кібербезпеки, а й ряд інших понять, що мають провідне значення для забезпечення безпечних умов використання кіберпростору: кіберзагроза, кібератака, кіберінцедент, кіберзлочин, кіберзлочинність тощо.

Згідно ч. 5 ст. 1 вказаного Закону кібербезпека визначається як захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі [13]. Як бачимо, законодавець використовує статичний підхід до формування поняття кібербезпеки. А от поняття забезпечення кібербезпеки в законі відсутнє.

Виходячи з результатів комплексного аналізу статей вказаного закону можна запропонувати розуміти під забезпеченням безпеки комплекс взаємопов'язаних заходів політичного, науково-технічного, інформаційного, освітнього характеру, організаційних, правових, оперативно-розшукових, розвідувальних, контррозвідувальних, оборонних, інженерно-технічних заходів, а також заходів криптографічного і технічного захисту національних інформаційних ресурсів, кіберзахисту об'єктів критичної інформаційної інфраструктури [13]. Близьке до наданого поняття кіберборотьби, під якою запропоновано розуміти комплекс заходів, спрямованих на здійснення управлінського і/або деструктивного впливу на автоматизовані ІТ-системи протиборчої сторони та захисту від такого впливу власних інформаційно-обчислювальних ресурсів завдяки використанню спеціально розроблених програмно-апаратних засобів, а також проведенню системи спеціалізованих навчань[6, с. 11].

Якщо конкретизувати дане визначення стосовно Національної поліції, то можна погодитись, що боротьба із кіберзлочинністю є процесом, який передбачає комплексне застосування заходів, а нормативно-правове регулювання забезпечує закріплення відповідних механізмів, як вважає С. А. Буяджи [14, с. 107]. Уточнення потребує лише обмеження заходів із забезпечення кібербезпеки боротьбою, поза увагою залишаючи попередження кіберзлочинів [15], інформування про кіберзлочинність та кіберзлочини та підвищення поінформованості громадян про безпеку в кіберпросторі.

Як вказує О. І. Гончаренко, питання протидії кіберзлочинам, їх виявлення та попередження у наш час набирає все більшої актуальності, через велику кількість атак, як на промислових гігантів, так і на рядових користувачів мережі Інтернет [16, с. 30, 31]. Україна поступово нагромаджує важливий досвід у захисті власної ІТ-інфраструктури від кіберзагроз сучасності та протидії проявам кібертероризму. Утім протистояти фізичному руйнуванню технічних засобів, дезорганізації роботи інформаційних систем і мереж, порушенню функціонування об'єктів нападу,

а також протиправній діяльності соціальних інженерів в умовах інтенсифікації кібервтручань з дня на день стає все важче [6, с. 5]. Нині для України питання кібербезпеки, нарощування потенціалу кібермогутності стоять на порядку денному [12, с. 119]. Вітчизняні реалії кібербезпекової сфери свідчать про низку важливих проблем, що заважають створити ефективну систему протидії загрозам у кіберпросторі, доходить висновку С. Х. Барегамян [5, с. 24]. Питання їх вирішення тим більше актуалізується з початком російської гібридної війни, де кіберагресія є однією з її визначних складових. Не можна заперечувати, що за таких умов Україні необхідно самостійно шукати шляхи і механізми забезпечення кібербезпеки від сучасних загроз, які постають [12, с. 119]. А для цього критичній оцінці підлягає сучасний стан забезпечення кібербезпеки з виділенням проблем, вирішення яких сприятиме досягненню стану кібербезпеки.

Актуальним для України питанням на сьогодні є відсутність чи не конкурентоспроможність вітчизняних програмних продуктів та використання закордонної бази. Як вказують з цього приводу М. М. Присяжнюк та Є. І. Цифра, Україна все ще залишається вразливою (особливо її телекомунікаційна складова), не в останню чергу через надмірно широке впровадження західних програмних продуктів і використання матеріально-технічної бази іноземного виробництва. Необхідним є створення національної операційної системи (принаймні для використання у системі органів державної влади, хоча для такого переходу до програмного забезпечення з відкритим кодом є і суттєві зауваження з боку ключових вітчизняних безпекових організацій), відновлення вітчизняних потужностей з виробництва матеріально-технічної телекомунікаційної бази (особливо для потреб закритих відомчих інформаційних систем), стимулювання з боку держави створення національного антивірусу [1, с. 66]. Підтримуючи позицію науковців, зауважимо, що для вирішення вказаної проблеми необхідним є вирішення питання оплати праці фахівців сфери у державному секторі та її конкурентоздатності з приватним, що сприятиме вирішенню проблеми кваліфікованих кадрів.

Це означає, що значна вразливість інфосфери України через надмірну присутність у ній західних програмних продуктів (зокрема, фірми Microsoft) та використання матеріально-технічних засобів іноземного виробництва обтяжується деградацією науково-технічного потенціалу України, нерозвиненістю національної інноваційної системи в інфосфері та низьким рівнем конкурентоспроможності в ній [2, с. 23]. Наразі найбільш кваліфіковані спеціалісти з досвідом роботи приймають пропозиції переїзду за кордон через більш сприятливі умови праці та вищу оплату, що беззаперечно відзначається не тільки на якості та кількості вітчизняних продуктів, але і на ефективності функціонування національної системи кібербезпеки.

Аналізуючи дану проблему фахівці доходять висновку, що протистояти фізичному руйнуванню технічних засобів, дезорганізації роботи інформаційних систем і мереж, порушенню функціонування об'єктів нападу, а також протиправній діяльності соціальних інженерів в умовах інтенсифікації кібервтручань з дня на день стає все важче. Одна з головних причин цих негараздів полягає у відчутній нестачі професіоналів з інформаційної та кібербезпеки, здатних: 1) відшукувати, збирати або добувати інформацію про ІТ-системи й мережі протиборчих сторін, а також про технології та засоби їхнього впливу на власну інфосферу; 2) виявляти ознаки стороннього кібервпливу й моделювати можливі ситуації такого впливу, прогнозуючи відповідні наслідки; 3) протидіяти несанкціонованому проникненню протиборчих сторін у власні ІТ-системи й мережі, забезпечуючи стійкість їхньої роботи, а також відновлення нормального функціонування після здійснення кібернападів тощо [2, с. 5]. При цьому складнощами з кадровим наповненням [5, с. 24] не вичерпуються проблеми організації і діяльності системи кібербезпеки України. До вад її функціонування відносять відсутність загальнонаціональних міжвідомчих координаційних структур, що могли б узгоджувати та координувати діяльність різних силових відомств під час розслідування злочинів у кіберпросторі (співпраця реально існує не на чітко визначеному, а швидше, міжособистісному рівні, а отже, є уразливою) [5, с. 24]; дефіцит щодо методичного забезпечення та кадрового наповнення відповідних структурних підрозділів, відсутність чіткого усвідомлення ролі та значення кібербезпекової складової в системі забезпечення національної безпеки держави [2, с. 16]. До названого переліку доцільно додати і недосконалість нормативно-правового забезпечення.

Враховуючи сучасний стан та проблеми кібербезпеки в Україні до пріоритетів України у забезпеченні кібербезпеки пропонують відносити: розвиток інформаційної інфраструктури держави; розвиток мережі реагування на комп'ютерні надзвичайні події (CERT – Computer Emergency Response Team – команда реагування на комп'ютерні надзвичайні події), розвиток спроможностей правоохоронних органів щодо розслідування кіберзлочинів, забезпечення

захищеності об'єктів критичної інфраструктури, державних інформаційних ресурсів від кібератак, створення системи підготовки кадрів у сфері кібербезпеки для потреб органів сектору безпеки і оборони, розвиток міжнародного співробітництва у сфері забезпечення кібербезпеки, інтенсифікацію співпраці України та НАТО, зокрема в межах Трастового фонду НАТО для посилення спроможностей України у сфері кібербезпеки [17, с. 249–250]. Також для попередження кіберзлочинів, слід погодитись, необхідно постійно проводити моніторинг інформаційних загроз, ґрунтовні дослідження функціонування та розвитку кіберзлочинності. Не останнє місце також повинно займати спеціалізоване правове виховання суб'єктів інформаційного обороту та користувачів комп'ютерної техніки [16, с. 30, 31]. Окрім названих напрямків окремим аспектом доцільно визначати формування культури та проведення інформаційно-пропагандистської кампанії про значущість проблематики кібербезпеки держави за допомогою: 1) активного інформування про кібернетичні втручання і загрози, про потенційні уразливості ІТ-систем і мереж, а також способи їх компенсації; 2) розширення співпраці державних органів з ІТ-компаніями, некомерційними організаціями з метою популяризації та впровадження на практиці безпечної поведінки в кіберпросторі; 3) стимулювання заходів боротьби з кіберзлочинністю і кібертероризмом, кібершпіонажем і кіберактивізмом; 4) підвищення рівня безпеки електронних послуг, що надаються державою власному населенню; 5) організації профілактичної роботи з потенційними жертвами кіберзлочинів, керівниками малого і середнього бізнесу [2, с. 19].

Висновки. Враховуючи вищевикладене, доходимо висновку, що кіберпростір як цілком відмінне від фізичного простору середовище має специфіку при реалізації в ньому суспільних відносин. Віртуалізація зв'язків та комунікацій суб'єктів права має ряд позитивних наслідків (швидкість зв'язку, можлива відсутність фізичного контакту, глобальність мережі Інтернет, зв'язок з будь-якої точки світу тощо), але при цьому є передумовою для виникнення нових складів правопорушень, які будуються на специфічних ознаках кіберпростору. А тому з використанням кіберпростору постало питання кібербезпеки як певного стану його захищеності від реальних і потенційних загроз; охорони та захисту важливих інтересів людини і громадянина, суспільства та держави під час його використання як умови сталого розвитку інформаційного суспільства та цифрового комунікативного середовища.

Цей стан досягається через діяльність по забезпеченню кібербезпеки, яка має вигляд заходів різнорідного характеру суб'єктів національної системи кібербезпеки, та суб'єктів, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки. Практика забезпечення ними кібербезпеки в Україні викриває ряд проблем, які за напрямками вирішення можна згрупувати у наступні групи: 1) підвищення рівня оплати праці як передумова вирішення кадрового питання сфери; 2) розробка вітчизняного програмного та матеріально-технічного забезпечення; 3) інформування про стан кібербезпеки, кіберзлочинність всіх зацікавлених суб'єктів; 4) налагодження координації та взаємодії суб'єктів забезпечення кібербезпеки на партнерських засадах як на національному. Так і на міжнародному рівнях; 5) моніторинг кіберзагроз, кібератак та кіберінцедентів як основи для попередження правопорушень, розробки методологічних рекомендацій по забезпеченню кібербезпеки, моделювання та прогнозування кібератак, виявлення та нейтралізації кіберзагроз; 6) удосконалення нормативно-правового регулювання питань забезпечення кібербезпеки.

Список використаних джерел:

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

2. Інформаційна та кібербезпека: соціотехнічний аспект : підручник / В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа ; за заг. ред. д-ра техн. наук, проф. В. Б. Толубка. Київ : ДУТ, 2015. 288 с.

3. Діордіца І. В. Основні поняття та ідеї кібернетики як засади виділення кібернетичної функції держави. *Науковий вісник Міжнародного гуманітарного університету. Серія : Юриспруденція*. 2017. Вип. 30 (1). С. 86–88.

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

5. Барегамян С. Х. Система забезпечення безпеки кіберпростору в Україні. *Кібербезпека та системи захисту інформації: виклики сьогодення* : зб. матеріалів круглого столу, м. Маріуполь, 26 жовт. 2017 р. / уклад. І. Б. Тимофєєва ; Маріупольський державний університет ; Кафедра математичних методів та системного аналізу. Маріуполь, 2017. С. 23–26.

6. Бухарєв В. В. Адміністративно-правові засади забезпечення кібербезпеки України : дис. ... канд. юрид. наук : 12.00.07. Суми, 2018. 221 с.

7. 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.

8. Камчатний М. В. Основні ознаки поняття «кібервійна» в сучасному міжнародному праві. Альманах міжнародного права. 2017. Вип. 15. С. 12–22.

9. Вінаков А. В. Зміст підготовки фахівців для підрозділів боротьби з кіберзлочинністю в в сучасних умовах. *Використання інноваційних технологій у попередженні злочинів* : матеріали наук.-практ. семінару, м. Харків, 6 груд. 2012 р. / МВС України ; Харк. нац. ун-т внутр. справ. Харків, 2012. С. 34–36.

10. Окінавська хартія глобального інформаційного суспільства : прийнята 22 лип. 2000 р. Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/998_163.

11. Світличний В. А. Вдосконалення підготовки курсантів вищих навчальних закладів із специфічними умовами навчання як фахівців з кібербезпеки. *Актуальні питання протидії кіберзлочинності та торгівлі людьми* : зб. матеріалів Всеукр. наук.-практ. конф., м. Харків, 23 листоп. 2018 р. / МВС України ; Харків. нац. ун-т внутр. справ ; Координатор проектів ОБСЄ в Україні. Харків, 2018. С. 357–360.

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

13. Про основні засади забезпечення кібербезпеки України : Закон України від 05 жовт. 2017 р. № 2163-VIII. *Офіційний вісник України*. 2017. № 91. Ст. 2765.

14. Буяджи С. А. Правове регулювання боротьби із кіберзлочинністю: теоретико-правовий аспект : дис. ... канд. юрид. наук : 12.00.01. Івано-Франківськ, 2018. 203 с.

15. Орлов О. В., Онищенко Ю. М. Попередження кіберзлочинності – складова частина державної політики в Україні. *Теорія та практика державного управління*. 2014. Вип. 1. С. 9–15.

16. Гончаренко О. І. Правоохоронна діяльність щодо попередження кіберзлочинів. *Актуальні питання протидії кіберзлочинності та торгівлі людьми* : зб. матеріалів Всеукр. наук.-практ. конф., 23 листоп. 2018 р., м. Харків / МВС України ; Харків. нац. ун-т внутр. справ ; Координатор проектів ОБСЄ в Україні. Харків, 2018. С. 29–32.

17. Гібридна війна і журналістика. Проблеми інформаційної безпеки : навч. посіб. / ред.-упор. : О. І. Харитоненко, Ю. С. Полтавець ; за заг. ред. В. О. Жадька. Київ : НПУ імені М. П. Драгоманова, 2018. 356 с.