КРИМІНАЛЬНЕ ПРАВО, КРИМІНОЛОГІЯ

УДК 343.2

І. В. Діордіца
кандидат юридичних наук, доцент,
доцент кафедри кримінального права і процесу
Національного авіаційного університету

НАПРЯМИ ДЕРЖАВНОЇ ПОЛІТИКИ КІБЕРБЕЗПЕКИ

Національна безпека України, її економічне процвітання, соціальний та інформаційний добробут все більше залежать від доступності, цілісності та конфіденційності інформаційних ресурсів, що забезпечуються інформаційно-комунікаційними технологіями, або в більш широкому розумінні – кіберпростором. Водночас зростання залежності від інформаційних технологій робить сучасне українське суспільство більш уразливим до можливих негативних наслідків протиправного використання кіберпростору. Кожного року зростає кількість кібернападів і різноманітних кіберінцидентів у найбільш важливих сферах життєдіяльності нашої держави.

За таких умов одним із головних завдань держави є вжиття проактивних заходів, що сформують гарантовані умови для реалізації національних інтересів у кіберпросторі. Одним із напрямів реалізації такого завдання є формування резервних копій (бекапів) інформаційних ресурсів держави, а також формування ефективної національної системи кібербезпеки, що дозволить принципово зменшити (а подекуди – цілком унеможливити) наслідки кібератак.

Зазначені й інші факти й обумовлюють актуальність теми дослідження.

Через недостатній розвиток інформатизації в нашій країні проблеми, що безпосередньо пов'язані із проникненням в інформаційні системи, почали досліджуватися лише останніми роками. Кіберпростір як середовище вчинення злочинів вивчали: О. Косогов [1], Т. Попова, В. Ліпкан [2–5], Л. Рудник [6–7], І. Діордіца [8–10], В. Залізняк [11], Б. Кормич [12] та інші.

Метою статті є визначення напрямів державної політики кібербезпеки.

Для досягнення поставленої мети, автором було сформульовано завдання – здійснити аналіз нормативно-правових актів у безпековій сфері та виокремити ті норми, які безпосередньо стосуються державної політики кібербезпеки, визначити основні напрями державної політики кібербезпеки, виявити чинники, які визначають державну політику кібернетичної безпеки та її основну мету.

Виклад основного матеріалу. Сьогодні поняття політики втрачає свою початкову суть завдяки тому, що основна діяльність держави спрямована все ж таки не на перерозподіл влади (хоча це лежить в основі), а на задоволення потреб громадян, та сама політика вже трактується як певна стратегія прийняття і практичної реалізації обов'язкових для суспільства рішень по тому чи іншому питанню. Оскільки центральним гравцем політичного життя залишається держава, то призначення політики полягає у визначенні суті проблеми, розв'язання якої потребує втручання державних органів влади, а це вже державна політика, тому що пов'язана з діяльністю зі здійснення державної влади.

Отже, державна політика – це цілеспрямована діяльність органів державної влади для створення умов по реалізації національних інтересів, вирішення суспільних проблем, формування, досягнення й реалізації загальнозначущих національних цілей розвитку в найбільш важливих сферах життєдіяльності. Саме тому Л. Пал визначає державну політику як «напрям дії або утримання від неї, обрані державними органами для розв'язання певної чи сукупності взаємно пов'язаних проблем».

Для пострадянських країн термін «державна політика» не обмежується лише діями одного гравця в особі держави, а вміщує дії всіх гравців політичної системи, які пов'язані із предметом справи і можуть посприяти розв'язанню конкретної проблеми. Для української науки більш характерним є вживання терміну «державна політика», який вміщує майже всі аспекти управління країною [13].

Державну політику також можна визначити як напрям дій (або бездіяльність), що обирає державна влада (або орган державної влади, що має повноваження: правові, політичні, інформаційні й фінансові) для вирішення певної проблеми або сукупності взаємозалежних проблем.

Отже, державна політика з позицій реактивного підходу може трактуватися також як реакція держави на конкретні проблеми суспільства, або груп у такому суспільстві, наприклад, громадян, неурядових організацій. Вона покликана погоджувати інтереси різноманітних соціальних груп, формувати механізми балансу і консенсусу, який є необхідним для стабільності та розвитку суспільства. Зважаючи на таке, державна полі-

тика кібербезпеки повинна бути спрямована на вирішення конкретних проблем, які виникають у кіберпросторі.

Оскільки питання кібербезпеки безпосередньо стосується безпеки загалом, то для здійснення дослідження використаю основоположні нормативно-правові акти у сфері безпекознавства.

Протягом останніх років керівництвом держави було здійснено низку важливих кроків, спрямованих на посилення боротьби з кіберзагрозами, та вжито низку заходів, спрямованих на розбудову повноцінної національної системи кібербезпеки, посилення заходів кібербезпеки держави [1].

Наприклад, у Законі України «Про основи національної безпеки України» [14] зазначено, що «національна безпека України забезпечується шляхом проведення виваженої державної політики», без уточнення економічної, соціальної, інформаційної, кібернетичної та ін. Тому політику і визначу основним засобом, який використовується для досягнення необхідних безпечних умов суспільного і державного життя. Також у згаданому законі акцентовано увагу на державній політиці.

Перефразовуючи дефініцію «державна політика національної безпеки», запропоновану В. Ліпканом і О. Ліпкан [3, с. 85], визначу «державну політику кібернетичної безпеки» як діяльність уповноважених органів державної влади й управління, яка визначає цілі, функції, принципи, пріоритети кібернетичної безпеки, методи і засоби їх забезпечення.

Оскільки державна політика кібербезпеки на сучасному етапі трактується як складова частина інформаційної політики, то, використовуючи словник Стратегічні комунікації [2, с. 80], зазначу, що державна політика кібербезпеки складається із двох основних взаємопов'язаних блоків:

1) діяльності винятково державних органів;

2) діяльності недержавних інституцій, інституцій громадянського суспільства, інформаційного суспільства в інформаційній сфері.

Наприклад, поняття «інформаційне суспільство» увійшло в науковий обіг порівняно нещодавно. Його виробили і почали активно використовувати юристи, інформаціологи, економісти й маркетологи, безпекознавці, соціологи та філософи, програмісти і політики. Таке поняття відображає об'єктивну тенденцію нового етапу еволюції цивілізації, який пов'язується з появою нових інформаційних і телекомунікаційних технологій, нових потреб і нового способу життя. У зв'язку із цим, пропоную кібернетичне суспільство інтерпретувати як суспільство, в якому діяльність людей ґрунтується на використанні послуг, що надаються за допомогою надбань кібернетики.

Повертаючись до аналізу положень Закону «Про основи національної безпеки України», зауважу, що в ньому акцент зроблено саме на державній політиці, тобто такій, що проводиться від імені держави її владними органами. І це не дивно, адже саме в арсеналі державних засобів проведення політики є всім відомий інструмент державного примусу, який здебільшого й асоціюється з такими термінами, як «захист», «безпека», «охорона» тощо [12, с. 133]. Тобто державна політика кібербезпеки і має в своєму «арсеналі» певні засоби захисту, охорони та гарантування безпеки. Здійснений мною формально-юридичний і логіко-семантичний аналіз текстів кібербезпекового законодавства уможливив виділення адекватної операціоналізації таких понять. Так, у текстах нормативно-правових актів не як синонімічні, а як окремі надибуємо терміни: «кібероборона», «кібернапад», «кібербезпека», «кіберзахист».

Варто пам'ятати, що альтернатива вибору засобів, методів, способів і шляхів гарантування кібернетичної безпеки України безпосередньо обумовлена необхідністю доречного вжиття заходів, які є адекватними характеру і масштабам загроз національним інтересам у різних сферах життєдіяльності.

Також зазначу, що державна кібербезпекова політика повинна проводитися переважно тими методами, способами і засобами, які ґрунтуються на принципах реалізації національних інтересів, враховуючи цінності демократії та верховенства права.

Базуючись на Законі України «Про основи національної безпеки України», можна виокремити дві ключові категорії, які зумовлюють зміст і напрями державної політики кібернетичної безпеки:

1) загрози національним інтересам і національній безпеці України в кібернетичній сфері;

2) основні напрями державної політики з питань національної без-пеки в кібернетичній сфері.

Беручи до уваги наукові положення дослідження В. Ліпкана [5] та виходячи з того, що кібербезпека є складовою інформаційної безпеки, адаптую їх до теми свого дослідження.

Отже, державну політику кібербезпеки варто розуміти як діяльність держави в кібернетичній сфері, спрямовану на задоволення інформаційних потреб людини і громадянина через формування відкритого інформаційного суспільства (кібернетичного суспільства – І. Д.) на основі розвитку єдиного кібернетичного простору цілісної, інформаційно розвиненої держави та її інтеграції у світовий кібернетичний простір з урахуванням збереження національної ідентичності, реалізації національних інтересів за гарантування кібернетичної безпеки на внутрішньодержавному та міжнародному рівнях.

Основною метою державної політики кібербезпеки є управління реальними та потенційними кіберзагрозами і небезпеками для створення необхідних умов для задоволення кібернетичних потреб людини і громадянина, а також реалізації національних інтересів у зазначеній сфері.

Отже, державна політика кібернетичної безпеки України – діяльність державно-правових інституцій щодо управління реальними та потенційними кіберзагрозами і небезпеками з метою задоволення кібернетичних потреб людини та громадянина, а також реалізації національних інтересів у зазначеній сфері.

Нині не всі нормативно-правові акти відповідають викликам сьогодення та реальним кіберзагрозам, тому підтримую пропозиції І. Арістової [5, с. 156], яка зазначила, що для реалізації національних інтересів в інформаційній (кібернетичній – І. Д.) сфері треба переглянути пріоритети державної політики, розробити нові концептуальні підходи щодо регулювання ринку інформаційно-комунікаційних технологій, інформаційної й інвестиційної політики, розвитку інформаційного (кібернетичного – І. Д.) законодавства і гарантування інформаційної (кібернетичної – І. Д.) безпеки.

Щодо напрямів державної політики кібербезпеки, то, насамперед, зауважу, що вона повинна бути чітко визначена та зафіксована в національному законодавстві. Нині такі спроби було зроблено під час розроблення проекту Закону України «Про основні засади забезпечення кібербезпеки України» [15].

У вищезазначеному законі так визначені напрями державної політики:

– створення захищеного національного сегмента кіберпростору, що сприятиме підтриманню відкритого суспільства і гарантуватиме безпечне використання такого простору суспільством. Категорія «відкрите суспільство» є новою в юридичній термінології, тому потребує свого тлумачення для уникнення прогалин і колізій у законодавстві. Відкрите суспільство – це суспільство, яке базується на визнанні того факту, що ніхто не має монополії на істину (плюралізм – І. Д.), що різні люди мають різні погляди й інтереси, і що існує потреба в установах, які б захищали права всіх людей і давали б їм змогу жити разом у мирі і злагоді (філософська категорія – І. Д.). Основними рисами, що характеризують відкрите суспільство, є верховенство права, демократично обрана влада, інститути громадянського суспільства, захист прав меншин [16], тобто, на мою думку, відкритим є суспільство в правовій державі. Відкрите суспільство – тип суспільства, головною засадою якого є свобода особи та її відповідальність. Також припускаю, що під «безпечним використанням» мається на увазі уникнення створення чи виникнення будь-яких загроз, зокрема кібернетичних;

– запобігання втручанню у внутрішні справи України (тобто ті, що належать до внутрішньої компетенції держави – І. Д.) і нейтралізація посягань на її інформаційні ресурси з боку інших держав;

– посилення обороноздатності держави в кіберпросторі (кібероборона – І. Д.);

– боротьба з кіберзлочинністю та кібертероризмом. Необхідне чітке визначення відповідальних суб'єктів за забезпечення такого напряму, як і всіх інших напрямів державної безпеки у будь-якій сфері. Нині кіберзлочинність – актуальна проблема, з якою зіштовхнулись усі країни у XXI ст., і яка постійно збільшується за масштабами та завданими збитками. Так, у липні 2017 р. в Національному банку України (далі – НБУ) заявили про створення Центру кіберзахисту НБУ [21]. Акцентую увагу на відсутності законодавчого визначення поняття вищезазначеного явища. У проекті закону «Про основні засади забезпечення кібербезпеки України», кіберзлочином називають суспільно небезпечне винне діяння в кіберпросторі, передбачене законодавством України про кримінальну відповідальність, а кіберзлочинністю – сукупність кіберзлочинів [8]. Поняття кібертероризму виникло на межі XX – XXI ст. задовго до початку масового використання Інтернету. Термін «кібертероризм» є синтезом понять «кібербезпековий простір» і «тероризм». Кібертероризм пропонується розуміти як протиправне діяння, яке вчиняється для досягнення негативних наслідків, наприклад, отримання матеріальних благ чи загроза інформаційній безпеці держави. Кібертероризм має місце в кібербезпековому просторі [9];

– зниження рівня уразливості об'єктів кіберзахисту, зокрема й об'єктів критичної інформаційної інфраструктури. Такий напрям потребує подальших досліджень, оскільки категорія «об'єкт кіберзахисту» є новою та невизначеною, і, на мою думку, формулювання «зниження рівня уразливості» є абстрактним за відсутності чіткої методики та критеріїв визначення такої уразливості. Виникає логічне питання: хто і яким чином повинен визначати такий рівень? Як варіант – «попередження уразливості об'єктів кіберзахисту та ліквідація негативних наслідків»;

– забезпечення повноправної участі України в загальноєвропейській і регіональних системах гарантування кібербезпеки. Україна бере активну участь у міжнародній безпековій діяльності, наприклад, ратифікація Конвенції про кіберзлочинність, участь у розробленні та прийнятті Статуту Організації Об'єднаних Націй (далі – ООН). Отже, обмеження напрямів участі України лише загальноєвропейською та регіональною системою гарантування кібербезпеки є некоректним. У вузькому сенсі система гарантування кібербезпеки – сукупність суб'єктів, які здійснюють свою діяльність у кіберпросторі [10], тобто регіональні й європейська системи представлені більшим колом суб'єктів і масштабом здійснення ними своєї діяльності;

– дотримання міжнародних зобов'язань щодо боротьби з кіберзлочинністю та кібертероризмом [15]. Нині існує незначна кількість спеціальних нормативно-правових актів як універсального, так і регіонального характеру, в яких держави сформулювали певні зобов'язання щодо боротьби з кібертероризмом і кіберзлочинністю. Серед них і Конвенція про кіберзло-

чинність. Держави, що приєдналися до Конвенції, взяли зобов'язання переглянути своє законодавство з метою узгодження його з рекомендаціями, викладеними в зазначеному міжнародному документі.

Оскільки кібербезпека є складником інформаційної безпеки, яка, своєю чергою, є складником національної безпеки, доцільним під час визначення напрямів державної політики кібербезпеки буде використання положень Закону «Про основи національної безпеки України».

Основними напрямами державної політики в інформаційній сфері є:

– забезпечення інформаційного суверенітету України. Ще одна нова правова категорія, дефініція якої міститься в проекті Закону «Про інформаційний суверенітет та інформаційну безпеку України» [17]. Інформаційний суверенітет України – це право держави на формування і здійснення національної інформаційної політики відповідно до Конституції та законодавства України, міжнародного права в національному інформаційному просторі України. Також у Словнику Стратегічних комунікацій міститься таке визначення: «Інформаційний суверенітет – незалежність і самостійність держави в реалізації державної інформаційної політики; здатність держави здійснювати контроль над власним інформаційним простором через організацію управління процесами створення, збирання, одержання, зберігання, використання, поширення, охорони та захисту інформації відповідно до національних інтересів» [2, с. 168–169]. Зважаючи на вищезазначені положення, і це можна вважати елементом наукової новизни, можна виокремити і феномен «кібернетичного суверенітету», який пропонується розуміти як невід'ємне право держави на формування і здійснення національної кібербезпекової політики відповідно до національних інтересів, ґрунтуючись на Конституції України та законодавстві України, нормах міжнародного права в кібернетичному просторі України. Тобто як один із напрямів державної політики кібербезпеки варто визначити і забезпечення кібернетичного суверенітету України;

– вдосконалення державного регулювання розвитку інформаційної сфери шляхом створення нормативно-правових і економічних передумов для розвитку національної інформаційної інфраструктури та ресурсів, впровадження новітніх технологій у такій сфері, наповнення внутрішнього та світового інформаційного простору достовірною інформацією про Україну. Щодо створення нормативно-правових умов, то маю певні корективи. Нині вже ухвалені та діють багато законів і підзаконних нормативних актів у сфері інформаційних відносин (понад 4 000) [6, с. 127], тому ухвалення нових актів має бути не самоціллю, а дійсно відбивати об'єктивну потребу в регулюванні нових суспільних відносин. У такому аспекті проблематика систематизації інформаційного законодавства ще не вичерпала свою актуальність [11]. А як напрям державної політики кібербезпеки можна визначити здійснення систематизації інформаційного (кібербезпекового) законодавства України, створення необхідних передумов для розвитку кіберсфери загалом і гарнтування кібербезпеки зокрема;

– активне залучення засобів масової інформації до запобігання і протидії корупції, зловживанням службовим становищем, іншим явищам, які загрожують національній безпеці України. Протидія будь-яким явищам, які загрожують кібербезпеці України, шляхом залучення засобів масової інформації (далі – ЗМІ) матиме позитивні наслідки в тому разі, якщо вони будуть незалежними, але, на жаль, майже всі українські ЗМІ належать або підконтрольні певним політичним силам. Як напрям виокремлю залучення ЗМІ для протидії кіберзагрозам;

– забезпечення неухильного дотримання конституційних прав на свободу слова, доступ до інформації, недопущення неправомірного втручання органів державної влади, органів місцевого самоврядування, їх посадових осіб у діяльність засобів масової інформації та журналістів, заборони цензури, дискримінації в інформаційній сфері та переслідування журналістів за політичні позиції, за виконання професійних обов'язків, за критику. Тобто забезпечення існування правової держави;

– вжиття комплексних заходів щодо захисту національного інформаційного простору і протидії монополізації інформаційної сфери України [14]. Знову ж таки, адаптуючи таку норму до теми дослідження, як напрям державної політики кібербезпеки визначу вжиття комплексних заходів щодо захисту національного кібернетичного простору та протидії монополізації кібернетичної сфери України.

Акцентую увагу на тому, що перелік напрямів державної політики кібербезпеки не може бути статичним, оскільки відбуваються постійні зміни в кіберсуспільстві, тому існує потреба швидкої реакції й ужиття відповідних заходів.

Корисним для запозичення є Указ Президента Російської Федерації (далі – РФ) «Про Стратегію національної безпеки Російської Федерації». У документі зазначено, що головними напрямами гарантування державної та суспільної безпеки є посилення ролі держави як гаранта безпеки особистості і прав власності, вдосконалення правового регулювання попередження злочинності (зокрема й в інформаційній сфері), корупції, тероризму й екстремізму, поширення наркотиків і боротьби з такими явищами, розвиток взаємодії органів гарантування державної безпеки та правопорядку із громадянським суспільством, підвищення довіри громадян до правоохоронної та судової систем РФ, ефективності захисту прав і законних інтересів російських громадян за кордоном, розширення міжнародного співробітництва в області державної та громадської безпеки [18].

У Доктрині інформаційної безпеки України [19] можна також виокремити напрями державної політики кібербезпеки. У документі сформульовано 4 пункти, що мають бути пріоритетами державної політики в інформаційній сфері. Зважаючи на тему мого дослідження, визначу лише деякі з них:

– необхідність створення інтегрованої системи моніторингу (аналізу, оцінки, прогнозу) кіберзагроз і формування алгоритмів реагування на них на оперативному, тактичному та стратегічному рівнях;

– удосконалення системи управління національною системою кібербезпеки, зокрема й через підвищення рівня відповідальності та контролю виконання покладених на суб'єкти кібербезпеки завдань;

– законодавче регулювання механізму виявлення, фіксації, блокування та видалення з кібернетичного простору держави інформації, яка становить загрозу національним інтересам у кібернетичній сфері, тобто є кіберзагрозою;

– створення і розвиток структур, що відповідають за інформаційно-психологічну безпеку (кібернетично-психологічну), насамперед, у Збройних силах України, з урахуванням практики держав-членів НАТО, а також і в Національній поліції – Кіберполіції, згідно з загальною концепцію розумного балансу розмежування повноважень у реалізації державної кібербезпекової політики її суб'єктами;

– розвиток і захист технологічної інфраструктури гарантування кібернетичної безпеки України;

– удосконалення механізмів гарантування безпеки об'єктів критичної інформаційної інфраструктури;

– побудова дієвої та ефективної системи стратегічних комунікацій [7];

– розвиток механізмів взаємодії держави й інститутів громадянського суспільства в реалізації державної кібербезпекової політики, зокрема і в частині протидії гібридній війні й одному з її проявів – інформаційній агресії проти України та кібернетичним атакам;

– ефективна, проактивна і наступальна боротьба з дезінформацією та ворожою пропагандою з боку Російської Федерації. Окрім України, російська пропаганда впливає і на розвиток інших розвинених демократичних європейських країн. Факт впливу російської пропаганди на Європу було визнано у відповідній резолюції щодо протидії ворожій Євросоюзу пропаганді, яка надходить із Росії. Основною метою дезінформації та ворожої пропаганди є підрив і компрометація єдності, сіяння сумніву щодо сталих європейських цінностей та інтересів. У згаданому документі зазначено, що така пропаганда є частиною гібридної війни і націлена на те, щоб: 1) викривити правду; 2) посіяти сумніви і ворожнечу між країнами союзу; 3) послабити стратегічну єдність Європейського Союзу (далі – ЄС) та північноамериканських партнерів; 4) паралізувати процес прийняття рішень; 5) дискредитувати інститути ЄС і трансатлантичне партнерство. Європарламент у зазначеній резолюції визнав, що російській уряд активно використовує цілий спектр інструментів і засобів для атак на диплматичні цінності з метою розколу Європи, для забезпечення підтримки зсередини країни і створення уявлення про розбіжності між країнами Східного сусідства та ЄС [22].

– посилення спроможностей суб'єктів гарантування національної безпеки щодо протидії спеціальним кібернетичним операціям, які несуть кіберзагрозу українській державі загалом;

– виявлення і притягнення до відповідальності, забезпечення невідворотності покарання винних згідно з українським законодавством суб'єктів українського кібернетичного простору, що створені та/або використовуються державою-агресором для ведення кібернетичної війни проти України, унеможливлення їхньої підривної діяльності;

– недопущення використання кібернетичного простору держави в деструктивних цілях або для дій, що спрямовані на дискредитацію України на міжнародному рівні [19].

Беручи до уваги існування такого новоствореного органу, як Національний координаційний центр кібербезпеки, який є робочим органом Ради національної безпеки і оборони України, доцільно говорити і про те, що частина його завдань також можуть бути покладені в основу аналізованої мною кібербезпекової політики.

Центр має забезпечити координацію діяльності суб'єктів національної безпеки й оборони України під час реалізації Стратегії кібербезпеки України, підвищити ефективність системи державного управління у формуванні та реалізації державної політики у сфері кібербезпеки. Тому, аналізуючи його основні завдання, зауважу, що вони також можуть бути визначені як напрями державної кібербезекової політики.

Такими напрямами, на мою думку, є:

– узагальнення (імплементація – І. Д.) міжнародного досвіду у сфері гарантування кібербезпеки, оскільки наша держава, як і всі інші, існує не ізольовано, а в тісній співпраці в різних сферах;

– прогнозування та виявлення потенційних і реальних загроз у сфері кібербезпеки, яке сприятиме їх відверненню та полегшенню ліквідації негативних наслідків;

– визначення пріоритетів для залучення міжнародної технічної допомоги у сфері гарантування кібербезпеки;

– вивчення міжнародного досвіду створення і функціонування національних систем кібербезпеки, поширення його між організаціями, установами і закладами відповідно до компетенції, проведення моніторингу щодо його впровадження в Україні;

– участь у забезпеченні розроблення і впровадження суб'єктами гарантування кібербезпеки

механізмів обміну інформацією, необхідною для організації реагування на кібератаки та кіберінциденти, усунення їх чинників і негативних наслідків [20].

Пріоритетними напрямами державної політики щодо посилення інформаційної (зокрема й кібернетичної) безпеки держави є:

– реформування кібернетичного законодавства як сегмента інформаційного законодавства України, особливо в частині не лише чіткого визначення сучасних загроз кібернетичній безпеці держави, але й механізмів державної політики, зокрема і симетричних кібернетичних заходів;

– дослідження питань захисту об'єктів критичної інфраструктури від кібератак. З такою метою має бути визначено та класифіковано критичні об'єкти, кібератаки на які можуть завдати значної шкоди державі та створити загрози міжнародним стосункам у кіберпросторі;

– сприяння розробці вітчизняної інноваційної продукції, що може бути використана з метою посилення кібернетичної безпеки держави;

– завершення імплементації положень Конвенції Ради Європи про кіберзлочинність у національне законодавство;

– оптимізація системи підготовки кадрів у сфері кібербезпеки для потреб Збройних сил України й інших органів сектору безпеки й оборони України;

– сприяння більш активній політиці державних безпекових інституцій щодо інформування населення про кіберзагрози;

– забезпечення безперервного підвищення кваліфікації військовослужбовців, державних службовців і працівників, що задіяні на ключових об'єктах критичної інфраструктури;

– сприяння недопущенню мілітаризації кіберпростору;

– підтримка наявних багатосторонніх навчань із протидії кібернападам на державну інформаційну інфраструктуру, ініціювання нових видів таких навчань [23, с. 129].

Отже, у результаті здійсненого дослідження, можу дійти висновку, що державна політика кібернетичної безпеки визначається, зважаючи на пріоритетність національних інтересів і загроз кібернетичній безпеці України, і здійснюється шляхом реалізації відповідних концепцій, доктрин, стратегій і програм у різних сферах кібернетичної безпеки відповідно до чинного законодавства.

Державна кібербезпекова політика складається із двох основних взаємопов'язаних блоків:

1) діяльності винятково державних органів;

2) діяльності недержавних інституцій, інституцій громадянського суспільства, інформаційного суспільства в інформаційній сфері.

Запропоновано легітимізувати в законодавчих актах категорію «кібернетичне суспільство», тобто суспільство, в якому діяльність людей ґрунтується на використанні послуг, що надаються за допомогою надбань кібернетики.

Основною метою державної політики кібербезпеки є управління реальними та потенційними кіберзагрозами та небезпеками з метою створення необхідних умов для задоволення кібернетичних потреб людини і громадянина, а також реалізації національних інтересів у кібернетичній сфері.

Як напрями державної політики кібербезпеки варто визначити: забезпечення кібернетичного суверенітету України; здійснення систематизації інформаційного (кібербезпекового) законодавства України; створення необхідних передумов для розвитку кіберсфери загалом і гарантування кібербезпеки зокрема; залучення ЗМІ для протидії кіберзагрозам; забезпечення існування правової держави; вжиття комплексних заходів щодо захисту національного кібернетичного простору та протидії монополізації кібернетичної сфери України.

Акцентую увагу на тому, що перелік напрямів державної політики кібербезпеки не може бути статичним, оскільки відбуваються постійні зміни в кіберсуспільстві, тому існує потреба швидкої реакції та ужиття відповідних заходів.

Література

1. Порошенко ввел в действие решение СНБО об усилении мер по кибербезопасности [Электронный ресурс]. – Режим доступа : https://www.rbc.ua/rus/news/belarusi-ofitsialno-podtverdili-vezd-ukraintsa-1504166704.html.

2. Стратегічні комунікації : [словник] / Т. Попова, В. Ліпкан ; за заг. ред. доктора юридичних наук В. Ліпкана. – К. : ФОП О.С. Ліпкан, 2016. – 416 с.

3. Ліпкан В., Ліпкан О. Національна і міжнародна безпека у визначеннях та поняттях. – Вид. 2-ге, доп. і перероб. – К. : Текст, 2008. – 400 с.

4. Ліпкан В. Національна безпека України : [навчальний посібник] / В. Ліпкан. – 2-ге вид. – К. : Видавництво «КНТ», 2009. – 576 с.

5. Ліпкан В. Інформаційна безпека України в умовах євроінтеграції : [навчальний посібник] / В. Ліпкан, Ю. Максименко, В. Желіховський. – К. : Видавництво «КНТ», 2006. – 280 с.

6. Рудник Л. Право на доступ до інформації : дис. … канд. юрид. наук : спец. 12.00.07 «Адміністративне право і процес; фінансове право; інформаційне право» / Л. Рудник ; Національний університет біоресурсів і природокористування України. – К., 2015. – 247 с.

7. Рудник Л. Роль та місце стратегічних комунікацій в сучасному суспільстві знань / Л. Рудник [Електронний ресурс]. – Режим доступу : http://goal-int.org/rol-ta-mistse-strategichnih-komunikatsij-v-suchasnomu-suspilstvi-znan.

8. Діордіца І. Поняття та зміст кіберзлочинності / І. Діордіца [Електронний ресурс]. – Режим доступу : http://goal-int.org/ponyattya-ta-zmist-kiberzlochinnosti.

9. Діордіца І. Сучасний кібертероризм : аспекти правового регулювання / І. Діордіца [Електронний ресурс]. – Режим доступу : http://goal-int.org/suchasnij-kiberterorizm-aspekti-pravovogo-regulyuvannya.

10. Діордіца І. Система забезпечення кібербезпеки : сутність та призначення / І. Діордіца [Електронний

ресурс]. – Режим доступу : http://goal-int.org/sistema-zabezpechennya-kiberbezpeki-sutnist-ta-priznachennya.

11. Залізняк В. Систематизація інформаційного законодавства України : автореф. дис. … докт. юрид. наук : спец. 12.00.07 «Адміністративне право і процес; фінансове право; інформаційне право» / В. Залізняк. – К., 2011. – 23 с.

12. Кормич Б. Інформаційне право : [підручник для вузів] / Б. Кормич. – Харків : Бурун і К, 2011. – 333 с.

13. Андріяш В. Державна політика : концептуальні аспекти визначення / В. Андріяш. // Державне управління: удосконалення та розвиток. – 2013. – № 9 [Електронний ресурс]. – Режим доступу : http://nbuv.gov.ua/UJRN/Duur_2013_9_6.

14. Про основи національної безпеки України : Закон України від 19 червня 2003 р. [Електронний ресурс]. – Режим доступу : http://zakon0.rada.gov.ua/laws/show/964-15.

15. Проект Закону «Про основні засади забезпечення кібербезпеки України» [Електронний ресурс]. – Режим доступу : http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=55657.

16. Відкрите суспільство : базові цінності [Електронний ресурс]. – Режим доступу : http://sd.net.ua/2010/07/10/vidkrite-suspilstvo-bazovi-cinnosti.html

17. Проект Закону України «Про Інформаційний суверенітет та інформаційну безпеку України» [Електронний ресурс]. – Режим доступу: http://uacm.kharkov.ua/ukr/index.shtml?ulaws/usuvetr.htm.

18. «О Стратегии национальной безопасности Российской Федерации» : Указ Президента Российской Федерации от 31 декабря 2015 г. [Электронный ресурс]. – Режим доступа : https://rg.ru/2015/12/31/nac-bezopasnost-site-dok.html.

19. Доктрина інформаційної безпеки України від 25 лютого 2017 р. [Електронний ресурс]. – Режим доступу : http://www.president.gov.ua/documents/472017-21374.

20. Положення про Національний координаційний центр кібербезпеки від 7 червня 2016 р. [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/242/2016.

21. НБУ создаст Центр киберзащиты для банков [Электронный ресурс]. – Режим доступа : Новости https://www.rbc.ua/rus/news/nbu-sozdast-tsentr-kiberzashchity-bankov-1499335025.html.

22. В Европарламенте признали российскую пропаганду и призвали бороться с ней [Электронный ресурс]. – Режим доступа : http://www.segodnya.ua/world/v-evroparlamente-priznali-rossiyskuyu-propagandu-i-prizvali-borotsya-s-ney-772845.html.

23. Косогов О. Пріоритетні напрямки державної політики щодо забезпечення безпеки національного кіберпростору / О. Косогов // Збірник наукових праць Харківського національного університету Повітряних Сил імені Івана Кожедуба. – 2014. – Вип. 3. – С. 127–130.

Анотація

Діордіца І. В. **Напрями державної політики кібербезпеки. –** Стаття.

У статті автором було здійснено аналіз нормативно-правових актів у безпековій сфері та виокремлено ті норми, які безпосередньо стосуються державної політики кібербезпеки, визначено основні напрями державної політики кібербезпеки, виявлено чинники, які визначають державну політику кібернетичної безпеки та її основну мету. Запропоновано авторське розуміння категорії «кібернетичне суспільство». Акцентовано увагу на тому, що перелік напрямів державної політики кібербезпеки не може бути статичним, оскільки відбуваються постійні зміни в кіберсуспільстві, тому існує потреба швидкої реакції та вжиття відповідних заходів.

Ключові слова: кібербезпека, кіберпростір, державна політика, напрями державної політики, кіберсфера, напрями державної політики кібербезпеки.

Аннотация

Диордица И. В. **Направления государственной политики кибербезопасности. –** Статья.

В статье автором осуществлен анализ нормативно-правовых актов в сфере безопасности, и выделены те нормы, которые имеют непосредственное отношение к государственной политике кибербезопасности, определены основные направления государственной политики кибербезопасности, выявлены факторы, определяющие государственную политику кибернетической безопасности и ее основную цель. Предложено авторское видение категории «кибернетическое общество». Акцентировано внимание на том, что перечень направлений государственной политики кибербезопасности не может быть статичным, поскольку происходят постоянные изменения в киберсообществе, поэтому необходима быстрая реакция и возможность применения соответствующих мер.

Ключевые слова: кибербезопасность, киберпространство, государственная политика, направления государственной политики, киберсфера, направления государственной политики кибербезопасности.

Summary

Diorditsa I. V. **Directions of the state policy of cybersecurity. –** Article.

It was concluded that the state policy on cybernetic security is determined taking into account the priority of the national interests and threats to the cyber security of Ukraine and is carried out by implementing of the relevant doctrines, strategies, concepts and programs in various spheres of the cyber security in accordance with the current legislation.

It was marked that the state policy of cyber security consists of two main interconnected blocks: the activities of exclusively state bodies and the activities of non-state institutions, civil society institutions, information society in the information sphere.

Authors vision for category “cyber society” was proposed, that is, a society in which the activities of people are based on the use of services provided through the achievements of cybernetics.

It was defined that the main goal of the state policy of cybersecurity is to manage actual and potential cyber threats and dangers in order to create the necessary conditions for meeting the information needs of man and citizen, as well as the realization of national interests.

It was offered to define as the directions of the state policy on cybersecurity: ensuring of the cybernetic sovereignty of Ukraine; carrying out of the systematization of information (cybersecurity) legislation of Ukraine; the creation of the necessary prerequisites for the development of the cyber sphere as a whole, as well as the provision of cyber security in particular; involvement of the media in countering the cyber threats; ensuring of the existence of a law-governed state; taking of the comprehensive measures to protect the national cyber space and counteracting the monopolization of the cyber sphere of Ukraine.

It was emphasized that the list of state policies for cybersecurity cannot be static, as there are ongoing changes in the cybersociety, therefore, there is a need for quick reaction and taking of the appropriate measures.

Key words: cybersecurity, cyberspace, state policy, directions of state policy, cybersphere, directions of state policy on cybersecurity.