УДК 342.9

DOI 10.37566/2707-6849-2020-4(33)-3

Ігор ДІОРДИЦА,
*професор кафедри приватного та публічного права
Київського національного університету технологій та
дизайну, доктор юридичних наук, доцент
ORCID 0000-0001-7765-6591*

СУЧАСНИЙ ПРАВОВИЙ ЗМІСТ ОПТИМІЗАЦІЇ НАПРЯМІВ АДМІНІСТРАТИВНО-ПРАВОВОГО РЕГУЛЮВАННЯ ДЕРЖАВНОЇ КІБЕРБЕЗПЕКОВОЇ ПОЛІТИКИ

Постановка проблеми дослідження. Національна безпека України, її економічне процвітання, соціальне та інформаційне благополуччя дедалі 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 перед можливими негативними наслідками протиправного використання кіберпростору. Щороку зростає кількість кібернападів та різноманітних кіберінцидентів у найбільш важливих сферах життєдіяльності нашої держави.

З цих умов одним із головних завдань держави є вжиття проактивних заходів, що сформулюють гарантовані умови для реалізації національних інтересів у кіберпросторі. Один із напрямів реалізації даного завдання полягає у формуванні резервних копій (бекапів) інформаційних ресурсів держави, а також формування ефективної національної системи кібербезпеки, у тому числі системи забезпечення кібербезпеки, що дозволять принципово зменшити (а подекуди – унеможливити

повністю) наслідки від кібератак, а також створити умови для своєчасного прогнозування імовірності реалізації тих чи інших кіберінцидентів, що й зумовлює **актуальність дослідження**.

Сьогодні поняття політики втрачає свою початкову суть тому, що основна діяльність держави прямує все ж таки не на перерозподіл влади (хоча це лежить в основі), а на задоволення потреб та законних інтересів громадян, та сама політика вже трактується як певна стратегія прийняття і практичної реалізації обов'язкових для суспільства рішень із того чи іншого питання. Оскільки центральним актором 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, оскільки пов'язана з діяльністю зі здійснення державної влади.

Метою дослідження є аналіз сучасного стану державної політики у сфері кібербезпеки та вироблення пропозицій щодо оптимізації напрямів адміністративно-правового регулювання державної кібербезпекової політики.

Виклад основного матеріалу. Державна політика – це цілеспрямована діяльність органів державної влади для створення умов з 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 «напрямок дій або утримання від неї, обрані державними органами для розв'язання певної чи сукупності взаємно пов'язаних проблем». Водночас для пострадянських країн термін «державна політика» не обмежується лише діями одного актора в особі держави, а вміщує дії всіх акторів політичної системи, які мають відношення до предмета справи і можуть посприяти розв'язанню конкретної проблеми чи пропозиції. Для української науки більш характерним є вживання терміна «державна політика», який вміщує майже всі аспекти управління країною [1].

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 і як реакція держави на конкретні проблеми суспільства, або груп у цьому 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. Виходячи з цього, державна політика кібербезпеки повинна бути спрямована на вирішення конкретних проблем, які виникають у кіберпросторі, тобто тих, які вже реально існують і чинять негативний вплив на суспільні відносини.

Оскільки питання кібербезпеки має безпосереднє відношення до безпеки в цілому, то для здійснення дослідження використаю основоположні нормативно-правові акти у сфері безпекознавства.

Протягом останніх років керівництвом держави було здійснено низку важливих, однак поки що здебільшого декларативних заходів, спрямованих на розбудову за початковим задумом повноцінної національної системи кібербезпеки, посилення заходів кібербезпеки держави [2]. Наприклад, у Законі України «Про основи національної безпеки України» 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 цьому Законі акцентована увага на державній політиці.

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

Оскільки державна політика кібербезпеки на даному етапі трактується в якості складової частини інформаційної політики, то, використовуючи словник «Стратегічні комунікації» [4, с. 80], зазначу, що державна політика кібербезпеки складається із двох основних взаємопов'язаних блоків:

- 1) діяльність винятково державних органів;
- 2) діяльність недержавних інституцій, інституцій громадянського суспільства, інформаційного суспільства в інформаційній сфері.

Повертаючись до аналізу положень Закону «Про основи національної безпеки України», зауважу, що в ньому наголос 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 із такими термінами, як «безпека», «захист», «охорона», «оборона» тощо [5, с. 133]. Відповідним чином дані напрями в контексті кібербезпеки знайшли своє відображення у чотирьох базових концептах: кіберзахист, кібербезпека та кіберохорона, кібероборона.

Варто пам'ятати, що альтернатива вибору засобів, методів, способів і шляхів забезпечення кібернетичної безпеки України безпосередньо зумовлена 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 безпеки в кібернетичній сфері.

Отже, під державною політикою кібербезпеки варто розуміти діяльність держави в кібернетичній сфері, що спрямована на задоволення інформаційних потреб людини і громадянина через формування відкритого інформаційного суспільства (кібернетичного суспільства) 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 при забезпеченні кібернетичної безпеки на внутрішньодержавному та міжнародному рівнях.

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

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

Нині не всі нормативно-правові акти відповідають викликам сьогодення та реальним кіберзагрозам. Тому підтримую пропозиції І. Арістової [6, с. 156], яка вважає, що для реалізації національних інтересів в інформаційній (кібернетичній. – Авт.) сфері слід переглянути пріоритети державної політики, розробити нові концептуальні підходи щодо регулювання ринку інформаційно-комунікаційних технологій, інформаційної та інвестиційної політики, розвитку інформаційного (кібернетичного. – Авт.) законодавства і забезпечення інформаційної (кібернетичної. – Авт.) безпеки.

Напрями державної кібербезпекової політики (далі – ДКБП) відповідно до Закону України «Про основні засади забезпечення кібербезпеки України». У цьому Законі напрями державної політики визначені таким чином:

– створення захищеного національного сегмента кіберпростору, що сприятиме підтриманню відкритого суспільства і забезпечуватиме безпечне використання цього простору суспільством. Категорія «відкрите суспільство» є новою в юридичній термінології і тому потребує тлумачення задля уникнення виникнення прогалин та колізій у законодавстві. Відкрите суспільство – це суспільство, яке базується на визнанні того факту, що ніхто не має монополії на істину (плюралізм), що різні люди мають різні погляди та інтереси, і що існує потреба в установах, які захищали б права усіх людей і давали б їм змогу жити разом у

мирі і злагоді (філософська категорія. – Авт.). Основними рисами, що характеризують відкрите суспільство, є верховенство права, демократично обрана влада, інститути громадянського суспільства, захист прав меншин [7], 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 відносяться до внутрішньої компетенції держави. – Авт.) і нейтралізація посягань на її інформаційні ресурси з боку інших держав;

- посилення обороноздатності держави у кіберпросторі (кібероборона);

- боротьба з кіберзлочинністю та кібертероризмом.

Необхідне чітке визначення відповідальних суб'єктів за забезпечення цього напрямку, як і всіх інших напрямів державної безпеки в будь-якій сфері. Нині кіберзлочинність – актуальна проблема, з якою зіткнулись усі країни і яка постійно збільшується за масштабами та завданими збитками. Зокрема, у липні 2017 року Національним банком України було заявлено про створення Центру кіберзахисту Національного банку України [8]. Акцентую увагу на відсутності законодавчого визначення поняття вищезазначеного явища. У Законі України «Про основні засади забезпечення кібербезпеки України» під кіберзлочином визначають суспільно небезпечне винне діяння у кіберпросторі, передбачене законодавством України про кримінальну відповідальність, а під кіберзлочинністю – сукупність кіберзлочинів.

Поняття кібертероризму виникло на межі XX–XXI століть, задовго до початку масового використання Інтернету. Термін «кібертероризм» є синтезом понять «кібербезпековий простір» та «тероризм». Під кібертероризмом пропонується розуміти протиправне діяння, яке вчиняється з ціллю досягнення негативних наслідків, наприклад отримання матеріальних благ чи загрози інформаційній безпеці держави. Кібертероризм має місце в кібербезпековому просторі [9];

- зниження рівня уразливості об'єктів кіберзахисту, в тому числі об'єктів критичної інформаційної інфраструктури. Даний 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 цей рівень? Як варіант – «попередження уразливості об'єктів кіберзахисту та ліквідація негативних наслідків»;

- забезпечення повноправної участі України в загальноєвропейській та регіональних системах забезпечення кібербезпеки. Україна бере активну участь у міжнародній безпековій діяльності, наприклад ратифікація Конвенції про кіберзлочинність, участь у розробленні та прийнятті Статуту ООН. Таким чином,

обмеження напрямів участі України лише загальноєвропейською та регіональною системою забезпечення кібербезпеки є некоректним. У вузькому сенсі система забезпечення кібербезпеки – сукупність суб'єктів, які здійснюють свою діяльність у кіберпросторі [10], тобто регіональні та європейська системи є представленими більшим колом суб'єктів та масштабом здійснення ними своєї діяльності;

- дотримання міжнародних зобов'язань щодо боротьби з кіберзлочинністю та кібертероризмом. Нині існує незначна кількість спеціальних нормативно-правових актів як універсального, так і регіонального характеру, в яких держави сформулювали б певні зобов'язання щодо боротьби з кібертероризмом та кіберзлочинністю. Одним із таких актів є Конвенція про кіберзлочинність. Держави, що приєдналися до Конвенції, взяли зобов'язання переглянути своє законодавство з метою приведення його у відповідність з рекомендаціями, викладеними в цьому міжнародному документі.

Напрями ДКБП відповідно до Закону України «Про основи національної безпеки України». Також, зважаючи на постулювання мною того факту, що нині кібербезпека є не лише складовою інформаційної безпеки, а й виступає окремим компонентом національної безпеки, то доцільним при визначенні 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. Це ще одна нова правова категорія, дефініція якої міститься в проекті Закону «Про інформаційний суверенітет та інформаційну безпеку України». Інформаційний суверенітет України – це право держави на формування і здійснення національної інформаційної політики відповідно до Конституції і законодавства України, міжнародного права в національному інформаційному просторі України. Також у словнику «Стратегічні комунікації» 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 [4, с. 168–169]. Виходячи із вищезазначених положень вважаю за необхідне виокремити феномен «кібернетичного суверенітету», під яким пропонується розуміти невід'ємне право держави на формування і здійснення національної кібербезпекової політики відповідно до національних інтересів, ґрунтуючись на Конституції України і законодавстві України, враховуючи норми міжнародного права в кібернетичному просторі України. Тобто одним із напрямів державної політики кібербезпеки варто визначити забезпечення кібернетичного суверенітету України;

- вдосконалення державного регулювання розвитку інформаційної сфери шляхом створення нормативно-правових та економічних передумов для розвит-

ку національної інформаційної інфраструктури та ресурсів, впровадження новітніх технологій у цій сфері, наповнення внутрішнього та світового інформаційного простору достовірною інформацією про Україну. Щодо створення нормативно-правових умов, то маю певні корективи. Нині вже ухвалена та діє значна кількість законів та підзаконних нормативних актів у сфері інформаційних відносин (більше 4500) [11, с. 127], тому прийняття нових актів має виступати не самоцілью, а справді відбивати об'єктивну потребу в регулюванні нових суспільних відносин. У даному аспекті проблематика систематизації інформаційного законодавства ще не вичерпала своєї актуальності [12]. А як напрям державної політики кібербезпеки можна визначити здійснення систематизації інформаційного (кібербезпекового) законодавства України, створення необхідних передумов для розвитку кіберсфери в цілому, а також забезпечення 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 ЗМІ матиме позитивні наслідки в тому випадку, 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, заборона 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 та протидії монополізації інформаційної сфери України. Знову ж таки, адаптуючи дану 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 та ужиття відповідних заходів. Переконали, що теоретично потрібно спрямовувати науковий пошук не лише на механізми захисту прав і свобод людини, а й на роль держави в трансформації суспільства і зростання ролі інформаційного чинника, зокрема кібернетичній глобалізації.

Напрями ДКБП відповідно до Доктрини інформаційної безпеки України. Оскільки кібербезпека є тісно пов'язаною з інформаційною безпекою, доцільно згадати і про Доктрину інформаційної безпеки України, аналіз положень якої

дозволив виокремити напрями державної політики кібербезпеки. У документі сформульовано чотири пункти, що мають бути пріоритетами державної політики в інформаційній сфері. З урахуванням теми мого дослідження визначу лише деякі з них:

- необхідність створення інтегрованої системи моніторингу (аналіз, оцінки, прогноз) кіберзагроз та формування алгоритмів реагування на них на оперативному, тактичному та стратегічному рівнях;
- удосконалення системи управління національною системою кібербезпеки, у тому числі через підвищення рівня відповідальності та контролю за виконанням покладених на суб'єктів 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 концепцією розумного балансу розмежування повноважень у реалізації державної кібербезпекової політики її суб'єктами;
- розвиток і захист технологічної інфраструктури забезпечення кібернетичної безпеки України;
- удосконалення механізмів забезпечення безпеки об'єктів критичної інформаційної інфраструктури;
- побудова дієвої та ефективної системи стратегічних комунікацій;
- розвиток механізмів взаємодії держави та інститутів громадянського суспільства в реалізації державної кібербезпекової політики, в тому числі в частині протидії гібридній війні та одному з її проявів – інформаційній агресії проти України та кібернетичним атакам;
- ефективна, проактивна та 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 з Росії. Основною метою дезінформації та ворожої пропаганди є підриз та компрометація єдності, посів сумніву щодо сталих європейських цінностей та інтересів. У згаданому документі визначено, 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 ЄС та північноамериканських партнерів; 4) паралізувати процес прийняття рішень; 5) дискредитувати інститути ЄС і трансатлантичне партнерство. Європарламент у даній резолюції визнав, що російській уряд активно використовує цілий спектр засобів та інструментів

для атак на дипломатичні цінності з метою розколу Європи, для забезпечення підтримки зсередини країни і створення уявлення про розбіжності між країнами Східного сусідства та ЄС [13];

- посилення спроможностей суб'єктів забезпечення національної безпеки щодо протидії спеціальним кібернетичним операціям, які несуть кіберзагрозу Українській державі в цілому;

- виявлення та 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, та унеможливлення їхньої підривної діяльності;

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

Висновки. Отже, пріоритетними напрямками оптимізації державної політики щодо посилення адміністративно-правового регулювання кібернетичної безпеки держави варто виділити й такі:

- реформування кібернетичного законодавства як сегмента інформаційного законодавства України, особливо в частині не лише чіткого визначення сучасних загроз та небезпек кібернетичній безпеці держави, а й механізмів державної політики, в тому числі симетричних кібернетичних заходів;

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

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

- завершення імплементації положень Конвенції РЄ про кіберзлочинність у національне законодавство;

- оптимізація системи підготовки кадрів у сфері кібербезпеки для потреб Збройних сил України та інших органів сектору безпеки і оборони України;

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

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

- сприяння недопущенню мілітаризації кіберпростору;

- підтримка як існуючих багатосторонніх навчань з протидії кібернападам на державну інформаційну інфраструктуру, так і ініціювання нових видів таких навчань.

Перелік використаних джерел

1. Андріяш В. І. Державна політика: концептуальні аспекти визначення. Державне управління: удосконалення та розвиток: електрон. наук. фахове вид. 2013. № 9. URL: http://nbuv.gov.ua/UJRN/Duur_2013_9_6
2. Порошенко ввел в действие решение СНБО об усилении мер по кибербезопасности. URL: <https://www.rbc.ua/rus/news/belarusi-ofitsialno-podtverdili-vezd-ukraintsa-1504166704.html>
3. Ліпкан В. А., Ліпкан О. С. Національна і міжнародна безпека у визначеннях та поняттях. 2-е вид. допов. і перероб. Київ: Текст, 2008. 400 с.
4. Попова Т. В., Ліпкан В. А. Стратегічні комунікації: словник /за заг. ред. д-ра юрид. наук. В. А. Ліпкана. Київ: О. С. Ліпкан, 2016. 416 с.
5. Кормич Б. А. Інформаційне право: підручник для вузів. Харків: Бурун і К, 2011. 334 с.
6. Арістова І. В. Державна інформаційна політика: організаційно-правові аспекти: монографія / за заг. ред. О. М. Бандурки. Харків: Ун-т внутр. справ, 2000. 368 с.
7. Відкрите суспільство: базові цінності. ASD inform Україна: сайт. URL: <http://sd.net.ua/2010/07/10/vidkrite-suspilstvo-bazovi-cinnosti.html>
8. НБУ создаст Центр киберзащиты для банков. РБК – Украина. Новости: сайт. URL: <https://www.rbc.ua/rus/news/nbu-sozdast-tsentr-kiberzashchity-bankov-1499335025.html>
9. Діордіца І. В. Поняття і зміст кібертероризму. Прикарпатський юридичний вісник. 2016. № 3(12). URL: http://nbuv.gov.ua/UJRN/Pjyv_2016_3_15.
10. Діордіца І. В. Система забезпечення кібербезпеки: сутність та призначення. Підприємництво, господарство і право. 2017. № 7 (257). С. 109–116.
11. Паращич І. М. Права громадян і права пацієнтів та їх захист у системі охорони здоров'я України. Економіка та держава. 2009. № 2. С. 71–72.
12. Залізняк В. А. Систематизація інформаційного законодавства України: автореф. дис. ... канд. юрид. наук: 12.00.07. Київ, 2011. 18 с.
13. В Европарламенте признали российскую пропаганду и призвали бороться с ней. Сегодня. 2016. 23 ноября. URL: <http://www.segodnya.ua/world/v-evroparlamente-priznali-rossiyskuyu-propagandu-i-prizvali-borotsya-s-ney-772845.html>

References

1. Andriyash V. I. State policy: conceptual aspects of definition. Public administration: improvement and development. 2013. Vol. 9. URL: http://nbuv.gov.ua/UJRN/Duur_2013_9_6. [ukr.]
2. Poroshenko enacted NSDC decision to strengthen cybersecurity measures. URL: <https://www.rbc.ua/rus/news/belarusi-ofitsialno-podtverdili-vezd-ukraintsa-1504166704.html>. [russ.]
3. Lipkan V. A., Lipkan O. S. National and international security in definitions and concepts. Kyiv: Text, 2008. 400 p. [ukr.]

4. Popova T. V., Lipkan V. A. *Strategic communications: a dictionary*. Kyiv: O. S. Lipkan, 2016. 416 p. [ukr.]
5. Kormich B. A. *Information law: a textbook for universities*. Kharkiv: Burun and K, 2011. 334 p. [ukr.]
6. Aristova I. V. *State information policy: organizational and legal aspects: monograph*. Kharkiv: University of Internal Affairs, 2000. 368 p. [ukr.]
7. *Open society: basic values*. ASD inform Ukraine. URL: <http://sd.net.ua/2010/07/10/vidkrite-suspilstvo-bazovi-cinnosti.html>. [ukr.]
8. *The NBU will create a Cyber Security Center for banks*. RBC - Ukraine. News. URL: <https://www.rbc.ua/rus/news/nbu-sozdast-tsentr-kiberzashchity-bankov-1499335025.html>. [russ.]
9. Diorditsa I. V. *The concept and content of cyberterrorism*. Prykarpattya Legal Bulletin. 2016. Vol. 3 (12). URL: http://nbuv.gov.ua/UJRN/Pjyv_2016_3_15. [ukr.]
10. Diorditsa I. V. *Cybersecurity system: essence and purpose*. Entrepreneurship, economy and law. 2017. Vol. 7 (257). P. 109–116. [ukr.]
11. Parashchych I. M. *Rights of citizens and rights of patients and their protection in the health care system of Ukraine*. Economy and state. 2009. Vol. 2. P. 71–72. [ukr.]
12. Zalzniak V. A. *Systematization of information legislation of Ukraine*. (Candidate's thesis). Kyiv, 2011. 18 p. [ukr.]
13. *The European Parliament recognized Russian propaganda and called on to fight it*. Today. 2016, November 23. URL: <http://www.segodnya.ua/world/v-evroparlamente-priznali-rossiyskuyu-propagandu-i-prizvali-borotsya-s-ney-772845.html>. [russ.]

ДИОРДИЦА І. Сучасний правовий зміст оптимізації напрямів адміністративно-правового регулювання державної кібербезпекової політики.

У статті надано авторські результати визначення концептуальних положень оптимізації напрямів адміністративно-правового регулювання державної кібербезпекової політики. Розглянуто зміст сучасного стану державної політики у сфері кібербезпеки. Проаналізовано теоретичні та практичні аспекти оптимізації правовідносин у сфері державної кібербезпекової політики. Визначено трактування державної політики кібернетичної безпеки України – діяльність державно-правових інституцій щодо управління реальними та потенційними кіберзагрозами та небезпеками з метою задоволення кібернетичних потреб людини та громадянина, а також реалізації національних інтересів у даній сфері.

Ключові слова: кібербезпека, кіберпростір, державна політика, кібербезпекова політика, кіберзлочин.

ДИОРДИЦА І. Современное правовое содержание оптимизации направлений административно-правового регулирования государственной политики кибербезопасности.

В статье предложены авторские результаты определения концептуальных положений оптимизации направлений административно-правового регулирования

государственной политики кибербезопасности. Рассмотрено содержание современного состояния государственной политики в сфере кибербезопасности. Проанализированы теоретические и практические аспекты оптимизации правоотношений в сфере государственной политики кибербезопасности. Определена трактовка государственной политики кибернетической безопасности Украины – деятельность государственно-правовых институтов по управлению реальными и потенциальными киберугрозами и опасностями для удовлетворения кибернетических потребностей человека и гражданина, а также реализации национальных интересов в данной сфере.

Ключевые слова: кибербезопасность, киберпространство, государственная политика, політика кибербезпеки, киберпреступление.

DIORDITSA I. Modern legal content of optimization of directions of administrative and legal regulation of the state cybersecurity policy.

The article proposes to consider the author's results of determining the conceptual provisions for optimizing the areas of administrative and legal regulation of state cybersecurity policy. The content of the current state of state policy in the field of cybersecurity is considered. Theoretical and practical aspects of optimization of legal relations in the field of state cybersecurity policy are analyzed. The interpretation of the state cybersecurity policy of Ukraine is determined – the activity of state and legal institutions to manage real and potential cyber threats and dangers to meet the cyber needs of man and citizen, as well as the realization of national interests in this area. The own vision of directions of the state cybersecurity policy according to the maintenance of a number of regulatory legal acts is offered, namely: directions of the state cybersecurity policy according to the Law of Ukraine «About the basic principles of maintenance of cybersecurity of Ukraine»; directions of the state cybersecurity policy in accordance with the Law of Ukraine «On Fundamentals of National Security of Ukraine»; directions of the state cybersecurity policy in accordance with the Doctrine of Information Security of Ukraine. It is concluded that the priority areas for optimizing state policy to strengthen the administrative and legal regulation of cybersecurity of the state are the following reforming cyber law as a segment of information legislation of Ukraine, especially in terms of not only clearly defining current threats and threats to cyber security, but also mechanisms public policy, including symmetric cyber measures; research on the protection of critical infrastructure from cyberattacks; promoting the development of domestic innovative products that can be used to strengthen the cybersecurity of the state; completion of the implementation of the provisions of the Council of Europe Convention on Cybercrime into national law; optimization of the training system in the field of cybersecurity for the needs of the Armed Forces of Ukraine and other bodies of the security and defense sector of Ukraine; promoting a more active policy of state security institutions to inform the public about cyber threats; promoting the militarization of cyberspace; support for both existing multilateral training sessions on countering cyberattacks on the state information infrastructure, and initiating new types of such training sessions.

Key words: cybersecurity, cyberspace, state policy, cybersecurity policy, cybercrime.