УДК 342.95
DOI https://doi.org/10.32837/yuv.v0i6.2293

Е. Мамедова,
ад'юнкт кафедри адміністративного права,
процесу та адміністративної діяльності
Дніпропетровського державного університету внутрішніх справ

КАТЕГОРІАЛЬНІ ТА ІСТОРИКО-ПРАВОВІ АСПЕКТИ ДЕРЖАВНОЇ ПОЛІТИКИ КІБЕРБЕЗПЕКИ В УКРАЇНІ

Постановка проблеми. Доктрина інформаційної безпеки України визначає інформаційну безпеку як невід'ємну складову кожної зі сфер національної безпеки і водночас важливу самостійну сферу забезпечення національної безпеки [1]. Саме тому розвиток України як суверенної, демократичної, правової та економічно стабільної держави можливий тільки за умови забезпечення належного рівня її інформаційної безпеки, наголошує Г.О. Блінова [2, с. 40]. Водночас важливим компонентом інформаційної безпеки є кібербезпека.

Проблема реалізації кіберзагроз характерна для всіх сучасних держав в глобалізованому інформаційному світі. Європейський парламент для протидії таким негативним сучасним викликам ухвалив низку документів, серед яких Директива Європейського Парламенту і Ради «Про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу» [3], що визначає важливість міжнародної співпраці у сфері кібербезпеки та боротьби з кіберзлочинністю. Зі свого боку, Україна створила такі нормативно правові документи, як стратегії, доктрини, програми, які спрямовані на визначення національних інтересів України в інформаційному просторі, ідентифікацію загроз їх реалізації, напрямів і пріоритетів державної політики в інформаційному просторі [4; 5, с. 16].

Відповідно до цих стратегічних документів кібербезпека розглядається, з одного боку, як протиотрута від «кібератак» на найважливіші інформаційні інфраструктури, від дій «кібертерористів» і «кіберзлочинців», а з іншого боку, як засіб створення більш сприятливого середовища для бізнесу, а також можливості уряду використовувати кіберпростір як засіб досягнення цілей національної безпеки. У традиційному стратегічному сенсі кібербезпека включає як наступальні, так і оборонні операції. Ця дихотомія між настанням і захистом простежується у багатьох первинних документах і заявах політиків і державних службовців. У реалізації такого глобального завдання як визначення та дослідження кібербезпеки потребує масштабної та кропіткої праці, а також якісного правового забезпечення.

Аналіз останніх досліджень і публікацій. Питання впровадження кібербезпекового правового регулювання та методику історичного дослідження постійно висвітлюються у науково-практичних статтях, наприклад, таких науковців, як І.В. Сопілко, В.В. Куцаєв, Г.О. Блінова, Є.О. Живило, Д.С. Мінін, В.П. Шеломенцев, В.Л. Бурячок, С.О. Гнатюк та інших вчених Проте ці пошуки здебільшого зосереджені на сфері правового регулювання та формування системи інформаційної безпеки України. Однак навіть при самому

поверхневому розгляді літератури з кібербезпеки стає очевидним, що визначення і терміни, використовувані при обговоренні кібербезпеки як явища та правової категорії, дуже рухливі. Ці дослідження надають нам складні технічні терміни, котрі нерідко суперечать один одному або певною мірою є внутрішньо несумісними.

Метою дослідження є комплексний аналіз сучасного стану політики кібернетичної безпеки нашої країни та історичний аналіз її становлення, визначення ознак поняття державна політика у сфері кібербезпеки та формулювання відповідного авторського поняття.

Виклад основного матеріалу. Цифровий електронний комп'ютер був створений в середині двадцятого століття, і його подальше поширення і впровадження були настільки поширеним, що ми інстинктивно звертаємося до комп'ютера, коли стикаємося зрізними задачами у повсякденні. Було б грубою несправедливістю стосовно історичних джерел кібербезпеки зводити її до існування тільки комп'ютерів, але вони зберігають центральне матеріальне становище в країнах, що розвивають відносини між інформаційними технологіями та безпекою. «Комп'ютер» використовувався в 1942 році для позначення осіб, залучених до інтенсивної обробки даних, тільки в 1945 році «комп'ютер» став асоціюватися не тільки з людьми, але і з машинами. Як і багато аналогів комп'ютера, інформаційно-технологічні його попередники, джерела сучасних цифрових комп'ютерів були тісно пов'язані з сучасними умовами національної безпеки. Від спартанських військових шифрів до телеграфа Шапе в революційній Франції, від азбуки Морзе та електричного телеграфування дев'ятнадцятого століття до бойових радіоприймачів та інших сучасних способів зв'язку, розвиток між інформаційними технологіями та національною безпекою, численний та взаємно підсилюючий один одного. Це відповідало інтересу військових до тактичної обробки даних, організаційній адаптації та автоматизації. У військовому контексті збільшення обсягу інформації, необхідної для управління компаніями в дев'ятнадцятому столітті, вплинуло на створення генеральних штабів для цілей більш якісної обробки даних. Ще одним ключовим фактором були вимоги криптографії, створення і злому секретних кодів. Розшифровка кодів «Енігми» криптографами союзників розглядається багатьма як ключовий фактор кінцевої поразки Німеччини в 1945 році, а обладнання, яке вони розробили, є одним із перших, якщо не першим, серед цифрових, електронних і програмованих комп'ютерів. Тому не дивно, що ефективні інформаційні процесори у вигляді комп'ютерів з'явилися в кінцевому підсумку у військовому криптологічному контексті Другої світової війни.

Після війни урядові, академічні установи та корпорації скористалися математичними можливостями цього нового покоління машин і використовували їх для виконання великомасштабних обчислювальних задач. У цю епоху великомасштабної обробки даних відносини між комп'ютерами й безпекою змінилися: замість використання комп'ютерів з метою забезпечення національної безпеки виник ряд нових проблем безпеки, що виникають в результаті використання й архітектури самих обчислювальних технологій. Через можливість зловмисної поведінки системи почали мати потребу в захисті від своїх користувачів, а користувачі – один від одного [6, с. 112].

Додаткові проблеми безпеки виникли у зв'язку з випадковою втратою або навмисним розкриттям конфіденційних даних, особливо у зв'язку з тим, що багато баз даних керувалися страховими компаніями, банками, авіакомпаніями та іншими організаціями, які мають доступ до

особистих біографічним, демографічних і фінансових даних. Громадське занепокоєння прослідковується реакцією на використання комп'ютерів для цілей перепису. Бюро перепису США було одним з перших спонсорів комп'ютерних досліджень і розробок і використовувало знамениту машину UNIVAC при перепису 1950 року. У 1971 році перепис в Нідерландах зіткнувся з високим ступенем громадського спротиву і неучасті. Це призвело до скасування всіх наступних переписів та підрахунку населення більш традиційними методами, наголошує О.В. Островий [7, с. 80].

Формальні методи перевірки й сертифікації безпеки, розроблені для більш ранніх закритих обчислювальних систем, були менш застосовні в більш різноманітних технологічних середовищах розподілених комп'ютерних мереж. Компанії та установи розгорнули сотні тисяч персональних обчислювальних терміналів, в той час, як локальне зберігання даних і маніпулювання ними обходили централізований контроль безпеки мейнфреймів та їх спеціалізованого персоналу. На недосвідчених початківців користувачів неявно покладалися обов'язки по забезпеченню безпеки; конфіденційні дані зберігалися, обмінювалися і губилися. Слідом за цими подіями було прийнято законодавство щодо стримування злочинного використання комп'ютерних мереж у Сполучених Штатах за допомогою Закону про комп'ютерне шахрайство і зловживання (1986 рік), а в Сполученому Королівстві – за допомогою Закону про неправомірне використання комп'ютерів (1990 рік).[8]

Пізніше Україна почне приймати законодавчі акти, котрі будуть забезпечувати держану інформаційну політику: Конституцію України (1996 рік), Закони України «Про наукову і науково-технічну діяльність» (1991 рік), «Про інформацію» (1992 рік), «Про друковані засоби масової інформації» (1992 рік), «Про науково-технічну інформацію» (1993 рік), «Про авторське право та суміжні права» (1993 рік), «Про національний архівний фонд і архівні установи» (1993 рік), «Про захист інформації в інформаційно-телекомунікаційних системах» (1994 рік), «Про телебачення і радіомовлення» (1995 рік), «Про Концепцію Національної програми інформатизації» (1998 рік), «Про Національну програму інформатизації» (1998 рік), а також інші акти: укази, накази, інструкції [9].

Проблеми мережевої безпеки ще більш загострилися. Поява Інтернету принесла з собою нові проблеми безпеки й нові способи заподіяння шкоди комп'ютерним мережам. Перший комп'ютерний «хробак» з'явився в 1989 році, наступним за ним був упізнаваний сектор промислової «комп'ютерної безпеки». Перші віруси почали заражати мільйони персональних комп'ютерів і системи електронної пошти в 1990-х роках, що призвело до розробки антивірусного програмного забезпечення. Кібератаки стали більш цілеспрямованими у 2000-х роках, коли були здійснені перші серйозні зломи баз даних кредитних карт з метою отримання злочинної вигоди та у подальшому усвідомлення впливу цих атак на бізнес, держава, довіри громадян, репутацію й ін.

В останні роки «кібербезпека» виникла як режим безпеки, пов'язаний з захистом інфраструктурних інформаційних систем. Технологічно розвинені країни Північної Америки, Європи та Азійсько-Тихоокеанського регіону в найбільшій мірі покладаються на ці інфраструктури. З 1980-х років «кіберзагрози» і критичні інфраструктури були пов'язані, так що в Сполучених Штатах інформаційні технології не тільки давали можливість створити конкурентну перевагу, але також розглядалися як джерело асиметричної уразливості «інформаційної переваги». Як зауважили вчені В.В. Лук'яненко, В.А. Кротюк, що асиметричність реалізується, коли

відомі місця вразливості системи, що атакується [10].

Сьогодні найбільше уваги приділяється іноземним учасникам, які використовують інформаційні технології зі стратегічною метою – іншим державам, їх довіреним особам і терористам, а також транснаціональним злочинцям, повстанцям і «внутрішньої загрози» в бізнесі та уряді. До цього списку ми можемо додати інформаторів, цілий ряд хакерів, зламувачів, які представляють загрозу безпеці для уряду, промисловості та громадськості. На наш погляд, помилки та інші дефекти безпеки інформаційних систем можуть бути використані зловмисниками, так що залежно критично важливі сектори інфраструктури – це фінанси, енергетика, транспорт, уряд та інше, які перестануть нормально функціонувати, що призведе до широкого діапазону негативних соціальних сценаріїв.

Кібербезпека повсюдна, у всякому разі, в матеріальному плані, і з її наростаючою увагою до онлайн-контенту та самовираження вона вторгається в дії громадян, зазвичай мало стурбованих вимогами національної або економічної безпеки. Розвиток кібербезпеки є довгим і складним процесом. Важливо відзначити, що він виник не тільки з міркувань комп'ютерів і комп'ютерних мереж або їхнього значення для національної безпеки, а й з міркувань безпеки людей і їхніх даних, а також безпеки соціальних інфраструктур та економіки. На початку двадцять першого століття кібербезпека є ключовим завданням сучасних, технологічно розвинених країн і міжнародної системи в цілому.

Як зазначив вчений О.В. Островий, для забезпечення кібернетичної безпеки в нашій державі, уряд у партнерстві із суспільством та приватним сектором, а також громадянами, має підвищити ефективність державного управління у цій сфері, здійснити впорядкування нормативно-правового поля та забезпечити розвиток інфраструктури кібернетичної безпеки [7].

І. Діордіца в дослідженні «Система забезпечення кібербезпеки: сутність та призначення» наголошує, що проблема кібербезпеки в цілому та системи її забезпечення зокрема через свою специфіку є глобальною і неізольованою і у зв'язку з цим найефективніше може бути вирішена лише за умови скоординованої діяльності суб'єктів кібербезпеки [6]. Таку координацію суб'єктів кібербезпеки забезпечує саме державна політика у цій сфері. Одним з інституційних проявів такого систематизуючого впливу держави на систему органів, що забезпечують кібербезпеку в Україні є утворення робочого органу Ради національної безпеки і оборони України – Національного координаційного центру кібербезпеки. Метою цього органу є покращення координації діяльності суб'єктів сектору безпеки і оборони, які забезпечують кібербезпеку, та прийняття рішень, що сприяють вирішенню найбільш складних проблем у цій сфері [11].

Варто зазначити, що кібербезпека – це відповідь на передбачувані ризики і загрози сучасної глобальної інформаційно-технологічної інфраструктури, яку найчастіше називають «Інтернетом». У широкому сенсі, це стосується кого-небудь або чого-небудь, що обмінюється даними з допомогою цифрових, електронних засобів. Сучасне інформаціне середовище насичено такими прикладами. Так, The Washington Post 10 листопада 2014 року оголосила, що невідомі хакери, які проникли в її внутрішню комп'ютерну мережу, отримали доступ до персональних даних 500 тис. співробітників відомства. У липні 2021 року Російські хакери атакували сайт ВМС України та розмістили фейки про Sea Breeze-2021. 9 липня мали місце випадки хакерських атак структур держави-агресора на вебпортал Військово-морських сил Збройних сил

України [12]. У травні 2021 в Сполучених Штатах хакери здійснили масштабну кібератаку проти 200 американських компаній [13].

Таку ситуацію, ймовірно, слід було очікувати, враховуючи, що кібербезпека має складні історичні та концептуальні відносини з широким спектром практик, дисциплін і спільнот. Навіть попри те, що кібербезпека швидко піднялася на порядку денному урядів, бізнесу, громадянського суспільства і міжнародних організацій, для багатьох залишається незрозумілим, зміст поняття політика кібербезпеки.

Якщо проаналізувати дослідження українських вчених, таких як В.В. Бухарєв, О.В. Островий, В.О. Манжай, М.М. Ожеван, Ю.Ю. Орлов, І.В Діордіца та інших, ми можемо прийти до висновку, що кожен із цих авторів виносить своє бачення та свої формальності стосовно кібербезпеки. Тобто, на наш погляд, ніхто не може прийти до єдиної думки про те, що таке кібербезпека. Загалом кібербезпека – це широкий термін, що позначає сучасний тривалий зв'язок відносин між інформаційними технологіями та безпекою. Для розкриття змісту категорії політика кібербезпеки необхідно з'ясувати що таке «правова категорія», «категорія права».

Категорії права, зазначає О.І. Біік, є засобами конструювання і розуміння права як системного утворення для регулювання суспільних відносин. О.І. Біік визначає «категорію» у податковому праві як загальні та фундаментальні поняття, які характеризують закономірні зв'язки й відношення, що існують у податковому праві [14, с. 13]. Д.Г. Заброда, досліджуючи адміністративно-правові засади як категорію адміністративного права, розглядав у їх змісті категоріальний елемент (складову), що передбачає висвітлення понять і ознак явища, змодельованих у правових актах, порівняння її з правовим і соціальним буттям і формування науково-правової категорії, що адекватно відображає правову реальність [15, с. 13]. К.В. Ростовська адміністративно-правову категорію як загальне та фундаментальне поняття, сформульоване в результаті узагальнення знань про суспільні відносини управлінського характеру, які складаються у сфері виконавчої влади, пов'язані із адміністративним законодавством, нормами адміністративного права і практичним їх застосуванням [15, с. 72].

У сучасній політико-філософській традиції безпека є важливим оплотом проти невідкладних обставин в майбутньому [17]. Безпека виникає як центральна риса соціального контракту між людьми й державою, в якому прагнення до безпеки і її практика покликані заспокоїти нервозність, викликана встановленням порядку в прийдешні часи. Безпека за загальноприйнятим уявленням – це такі умови, в яких перебуває складна система, коли дія зовнішніх факторів і внутрішніх чинників не призводить до процесів, що вважаються негативними щодо конкретної складної системи у відповідності до наявних на вказаному етапі потреб, знань та уявлень [18].

У попередніх наукових роботах ми визначили ознаки кібербезпеки патрульної поліції, а саме: 1) це стан захищеності службових інтересів патрульної поліції; 2) досягається шляхом дотримання правових, організаційних технічних вимог з використання інформаційних ресурсів, мереж, носіїв інформації, програмного забезпечення, засобів фото та відеозйомки в роботі патрульних поліцейських; 3) забезпечується спеціальними підрозділами патрульної поліції та кожним патрульним поліцейським в межах своїх функціональних обов'язків та обсягу спеціальних знань; 4) проявляється у сфері кіберпростору; 5) мета – своєчасне виявлення, запобігання і нейтралізація реальних і потенційних кіберзагроз. Тому кібербезпеку патрульної

поліції було сформульовано як стан захищеності службових інтересів патрульної поліції у кіберпросторі, що досягається шляхом дотримання правових, організаційних, технічних вимог з використання інформаційних ресурсів, мереж, програмного забезпечення, носіїв інформації, засобів фото- та відеозйомки в роботі патрульних поліцейських для ефективного інформаційного забезпечення функціонування патрульної поліції, своєчасного виявлення, запобігання і нейтралізації реальних і потенційних кіберзагроз [5, с. 24].

Як і безпека, зокрема кібербезпека, політика завжди піклується про час, тобто кожен прийнятий нормативно-правовий акт завжди представляється «процесом у часі», орієнтованим на конкретну мету, концепція якого, завжди має на увазі майбутнє посилання на стан безпеки в державі. Політика також стурбована минулим, постійно звертаючись до історичних пам'яток, як політична практика показує, безпека також є ретроспективної, вона аналізує минуле, щоб сформувати наративи ідентичності, котрі узаконюють і виправдовують її втручання.

С.О. Кравченко наголошує, що вироблення будь-якої політики має починатися з визначення місії – головної загальної мети політики, що розкриває призначення такої діяльності. Місія задає загальний орієнтир, без якого неможливо сформувати єдину систему цілей, тому її визначення має передувати постановці цілей [19, с. 30]. Такі цілі державної політики у сфері кібербезпеки визначені у Стратегії кібербезпеки України [11] та у Законі України «Про основні засади забезпечення кібербезпеки України» [20].

За роки реалізації Стратегії кібербезпеки України, затвердженої Указом Президента України від 15 березня 2016 року № 96, було докладено зусиль до становлення та розвитку національної системи кібербезпеки. Важливим етапом її інституалізації стало прийняття Закону України «Про основні засади забезпечення кібербезпеки України», який визначив правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки [4]. Хоча у преамбулі Закону України «Про основні засади забезпечення кібербезпеки України» визначено, що він закріплює основні цілі державної політики у сфері кібербезпеки, проте окремої статті, яка б їх закріплювала немає.

Таким чином, це стало однією з виявлених і закріплених у Стратегії кібербезпеки Укріани проблем, а саме недостатня чіткість визначених пріоритетів та напрямів забезпечення кібербезпеки України, значна частина яких не мала зрозумілої кінцевої мети та була не конкретною [11]. На наш погляд, це обумовлює і відсутність конкретизованої мети і завдань державної політики у сфері кібербезпеки.

У статті 31 «Стратегія кібербезпеки України» Закону України «Про національну безпеку України» визначено, що Стратегія кібербезпеки України є документом довгострокового планування, в якому визначаються пріоритети національних інтересів України у сфері кібербезпеки, наявні та потенційно можливі кіберзагрози життєво важливим інтересам людини і громадянина, суспільства та держави в кіберпросторі, пріоритетні напрями, концептуальні підходи до формування та реалізації державної політики щодо безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави, підвищення ефективності основних суб'єктів

забезпечення кібербезпеки, насамперед суб'єктів сектору безпеки і оборони, щодо виконання завдань у кіберпросторі, а також потреби бюджетного фінансування, достатні для досягнення визначених цілей і виконання передбачених завдань, та основні напрями використання фінансових ресурсів. Також Стратегія кібербезпеки України є основою для підготовки державних програм та нормативно-правових актів, що стосуються забезпечення кібербезпеки України [21]. Таким чином Стратегія кібербезпеки України є тим документом, який розкриває цілі, задачі та зміст державної політики у сфері кібербезпеки України.

У законодавстві визначена мета Стратегії кібербезпеки України - створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави. А також визначено стратегічні завдання, які на наш погляд і відображають завдання державної політки у сфері кібербезпеки в Україні: 1) формування системи дієвої кібероборони; 2) ефективної протидії розвідувально-підривній діяльності у кіберпросторі та кібертероризму; 3) посилення спроможності у протидії кіберзлочинності; 4) запровадження асиметричних інструментів стримування; 5) убезпечення кіберпростору задля захисту суверенітету держави та розвитку суспільства; 6) захист прав, свобод і законних інтересів громадян України у кіберпросторі; 7) європейська і євроатлантична інтеграція у сфері кібербезпеки [11].

Словник-довідник «Державне управління» визначає державну політику як засіб, що дозволяє державі досягнути певної мети в конкретній галузі, використовуючи правові, економічні, адміністративні методи впливу, спираючись на ресурси, які є в її розпорядженні [22, с. 63], а Енциклопедичний словник з державного управління визначає, що державна політика – це дії системи органів державної влади згідно з визначеними цілями, напрямами, принципами для розв'язування сукупності взаємопов'язаних проблем у певній сфері суспільної діяльності [23, с. 144–145]. К.В. Ростовська, наприклад, досліджуючи державну антикорупційну політику визначила її як передбачений у законодавстві комплекс організаційно-правових, адміністративних, економічних, ідеологічних, освітньо-виховних та інших заходів, що ініціюються, розробляються та реалізуються публічною адміністрацією у взаємодії з громадянським суспільством з метою усунення причин та умов, що сприяють корупції, зниження рівня корупції в усіх сферах суспільного життя, виявлення та припинення фактів корупції, відновлення порушених прав і законних інтересів фізичних та юридичних осіб, а також держави [16, с. 94].

Враховуючи те, що інтеграція комп'ютерних мереж, інформації та безпеки є фактом глобальної політики та економіки, а кібербезпека являє собою набір практик, процесів та політик, які з'явилися для протидії менш бажаним наслідкам глобального інформаційного суспільства, можна прийти до наступних висновків.

Висновки та пропозиції. На дослідження державної політики у сфері кібербезпеки в нашій країні впливає безліч умов, проте по перше необхідно конкретизувати цілі та завдання державної політики у сфері кібербезпеки, закріпивши їх на законодавчому рівні. Проте це неможливо без розуміння сутності правової категорії «державна політика у сфері кібербезпеки».

На наш погляд, ознаками державної політики у сфері кібербезпеки є: 1) за замістом це дії системи органів державної влади, що дозволяє державі досягнути певної мети в галузі кібербезпеки; 2) мета – створення та забезпечення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави; 3) завдання:

формування системи дієвої кібероборони; ефективної протидії розвідувально-підривній діяльності у кіберпросторі та кібертероризму; посилення спроможності у протидії кіберзлочинності; запровадження асиметричних інструментів стримування; убезпечення кіберпростору задля захисту суверенітету держави та розвитку суспільства; захист прав, свобод і законних інтересів громадян України у кіберпросторі; європейська і євроатлантична інтеграція у сфері кібербезпеки; 4) реалізується через правові, організаційні, економічні, адміністративні методи впливу та здійснення комплексу інформаційно-технічних заходів.

Таким чином, державна політика у сфері кібербезпеки як правова категорія – це система правових, організаційних, економічних, інформаційно-технічних заходів, що реалізуються органами державної влади у взаємодії з громадянським суспільством з метою створення та забезпечення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави.

На наш погляд, необхідно доповнити частину 1 статті 1 пунктом 22 Закону України «Про основні засади забезпечення кібербезпеки України» визначенням державної політики у сфері кібербезпеки та статтю 7 переліком цілей та завдань державної політики у сфері кібербезпеки.

У науковій статті розглянуто правові, політичні, історичні передумови необхідності активізації процесів кібербезбпеки держави, взаємодії між державними інформаційними ресурсами. Визначено, що у процесуальних формах кібербезпека містить широкий спектр політичних і технічних практик, від оборонних і захисних до наступальних і підривних. Також визначено що кібербезпека являє собою, не тільки засіб захисту суспільства і його основних інформаційних інфраструктур, але також спосіб проведення національної й міжнародної політики за допомогою інформаційно-технологічних засобів. Розглянуто нормативні акти інших держав та України, щодо становлення кібербезпеки що визначають засади електронної взаємодії між державними інформаційними ресурсами. Виявлено проблемні аспекти котрі вливають на дослідження державної політики кібербезпеки в нашій країні. Визначено ознаки державної політики у сфері кібербезпеки: за змістом це дії системи органів державної влади, що дозволяє державі досягнути певної мети в галузі кібербезпеки; мета її – створення та забезпечення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави; завдання: формування системи дієвої кібероборони; ефективної протидії розвідувально-підривній діяльності у кіберпросторі та кібертероризму; посилення спроможності у протидії кіберзлочинності; реалізується через правові, організаційні, економічні, адміністративні методи впливу та здійснення комплексу інформаційно-технічних заходів. Запропоновано авторське поняття державної політики у сфері кібербезпеки як правової категорії, а саме як системи правових, організаційних, економічних, інформаційно-технічних заходів, що реалізуються органами державної влади у взаємодії з громадянським суспільством з метою створення та забезпечення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави. Запропоновано зміни до Закону України «Про основні засади забезпечення кібербезпеки України».

Ключові слова: безпека, кібербезпека, державна політика, правова категорія.

Mamedova E. Categorical and historical and legal aspects of state cybersecurity policy in Ukraine

The scientific article considers the legal, political, historical prerequisites for the need to intensify the processes of cybersecurity of the state, the interaction between state information resources. It is determined that in procedural forms cybersecurity contains a wide range of political and technical practices, from defense and defense to offensive and subversive. It is also defined that cybersecurity is not only a means of protecting society and its basic information infrastructures, but also a way of conducting national and international policy through information technology. Regulations of other states and Ukraine on the formation of cybersecurity that determine the principles of electronic interaction between state information resources are considered. Problematic aspects that affect the study of state cybersecurity policy in our country have been identified. The features of the state policy in the field of cybersecurity are determined: instead, it is the actions of the system of public authorities, which allows the state to achieve a certain goal in the field of cybersecurity; goal - to create and provide conditions for the safe functioning of cyberspace, its use in the interests of the individual, society and the state; tasks: formation of an effective cyber defense system; effective counteraction to intelligence and subversive activities in cyberspace and cyberterrorism; capacity building in the fight against cybercrime; implemented through legal, organizational, economic, administrative methods of influence and implementation of a set of information and technical measures. The author's concept of state policy in the field of cybersecurity as a legal category, namely as a system of legal, organizational, economic, information and technical measures implemented by public authorities in cooperation with civil society to create and provide conditions for safe functioning of cyberspace, its use in the interests of the individual, society and the state. Amendments to the Law of Ukraine "On Basic Principles of Cyber Security of Ukraine" are proposed.

Key words: security, cybersecurity, state policy, legal category.

Література

1. Про доступ до інформації, що знаходиться у розпорядженні державних органів: Рекомендація № R (81) 19 Комітету Міністрів Ради Європи 1981 р. URL: http://cedem.org.ua/library/re81-19.

2. Блінова Г.О. Адміністративно-правові засади інформаційного забезпечення органів публічної адміністрації в Україні: актуальні питання теорії та практики : дис. ... докт. юрид. наук. Запоріжжя, 2019. 458 с.

3. Про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу : Директива Європейського Парламенту і Ради від 6 липня 2016 року № 2016/1148. Офіційний вісник Європейського Союзу від 19 липня 2016 р. 2016 р., L 194, с. 1.

4. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» : Указ Президента України від 15 березня 2016 року № 96/2016. Урядовий кур'єр. 2016. № 52.

5. Блінова Г.О., Мамедова Е.А. Інформаційне забезпечення та кібербезпека патрульної поліції: співвідношення понять. Науковий вісник Дніпропетровського державного університету внутрішніх справ. 2020. № 4. С. 15–24.

6. Діордіца І. Система забезпечення кібербезпеки: сутність та призначення. Підприємництво, господарство і право. 2017. № 7. С. 109–116. URL: http://nbuv.gov.ua/UJRN/Pgip_2017_7_24

7. Островий О.В. Деякі підходи до удосконалення державної політики забезпечення кібернетичної безпеки України. Збірник наукових праць ДонДУУ «Сучасні проблеми державного управління в умовах системних змін». Серія «Державне управління». 2016. Т. XVII, вип. 298. С. 77–85.

8. Computer Misuse Act (1990). URL: https://www.bbc.co.uk/bitesize/guides/z8m36yc/revision/5

9. Брижко В.М., Радянська А.І., Швець М.Я. Порівняльно-правове дослідження відповідності законодавства України законодавству ЄС у сфері персональних даних. Київ : Тріумф, 2006. 256 с. URL: https://just.odessa.gov.ua/files/upload/files/24.pdf

10. Лук'яненко В.В., Кротюк В.А. Асиметричний характер сучасної інформаційної війни. Науковий семінар ХНУ ПС ім. І.Кожедуба. С. 25. URL: http://www.hups.mil.gov.ua/assets/doc/science/stud-conf/informacijna-agresiya-rf-proti-ukraini/11.pdf

11. Стратегія кібербезпеки України. Безпечний кіберпростір – запорука успішного розвитку країни. Указ Президента України від 26 серпня 2021 року № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text

12. Сайт ВМС України атакували російські хакери, розмістивши неправдиву інформацію про Sea Breeze-2021. 2021. URL: https://ua.interfax.com.ua/news/general/754877.html

13. У Сполучених Штатах хакери здійснили масштабну кібератаку проти 200 американських компаній. URL: https://www.ukrinform.ua/rubric-world/3274439-hakeri-atakuvali-200-amerikanskih-kompanij-zmi.html.

14. Баїк О.І. Поняття і категорії як основа науки податкового права України. Lviv Polytechnic National University Institutional Repository. URL: URL: http://ena.lp.edu.ua:8080/bitstream/ntb/31262/1/03-10-13.pdf. С. 10–13.

15. Заброда Д.Г. Адміністративно-правові засади: сутність та зміст категорії. URL: http://applaw.knu.ua/index.php/arkhiv-nomeriv/2-4-2013/item/180-administratyvno-pravovi-zasady-sutnist-ta-zmist-katehoriyi-zabroda-d-h

16. Ростовська К.В. Адміністративно-правові основи державної антикорупційної політики в Україні : дис. ... докт. юрид. наук. Дніпро, 2019. 443 с.

17. Трофимнеко О., Прокоп Ю., Логінова Н., Задерейко О. Кібербезпека України: аналіз сучасного стану. Захист інформації. 2019. Т. 21. № 3. URL: http://dspace.onua.edu.ua/bitstream/handle/11300/12213/statya_Trofymenko_Prokop_Loginova_Zadereyko_CYBERSECURITY%20OF%20UKRAINE.pdf?sequence=1&isAllowed=y.

18. Безпека. Вікіпедія. URL: https://uk.wikipedia.org/wiki/Безпека

19. Кравченко С.О. Підходи до розуміння антикорупційної політики в публічному управлінні. Вчені записки Таврійського національного університету імені В.І. Вернадського. Серія : «Державне управління». 2018. Т. 29(68), № 2. С. 28–33. URL: http://nbuv.gov.ua/UJRN/sntvupa_2018_29_2_7

20. Про основні засади забезпечення кібербезпеки України : Закон України від 5 жовтня 2017 року № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

21. Про національну безпеку України : Закон України від 21 червня 2018 року № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19#Text

22. Державне управління : словн.-довід. / уклад. В.Д. Бакуменко ; за заг. ред. В.М. Князєва, В.Д. Бакуменка. Київ : Вид-во УАДУ, 2002. 228 с.

23. Енциклопедичний словник з державного управління / укл. : Ю.П. Сурмін, В.Д. Бакуменко, А.М. Михненко та ін. ; за ред. Ю.В. Ковбасюка, В.П. Трощинського, Ю.П. Сурміна. Київ : НАДУ, 2010. 820 с.