УДК 351.86:007:659

Таволжанський Олексій Володимирович,
кандидат юридичних наук,
асистент кафедри кримінології та кримінально-виконавчого права
Національного юридичного університету імені Ярослава Мудрого

ОСНОВИ ДЕРЖАВНОЇ КІБЕРПОЛІТИКИ УКРАЇНИ: ФОРМУВАННЯ ТА РЕАЛІЗАЦІЯ

Здійснено аналіз заходів із забезпечення кібербезпеки держави, виділені основні сфери внутрішньої політики держав з урахуванням зростання кіберзагроз. Запропоновані шляхи покращення кібербезпекової політики України з метою приведення її до вимог сучасності та забезпечення суверенітету держави в умовах активізації процесу геополітичного тиску, інформаційних війн та мілітаризації кіберпростору.

Ключові слова: *державна інформаційна політика, кіберполітика, кібербезпека, кіберпростір, інформаційне законодавство.*

Постановка проблеми. На сьогодні все ще залишається недостатньо розкритим питання здійснення державного стратегічного планування у сфері забезпечення кібербезпеки, що передбачає, насамперед, розробку щорічних планів реалізації положень Стратегії кібербезпеки, упровадження їх у практичну площину, визначення першочергових заходів, ужиття яких дасть змогу гарантувати кіберзахист державних інформаційних ресурсів та об'єктів критичної інформаційної інфраструктури.

Термін «політика» (politika) грецького походження. У буквальному перекладі має наступне значення: державні справи (від polis – держава), словом, мистецтво керувати державою. Відповідно до статті 17 Конституції України захист інформаційної безпеки, зокрема, є однією з найважливіших функцій держави, справою всього Українського народу [3].

Метою статті є спроба виявлення новітніх тенденцій політики у сфері кібербезпеки. Проблеми комунікаційної безпеки та кіберпростору досліджують і вивчають останнім часом все активніше. Серед найбільш актуальних сфер вирізняють, зокрема: проблеми інформаційної безпеки, як інформаційна безпека у контексті глобалізації і трансформації безпекових викликів; питання міжнародного та національного аспектів боротьби з кіберзлочинністю; інформаційні та кібервійни; проблеми формування політики (в тому числі й правової) протидії комп'ютерній злочинності; відмивання коштів тощо.

Аналіз останніх досліджень і публікацій. Питанням політики у сфері кібербезпеки займались ряд науковців, зокрема деякі аспекти проблем кібернетичної безпеки та кібернетичних загроз досить успішно було проаналізовано у наукових працях таких учених, як наукова І.В. Арістова, В. Бутузов, А. Леонов, В.А. Ліпкана, Є. Макаренко, О. Потій, І.В. Сопілко, Р. Шафранскі та інші, проте питання правового регулювання політики держави у сфері кібербезпеки на сучасному етапі є не досить вивченим, що зумовлює потребу в його ґрунтовному дослідженні.

Постановка завдання. Становлення інформаційного, відкритого, гласного, демократичного суспільства не лише дає змогу будувати більш ефективне та успішне суспільство, але й надає нових імпульсів невідомим раніше загрозам безпеки держави, створює принципово нові складнощі для системи національної безпеки. Належне і успішне формування кіберполітики безумовно запорука успіху всього суспільства.

Виклад основного матеріалу дослідження. Сфера кібербезпеки знаходиться на стику інтересів конфіденційності, приватності і необхідності державного захисту прав і законних інтересів людини. Законом України «Про Засади державної політики України в галузі прав людини» одним з основних напрямів державної політики України визнано забезпечення захисту людини і громадянина від посягань з боку іншої людини та посягань з боку держави. Законом

задекларовано визнання презумпції особистої свободи людини відповідно до принципу, згідно з яким дозволено все, крім того, що прямо забороняється законом, в той же час визнання обмеженості свободи держави, її органів і посадових осіб відповідно до принципу, згідно з яким дозволено лише те, що прямо передбачається законом.

Держава гарантує таємницю листування, телефонних розмов, телеграфної та іншої кореспонденції. Винятки можуть бути встановлені лише судом у випадках, передбачених законом, з метою запобігти злочинові чи з'ясувати істину під час розслідування кримінальної справи, якщо іншими способами одержати інформацію неможливо (ст. 31 Конституції України) [3]. Не виключенням є і кіберпростір. Так само в Україні не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини (ст. 32 Конституції України) [3].

На наше переконання саме ці принципи були в авангарді національної інформаційної політики України останні десятиріччя. Але новітні тенденції вимагають від суспільства і держави нових підходів до сучасних проблем.

Урядова активність з боку світових лідерів у кіберпросторі, лобіювання інтересів поза територіальними і національними рамками інформаційної політики та організація і успішна діяльність транснаціональних злочинних угруповань, що «фахово» вузько спрямовано займаються кіберзлочинністю все це обумовлює необхідність виробленні рекомендацій щодо обрання напрямків і сфер видозміни вітчизняного безпекового сектору з урахуванням вищезазначених об'єктивних детермінант.

Дискусії юристів науковців і практиків точаться за декількома векторами, зокрема:

1) адміністративно-правові дослідження – організаційно-правове забезпечення політики інформаційної безпеки в умовах глобалізації, інтеграції, становлення інформаційного суспільства, зокрема захисту персональних даних, інформаційних ресурсів, забезпечення інформатизації, регулювання суспільних відносин щодо комп'ютерних програм, права громадян на інформацію у сфері державного управління, інформаційного забезпечення діяльності різних державних органів, адміністративно-правових форм, засобів і методів забезпечення інформаційної безпеки, а також проблем інформаційної культури в управлінській діяльності та теоретико-методологічних засад інформаційного права.

2) цивільно-правові дослідження – забезпечення інформаційної безпеки, до яких переважно належать проблеми цивільно-правової охорони, захисту та реалізації авторського права в умовах розвитку інформаційно-комунікаційних технологій, авторського права у сфері новітніх комп'ютерних технологій (комп'ютерних програм, комп'ютерних мереж, зокрема Інтернету), а також загальні цивільно-правові проблеми інформаційних відносин.

3) кримінально-правові, кримінологічні й криміналістичні дослідження – нормативне подолання загроз в інформаційній сфері, як кіберзлочинність, зокрема її проявів – комп'ютерного піратства та шахрайства, хакерства тощо, а також потенційної загрози – кібертероризму. У зв'язку з цим предметом кримінально-правових та кримінологічних досліджень виступають особливості кримінальної відповідальності за злочини у сфері комп'ютерної інформації, шляхи кримінально-правової охорони інформації в комп'ютерних системах та телекомунікаційних мережах, незаконний збут і розповсюдження комп'ютерної інформації з обмеженим доступом, концептуальні питання забезпечення інформаційної безпеки кримінально-правовими засобами та інші.

Окреме місце в системі правових досліджень інформаційної безпеки займають теоретико-правові дослідження, покликані сформувати цілісну систему правових поглядів на вирішення проблем інформаційної безпеки. До завдань таких досліджень входять правове осмислення інформаційної безпеки як явища загалом та кожної його складової зокрема, визначення шляхів правового впливу на інформаційну безпеку та особливості правових форм її забезпечення, з'ясування взаємозв'язку інформаційної безпеки з іншими правовими явищами, вироблення концептуальних рекомендацій щодо вдосконалення інформаційного законодавства, у тому числі

нормативно-правових актів, що визначають фундаментальні основи державної політики забезпечення інформаційної безпеки тощо [13].

Формування засад державної політики у будь якій сфері відбувається шляхом регламентування чи визначення у Законі суспільної волі. У сучасних умовах вітчизняні інформаційні відносини, пов'язані із забезпеченням кібернетичної безпеки в державі, частково врегульовані деякими нормативно-правовими актами, зокрема Законами України: «Про інформацію» [7], «Про телекомунікації» [9], «Про захист інформації в інформаційно-телекомунікаційних системах» [6], «Про доступ до публічної інформації» [5], а також Законом України «Про основні засади забезпечення кібербезпеки України» [8], що набуває сили у 2018 році і т.д.

За часів незалежності України галузь інформаційних технологій розвивалася практично без підтримки з боку держави, роль якої переважно зводилася до збирання статистичних відомостей, що часто не відображали реального стану справ. Основний комплекс переваг інформаційних технологій у системі державного управління практично не застосовується [2, с. 264]

Державне стратегічне планування у сфері забезпечення кібербезпеки залишається важливою складовою політики національної безпеки. Сучасна Державна політика у сфері кібербезпеки базується на положеннях Конвенції про кіберзлочинність, ратифікованої Законом України від 7 вересня 2005 року № 2824-IV, законодавства України щодо основ національної безпеки, засад внутрішньої та зовнішньої політики, електронних комунікацій, захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом та спрямована на реалізацію до 2020 року Стратегії національної безпеки України, затвердженої Указом Президента України від 26 травня 2015 року № 287 «Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України» [11], Указі Президента України Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» тощо.

Далеко не кожний з наведених актів відповідає викликам сьогодення та реальним кіберзагрозам, тому підтримую пропозиції І. В. Арістової [1, с. 156], яка зазначила, що для реалізації національних інтересів в інформаційній сфері слід переглянути пріоритети державної політики, розробити нові концептуальні підходи щодо регулювання ринку інформаційно-комунікаційних технологій, інформаційної та інвестиційної політики, розвитку інформаційного законодавства і забезпечення інформаційної безпеки.

Національна система кібербезпеки має насамперед забезпечити взаємодію з питань кібербезпеки державних органів, органів місцевого самоврядування, військових формувань, правоохоронних органів, наукових установ, навчальних закладів, громадських об’єднань, а також підприємств, установ та організацій незалежно від форми власності, які здійснюють діяльність у сфері електронних комунікацій, захисту інформації та є власниками (розпорядниками) об’єктів критичної інформаційної інфраструктури. Адже забезпечення кібербезпеки неможливо здійснювати без державного стратегічного планування як функції державного управління, що визначає мету, завдання, пріоритети та комплекс заходів щодо реалізації державної політики в зазначеній сфері.

При формуванні державної кіберполітики щодо запобігання кіберзлочинності необхідно виходячи із суті та класифікації кіберзлочинів, враховувати наступні загрози суспільству та державі: відкритість суспільства та держави; швидкість та не завжди висока ціна злочину; висока технологічність; зазвичай складний характер злочину; анонімність злочинця; транснаціональний та популярний характер злочину; організований характер та змішаний склад учасників злочину, тощо.

Проведений Національним інститутом стратегічних досліджень аналіз тенденцій у політиці провідних держав щодо протидії загрозам в кіберпросторі пропонуються наступні рекомендації: впорядкування політики Української держави у сфері кібербезпеки, а саме: визначення цілей та методів їх досягнення; провести попередній огляд кібербезпекової сфери держави (наприклад в рамках створення відповідної «Білої книги» [12, с. 95]); вирішення термінологічних проблеми в сфері кібербезпеки. (визначення основних понять в кібербезпековій сфері – «кіберпростір»,

«кібербезпека», «кібератака», «кібернапад», «кіберзахист», «кібертероризм», «кіберзлочин»; імплементації необхідної термінології до законодавства України; створення окремого «Міжвідомчого координаційного центру із кібербезпеки» тощо.

Підтримуючи думку висловлену в дослідженнях В. А. Ліпкана [4, с. 95] можна стверджувати, що кібербезпека є складовою інформаційної безпеки. Держана політика у сфері кібербезпеки, запобігання кіберзлочинів, зокрема, включає наступні сфери: безпеки кіберпростору, запровадження електронного урядування, гарантування безпеки й сталого функціонування електронних комунікацій та державних електронних інформаційних ресурсів. Формування і реалізація державної політики у сфері кібербезпеки є невідємною складовою державної політики у сфері розвитку інформаційного простору та становлення інформаційного суспільства в Україні.

Перед суспільством і державою постає складне завдання сформувати основні напрями та цілі державної політики щодо запобігання кіберзлочинності і забезпечення кібербезпеки, визначити реальні і потенційні загрози національній безпеці України кібернетичного характеру. В свою чергу визначити державну політику не можливо без окреслення головних завдань та функцій суб'єктів забезпечення національної безпеки в кіберсфері. Ну і звичайно виникає необхідність на законодавчому рівні визначити зміст та обсяг таких явищ, як: «кіберзагроза», «кіберзлочин», «кібербезпека» та «кіберпростір» тощо.

Державна політика у сфері кібербезпеки – 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, у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки.

Пунктом 5 статті 85 Конституції України визначено що визначення засад внутрішньої і зовнішньої політики віднесено до повноважень Верховної Ради України, не виключенням є і сфера кібербезпеки. Координація діяльності у сфері кібербезпеки як складової національної безпеки України здійснюється Президентом України через очолювану ним Раду національної безпеки і оборони України.

Кабінет Міністрів України забезпечує формування та реалізацію державної політики у сфері кібербезпеки, захист прав і свобод людини і громадянина, національних інтересів України у кіберпросторі, боротьбу з кіберзлочинністю; організовує та забезпечує необхідними силами, засобами і ресурсами функціонування національної системи кібербезпеки; формує вимоги та забезпечує функціонування системи аудиту інформаційної безпеки на об’єктах критичної інфраструктури (крім об’єктів критичної інфраструктури у банківській системі України).

Національний координаційний центр кібербезпеки як робочий орган Ради національної безпеки і оборони України здійснює координацію та контроль за діяльністю суб’єктів сектору безпеки і оборони, які забезпечують кібербезпеку, вносить Президентові України пропозиції щодо формування та уточнення Стратегії кібербезпеки України.

Центральним органом виконавчої влади, що забезпечує формування та реалізацію державної політики у сферах організації спеціального зв'язку, захисту інформації, телекомунікацій та користування радіочастотним ресурсом є Адміністрація Державної служби спеціального зв'язку та захисту інформації України.

Напрямками формування та реалізації державної політики у сфері кібербезпеки є: криптографічного та технічного захисту інформації, телекомунікацій, користування радіочастотним ресурсом України, поштового зв'язку спеціального призначення, урядового фельд'єгерського зв'язку, захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом, в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах і на об'єктах інформаційної діяльності, а також у сферах використання державних інформаційних ресурсів в частині захисту інформації, протидії технічним розвідкам, функціонування, безпеки та розвитку державної системи урядового зв'язку, Національної системи конфіденційного зв'язку; участь у формуванні та реалізації державної політики у сфері електронного документообігу в частині захисту інформації державних органів та

органів місцевого самоврядування, розробленні та впровадженні електронного цифрового підпису, крім питань правового регулювання його застосування, в державних органах та органах місцевого самоврядування; забезпечення в установленому порядку та в межах компетенції діяльності суб'єктів, які безпосередньо здійснюють боротьбу з тероризмом.

Вважаємо що побудова державної політики має ґрунтуватись на аналогічних принципах на яких має буди побудована Доктрина інформаційної безпеки, а саме: ієрархічної залежності, спадковості, несуперечності та конституційності формування Доктрини інформаційної безпеки; історичності та змінності Доктрини; комплексності розробки Доктрини; відкритості розробки Доктрини; реалізації (практичної значимості) Доктрини; єдності форми і змісту Доктрини; цілеспрямованості; моделюємості процесів забезпечення інформаційної безпеки держави; паралельності розробки Доктрини [10, с. 18].

Викладене вище дозволяє стверджувати, що орієнтирами для державної політики України в напрямі вирішення проблем кібербезпеки мають бути: активне продовження міжнародної, співпраці з інформаційно технологічними державами, спрямованої на повноцінне приєднання до концепцій інформаційного розвитку та інформаційної безпеки та виважене впровадження отриманого досвіду в розвиток національних правовідносин; продовження адаптації національних норм до положень міжнародних актів (особливо це стосується вимог Конвенції про кіберзлочинність); посиленого впровадження задекларованих намірів щодо розвитку національної інформаційно-комунікаційної інфраструктури, створення якісних і доступних інформаційних ресурсів, інформатизації освіти й науки, підтримання національної інформаційної продукції, у тому числі за рахунок держави забезпечення доступу всіх громадян до мережі Інтернет, розширення можливостей отримання телекомунікаційних послуг, широке впровадження визнаних світових стандартів у сфері безпеки інформаційно-телекомунікаційних технологій тощо.

Реалізацією державної політики у сфері кібербезпеки у межах своєї компетенції займаються: міністерства та інші центральні органи виконавчої влади; місцеві державні адміністрації; органи місцевого самоврядування; правоохоронні, розвідувальні і контррозвідувальні органи, суб'єкти оперативно-розшукової діяльності; Збройні Сили України, інші військові формування, утворені відповідно до закону; Національний банк України; підприємства, установи та організації, віднесені до об'єктів критичної інфраструктури; суб'єкти господарювання, громадяни України та об'єднання громадян, інші особи, які провадять діяльність та/або надають послуги, пов'язані з національними інформаційними ресурсами, інформаційними електронними послугами, здійсненням електронних правочинів, електронними комунікаціями, захистом інформації та кіберзахистом.

Варто наголосити, що нормативно-правова база у сфері регулювання розвитку інформаційного суспільства і заходи щодо формування державної інформаційної політики мають повною мірою узгоджуватися із завданнями в сфері інформаційної безпеки, практикою забезпечення збереження державної таємниці, захисту інформаційно-телекомунікаційної інфраструктури та інформаційних ресурсів від кібератак й інших загроз в інформаційному просторі. Важливо створити сприятливі умови для удосконалення вітчизняних систем інформаційного захисту, що набуває особливої актуальності у зв'язку з розширенням інформаційного обміну за допомогою мережі Інтернет. Існує нагальна потреба щодо напрацювання узгоджених правил і процедур захисту національних інтересів України в процесі інтегрування в міжнародні інформаційні мережі.

Висновки. Державна кіберполітика повинна закласти базу для владнання основних завдань розвитку демократичного і вільного суспільства, головними з яких є формування єдиного безпечного інформаційного простору України та її входження у світовий віртуальний простір, кібербезпеки особистості, суспільства й держави. Крім того, велика увага повинна приділятися формуванню демократично орієнтованої масової свідомості, становленню галузі інформаційних послуг, законодавчому регулюванню суспільних відносин, у тому числі пов'язаних з одержанням, поширенням і використанням інформації. Таким чином, врахування вищезазначених проблем при визначенні основних засад формування і реалізації державної інформаційної політики сприятиме

посиленню безпеки держави в політичній, економічній та соціальній сферах, стане дієвим засобом протидії загрозам національної безпеки України.

Список використаних джерел

1. Арістова І.В. Державна інформаційна політика: організаційно-правові аспекти / За загальною редакцією д-ра юрид. наук, проф. Бандурки О. М..: Монографія. – Харків: Вид-во Ун-ту внутр. Справ, 2000. – 368 с.
2. Інформаційна складова державної політики та управління : монографія / С. Г. Соловйов, О.Є. Бух- татий, Ю.В. Нестеряк [та ін.] ; за заг. ред. Н. В. Грицяк ; Нац. акад. держ. упр. при Президентові України. – К. : К.І.С., 2015. – 319 с.
3. Конституція України від 28 червня 1996 р. // Відомості Верховної Ради України.-1996.-№30.-ст.141.
4. Ліпкан В. А. Національна безпека України : навчальний посібник / В. А. Ліпкан. – 2-ге вид. – К. : КНТ, 2009. – 576 с
5. Про доступ до публічної інформації : Закон України від 13.01.2011 № 2939-VI // Голос України. – 2011. – № 24. – 9 лютого. – С. 15.
6. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України // Відом. Верховн. Ради України. – 1994. – № 31. – Ст. 286.
7. Про інформацію: Закон України // Відомості Верховної Ради. – 1992. – № 48. – ст.650. Про інформацію: Закон України // ВВР України. – 1992. – № 48. – Ст. 650.
8. Про основні засади забезпечення кібербезпеки України: Закон України від 05 жовтня 2017 [Електронний ресурс]. – Режим доступу: http://zakon3.rada.gov.ua/laws/show/2163-19.
9. Про телекомунікації: Закон України від 18.11.2003 р. № 1280-IV // Офіційний вісник України. – 2003. – № 51. – Ст. 2644.
10. Системний аналіз переходу від концепції національної інформаційної політики до доктрини інформаційної безпеки України / І. Горбенко, О. Потій, С. Черних, М. Прокофьєв // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні : науково-технічний збірник. – 2002. – Вип. 5. – С. 12-26. – Бібліогр.: 14 назв.
11. Стратегія національної безпеки України : затв. Указом Президента України від 26 трав. 2015 р. № 287 // Уряд. кур'єр. – 2015. – 29 трав. – № 95.
12. Сучасні тренди кібербезпекової політики: висновки для України. Аналітична записка / [Електронний ресурс]. – Режим доступу: http://www.niss.gov.ua/articles/294/
13. Тихомиров О. О. Забезпечення інформаційної безпеки як функція сучасної держави : моногр. / О. О. Тихомиров ; заг. ред. Р. А. Калюжний. − Центр навч.-наук. та наук.-практ. вид. НА СБ України, 2014. – 196 с.

Таволжанский А. В. Основы государственной киберполитики Украины: формирование и реализация

Осуществлен анализ мероприятий по обеспечению кибербезопасности государства, выделенные новые сферы внутренней политики государства с учетом роста киберугроз. Предложены пути улучшения кибербезпековои политики Украины с целью приведения ее к требованиям современности и обеспечения суверенитета государства в условиях активизации процесса геополитического давления, информационных войн и милитаризации киберпространства.

Ключевые слова: *государственная информационная политика, кибеполитика, кибербезопасность, киберпространство, информационное законодательство.*

Tavolzhanskyi A. V. Bases of the state cyber policy of Ukraine: formation and realization

The analysis of measures to ensure the cyber security of the state, the new areas of the internal policy of the states are allocated, taking into account the growth of cyber threats. The ways of improving the cyber-security policy of Ukraine in order to bring it to the requirements of the present and ensure the

state's sovereignty in the conditions of activation of the process of geopolitical pressure, information wars and militarization of cyberspace are proposed.

The term «politics» (politics) of Greek origin. The literal translation has the following meaning: state affairs (from polis – state), in other words, art to govern the state. In accordance with Article 17 of the Constitution of Ukraine, the protection of information security, in particular, is one of the most important functions of the state, the cause of the entire Ukrainian people.

The purpose of the article is to identify new trends in cybersecurity policy. The problems of telecommunication and information security and cyberspace are being explored and studied more and more actively in recent times. Among the most relevant areas are the following: information security issues, such as information security in the context of globalization and the transformation of security challenges; the question of the international and national aspects of the fight against cybercrime; information and cyberwar problems of policy formation (including legal) counteraction to computer crime; money laundering, etc.

Key words: *state information policy, cyberpolicy, cybersecurity, cyberspace, information legislation.*

Надійшла до редакції 20 жовтня 2017 р.