Удосконалення нормативно-правового регулювання професійної діяльності суб'єктів кібербезпекової політики

Improvement of the legal regulation of professional activity of subjects cybersecurity policy

Діордіца Ігор

Ключові слова:

кібербезпека, державна політика у сфері кібербезпеки, кібербезпекова політика, політика кібербезпеки, суб'єкти кібербезпекової політики.

Key words:

cyber security, state policy in the field of cyber security, cyber security policy, subjects of cyber security policy.

Постановка проблеми. Науково-технічний прогрес настільки змінив світ, що традиційні, непорушні до цього часу поняття трансформувалися корінним чином. Якщо раніше у сфері політики домінантними були категорії держави, її внутрішнього і зовнішнього курсу, пріоритетів у діяльності державних органів, то нині поява кібернетичного простору робить кордони доволі умовними, а значить, необхідні принципово нові підходи до вирішення проблем, що їх висуває сьогодення.

Стан дослідження проблеми. Поняття кібербезпекової політики є відносно новим у сфері науки. За нашими спостереженнями, з огляду на його кроснауковий характер воно входить до сфери інтересів як фахівців з інформаційних технологій (А. Момот, П. Седаков, В. Панченко), так і політологів (В. Вознюк, А. Гольцов, М. Гримська, Д. Дубов, В. Лебідь, А. Луценко, М. Ожеван, О. Олійник, Ю. Романчук), соціологів (А. Марченко, П. Федорук, М. Шевченко, Я. Базилюк), правників (В. Бутузов, М. Погорецький, І. Сопілка, В. Шеломенцев) і навіть лінгвістів (Ю. Федорова). Основна увага науковців, що займаються питаннями кібербезпеки й державної політики у цій галузі, зосереджена на понятєво-категоріальному апараті цієї наукової сфери, визначенні світових тенденцій, порівняльному аналізі досвіду провідних держав світу й України, визначенні можливостей адаптації передового досвіду для України.

Слід виокремити значний доробок Інституту стратегічних комунікацій Глобальної організації союзницького лідерства, зокрема наукової школи доктора юридичних наук В. Ліпкана (В. Баскаков, Р. Банк, М. Дімчогло, В. Залізняк, Є. Збінський, О. Климентьєв, В. Кобринський, О. Кушнір, Д. Лобов, В. Майоров, Ю. Максименко, О. Мандзюк, П. Матвієнко, М. Микитенко, Д. Перов, В. Політило, С. Правдюк, Л. Рудник, О. Стоєцький, К. Татарникова, А. Тунік, К. Череповський, О. Шепета та ін.). У цих роботах закладено суттєвий фундамент для вивчення стану підготовки фахівців із кібербезпеки [1–10].

Попри значну кількість досліджень із питань забезпечення кібернетичної безпеки, проблеми нормативно-правового регулювання професійної діяльності суб'єктів кібербезпекової політики залишилося недостатньо висвітленим у наукових працях. На термінологічному рівні фіксується деяка невпорядкованість уживання ключових лексичних одиниць, а через це – й підміна понять. Перераховані чинники негативно впливають на можливості вдосконалення нормативно-правової бази, що покликана забезпечувати безпеку держави у кібернетичному просторі.

Метою статті є аналіз нормативно-правових актів, якими регулюється професійна діяльність суб'єктів кібербезпекової політики, та визначення шляхів удосконалення концептуальних засад документів зазначеної сфери.

Виклад основного матеріалу. Багатомірність політичної діяльності нещодавно доповнилася ще однією гранню – кібербезпековою. Її поява детермінована тим, що віртуальний простір настільки широко й органічно ввійшов у життя людей, що несе не тільки блага, а й реальні загрози. Через нього можуть здійснювати пропаганду й агітацію, вести інформаційні війни, розповсюджувати заборонений контент, здійс-

нювати шпіонаж, зокрема промисловий, вчинювати викрадення коштів з електронних рахунків тощо. Діапазон кіберзагроз є доволі широким – від національних інтересів держави, окремих органів, організацій, установ і закладів до духовних цінностей суспільства, окремих спільнот, прав і свобод кожної людини. У зв'язку з цим держава не може залишатись осторонь, а повинна протидіяти, зокрема через правовий механізм, усім правопорушенням, що відбуваються у кібернетичному просторі, з урахуванням їхнього транснаціонального характеру, а також створювати всі належні умови задля їх превенції.

Виокремлюючи структурні елементи кібернетичної безпеки, В. Бутузов включає до них державну політику щодо забезпечення кібербезпеки; державні й громадські інститути й організації, а також суб'єктів приватного сектору, що правомочні вживати заходів для забезпечення безпеки людини, суспільства й держави в кіберпросторі; засоби й методи забезпечення кібербезпеки [11, с. 170].

Як бачимо, вчений уникає термінологічного сполучення «кібербезпекова політика», а говорить про «державну політику щодо забезпечення кібербезпеки». Це потребує наукових коментарів.

Нині немає єдиного тлумачення поняття «кібербезпекова політика». Більшість теоретиків розглядає його в контексті політики національної безпеки, зокрема в сегменті інформаційної безпеки [12–16]. Основна термінологічна проблема сьогодення полягає в амбівалентності дефініцій понятєво-категоріального апарату того сегменту науки і практики, що присвячений діяльності держави у кібернетичному просторі. Зокрема, в аналітичній записці Національного інституту стратегічних досліджень «Сучасні тренди кібербезпекової політики: висновки для України» зазначається, що «в Україні відсутні системні нормативні документи, що описували б саме загрози України у кіберпросторі, давали їх визначення та формували цілісну державну політику із кібербезпеки» [17].

Отже, насамперед потребується визначитись у сутності ключових понять: що слід розуміти під «кібербезпековою політикою», а залежно від цього – хто є її суб'єктами.

Словотворча основа атрибутиву «кібербезпековий» походить від терміна «кібербезпека». За нашими спостереженнями, даючи визначення цього поняття, вчені погоджуються з тим, що це є «стан захищеності життєво важливих прав та інтересів людини, суспільства, держави у кіберпросторі». Відмінності у поглядах полягають у розумінні небезпечних чинників (внутрішні і зовнішні протиправні посягання та загроза таких посягань) [11, с. 176] або у спрямуванні діяльності на «безперешкодне створення, збирання, одержання, зберігання, використання, поширення, охорону, захист інформації» [13].

Залежно від позиціонування суб'єктів діяльності ми пропонуємо розрізняти поняття «кібербезпекова політика» і «політика кібербезпеки». На нашу думку, ***кібербезпекова політика*** є більш широким поняттям, під яким ми розуміємо ***взаємно скоординовану діяльність органів державної влади, органів місцевого самоврядування, правоохоронних органів, уповноважених осіб і вчених із забезпечення як на міждержавному, так і державному рівні кібернетичної безпеки, що базується на системних науково обґрунтованих засадах, концептуальних стратегіях та їх втіленні через узгоджені дії визначених законом суб'єктів у парадигмі системи національної інформаційної безпеки, забезпеченні політичних, економічних та інформаційних прав і свобод людини та громадянина, захисту матеріальних і духовних цінностей держави і суспільства***.

Поняття «***політика кібербезпеки***», на наш погляд, є більш вузьким і конкретним. Під ним пропонується розуміти ***науково обґрунтований комплекс технічних, управлінських, просвітницьких заходів у межах окремої організації, підприємства, установи, закладу щодо забезпечення ефективних умов діяльності на сучасному рівні, упередження несанкціонованих втручань у роботу комп'ютерних систем, об'єктів критичної інфраструктури, витоку важливої, зокрема таємної, конфіденційної інформації***.

Подібне розмежування необхідно для того, щоб у подальшому чітко структурувати цілі і завдання окремих суб'єктів. Якщо, виходячи з першої дефініції, такими суб'єктами є юридичні й фізичні особи, які згідно з чинним законодавством мають виконувати державні функції, то у другому випадку до кола суб'єктів можуть додаватися працівники комерційних структур, приватні підприємці та ін. Бінарний характер двох суміжних, але не тотожних понять проявляється у тому, що, наприклад, певний уповноважений орган, виконуючи свої функції, водночас утілює (у межах держави, на міжнародному рівні) кібербезпекову політику і (щодо власного апарату) політику кібербезпеки. Водночас не уповноважені нормативно–правовими актами суб'єкти здійснюють лише політику кібербезпеки, хоча й не обмежуються у праві виходити з пропозиціями щодо змін у кібербезпековій політиці держави.

Табл. 1

Порівняльний аналіз суб'єктів забезпечення національної і кібернетичної безпеки згідно з нормативно-правовими актами України

Номінація суб'єкта	Закон України «Про основи Національної безпеки України»	Проект Закону «Про основні засади забезпечення кібербезпеки України»	Стратегія кібербезпеки України
Президент України	+	+	
Верховна Рада України	+		
Кабінет Міністрів України	+	+	
Рада національної безпеки і оборони України	+	+	+
Національний координаційний центр кібербезпеки		+	
Міністерства та інші центральні органи виконавчої влади	+	+	
Національний банк України	+		+
Суди загальної юрисдикції	+		
Прокуратура України	+		
Національне антикорупційне бюро України	+		
Місцеві державні адміністрації та органи місцевого самоврядування	+	+	
Міністерство оборони України			+
Збройні сили України	+	+	
Служба безпеки України	+		+
Служба зовнішньої розвідки України	+		
Правоохоронні, розвідувальні і контррозвідувальні органи України, суб'єкти оперативно-розшукової діяльності		+	+
Національна поліція України			+
Державна прикордонна служба України	+		
Державна служба спеціального зв'язку та захисту інформації України			+
Інші військові формування, утворені відповідно до законів України	+	+	
Органи і підрозділи цивільного захисту	+		
Підприємства, установи та організації, віднесені до критично важливих об'єктів інфраструктури		+	
Суб'єкти господарювання, інші особи, які провадять діяльність та/або надають послуги, пов'язані з національними інформресурсами, інформаційними електронними послугами, здійсненням електронних правочинів, електронними комунікаціями, захистом інформації та кіберзахистом		+	
Громадяни України, об'єднання громадян	+	+	

Нині немає єдності думок щодо переліку суб'єктів кібербезпекової політики. За спостереженнями О. Косогова, питаннями інформаційної, зокрема кібернетичної, безпеки в Україні опікуються понад 20 державних органів і центральних органів виконавчої влади [18, с. 129].

В. Шеломенцев вважає, що є підстави виокремлювати суб'єктів забезпечення кримінологічної кібербезпеки і вирізняти серед них загальних та спеціальних суб'єктів [19, с. 346]. До загальних суб'єктів він пропонує відносити всі державні органи та громадські організації, діяльність яких спрямована на протидію кіберзлочинності. До спеціальних суб'єктів, на його думку, потрапляють правоохоронні органи, уповноважені на здійснення активного впливу на злочинність і злочинців у кіберпросторі. У такий спосіб протидія подібним загрозам покладається на Службу безпеку України, Міністерство внутрішніх справ, Державну службу спеціального зв'язку та захисту інформації, певною мірою – на Міністерство оборони України.

В аспекті нормативно-правового регулювання питання щодо визначення суб'єктів кібербезпекової політики ускладнено, оскільки нині не існує окремого законодавчого акту, який би консолідував у собі всі елементи реалізації кібернетичної безпеки. Проте певні кроки на цьому шляху робляться. Так, 20 вересня 2016 р. був прийнятий за основу проект Закону «Про основні засади забезпечення кібербезпеки України», в якому надаються визначення ключових термінів, закладаються підвалини діяльності державних і недержавних органів, громадських організацій у зазначеній сфері [20]. До речі, термінологічне словосполучення «кібербезпекова політика» у вказаному проекті не застосовується. Вживається поняття «державна політика у сфері кібербезпеки», але його визначення у тексті не надається.

15 березня 2016 р. Указом Президента України була затверджена «Стратегія кібербезпеки України» [21]. У документі зазначається, що «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 провадять діяльність у сфері електронних комунікацій, захисту інформації та/або є власниками (розпорядниками) об'єктів критичної інформаційної інфраструктури».

Окремо Указом Президента України від 7 червня 2016 р. затверджено «Положення про Національний координаційний центр кібербезпеки», що створений як робочий орган Ради Національної безпеки і оборони України [22].

Оскільки кібернетична безпека є складовою національної безпеки України, доцільно провести порівняльний аналіз текстів зазначених актів із Законом України «Про основи національної безпеки України» щодо репрезентації суб'єктів, уповноважених згідно з нормативно-правовими актами забезпечувати кібернетичну і національну безпеку, та представити результати у вигляді таблиці [23].

Як видно з таблиці, сьогодні на рівні нормативно-правових актів є суттєві розбіжності у баченні суб'єктів, на які покладається обов'язок забезпечення національної/кібернетичної безпеки. Що ж до визначення суб'єктів кібербезпекової політики, то про них у цих документах узагалі не йдеться.

Більше того, фіксуються внутрішні невідповідності в межах Стратегії кібербезпеки України. Спочатку оговорюється, що Національна система кібербезпеки забезпечується у взаємодії низки суб'єктів, серед яких називаються наукові установи, навчальні заклади, а потім зазначені суб'єкти до переліку не вносяться.

Загалом контент-аналіз нормативно-правових актів, які регулюють діяльність суб'єктів кібернетичної безпеки, виявив суттєву недооцінку ролі науки у формуванні стратегій, концепцій, теорій державної політики у вказаній галузі. Здебільшого тексти спрямовані на опис суто виконавчих функцій державних органів. У такий спосіб втрачається превентивний характер науково обґрунтованих заходів із прогнозування й упередження протиправних дій у кіберпросторі.

Ми повністю погоджуємось із думкою Д. Дубова про те, що майже в усіх документах «насправді йдеться не про «кібербезпеку» як таку, а радше про «кіберзахист», причому в суто вузькому сегменті цього ключового поняття як захисту критичної інфраструктури» [24, с. 258].

Визначаючи основні питання, що потребують удосконалення у сфері нормативно-правового регулювання професійної діяльності суб'єктів кібербезпекової політики, слід було б зосередити увагу на таких:

– підготовка й ухвалення за встановленими процедурами Закону України «Про державну політику в сфері кібернетичної безпеки»;
– створення тезаурусу термінології кібернетичної безпеки та його легітимізація у тексті відповідних законів;
– гармонізація законодавства щодо єдиного бачення кола суб'єктів, на яких покладаються обов'язки забезпечення національної, зокрема кібернетичної, безпеки, визначення і провадження національної та міжнародної кібербезпекової політики;
– внесення до чинних нормативно-правових актів положень щодо ролі і місця наукових установ, вищих навчальних закладів у дослідженні проблем кібернетичної безпеки, формування кібербезпекової політики на науково обґрунтованих засадах.

Висновки. Проведений аналіз нормативно-правових актів дозволив встановити, що нині поза сферою державного регулювання опинилися питання професійної діяльності суб'єктів кібербезпекової політики. Запропонована авторська інтерпретація ключової термінології, на підставі якої диференціюються функції зазначених суб'єктів і визначаються цілі їхньої професійної діяльності.

Анотація

Статтю присвячено аналізу нормативно-правових актів, якими регулюється професійна діяльність суб'єктів кібербезпекової політики. Пропонується розрізняти поняття «кібербезпекова політика» і «політика кібербезпеки». Надаються авторські дефініції зазначених понять. Проводиться порівняння основних положень чинних нормативно–правових актів і проекту Закону України «Про основні засади забезпечення кібербезпеки України» в аспекті визначення кола суб'єктів та їхньої ролі у процесі виконання функцій держави. Констатується недооцінка науки і вчених у формуванні кібербезпекової політики. Запропоновано шляхи вдосконалення нормативно-правового регулювання у галузі, що досліджується.

Summary

Cyber security policy is one of the elements of national security, and therefore its study is extremely important. The article is devoted to the analysis of legal acts, regulating the professional activities of the subjects of cyber security policy. The author proposes a definition of key concepts. Cybersecurity policy he proposes to treat as mutually coordinated activities of state authorities, local government, law enforcement agencies, authorized persons and academics to ensure cyber security, which based on conceptual strategies and their implementation in the national paradigm. The analysis of existing legal acts and draft laws in the field of cyber security has allowed to establish that an understanding of the circle of subjects in each document presented differently. This suggests that the state has not yet developed a unified concept, how and who carries out the policy of cybersecurity. The author suggests ways to improve the current legislation. He believes that the necessary preparation and adoption of the Law of Ukraine "On the state policy in the field of cyber–security": the creation of a thesaurus of terminology and its legitimation in legislation: harmonization of the rules regarding the subjects of cyber security policy: made to the text of legal acts of the provisions of the role of science in this field.

Використана литература:

1. Ліпкан В.А. Адміністративно-правовий режим інформації з обмеженим доступом в Україні : [монографія] / В.А. Ліпкан, В.Ю. Баскаков ; за заг. ред. В.А. Ліпкана. – К. : О.С. Ліпкан, 2013. – 344 с.
2. Ліпкан В.А. Інкорпорація інформаційного законодавства України : [монографія] / В.А. Ліпкан, К.П. Череповський ; за заг. ред. В.А. Ліпкана. – К. : О.С. Ліпкан, 2014. – 408 с.
3. Ліпкан В.А. Консолідація інформаційного законодавства України : [монографія] / В.А. Ліпкан, М.І. Дімчогло ; за заг. ред. В.А. Ліпкана. – К. : О.С. Ліпкан, 2014. – 416 с.
4. Ліпкан В.А. Правовий режим податкової інформації в Україні : [монографія] / В.А. Ліпкан, О.В. Шепета, О.А. Мандзюк ; за заг. ред. В.А. Ліпкана. – К. : О.С. Ліпкан, 2015. – 440 с.

5. Ліпкан В.А. Систематизація інформаційного законодавства України : [монографія] / В.А. Ліпкан, В.А. Залізняк ; за заг. ред. В.А. Ліпкана. – К. : О.С. Ліпкан, 2012. – 304 с.
6. Ліпкан В.А. Стратегічні комунікації : [словник] / Т.В. Попова, В.А. Ліпкан ; за заг. ред. В.А. Ліпкана. – К. : О.С. Ліпкан, 2016. – 416 с.
7. Ліпкан В.А. Інформаційна безпека України в умовах євроінтеграції : [навч. посіб.] / [В.А. Ліпкан, Ю.Є. Максименко, В.М. Желіховський]. – К. : КНТ, 2006. – 280 с.
8. Ліпкан В.А. Правові засади розвитку інформаційного суспільства в Україні : [монографія] / В.А. Ліпкан, І.М. Сопілко, В.О. Кір'ян / за заг. ред. В.А. Ліпкана. – К. : О.С. Ліпкан, 2015. – 664 с.
9. Мандзюк О.А. Правове регулювання аналітичної діяльності в Україні : [монографія] / О.А. Мандзюк, М.Г. Сабіна. – К. : Дорадо-Друк, 2016. – 312 с.
10. Рудник Л.І. Право на доступ до інформації : дис. ... канд. юрид. наук : спец. 12.00.07 / Л.І. Рудник ; Нац. ун-т біоресурсів і природокористування України. – К., 2015. – 247 с.
11. Бутузов В.М. Протидія комп'ютерній злочинності в Україні (системно-структурний аналіз) : [монографія] / В.М. Бутузов. – К. : КИТ, 2010. – 408 с.
12. Гурковський В.І. Організаційно-правові питання взаємодії органів державної влади у сфері національної інформаційної безпеки : дис. … канд. юрид. наук / В.І. Гурковський. – К., 2004. – 225 с.
13. Діордіца І.В. Поняття та зміст національної системи кібербезпеки / І.В. Діордіца [Електронний ресурс]. – Режим доступу : http://goal–int.org/ponyattya–ta–zmist–nacionalnoi–sistemi–kiberbezpeki/.
14. Ліпкан В.А. Національна безпека України: нормативно-правові аспекти забезпечення : [монографія] / В.А. Ліпкан. – К. : Текст, 2003. – 180 с.
15. Сопілко І.М. Засади інформаційної гносеології / І.М. Сопілко // Право і суспільство. – 2014. – № 3. – С. 228–234.
16. Цимбалюк В.С. Кодифікація інформаційного законодавства України : дис. … докт. юрид. наук : спец. 12.00.07 / В.С. Цимбалюк ; Нац. ун-т «Юрид. акад. України імені Ярослава Мудрого» МОН України. – Харків, 2013. – 435 с.
17. Сучасні тренди кібербезпекової політики: висновки для України: аналітична записка / Нац. ін-т стратег. досліджень [Електронний ресурс]. – Режим доступу : http://www.niss.gov.ua/articles/294/.
18. Косогов О.М. Пріоритетні напрямки державної політики щодо забезпечення безпеки національного кіберпростору / О.М. Косогов // Збірник наукових праць Харківського університету Повітряних Сил. – 2015. – Вип. 3 (40). – С. 127–130.
19. Шеломенцев В.П. Кримінологічна безпека у кіберпросторі: система понять / В.П. Шеломенцев // Боротьба з організованою злочинністю і корупцією (теорія і практика). – 2010. – № 23. – С. 342–348.
20. Про основні засади забезпечення кібербезпеки України : проект Закону України, прийнятий за основу згідно з постановою Верховною Ради України № 1524-VIII від 20.09.2016 р. [Електронний ресурс]. – Режим доступу : http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_2?pf3516=2126%D0%B0&skl=9.
21. Стратегія кібербезпеки України : Указ Президента України № 96/ 2016 від 15.03.2016 р. [Електронний ресурс]. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/96/2016.
22. Положення про Національний координаційний центр кібербезпеки : Указ Президента України № 242/2016 від 07.06.2016 р. [Електронний ресурс]. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/242/2016.
23. Про основи національної безпеки : Закон України від 19.06.2003 р. (в редакції 07.08.2015 р.) [Електронний ресурс]. – Режим доступу : http://zakon5.rada.gov.ua/laws/main/964–15.
24. Дубов Д.В. Кіберпростір як новий вимір геополітичного суперництва : [монографія] / Д.В. Дубов. – К. : НІСД, 2014. – 328 с.

Діордіца Ігор,
кандидат юридичних наук, доцент,
голова Інституту адміністративного правосуддя
Глобальної організації союзницького лідерства