УДК 344.326(045):004.056.5(477)
DOI https://doi.org/10.15421/391956

Веселова Л. Ю.,
кандидат юридичних наук,
доцент кафедри адміністративної діяльності підрозділів поліції
Одеського державного університету внутрішніх справ

ОСОБЛИВОСТІ ВЗАЄМОДІЇ СПЕЦІАЛЬНИХ ОРГАНІВ, СЛУЖБ ТА ПІДРОЗДІЛІВ У СФЕРІ ЗАБЕЗПЕЧЕННЯ КІБЕРБЕЗПЕКИ

PECULIARITIES OF INTERACTION WITH SPECIAL BODIES, SERVICES AND SUBSIDIES IN THE FIELD OF PROVIDING CYBER SECURITY

У статті проаналізовано особливості взаємодії спеціальних органів, служб та підрозділів у сфері забезпечення кібернетичної безпеки. Виокремлено специфіку інформаційних ресурсів у кібернетичному просторі, яка проявляється у стрімкому розвитку інформаційних та інформаційно-комунікаційних технологій. Говориться, що проблема забезпечення національної безпеки багатоаспектна, одним з найважливіших напрямів її забезпечення виступає створення ефективної правоохоронної системи, здатної протистояти негативним тенденціям в адміністративно-правовій сфері суспільних відносин. Також, відзначаючи важливість вищевказаного проблемного питання, виокремлено комплекс завдань, пов'язаних із забезпеченням кібернетичної безпеки, з визначенням ролі і місця в цьому процесі адміністративно-правових засобів регулювання. Сформульовано першочергове завдання усіх гілок державної влади на сучасному етапі розвитку інформаційного суспільства, яке полягає у запровадженні та реалізації механізмів генерації прийнятих рішень у сфері кібернетичної безпеки. Запропоновано прийняття Державної цільової програми забезпечення кібернетичної безпеки України, яка слугуватиме відправною точкою в реалізації реальної взаємодії суб'єктів забезпечення кібернетичної безпеки України. Охарактеризовано особливості проекту Державної цільової програми забезпечення кібернетичної безпеки України, які включають: визначення конкретних напрямів державної політики з протидії кібернетичним загрозам, основними серед яких мають стати концептуальна зміна філософії адміністрування у сфері забезпечення кібернетичної безпеки – від координації діяльності органів державної влади та правоохоронних органів до оперативного управління ними; розвиток державно-приватного партнерства в частині надання приватному бізнесу та громадськості реальних важелів впливу на стан забезпечення кібернетичної безпеки. В статті робиться акцент на зазначеному напряму, який може бути реалізований шляхом включення до числа суб'єктів забезпечення кібернетичної безпеки громадських інституцій та незалежних експертів; реалізація бізнес-проектів у напряму модернізації інформаційної та інформаційно-комунікаційної інфраструктури до рівня міжнародних стандартів; здійснення заходів, спрямованих на підвищення грамотності громадян у кібернетичної сфері на всіх рівнях освіти.

Ключові слова: *інформаційні ресурси, кібернетичний простір, інформаційно-комунікаційні технології, державна влада, інформаційне суспільство, державна політика, правоохоронні органи, державно-приватне партнерство.*

The article analyzes the peculiarities of the interaction of special bodies, services and units in the field of cybersecurity. The specificity of information resources in the cybernetic space, which manifests itself in the rapid development of information and information and communication technologies, is singled out. The problem of national security is multifaceted, one of the most important areas of its support is the creation of an effective law enforcement system that can withstand negative trends in the administrative and legal sphere of public relations. Also, noting the importance of the aforementioned problematic issue, a set of tasks related to ensuring cyber security was identified, with the definition of the role and place in this process of administrative and legal means of regulation. The primary task of all branches of state power at the present stage of the development of the information society is formulated, which consists in the introduction and implementation of mechanisms for generating adopted decisions in the field of cyber security. The adoption of the State Target Program for the Cyber security of Ukraine, which will serve as a starting point for the real interaction of the subjects of the cyber security of Ukraine, is proposed. The peculiarities of the State Target Program for Cyber security of Ukraine, which consist in determining the specific areas of the state policy on counteraction to cyber threats, are characterized, the main among which should be a conceptual change in the philosophy of administration in the field of cyber security, from coordination of activities of public authorities and law enforcement agencies to the operational management of them; the development of public-private partnerships, in terms of giving private business and the public real leverage on the state of cyber security. The article focuses on the aforementioned direction, which can be implemented by the inclusion of cybersecurity entities by public institutions and independent experts; implementation of business projects in the direction of modernization of information and information and communication infrastructure to the level of international standards; implementation of measures aimed at increasing the literacy of cyber-citizens at all levels of education.

Key words: *information resources, cyber space, information and communication technologies, state power, information society, state policy, law enforcement bodies, public-private partnership.*

Сьогодні значення інформації у найрізноманітніших соціальних процесах набуває дедалі більшого значення. Активне використання засобів обробки і передачі інформації, розвиток нових технологій викликають суттєві зміни в економічній, політичній та інших сферах суспільного життя. Багатьма дослідниками ставиться питання про формування нового – кібернетичного типу суспільства, яке приходить на зміну індустріальному суспільству. У зв'язку з цим останніми роками суттєво збільшилася зацікавленість до юридичних аспектів суспільних відносин, що виникають та існують в області інформації.

Проблема забезпечення національної безпеки багатоаспектна. Одним з найважливіших напрямів її забезпечення виступає створення ефективної правоохоронної системи, здатної протистояти негативним тенденціям в адміністративно-правовій сфері суспільних відносин. Відзначаючи важливість вищев-

казаного проблемного питання, слід особливо виділити комплекс питань, пов'язаних із забезпеченням кібернетичної безпеки, з визначенням ролі і місця в цьому процесі адміністративно-правових засобів регулювання.

Різке посилення суспільно-економічного значення використання міжнародної мережі Інтернет загострило правові проблеми, пов'язані з застосуванням високих комп'ютерних і телекомунікаційних технологій. Відносна новизна цих проблем, стрімке нарощування процесів комп'ютеризації суспільства, зростання комп'ютерної грамотності населення стали справжнім випробуванням для правоохоронних органів, які були не готовими до адекватного протистояння і боротьби з цим новим соціально-правовим явищем.

Зазначені процеси поставили перед законодавцем проблему ефективного юридичного упорядкування суспільних відносин у кібернетичній сфері та вироблення дієвої системи спеціальних органів, служб та підрозділів у сфері забезпечення кібернетичної безпеки.

Питання адміністративно-правового статусу суб'єктів державного управління, в тому числі й тих, які забезпечують національну безпеку у кіберсфері, у науковій літературі висвітлені доволі докладно такими вітчизняними та зарубіжними науковцями, як Є. Аушев, О.М. Бандурка, В.В. Бухарєв, Д.В. Дубов, И.И. Жбанкова, М. Кольцов, В.К. Колпаков, С.В. Пєтков, М.М. Присяжнюк, О. Приходько, О.П. Рябченко, Є.І. Цифра. Водночас вироблення ефективних механізмів взаємодії вищевказаних суб'єктів державного управління наразі є малодослідженим напрямом адміністративно-правової науки та потребує проведення подальших наукових досліджень.

Мета дослідження полягає у формуванні науково-обґрунтованих пропозицій до національного законодавства в частині вироблення ефективних механізмів взаємодії спеціальних органів, служб та підрозділів у сфері забезпечення кібербезпеки України.

В юриспруденції дефініція «правова взаємодія» як форма соціальної взаємодії до теперішнього часу не отримала належного наукового з'ясування, не зважаючи на те, що в нормативно-правових актах, в тому числі й тих, які прийняті останніми роками, вказана правова категорія використовується доволі часто.

Найбільш повно розуміння взаємодії розкривається в процесі дослідження наукової літератури, шляхом співставлення різноманітних її конструкцій, які використовуються у наукових публікаціях, з іншими правовими явищами та правовими категоріями.

У Великому тлумачному словнику сучасної української мови взаємодія визначається як взаємний зв'язок між предметами у дії, а також погоджена дія між ними [1, с. 125]. У наведеному визначенні яскраво простежуються специфічні критерії, які характеризують взаємодію не тільки з позиції спільної, але й злагодженої діяльності суб'єктів, яка виражається у взаємному зв'язку між ними, а також узгоджених діях.

Деякі науковці розглядають взаємодію комплексно, у правовій, філософській та соціологічній площині [2, с. 7]. Уявляється, що використовуючи такий підхід, В.К. Колпаков найбільш повно розкрив сутність зазначеного правового явища.

Поряд з цим заслуговує на увагу думка І.І. Жбанкової, яка розглядає взаємодію як одну з форм соціальних об'єктивно існуючих зав'язків, які нерозривно поєднані з іншими явищами правової дійсності [3, с. 17]. У цьому разі автор передовсім підкреслює соціальний аспект феномену взаємодії, розглядаючи його як частину соціального буття.

Водночас С.В. Пєтков під час характеристики взаємодії виокремлює умови її існування як соціально-правового явища, до яких передовсім належить взаємне існування декількох соціальних систем, а також наявність закономірних об'єктивних зав'язків між ними [4, с. 18].

Взаємодія як правова категорія також широко представлена й у національному законодавстві. Зокрема, Конституція України використовує дефініцію «взаємодія» лише одного разу, у статті 119, під час визначення функцій місцевих державних адміністрацій, зокрема, в частині забезпечення взаємодії з органами місцевого самоврядування [5]. Крім того, не зважаючи на положення частини 4 статті 5 Закону України «Про основні засади забезпечення кібербезпеки України», відповідно до якої місцеві державні адміністрації визначені як суб'єкти, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки, слід констатувати, що напрями їх діяльності в частині забезпечення кібербезпеки України у профільному законодавчому акті також не визначені.

Звертає на себе увагу відносно нова форма співпраці вказаних суб'єктів, механізм якої ретельно визначений у коментованому законодавчому акті та полягає у державно-приватній співпраці суб'єктів забезпечення кібербезпеки України.

Дійсно, останніми роками у протидії кіберзлочинності склалася ситуація, що змушує державу зміцнювати взаємодію з приватним бізнесом і в цій сфері. Зазначене завдання в частині забезпечення державно-приватного партнерства, широкої співпраці з громадянським суспільством у сфері забезпечення кібербезпеки та кіберзахисту також закріплено у Стратегії кібербезпеки України.

Водночас слід констатувати, що форми реалізації функцій, визначених у статті 10 коментованого законодавчого акту, на жаль, законодавцем не визначені. Однак з'ясування цього питання у науці державного управління має надвелике значення. Наприклад, за цілком обґрунтованим твердженням О.П. Рябченко, форма чинить безпосередній вплив (позитивний чи негативний) на зміст державно-управлінської діяльності. Від того, наскільки повно виражена форма державного управління, залежить якість реалізації змісту діяльності у сфері державного управління [6, с. 19–20]. На цій підставі спробуємо виокремити ключові форми реалізації положень, визначених у частині 1 статті 10 цього закону.

Вважаємо, що реалізацію конкретних напрямів державно-приватного партнерства у сфері забезпе-

чення кібербезпеки України доцільно здійснювати у таких формах:

– здійснення технічних експертиз, предметом яких виступають засоби телекомунікації та комп'ютерної техніки;

– сприяння фахівців у галузі забезпечення кібербезпеки щодо здійснення оперативно-розшукової діяльності;

– збір цифрових доказів;

– розробка та впровадження програмного забезпечення з метою виявлення та попередження кіберзагроз.

Розкриваючи зміст останнього напряму, слід зазначити, що ефективність застосування превентивних заходів у сфері забезпечення кібербезпеки дозволяє протидіяти кіберзагрозам на ранніх етапах можливого вчинення правопорушень у кібернетичній сфері. Натепер окремі українські компанії пропонують високотехнологічний продукт, заснований на останніх даних кіберрозвідки та аналізі реальних хакерських атак, призначення якого полягає у виявленні та попередженні різноманітних кіберзагроз. Застосування сучасних розробок у сфері забезпечення кібербезпеки спрямовано на захист інформаційних ресурсів критично важливих об'єктів інфраструктури, а також підвищення рівня захищеності об'єктів критичної інформаційної інфраструктури та сталості їх функціонування. Розуміння зазначених об'єктів сформульовано в Законі України «Про основні засади забезпечення кібербезпеки України». Аналіз їх співвідношення дає підстави для висновку, що останні виступають в ролі комунікаційних або технологічних систем критично важливих об'єктів інфраструктури та співвідносяться як загальне й часткове. Слід зазначити, що законодавець покладає відповідальність за розробку правил формування переліку об'єктів критичної інформаційної інфраструктури, а також критеріїв віднесення об'єктів до цього переліку на Кабінет Міністрів України. Аналіз Порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави, затвердженого постановою Кабінету Міністрів України від 23 серпня 2016 р. № 563 [7], дозволив дійти висновку, що до об'єктів критичної інфраструктури можуть бути віднесені підприємства, що працюють у сфері енергетики (наприклад, АЕС), хімічної промисловості, транспорту, інформаційно-комунікаційних технологій, електронних комунікацій, а також підприємства банківського і фінансового сектору.

На окрему увагу заслуговує питання щодо з'ясування особливостей взаємодії правоохоронних органів України у сфері забезпечення кібербезпеки України. Організуюча роль в процесі реалізації вказаного напряму належить Раді національної безпеки і оборони України, яка, відповідно до статті 3 Закону України «Про Раду національної безпеки і оборони України», наділена координаційними та контрольними функціями щодо діяльності органів виконавчої влади [8].

Зауважимо, що сьогодні в структурі РНБО України діють два координаційні органи, діяльність яких безпосередньо пов'язана з координацією діяльності суб'єктів забезпечення кібербезпеки України. Йдеться насамперед про Національний координаційний центр кібербезпеки (скорочено – Центр) та Міжвідомчу комісію з питань інформаційної політики та інформаційної безпеки (скорочено – Комісія).

Попри те, що обидва органи багато в чому дублюють функції, завдання та повноваження один одного, в їх організаційно-правовому статусі є і певні відмінності. Слід відмітити, що Комісія, відповідно до частини 1 Положення про неї, виступає в ролі консультативно-дорадчого органу при РНБО України. Відповідно, й повноваження Комісії випливають із її організаційно-правового статусу та мають переважно експертно-аналітичне спрямування, як-от: отримання інформаційних, статистичних, довідкових та інших матеріалів від суб'єктів забезпечення інформаційної безпеки, з метою вирішення питань, пов'язаних із забезпеченням інформаційної безпеки; проведення науково-експертної аналітичної роботи з підготовки та реалізації загальнонаціональних та галузевих програм розвитку інформаційно-комунікаційної сфери; реалізація інформаційної політики шляхом участі у засіданнях консультативно-дорадчих органів підприємств, установ та організацій; утворення експертних груп та залучення фахівців у галузі інформаційної безпеки в процесі вирішення питань, що віднесені до компетенції Комісії [9]. Отже, можемо твердити про доволі обмежену компетенцію Комісії у сфері забезпечення кібербезпеки України.

Таким чином, підбиваючи проміжний підсумок, слід констатувати, що переважна частина положень цього документу [9] є застарілими, розроблялись в умовах відсутності реального інформаційного впливу ззовні, а відтак – не враховують сучасної організаційно-правової специфіки забезпечення національної безпеки України у кібернетичній сфері.

На існуванні прогалин у механізмі координації діяльності суб'єктів забезпечення кібербезпеки також наголошує Д.В. Дубов. Учений зазначає, що брак координації у сфері забезпечення кібербезпеки передовсім породжується значною кількістю суб'єктів її забезпечення. Можливі шляхи щодо розв'язання цієї проблеми, на думку науковця, полягають насамперед у наданні більш широких повноважень РНБО України або ж у створенні нового державного органу із спеціальними функціями по забезпеченню кібербезпеки. Але все ж таки вчений констатує, що на цей час у державному управлінні ще не вироблено дієвих механізмів ефективної реалізації державної політики у сфері забезпечення національної безпеки у кібернетичній сфері [10, с. 332].

Окремо слід зупинитися на з'ясуванні ролі та місця Ради національної безпеки та оборони України в процесі забезпечення національної безпеки України у кібернетичній сфері.

По-перше, слід звернути увагу, що відповідно до статті 3 Закону України «Про Раду національної безпеки і оборони України» РНБО України виконує організаційну та контролюючу функції за діяльністю органів виконавчої влади у сфері національної

безпеки і оборони України [8]. Вказаний напрям діяльності РНБО реалізується через повноваження зазначеного правоохоронного органу. Наприклад, координаційна функція РНБО щодо реалізації державної політики із забезпечення кібербезпеки проявляється у наділенні РНБО компетенцією щодо прийняття рішень, пов'язаних із визначенням стратегічних національних інтересів України, концептуальних підходів та напрямів забезпечення національної безпеки і оборони в інформаційній сфері, а також виробленні заходів інформаційного характеру відповідно до масштабу потенційних та реальних загроз національним інтересам України.

У цьому контексті слід звернути увагу на рішення РНБО України від 29 грудня 2016 року «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації» [11].

На виконання вказаного рішення РНБО України Президенту України пропонується визначити Генерального державного замовника Національної програми інформатизації з урахуванням актуальних загроз кібербезпеці держави. Уявляється, що відповідно до положень цього документу координаційна роль Ради національної безпеки і оборони України проявляється у завданнях, визначених перед органами виконавчої влади та правоохоронними органами держави.

Цілком слушною виглядає позиція М.М. Присяжнюка та Є.І. Цифри, які стверджують, що метою визначення таких завдань є: забезпечення кіберзахисту об'єктів критичної інформаційної інфраструктури; посилення відповідальності за невиконання вимог законодавства стосовно захисту інформації в інформаційно-телекомунікаційних системах; забезпечення повного та об'єктивного розслідування кібератак на інформаційно-телекомунікаційні системи фінансового сектора держави; виявлення та припинення фактів використання органами державної влади програмних продуктів, що розроблені суб'єктами господарювання держави-агресора, використання яких заборонено відповідно до рішень РНБО України щодо застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій), уведених у дію указами Президента України [12, с. 66]. Зазначене свідчить про реалізацію Радою національної безпеки і оборони України координаційної функції, адже РНБО України, відповідно до покладених на неї повноважень, приймає рішення щодо координації діяльності суб'єктів забезпечення кібербезпеки України та надання пропозицій Президентові України щодо вдосконалення системи національної безпеки у сфері кіберзахисту.

За умови комплексного правового підходу до вироблення організаційно-правового механізму взаємодії суб'єктів забезпечення кібербезпеки необхідно враховувати специфіку інформаційних ресурсів у кібернетичному просторі, яка проявляється у стрімкому розвитку інформаційних та інформаційно-комунікаційних технологій. З цієї причини першочергове завдання усіх гілок державної влади на сучасному етапі розвитку інформаційного суспільства полягає не стільки у виробленні або вдосконаленні законодавчого базису, скільки у запровадженні та реалізації механізмів генерації вже прийнятих рішень.

А тому найбільш важливим кроком на етапі цілком сформованої законодавчої основи забезпечення кібербезпеки України вважаємо за доцільне запропонувати розроблення та якнайшвидше прийняття Державної цільової програми забезпечення кібербезпеки України, робота над якою наразі навіть не розпочата суб'єктами законодавчої ініціативи. Прийняття вказаного документу слугуватиме відправною точкою в реалізації реальної взаємодії суб'єктів забезпечення кібербезпеки України. Відмінною особливістю Державної цільової програми забезпечення кібербезпеки України повинно стати визначення конкретних напрямів державної політики з протидії кіберзагрозам, основними серед яких мають стати: а) концептуальна зміна філософії адміністрування у сфері забезпечення кібербезпеки, від координації діяльності органів державної влади та правоохоронних органів до оперативного управління ними; б) розвиток державно-приватного партнерства, в частині надання приватному бізнесу та громадськості реальних важелів впливу на стан забезпечення кібербезпеки. Зазначений напрям може бути реалізований шляхом включення до числа суб'єктів забезпечення кібербезпеки громадських інституцій та незалежних експертів; в) реалізація бізнес-проектів у напряму модернізації інформаційної та інформаційно-комунікаційної інфраструктури до рівня міжнародних стандартів; г) здійснення заходів, спрямованих на підвищення грамотності громадян у кіберсфері на всіх рівнях освіти.

ЛІТЕРАТУРА:

1. Великий тлумачний словник сучасної української мови : 250000 / уклад. та голов. ред. В.Т. Бусел. Київ ; Ірпінь : Перун, 2005. VIII. 1728 с.

2. Колпаков В.К. Взаимодействие милиции и общественности в сфере правопорядка. Київ : УАВД, 1993. 80 с.

3. Жбанкова И.И. Проблема взаимодействия. Минск : Наука и техника, 1970. 144 с.

4. Пєтков С.В. Ефективний менеджмент в органах внутрішніх справ : монографія. Сімферополь : Таврія, 2004. 564 с.

5. Конституція України від 28.06.1996 р. *Відомості Верховної Ради України*. 1996. № 30. Ст. 141.

6. Рябченко О.П. Держава і економіка: адміністративно-правові аспекти взаємовідносин : монографія / за заг. ред. О.М. Бандурки. Харків : Вид-во ун-ту внутр. справ, 1999. 304 с.

7. Про затвердження Порядку формування переліку інформаційно-телекомунікаційних систем об'єктів критичної інфраструктури держави. Постанова Кабінету Міністрів України від 23 серпня 2016 р. № 563. *Офіційний вісник України*. 2016. № 69. Ст. 2332.

8. Про Раду національної безпеки і оборони України : закон України від 05.03.1998 № 183/98-ВР. *Відомості Верховної Ради України*. 1998. № 35. Ст. 237.

9. Про Міжвідомчу комісію з питань інформаційної політики та інформаційної безпеки при Раді національної безпеки і оборони України : указ Президента України від 22.01.2002 № 63/2002. *Офіційний вісник України*. 2002. № 4. Ст. 132.

10. Дубов Д.В. Геополітичне суперництво у кіберпросторі як чинник впливу на національну безпеку України : дис. … докт. політ. наук : 21.01.01. Національний інститут стратегічних досліджень. Київ. 2016. 434 с.

11. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації» : указ Президента України від 13 лютого 2017 року №32/2017. *Офіційний вісник України*. 2017. № 16. Ст. 464.

12. Присяжнюк М.М., Цифра Є.І. Особливості забезпечення кібербезпеки. *Реєстрація, зберігання і обробка даних*. 2017. Т. 19, № 2. С. 61–68.