ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ВЗАЄМОДІЇ СУБ'ЄКТІВ ПУБЛІЧНОГО АДМІНІСТРУВАННЯ З ГРОМАДСЬКІСТЮ

Станіслав Григорович ОНОПРІЄНКО,

канд. юрид. наук, старший викладач кафедри правового забезпечення військового факультету фінансів і права Військового інституту Київського національного університету імені Тараса Шевченка

Під час визначення об'єкта забезпечення інформаційної безпеки у сфері публічного адміністрування слід пам'ятати, що забезпечення уявляє собою специфічний вид соціальної діяльності, тобто активності фізичних та юридичних осіб, спрямованої на перетворення оточуючої реальності з метою досягнення поставлених цілей. Головне питання, яке при цьому виникає – хто саме формулює цілі такої діяльності? З одного боку, безумовно, держава в особі суб'єктів забезпечення національної безпеки, одним із видів якої є інформаційна безпека. Однак, якщо б держава виступала основним суб'єктом формулювання цілей інформаційної безпеки, їх виконання та контролю за їх досягненням, Україна, скоріше за все, давно б втратила інформаційний суверенітет, оскільки 90% цілей, закладених у численних доктринах, концепціях, стратегіях, програмах, планах у сфері національної безпеки, традиційно не виконуються тими суб'єктами, на яких таке виконання покладено. Проте багатоманітність та плюралізм суб'єктів інформаційної діяльності, динамічний розвиток інформаційних відносин, залучення до сфери інформаційних технологій великої кількості інвестицій обумовлюють автономність вирішення завдання подолання загроз інформаційній безпеці недержавними суб'єктами (суб'єктами господарювання, громадськими організаціями, які отримують гранти для здійснення заходів з медіапросвіти тощо). Долаючи ті загрози інформаційній безпеці, які співвідносяться з їх статутними цілями, такі суб'єкти самостійно формулюють цілі забезпечення інформаційної безпеки, самостійно визначають шляхи та критерії їх досягнення, самостійно фінансують таку діяльність за рахунок своїх прибутків або грантів. У сукупності така діяльність істотно знижує руйнівний вплив інформаційних загроз в державі.

Це не заперечує цінності діяльності у сфері інформаційної безпеки деяких суб'єктів публічного адміністрування. Однак оцінювання такої діяльності науковими методами у відкритій науковій періодиці навряд чи можливо, оскільки вона охоплюється законодавством про захист державної таємниці або маж правовий режим службової інформації з обмеженим доступом. Проте аналіз інформації з відкритих джерел дозволяє стверджувати, що діяльність держави у досліджуваній сфері характеризується непослідовністю та хаотичністю – так, наприклад, на Міністерство інформаційної політики України Доктриною інформаційної безпеки України, затвердженою Указом Президента України від 25 лютого 2017 року № 47/2017, покладається функція моніторингу загроз національним інтересам і національній безпеці в інформаційній сфері. Вказане міністерство було реорганізоване з ліквідацією функцій та по-

вноважень 2 вересня 2019 року, а виконання функції моніторингу інформаційним загрозам на новоутворені Міністерство культури, молоді та спорту України та Міністерство цифрової трансформації України не покладено, і таких прикладів можна наводити ще багато (особливо стосовно багатьох центрів протидії інформаційним загрозам, правовий статус яких не визначено, діяльність практично не фінансується і через деякий час фактично припиняється).

Отже, розуміння цілей забезпечення інформаційної безпеки має свої відмінності залежно від суб'єктів такого забезпечення. Найлегше вивчити особливості цілей державного забезпечення інформаційної безпеки, оскільки вони закріплюються у відповідних доктринах, стратегіях, програмах і планах, однак їх виконання органами публічної влади носить переважно формальний характер. Складніше простежити особливості формулювання цілей забезпечення інформаційної безпеки суб'єктами господарської діяльності, оскільки вони можуть бути віднесені до комерційної таємниці, та громадськими організаціями, оскільки вони оприлюднюють результати своєї діяльності перед широким загалом у добровільному порядку. Однак у будь-якому разі можна стверджувати, що цілі забезпечення інформаційної безпеки мають багаторівневий характер, формулюються різними суб'єктами, можуть суперечити одне одному, при цьому єдиний центр управління, який би відстежував формулювання і досягнення таких цілей, відсутній.

За таких умов казати про єдиний і загальновизнаний перелік благ, які складали б об'єкт інформаційної безпеки, було б, на нашу думку, некоректним (так, для суб'єктів господарювання благом може вважатися відсутність жодного впливу держави на їх виробничі та організаційно-управлінські процеси, натомість, для органів публічного управління благом може вважатися контроль над поширенням певних видів інформації). Така ситуація притаманна не лише Україні, а й іншим державам [1].

Заслуговує на увагу думка О.Тихомирова, який вважає інтегруючою основою змісту діяльності по забезпеченню інформаційної безпеки є такі її елементи як об'єкт, предмет, суб'єкт, мета, засоби, методи, принципи, результати. При цьому об'єкти національної та інформаційної безпеки, на його думку, є спільними - особа, суспільство, держава; загальними об'єктами державного забезпечення інформаційної безпеки є інформаційна інфраструктура (держави, суспільства) та свідомість (особи, суспільства) [2, с.191]. Ми підтримуємо думку вченого про можливість виокремлення об'єктів державного забезпечення інформаційної безпеки. Поряд з ними, як нам здається, можна виділити ще об'єкти громадського, муніципального та господарсько-правового забезпечення інформаційної безпеки, кожен з яких буде мати свої особливості.

На підставі здійсненого аналізу можна зробити наступні висновки. Об'єкт забезпечення інформаційної безпеки уявляє собою мету, яку ставить перед собою суб'єкт діяльності у вказаній сфері (держава та її органи, органи місцевого самоврядування, суб'єкти господарювання, громадські організації, політичні партії, професійні спілки, релігійні організації, окремі громадяни тощо). Найменш ефективним з означених суб'єктів є держава, що пояснюється як традиційною для української реальності непослідовністю державної інформаційної політики, так і надмірною динамічністю технічних, технологічних, кадрових, організаційних та інших процесів в інформаційній сфері, що

утруднює їх централізоване регулювання. Отже, об'єкт забезпечення інформаційної безпеки постає як множинність неузгоджених між собою об'єктів різної ґенези та масштабу, сукупність яких породжує міцність протидії інформаційним ризикам, компенсуючи тим самим слабкість держави у досліджуваній сфері суспільних відносин. Звідси слідує, що зменшення руйнівного впливу інформаційних загроз у системі публічного адміністрування має своєю передумовою підвищення вільної конкуренції на ринку ІТ-технологій, зміцнення інститутів громадянського суспільства, забезпечення додержання правових приписів у діяльності партій та релігійних організацій, збільшення транспарентності їх діяльності, активізацію цифрової просвіти для всіх категорій здобувачів освіти, подолання цифрової нерівності. У поєднанні з функціонуванням вузькоспеціалізованих підрозділів із забезпечення інформаційної та кібербезпеки у структурі деяких суб'єктів публічного адміністрування сектору безпеки і оборони це, на нашу думку, здатне значно оптимізувати ситуацію із подолання руйнівного впливу інформаційних загроз.

Список використаних джерел:

1. Khomiakov D., Khrystynchenko N., Shopina I., Zhukov S., Shpenov D. Cybersecurity: Legal and Organizational Support in Leading Countries, NATO and EU Standards. *Journal of Security & Sustainability Issues*. 2020/3/1. Volume 9, Issue 3. P. 977–992.

2. Тихомиров О.О. Забезпечення інформаційної безпеки як функція держави: Дис. …канд.юрид.наук: 12.00.01. Київ, 2011. 234 с.