ОПТИМІЗАЦІЯ ДІЯЛЬНОСТІ НЕДЕРЖАВНИХ СУБ'ЄКТІВ У СИСТЕМІ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

***О. Прудникова**, доктор філософських наук, професор*
Національний юридичний університет імені Ярослава Мудрого
Ondokuz Mayıs University, Samsun, Turkey

Ефективна протидія зовнішнім та внутрішнім загрозам у сфері інформаційної безпеки потребує злагоджених дій як державних, так і недержавних суб'єктів. Події російсько-української війни наочно засвідчили, що недержавні структури набагато гнучкіше та ефективніше реагували на загрози національній безпеці, інформаційної зокрема, у порівнянні з державними інституціями. У зв'язку з цим, проблема взаємодії державного та недержавного секторів у сфері безпеки та оборони України є надактуальною.

На нашу думку, до недержавних суб'єктів інформаційної безпеки можна віднести: громадські організації, громадські рухи, недержавні аналітичні та наукові центри, об'єднання громадян − політичні, економічні, волонтерські, правозахисні, мережеві, культурно-просвітницькі тощо. Аналізуючи перебіг Помаранчевої революції, Революції гідності, російсько-української війни, можна прийти до висновку, що в нашій країні існує нагальна необхідність інституціалізації та оновлення правового статусу діяльності громадського сектору, який став локомотивом суспільних змін й дієвим суб'єктом у сфері національної та інформаційної безпеки (діяльність «кіберармії», громадського центру «Інформаційний спротив», волонтерського інтернет-проекту StopFake тощо).

В. Крутов та Г. Новицький констатують, що аналіз законодавства та практики забезпечення національної безпеки свідчить, що в інституціональній структурі суб'єктів забезпечення національної безпеки повинно бути чітко визначене місце недержавного сектору безпеки. Необхідно усвідомлювати, що забезпечення національної безпеки здійснюється не в державі взагалі, не в абстрактному просторі, а в конкретному місці. Воно безпосередньо пов'язане з безпекою конкретних людей [1, с. 166].

Проектуючи вищенаведені роздуми на проблему забезпечення інформаційної безпеки держави, суспільства та людини необхідно зауважити, що саме у співпраці державних та недержавних суб'єктів створюється потужна синергія дії, яка призводить до значних результатів щодо захисту вітчизняного інформаційно-культурного простору.

Ю. Лісовська доводить, що включення інститутів громадянського суспільства у систему захисту інформаційної безпеки забезпечує вирішення низки важливих завдань. По-перше, забезпечується участь громадськості у прийнятті рішень з питань інформаційної безпеки. По-друге, введення інститутів

громадянського суспільства у механізм політики інформаційної безпеки забезпечує процес залучення громадян у розв'язання проблем інформаційної безпеки, їхню активну позицію з відповідних питань [2, с. 110].

Досліджуючи проблему ефективної участі недержавних суб'єктів у забезпеченні інформаційної безпеки держави, варто звернутись до вітчизняної та закордонної нормативно-правової бази. На думку науковців, звернення до національного законодавства надає підстави виокремлення таких основних форм діяльності недержавних суб'єктів у сфері інформаційної безпеки:

– участь у роботі консультативно-дорадчих органів при органах державного управління в інформаційній сфері;

– участь у публічних громадських обговореннях, що проводяться органами державного управління в інформаційній сфері;

– участь у вивченні громадської думки, що проводяться органами державного управління в інформаційній сфері;

– направлення органам державного управління в інформаційній сфері інформаційних запитів та скарг в ході громадського контролю за їх діяльністю, а також скарг та заяв про інформаційні правопорушення в процесі громадського контролю за дотриманням законності в інформаційній сфері;

– направлення органам державного управління в інформаційній сфері заяв (клопотань) про задоволення прав та законних інтересів у цій сфері [3, с. 34].

З точки зору Л. Сіпайло та Н. Сіпайло, формами взаємодії неурядових і державних організацій щодо забезпечення інформаційної безпеки є:

– проведення загальних прес-конференцій, круглих столів, виступи в ЗМІ;

– подання один одному інформації про надання послуг для координації зусиль;

– проведення спільних акцій, нарад;

– навчання партнерів основам соціальної роботи, обмін досвідом;

– надання послуг, що доповнюють послуги, гарантовані законом;

– проведення спільних (або на замовлення) досліджень проблеми [4, с. 298].

В якості прикладу зауважимо, що досвід демократичних країн засвідчує – ефективними недержавними суб'єктами інформаційної безпеки країни є неурядові аналітичні центри. Роль неурядових аналітичних центрів як генераторів нових ідей та альтернативних підходів є особливо важливою на перехідних етапах, коли відбуваються глибокі внутрішні трансформації у всіх сферах суспільного життя, у сфері інформаційної безпеки зокрема. Неурядові аналітичні центри є також інструментом громадського контролю, вони впливають і на визначення цілей та цінностей суспільства, формують суспільну думку, яка є основним об'єктом інформаційних атак з боку інших держав. Їх потенціал, як посередника та ефективного каналу зв'язку між інтелектуальним середовищем і державними органами та суспільством, важко переоцінити.

Неурядові аналітичні центри − це ефективний інструмент громадського контролю за діями влади. Важлива їхня роль і у визначенні цілей та цінностей суспільства, формуванні громадської думки з актуальних для країни питань. Як правило неурядові аналітичні центри представлені у медіа-просторі країни: їх спеціалісти виступають у ЗМІ, фахівці аналітичних центрів надають коментарі з суспільно важливих питань, попереджають про загрози у сфері інформаційної безпеки.

Демократичні країни демонструють стабільну практику співпраці державних на недержавних суб'єктів інформаційної безпеки, що знайшло своє відображення і на законодавчому рівні. Наприклад, 26 листопада 2003 р. Конгресом США ухвалено закон «Про внутрішню безпеку» (Home Security Act), відповідно до якого створено Міністерство внутрішньої безпеки (Department of Homeland Security), на яке покладено координацію діяльності державних органів і всіх приватних структур з питань забезпечення інформаційної безпеки. Цим законом передбачено розробку Національної стратегії з забезпечення безпеки у кіберпросторі (National Strategy to Secure Cyberspace) та Національної стратегії фізичного захисту об'єктів життєзабезпечення населення (The National Strategy for the Physical Protection of Critical Infrastructures). Зазначеними документами передбачено створення єдиної національної системи протидії кібернетичному тероризму, в рамках якої ініційовано створення територіальних, відомчих і приватних центрів протидії, визначено їхні функції та порядок взаємодії [5, с. 93-94].

Натомість, у лютому 2011 р. уряд Нідерландів ухвалив Національну стратегію кібербезпеки «Сила через співпрацю», якою передбачено створення Національної ради з кібербезпеки. Завданням цього органу є забезпечення реалізації підходу, в основу якого покладено співробітництво державного та приватного секторів, а також різного роду наукових центрів. Передбачено також створення Національного центру з питань кібербезпеки, завданням якого є виявлення тенденцій та загроз інформаційній безпеці, а також сприяння подоланню наслідків інцидентів і кризових ситуацій у цій сфері [6, с. 30-31].

Таким чином, сучасні демократичні країни створюють політико-правові, організаційно-управлінські та соціально-економічні умови для розвитку недержавних суб'єктів інформаційної безпеки, що оптимізує їх всебічну співпрацю з державними безпековими інституціями. У нашій державі продовжується пошук оптимальної моделі взаємодії громадського та державного секторів у сфері безпеки та оборони, у царині інформаційного спротиву зокрема.

Список використаних джерел

1. Крутов В., Новицький Г. Щодо правового статусу структур недержавного сектору національної безпеки України. *Проблеми боротьби зі злочинністю.* 2009. №2 (57). С. 161-168.

2. Лісовська Ю. П. Адміністративно-правова діяльність недержавних органів та організацій як структурних елементів системи забезпечення інформаційної безпеки. *Наукові праці МАУП*. 2014. Вип. 2 (41). С. 108-113.

3. Бурило Ю. П. Участь недержавних суб'єктів у здійсненні державного управління інформаційною сферою. *Правова інформатика*. 2007. № 4. С. 31-41.

4. Сіпайло Л. Г., Сіпайло Н. А. Діяльність неурядових організацій у системі забезпечення інформаційної безпеки країни. *Електронне наукове видання «Глобальні та національні проблеми економіки».* 2017. Випуск 18. С. 296-299.

5. Алямкін Р. В., Федорін М. П. Правове забезпечення національної інформаційної безпеки. *Наукові записки Інституту законодавства Верховної Ради України.* 2013. № 4. С. 91-96.

6. Доповідь Групи урядових експертів з досягнень у сфері інформатизації та телекомунікацій у контексті міжнародної безпеки (A/65/201). Нью-Йорк, Організація Об'єднаних Націй. 2012. 57 с.