

УДК 323.21

Сіпайло Л.Г.

*кандидат економічних наук, доцент кафедри економіки підприємства
Національного університету водного господарства та природокористування*

Сіпайло Н.А.

*аспірант кафедри державного управління,
документознавства та інформаційної діяльності
Національного університету водного господарства та природокористування*

ДІЯЛЬНІСТЬ НЕУРЯДОВИХ ОРГАНІЗАЦІЙ У СИСТЕМІ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ КРАЇНИ

ACTIVITY OF NON-GOVERNMENTAL ORGANIZATIONS IN THE SYSTEM OF PROVIDING INFORMATIONAL SAFETY OF THE COUNTRY

АННОТАЦІЯ

У статті розглянуто досвід розвинутих країн щодо залучення неурядових організацій до вирішення проблем у системі забезпечення інформаційної безпеки країни. Досліджено форми залучення інститутів громадянського суспільства у систему забезпечення інформаційної безпеки. Обґрунтовано форми взаємодії неурядових і державних організацій щодо забезпечення інформаційної безпеки країни.

Ключові слова: неурядові організації, інститути громадянського суспільства інформаційна безпека, національна безпека.

АННОТАЦИЯ

В статье рассмотрен опыт развитых стран по привлечению неправительственных организаций к решению проблем в системе обеспечения информационной безопасности страны. Исследованы формы привлечения институтов гражданского общества в систему обеспечения информационной безопасности. Обосновано формы взаимодействия неправительственных и государственных организаций по обеспечению информационной безопасности страны.

Ключевые слова: неправительственные организации, институты гражданского общества информационная безопасность, национальная безопасность.

ANNOTATION

The article examines the experience of developed countries in involving non-governmental organizations in solving problems in the system of providing information security of the country. The forms of involvement of civil society institutes in the information security system are explored. Grounded forms of cooperation between NGOs and government organizations to ensure information security.

Keywords: non-governmental organizations, civil society institutes, information security, national security.

Постановка проблеми. В умовах глобальних небезпек і загроз національна безпека стає визначальною в теперішніх умовах. Проблема забезпечення національної безпеки держави має важливе значення у контексті загального розвитку країни та реалізації її національних інтересів. Невід'ємним складником національної безпеки є саме інформаційна безпека. Суттєвим для інформаційної безпеки, як і для національної безпеки будь-якої держави, є дотримання балансу інтересів суспільства і держави. Представниками з боку суспільства є саме неурядові організації.

Аналіз останніх досліджень і публікацій. Питанням впливу діяльності неурядових орга-

нізацій у системі забезпечення інформаційної безпеки держави присвячені праці вітчизняних і зарубіжних авторів, таких як І. Арістова, В. Бебик, А. Гальчинський, О. Голобуцький, П. Друкер, Я. Жаліло, О. Зоценко, І. Колідушко, А. Колодюк, Е. Лемберг, Є. Макаренко, Н. Марчук, Г. Почепцов, А. Пшеворський, М. Роуз, Е. Тофлер, Ф. Фукуяма, С. Чукут та інші.

Виділення невирішених раніше частин загальної проблеми. Водночас вплив діяльності неурядових організацій у системі забезпечення інформаційної безпеки України досліджений недостатньо.

Метою статті є дослідження діяльності неурядових організацій у системі забезпечення інформаційної безпеки країни.

Виклад основного матеріалу дослідження. Проблема безпеки на початку ХХІ століття набула універсального змісту, адже, крім військової та політичної сфери, вона поширилася на соціальні, економічні, правові, культурні, екологічні та інформаційні відносини. Інформаційні загрози становлять небезпеку для індивіда, суспільства та держави, тому вся система інформаційної безпеки має бути спрямована на захист життєво важливих інтересів особистості, суспільства та держави. Поєднання зусиль соціально відповідальних громадян, неурядових організацій і держави може служити гарантією безпеки для населення України. У науковій та спеціальній літературі інформаційна безпека розглядається як елемент або підсистема національної безпеки. У Законі України «Про основи національної безпеки України» визначено дев'ять основних напрямів державної політики щодо національної безпеки в різних сферах життєдіяльності. До однієї з них належить інформаційна, що дає усі підстави стверджувати, що інформаційна безпека є вагомим складником національної. Водночас автори цього закону поставили інформаційну сферу життєдіяльності на останнє місце, що свідчить про неусвідомлення значення та ролі інформаційної безпеки в розвитку і подальшому існуванні держави [1, с. 202].

На думку Б.А. Кормич, інформаційний аспект національної безпеки є її невід'ємним компонентом, і так само, як інформаційна безпека не може існувати поза межами загальної національної безпеки, впровадження заходів підвищення національної безпеки не будуть ефективними у разі позбавлення своїх інформаційних векторів [2, с. 9].

Згідно із Законом України «Про національну програму інформатизації» інформаційна безпека – це невід'ємна частина політичної, економічної, оборонної та інших складових частин національної безпеки [3].

Розглядаючи зарубіжний досвід, варто зауважити, що економічно розвинуті країни демонструють співпрацю державних та недержавних суб'єктів інформаційної безпеки, що знайшло своє відображення і на законодавчому рівні. Наприклад, 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 недержавних структур із питань забезпечення інформаційної безпеки. Цим законом передбачено розроблення Національної стратегії із 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). Цими документами передбачено створення єдиної національної системи протидії кібернетичному тероризму, в межах якої ініційовано створення територіальних, відомчих і приватних центрів протидії, визначено їхні функції та порядок взаємодії [4, с. 93-94]. 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 співробітництва державного та приватного секторів, а також різних 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 [4].

В економічно розвинутих країнах неурядові організації в межах законодавчого поля реалізують функції управління процесом прийняття рішень та поточною діяльністю структур сектору інформаційної безпеки за такими напрямками, як:

- політичний – контроль відповідності діяльності посадових осіб держави цілям, принципам та механізмам державної політики забезпечення національної безпеки, визначеним конституцією та чинним законодавством;

- правовий – участь у підготовці законодавчих актів, міжнародних договорів та угод;

- фінансовий – контроль за розподілом бюджетних витрат, рухом та розподілом коштів, поточними та додатковими витратами;

- управлінський – контроль за відповідністю внутрішньої організації державної структури і режиму її функціонування національному законодавству;

- інформаційний – участь у створенні такого потенціалу інформаційної сфери країни, за якого забезпечується її випереджальний розвиток, а зовнішні негативні впливи не створюють реальних небезпек національній інформаційній безпеці держави.

Інформаційна безпека – це стан захищеності життєво важливих інтересів людини, суспільства і держави, за якого запобігається нанесення шкоди через неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації [5].

Значний вплив неурядових організацій на процеси формування та збереження національної безпеки пояснюється вимогами сучасних міжнародних подій та результатами практичної діяльності неурядових організацій, їх високої активності в політичному та соціальному житті країни, високого професійного та наукового потенціалу активістів, глибоких знань соціальних, політичних, економічних проблем сучасної України, досвіду міжнародного спілкування, знайомства зі шляхами вирішення проблем у демократичних країнах світу.

На думку Ю. Лісовської, включення інститутів громадянського суспільства у систему захисту інформаційної безпеки забезпечує вирішення багатьох важливих завдань. По-перше, забезпечується участь громадськості у прийнятті рішень із питань інформаційної безпеки. По-друге, введення інститутів громадянського суспільства у механізм політики інформаційної безпеки забезпечує процес залучення громадян до розв'язання проблем інформаційної безпеки, їхню активну позицію з відповідних питань [6, с. 110].

Основними формами залучення інститутів громадянського суспільства до системи забезпечення інформаційної безпеки України є:

- участь у роботі консультативно-дорадчих органів при органах державного управління у сфері контролю та регулювання інформаційних ресурсів країни;

- участь у публічних громадських обговореннях, що проводяться органами державного управління у сфері інформаційної безпеки;

- вивчення громадської думки та доведення основних кризових явищ у суспільстві до органів державного управління у сфері інформаційної безпеки;

- підготовка інформаційних запитів та скарг про інформаційні правопорушення у процесі громадського контролю за дотриманням закон-

ності впроваджених заходів у сфері забезпечення інформаційної безпеки держави.

Варто зауважити, що 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.

Державні структури, що діють у сфері підтримки інформаційної безпеки, повинні постійно контролювати діяльність не зареєстрованих у державних органах країни неформальних громадських організацій. Оскільки громадські об'єднання можуть стати одним із ключових елементів недержавної системи впливу на національну безпеку України, зокрема на її складову інформаційну безпеку. Діяльність неурядових організацій може бути пов'язана зі створенням і розповсюдженням інформації про політичні та правові заходи з метою ефективної та цілеспрямованої дестабілізації суспільства, держави. Україна має бути країною з розвиненим громадянським суспільством, у якому присутній високий рівень інформованості населення та надійно захищені громадянські і політичні свободи. Проте реалізація цього завдання потребує консолідації зусиль суспільства і держави, а отже, підвищення соціальної ролі особи, реальної участі громадян, їх об'єднань у політиці інформаційного забезпечення національної безпеки.

Забезпечення інформаційної безпеки в країні повинно здійснюватися шляхом:

- формування функціональної інфраструктури інформаційного забезпечення безпеки держави та захисту її критичних елементів;
- зростання рівня координації діяльності державних органів та неурядових організацій щодо виявлення, оцінювання та прогнозування загроз інформаційній безпеці, запобігання таким загрозам та забезпечення ліквідації їх наслідків, здійснення міжнародного співробітництва із цих питань;
- удосконалення законодавчих актів щодо формування системи інформаційної безпеки у сфері забезпечення захищеності інформаційних ресурсів, протидії кіберзлочинності, захисту персональних даних громадян;
- побудова та розвиток Національної системи конфіденційного зв'язку як сучасної захищеної транспортної основи, здатної інтегрувати територіально розподілені інформаційні системи, в яких обробляється конфіденційна інформація.

В Україні політика забезпечення інформаційної безпеки будується на таких засадах:

– у разі необхідності може бути обмежено доступ до інформаційного ресурсу, проте це реалізується тільки відповідно до чинного законодавства;

– суб'єкти інформаційно-консультаційних послуг, які проводять роботу з персональними даними громадян, несуть відповідальність перед законом за збереження і використання таких даних;

– з метою нерозповсюдження недостовірної інформації через ЗМІ державні структури впроваджують заходи захисту суспільства від такої інформації;

– діяльність засобів масової інформації підлягає обов'язковій сертифікації та ліцензуванню з метою контролю за створенням і використанням ними інформаційних повідомлень;

– держава сприяє всебічному розвитку української мови як основного інструменту перетворення накопичених людством знань в інформаційний ресурс України [7].

Варто виокремити низку чинників, що негативно впливають на формування системи інформаційної безпеки країни, таких як:

– недовіра до цілісної системи інформаційно-аналітичної підтримки органів державної влади та управління;

– зниження ефективності використання інтелектуального потенціалу країни, недосконалість наявної системи освіти щодо забезпечення процесів сучасного розвитку держави;

– несформованість керівними колами державних структур зрозумілої і привабливої для суспільства національної ідеї;

– невисокий рівень захисту від експансії іноземними компаніями на ринку інформаційних послуг, у результаті чого відбувається руйнування національного інформаційного простору та виникнення можливості його використання в антидержавних інтересах;

– недієва система контролю за діяльністю окремих політичних сил, ЗМІ та окремих осіб, зусилля яких спрямовані на руйнування моральних цінностей, свідомості, підрив морального і фізичного здоров'я нації;

– зниження рівня довіри з боку населення до влади внаслідок застосування «брудних» політичних технологій, особливо під час виборчих кампаній;

– недобросовісна конкуренція у володінні ЗМІ певними провладними групами;

– маніпулювання громадською думкою (шляхом дезінформації, перекручування фактографічних даних, замовчування правдивих відомостей тощо).

Варто відзначити, що важливим недержавним суб'єктом впливу на інформаційну безпеку 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 в усіх сферах суспільного життя, зокрема

у сфері інформаційної безпеки країни. 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 із боку інших держав. Потенціал таких центрів як посередників та ефективного каналу зв'язку між інтелектуальним середовищем і державними органами та суспільством важко переоцінити. Неурядові аналітичні центри – це важливий інструмент громадського контролю за діями влади. Їхня роль важлива і у визначенні цілей та цінностей суспільства, у формуванні громадської думки з актуальних для країни питань. Як правило, неурядові аналітичні центри існують у медіапросторі країни: їх спеціалісти виступають у ЗМІ, фахівці аналітичних центрів дають коментарі із суспільно важливих питань, попереджають про загрози у сфері національної безпеки, зокрема в інформаційній [8, с. 42].

Висновки. Отже, функціонування системи забезпечення інформаційної безпеки держави за підтримки неурядових організацій може здійснюватися шляхом залучення неурядових організацій до налагодження дієвої інфраструктури інформаційного забезпечення національної безпеки держави; спрямування діяльності неурядових організацій з метою координації діяльності державних органів щодо визначення, попередження та прогнозування явищ у сфері впливу на інформаційну безпеку; сприяння залученню неурядовими організаціями досвіду міжнародного співробітництва у сфері забезпечення інформаційної безпеки; залучення неурядових організацій

до розроблення та обговорення пропозицій щодо зміни нормативно-правової бази у сфері забезпечення інформаційної безпеки держави.

БІБЛІОГРАФІЧНИЙ СПИСОК:

1. Логінов О.В. Сучасні проблеми забезпечення інформаційної безпеки в контексті формування системи державного управління // Науковий вісник Юридичної академії МВС України. – 2003. – № 3. – 224 с.
2. Кормич Б.А. Інформаційна безпека: організаційно-правові основи: Навч. посібник. – К.: Кондор, 2004. – 384 с.
3. Закон України «Про Національну програму інформатизації» [Електронний ресурс] / Верховна Рада України. – Режим доступу: <http://zakon0.rada.gov.ua/laws/show/74/98-%D0%B2%D1%80> – Назва з екрану.
4. Алямкін Р.В. Правове забезпечення національної інформаційної безпеки / Р.В. Алямкін, М.П. Федорін // Наукові записки Інституту законодавства Верховної Ради України. – 2013. – № 4. – С. 91-96.
5. Проект концепції інформаційної безпеки України [Електронний ресурс] / Міністерство інформаційної політики України. – Режим доступу: http://mip.gov.ua/done_img/d/30-project_08_06_15.pdf – Назва з екрану.
6. 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.
7. Марєєв С.В. Інформаційна безпека як складова національної безпеки України / Марєєв С.В., Перевезій С.С., Степова С.В. // [Електронний ресурс]. – Режим доступу: http://www.rusnauka.com/16_ADEN_2010/Informatica/68028.doc.htm
8. Захаренко К. Ефективність використання потенціалу недержавних суб'єктів інформаційної безпеки / К. Захаренко // Нова парадигма. – 2015. – Вип. 127. – С. 40-53.