УДК 341(045):004.056

ІНСТИТУЦІОНАЛЬНИЙ МЕХАНІЗМ СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

INSTITUTIONAL MECHANISMS OF THE INFORMATION SECURITY SYSTEM

Косиця О.О.,
кандидат юридичних наук,
доцент кафедри приватно-правових дисциплін
Університету сучасних знань

У статті здійснено аналіз поглядів на організаційно-функціональну характеристику суб'єктів забезпечення інформаційної безпеки, виділення їх рівнів. Автором досліджено проект Концепції інформаційної безпеки України від 09 червня 2015 року, розроблений Міністерством інформаційної політики України, сформульовано напрями вдосконалення інституціонального механізму сучасної системи інформаційної безпеки.

Ключові слова: система інформаційної безпеки, суб'єкти забезпечення інформаційної безпеки, національна безпека, інформаційна безпека.

В статье осуществлён анализ взглядов на организационно-функциональную характеристику субъектов обеспечения информационной безопасности, выделение их уровней. Автором исследован проект Концепции информационной безопасности Украины от 09 июня 2015 года, разработанный Министерством информационной политики Украины, сформулированы направления совершенствования институционального механизма современной системы информационной безопасности.

Ключевые слова: система информационной безопасности, субъекты обеспечения информационной безопасности, национальная безопасность, информационная безопасность.

The article deals the analysis of the organizational and functional characteristics of the subject of information security, the allocation of their levels. The author studied the draft of the Concept of information security of Ukraine dated June 09, 2015, developed by the Ministry of Information Policy of Ukraine, and formulated the ways of improvement of the institutional mechanism of modern information security .

Key words: information security, information security subjects, security, information security.

Постановка проблеми. Правовому регулюванню та практичному забезпеченню інформаційної безпеки України завжди приділялась належна увага науковців і законодавців. Останні роки стали надзвичайно важкими та вкрай загрозливими для національної безпеки України, саме тому у 2014–2016 рр. було вжито ряд рішучих заходів організаційного і правового характеру державного значення, спрямованих на врегулювання вказаної сфери та досягнення найвищого рівня національної безпеки.

Інформаційна безпека є не лише складовою національної, але й невід'ємною складовою економічної, екологічної, соціальної, оборонної, політичної безпеки. Інформаційна безпека є багатогранним соціальним «явищем», «станом», «видом діяльності», здійснюється на міжнародному, національному та галузевому рівнях, одночасно являючись стратегічно важливою самостійною сферою забезпечення національної безпеки, яка характеризує стан захищеності держави, суспільства та особи в інформаційній сфері від зовнішніх і внутрішніх загроз.

Стан дослідження. Загальні засади та проблемні питання національної безпеки та інформаційної безпеки як її складової досліджувались у працях В.Б. Авер'янова, А.Б. Агапова, О.М. Адрєєвої, І.В. Арістової, О.М. Бандурки, О.А. Баранова, Ю.М. Батуріна, І.Л. Бачило, В.Т. Білоуса, В.М. Брижка, В.П. Горбуліна, В.М. Желіховського, Р.А. Калюжного, В.В. Костицького, В.К. Колпакова, А.Б. Качинського, Ф.М. Медведя, О.Г. Даніляна, О.П. Дзьобаня, М.І. Панова та ін.

Адміністративні, теоретичні та правові основи інформаційної безпеки в державі взагалі та в окремих органах виконавчої влади зокрема були предметом наукових досліджень І.Р. Березовської, Б.А. Кормича, В.А. Ліпкана, Г.М. Линника, О.В. Логінова, Ю.Є. Максименка, О.В. Олійника, В.М. Петрика, Т.В. Субіної, В.М. Супруна, О.О. Тихомирова та ін.

Мета статті – аналіз поглядів на організаційно-функціональну характеристику суб'єктів забезпечення інформаційної безпеки, виділення їх рівнів, формулювання напрямків удосконалення інституціонального механізму сучасної системи інформаційної безпеки.

Виклад основного матеріалу. До основних причин низької ефективності системи забезпечення національної безпеки відносять:

– високу корумпованість і недостатній фаховий рівень керівників державних суб'єктів згаданої системи;

– відсутність суспільного консенсусу з ключових питань державного будівництва, а також належної взаємодії та координації дій між органами виконавчої влади і силовими структурами, в тому числі під час проведення комплексного огляду сектору безпеки та оборони;

– виконання окремими органами державної влади невластивих для них функцій, дублювання їхніх повноважень, розпорошення сил і засобів, відсутність їх консолідації;

– невідповідність правового регулювання дій суб'єктів забезпечення національної безпеки особливостям ситуації в безпековій сфері;

– незадовільні якість і рівень ресурсного забезпечення суб'єктів системи забезпечення національної безпеки [1, с. 36].

Варто звернути увагу на спільну ознаку, властиву перерахованим недолікам. Фактично відповідальність за низький рівень національної безпеки науковці покладають на суб'єктів їх забезпечення, їх корумпованість, незлагодженість дій, відсутність взаємодії та координації, рівень ресурсного забезпечення, дублювання повноважень тощо. Наведені причини та недоліки повною мірою відносяться і до інформаційної безпеки держави.

Складовими сучасної системи безпеки є такі:

– доктрина і правова основа, якими визначаються основні завдання і принципи державної діяльності щодо захисту безпеки;

– інституціональний механізм, тобто сукупність міжнародних і національних державних і громадських органів, які у своїй діяльності вирішують певні завдання щодо підтримання стану безпеки різних рівнів;

– методологічна база, тобто способи, засоби і ресурси, що використовуються для реалізації конкретних завдань у межах політики безпеки [2, с. 119].

М.Б. Левицькою запропоновано власну класифікацію суб'єктів забезпечення національної безпеки: 1) суб'єкти, діяльність яких безпосередньо підпорядкована завданням забезпечення національної безпеки як у комплексі, так і окремим із них (Рада національної безпеки і оборони України, правоохоронні та інші державні виконавчі органи спеціальної компетенції); 2) суб'єкти, для яких така діяльність є одним з основних, але не єдиним напрямом (вищі органи законодавчої, виконавчої та державної влади); 3) суб'єкти, для яких участь у забезпеченні національної безпеки не є основною діяльністю (всі інші державні й громадські організації) [3, с. 66].

Системний характер інформаційної безпеки дозволяє визначити її забезпечення як складний, комплексний вид діяльності, що висуває особливі вимоги до його структурної характеристики. Ґрунтуючись на цьому, забезпечення інформаційної безпеки доцільно розглядати як цілеспрямовану діяльність, провідним, але не єдиним елементом об'єктно-суб'єктного складу якої є держава [4, с. 165].

Аналіз наукових досліджень і законодавчих норм свідчить про плюралізм підходів до суб'єктного складу системи забезпечення інформаційної безпеки. Приділення достатньої уваги вказаному питанню є актуальним з огляду на виклики та загрози, які постають перед державою в умовах реформ усіх сфер діяльності суспільства, обраного євроінтеграційного вектору, гібридної війни тощо.

Суб'єкт забезпечення безпеки – одна з основних категорій, що використовується для розкриття змісту системи забезпечення як національної, так і інформаційної безпеки. Традиційно йому приділяється багато уваги на нормативно-правовому рівні, оскільки саме право в сучасній правовій державі є засобом визначення повноважень суб'єктів державної діяльності та окреслення сфери їх компетенції [5, с. 85].

Так, згідно з нормами Закону України «Про основи національної безпеки» суб'єктами забезпечення національної безпеки є: Президент України; Верховна Рада України; Кабінет Міністрів України; Рада національної безпеки і оборони України; 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; Збройні Сили України, Служба безпеки України, Служба зовнішньої розвідки України, Державна прикордонна служба України та інші військові формування, утворені відповідно до законів України; органи і підрозділи цивільного захисту; громадяни України, об'єднання громадян.

У зв'язку з тим, що правові відносини у сфері державної політики інформаційної безпеки залишаються неврегульованими, в наукових дослідженнях цих проблем переважає тенденція автоматичного надання всім суб'єктам забезпечення національної безпеки повноважень щодо забезпечення й інформаційної безпеки [6, с. 178]. Ми, безумовно, погоджуємось із тим, що надання всім суб'єктам забезпечення національної безпеки повноважень щодо забезпечення та інформаційної безпеки є безпідставним, адже суб'єктам забезпечення інформаційної безпеки відповідають окремі специфічні функції розробки та реалізації політики інформаційної безпеки.

Функція розробки державної політики інформаційної безпеки включає в себе діяльність компетентних органів держави щодо встановлення стратегічних цілей, завдань, основних принципів і напрямків державної діяльності в цій сфері, розробку концепцій та рішень загальнодержавного довгострокового значення. Функція реалізації політики інформаційної безпеки спрямована на досягнення тактичних та оперативних цілей, забезпечує вирішення конкретних завдань, застосування відповідних засобів, форм і методів державного впливу на суспільні відносини в цій сфері [7, с. 157].

Функцію розробки державної політики інформаційної безпеки покладено на Президента України, Верховну Раду України, Раду національної безпеки і оборони, їх дорадчі та консультаційні органи та ін. Проте не варто забувати, що участь у розробці державної політики інформаційної безпеки можуть брати міністерства, органи виконавчої влади, а також громадяни, надаючи свої пропозиції у вигляді конкретних планів, заходів, концепцій, проектів або зауважень до вже існуючих.

В юридичній літературі зустрічається формулювання системи органів державної влади у сфері національної інформаційної безпеки як сукупності взаємовідносин

суб'єктів державного управління (органів державної влади), які проводять державно-управлінську діяльність на основі розмежування компетенції між ними щодо об'єктів державного управління (сфери суспільного життя) з метою гарантування конституційних прав та свобод людини і громадянина, розвитку громадянського суспільства та захищеності інформаційного суверенітету держави [8, с. 29], та яка включає в себе дві складові: систему органів законодавчої влади, що здійснюють функцію нормативно-правового регулювання загальнодержавного керівництва у сфері забезпечення інформаційної безпеки, та систему органів виконавчої влади, які виконують функцію часткового формування в межах наданих повноважень і реалізації державної політики інформаційної безпеки в сучасних умовах [9, с. 152].

Під системою забезпечення інформаційної безпеки також розуміють організовану державою сукупність суб'єктів: державних органів і органів місцевого самоврядування, підприємств, установ і організацій незалежно від форм власності, громадських об'єднань, їх посадових осіб та громадян, що здійснюють діяльність, спрямовану на вирішення завдань реалізації державної політики інформаційної безпеки відповідно до їх адміністративно-правового статусу, визначеного законодавством [6, с. 350].

Так, наприклад, сучасний підхід до класифікації суб'єктів забезпечення інформаційної безпеки запропоновано в проекті Концепції інформаційної безпеки України від 09 червня 2015 року, розробленої Міністерством інформаційної політики України [10]. У Концепції суб'єктів розподілено на суб'єктів забезпечення та суб'єктів реалізації державної політики у сфері інформаційної безпеки.

Суб'єктами забезпечення інформаційної безпеки Концепція визначає:

1) громадян України, об'єднання громадян, громадські організації та інші інститути громадянського суспільства;

2) Президента України, Верховну Раду України, Кабінет Міністрів України, інші центральні органи виконавчої влади та органи сектору безпеки і оборони України;

3) засоби масової інформації та комунікації різних форм власності, підприємства, заклади, установи та організації різних форм власності, що здійснюють інформаційну діяльність;

4) наукові установи, освітні та навчальні заклади України, які, зокрема, здійснюють наукові дослідження та підготовку фахівців за різними напрямами інформаційної діяльності в галузі інформаційної безпеки.

Ураховуючи перспективу формування єдиного міжнародно-правового режиму інформаційної безпеки, доцільно розширити вказаний перелік і додати міжнародні міжурядові та міжнародні неурядові організації до суб'єктів забезпечення інформаційної безпеки. Безсумнівним є те, що вдосконалення національної нормативної бази з інформаційної безпеки неможливе без урахування положень конвенцій, директив, рекомендацій та резолюцій міжнародних організацій, які відіграють важливу роль у вдосконаленні національної правової доктрини та безпосередньо у формуванні системи забезпечення інформаційної безпеки як державного, так і світового масштабу.

Додатковим аргументом на користь вказаного твердження є науковий підхід О.О. Тихомирова, який справедливо відмітив, що значну частину концептуальних положень національних законодавств провідних країн світу у сфері безпеки, зокрема інформаційної, визначають домовленості, закріплені відповідними міжнародними актами, які є результатом діяльності міжнародних організацій, та серед суб'єктів забезпечення інформаційної безпеки узагальнено виділяє три групи: міжнародні організації; державу в особі державних організацій; недержавні організації, громадяни та їх об'єднання [4, с. 86]. Надана класифікація ґрунтується на положеннях нормативного акту, який на сьогодні вже втратив чинність, але заслуговує на ретельний аналіз з метою запозичення позитивних та ефективних елементів тогочасної моделі Доктрини інформаційної безпеки (Про Доктрину інформаційної безпеки України: Указ Президента України від 08 липня 2009 р. № 514/2009, втратив чинність на підставі Указу Президента України № 504/2014), яким передбачались такі рівні забезпечення інформаційної безпеки:

– міжнародне забезпечення (міжнародне співробітництво в галузі забезпечення інформаційної безпеки, гарантування інформаційного суверенітету держави, сприяння задоволенню інформаційних потреб громадян за кордоном);

– державне забезпечення (діяльність державних організацій, спрямована на забезпечення інформаційної безпеки);

– недержавне забезпечення (діяльність громадських і недержавних комерційних організацій та окремих громадян (або інститутів громадянського суспільства), спрямована на сприяння державному забезпеченню інформаційної безпеки).

Крім того, у проекті Концепції конкретизовано суб'єктів реалізації державної політики у сфері інформаційної безпеки: Служба безпеки України; Міністерство внутрішніх справ України; Міністерство оборони України; Служба зовнішньої розвідки України; Центральний орган виконавчої влади із спеціальним статусом, який забезпечує формування та реалізує державну політику у сферах організації спеціального зв'язку, захисту інформації, телекомунікацій і користування радіочастотним ресурсом України.

Слід зазначити, що ні проектом Концепції, ні чинним законодавством коло обов'язків і повноважень суб'єктів із питань забезпечення інформаційної безпеки не визначено. Тим не менш, варто звернути увагу на позитивні та стратегічно важливі норми, передбачені вказаним документом. Так, на концептуальному рівні здійснюється спроба закріпити поняття інформаційної безпеки, національного інформаційного простору, визначено основи державної політики у сфері інформаційної безпеки, здійснення громадського контролю та державно-громадське партнерство у сфері реалізації державної інформаційної політики та забезпечення інформаційної безпеки.

О.В. Олійником у своєму монографічному дослідженні запропоновано наступні рівні організаційно-функціональної системи забезпечення інформаційної безпеки.

І рівень – стратегічний, загальнодержавний, який включає Верховну Раду України, Президента України, Кабінет Міністрів України, та полягає у прийнятті політичних рішень, законодавчого і нормативно-правового забезпечення, встановлення порядку міжнародного співробітництва та ін.

ІІ рівень – організаційно-виконавчий, відомчо-територіальний, який включає центральні органи виконавчої влади, органи місцевого самоврядування, правоохоронні органи та органи судової влади. На вказаному рівні здійснюється організаційне і методичне забезпечення інформаційної безпеки у відповідних галузях та адміністративно-правових утвореннях, координація і контроль діяльності у сферах відповідальності державно-владних структур.

ІІІ рівень – критично важливі інфраструктури країни, до яких доцільне включення підприємств, установ, організацій, комунікацій національного інформаційного простору та інших об'єктів, управління якими здійснюється з використанням електронно-комунікаційних засобів та інформаційних технологій.

ІV рівень – рівень суб'єктів невладного характеру, до яких відносяться громадяни України, їх об'єднання, державні і приватні засоби масової інформації [6, с. 219–220].

Перш за все, слід розуміти, що визначення суб'єктів не може бути виключно декларативним, лише законодавчо

закріплений перелік не дасть змоги ефективно виконувати завдання із забезпечення безпеки та протистояти загрозам. Інформаційну безпеку різною мірою забезпечують всі без винятку органи влади (законодавчої, виконавчої та судової), громадяни та їх об'єднання, адже, як визначено в Конституції України, «..захист суверенітету і територіальної цілісності України, забезпечення її економічної та інформаційної безпеки є найважливішими функціями держави, справою всього Українського народу».

Для досягнення мети все ж є необхідність розподілу ролей та функцій кожного суб'єкта, а також виокремлення спеціального органу (органів), який координує, перевіряє, контролює та акумулює результати з метою усунення недоліків системи і зміцнення стану захищеності національних інтересів держави й суспільства в інформаційній сфері. Під час аналізу інституціонального механізму першочерговим є визначення керівного органу або органів у цій ієрархії. Враховуючи неврегульованість у національному законодавстві питань інформаційної безпеки, такі керівні функції мають бути законодавчо покладені на Президента України, Верховну Раду та Раду національної безпеки і оборони.

Для вирішення завдань забезпечення інформаційної безпеки України суб'єкти забезпечення інформаційної безпеки повинні ефективно взаємодіяти безпосередньо на організаційному та технічному рівні в установленому порядку з іншими державними органами, органами місцевого самоврядування, об'єднаннями громадян, установами і підприємствами, громадянами, міжнародними організаціями.

Висновки. Отже, аналіз інституціонального механізму системи забезпечення інформаційної безпеки в сучасних умовах свідчить, що його ефективне функціонування можливе за наступних умов: розробка та прийняття Концепції інформаційної безпеки; оновлення законодавства, а саме внесення змін до законів і положень, які регламентують діяльність суб'єктів забезпечення інформаційної безпеки, взаємоузгодження завдань і функцій із забезпечення інформаційної безпеки; встановлення механізму керівництва, контролю та нагляду у сфері забезпечення інформаційної безпеки з чітким розподілом ролей і повноважень; введення інституту відповідальності за неналежний рівень організації дотримання вимог внутрішньої інформаційної безпеки; запровадження системи загальної підготовки суб'єктів забезпечення інформаційної безпеки до виконання покладених на них завдань; активація взаємодії та інформаційного обміну між суб'єктами забезпечення інформаційної безпеки як ефективного інструменту вирішення покладених на них завдань. Дотримання вказаних умов сприятиме впровадженню та реалізації дієвої політики інформаційної безпеки як основоположної складової всіх елементів національної безпеки.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Резнікова О.О. Концептуальні засади розвитку системи забезпечення національної безпеки України : аналіт. доп. / О.О. Резнікова, В.Ю. Цюкало, В.О. Паливода, С.В. Дрьомов, С.В. Сьомін. – К. : НІСД, 2015. – 58 с.

2. Кормич Б.А. Інформаційне право / Б.А. Кормич. – Харків : БУРУН і К, 2011. – 334 с.

3. Левицька М.Б. Теоретико-правові аспекти забезпечення національної безпеки органами внутрішніх справ України : дис. … канд. юрид. наук : 12.00.01 / М.Б. Левицька. − К., 2002. − 206 с.

4. Тихомиров О.О. Класифікації забезпечення інформаційної безпеки / О.О. Тихомиров // Вісн. Запоріз. нац. ун-ту. – 2011. – № 1. – С. 164 –168.

5. Тихомиров О.О. Забезпечення інформаційної безпеки як функція сучасної держави / О.О. Тихомиров ; заг. ред. Р.А. Калюжний. − Центр навч.-наук. та наук.-практ. вид. НА СБ України, 2014. – 196 с.

6. Олійник О.В. Теоретико-методологічні засади адміністративно-правового забезпечення інформаційної безпеки України / О.В. Олійник. – К. : Укр. Пріоритет, 2012. – 400 с.

7. Кормич Б.А. Організаційно-правові основи політики інформаційної безпеки України : дис. … доктора юрид. наук : спец. 12.00.07 / Б.А. Кормич. – Одеса, 2004. – 427 с.

8. Гурковський В. Взаємовідносини органів державної влади у сфері забезпечення інформаційної безпеки України: організаційно-правові питання / В. Гурковський // Вісн. УАДУ : наук. журн. – 2002. – № 3. – С. 27–31.

9. Березовська І.Р. Суб'єкти у сфері забезпечення інформаційної безпеки в Україні / І.Р. Березовська // Наук. записки Львів. ун-ту бізнесу та права. – 2013. – Вип. 10. – С. 148–153.

10. Офіційний сайт Міністерства інформаційної політики України [Електронний ресурс]. – Режим доступу : http://mip.gov.ua/ru/documents/30.html.