ГЛАВА 8. АКТУАЛЬНІ ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ЯК ФУНКЦІЇ СУЧАСНОЇ ДЕРЖАВИ

Вступ

Сьогодні інформаційна сфера стала інтегруючою основою життєдіяльності суспільства, а забезпечення інформаційної безпеки визнається однією з концептуальних засад його подальшого розвитку. За таких умов особливого значення набуває формування виваженої державної інформаційної політики на основі системних наукових досліджень явищ інформаційної сфери, провідне місце серед яких займає інформаційна безпека [1–17].

Одним із важливих етапів системного дослідження інформаційної безпеки є аналіз загальної структури її забезпечення із застосуванням різних методологічних підходів, зокрема системного, функціонального, діяльнісного та класифікаційного. Виокремлення й деталізація складових забезпечення інформаційної безпеки за різними ознаками на основі цих методів сприятиме усвідомленню особливостей кожної з них і, відповідно, формуванню комплексу адекватних заходів державного та недержавного характеру, спрямованих на підтримання оптимального інформаційного розвитку й інтеграції до світового інформаційного простору.

Інформаційна безпека протягом двох останніх десятиліть є об’єктом актуальних наукових досліджень у різних сферах знань. Висвітлення загальнотеоретичних й окремих аспектів забезпечення інформаційної безпеки на монографічному та дисертаційному рівні здійснило багато вітчизняних і зарубіжних дослідників. Проте особливості загальної структури забезпечення інформаційної безпеки залишаються недостатньо розкритими, що гальмує процеси усвідомлення системності інформаційної безпеки та негативно позначається на формуванні державної інформаційної політики.

8.1. Правові засади забезпечення інформаційної безпеки

Статтею 17 Конституції України забезпечення інформаційної безпеки, поряд із захистом суверенітету і територіальної цілісності, визнається однією з найважливіших функцій держави і справою всього Українського народу. Виходячи з цього, забезпечення інформаційної безпеки доцільно розглядати як цілеспрямовану діяльність, домінуючим, але не єдиним елементом об’єктно-суб’єктного складу якої є держава. Така інтерпретація враховує синергетичні тенденції розвитку сучасного суспільства та субсидіарні особливості його взаємодії з державою й повною мірою відповідає положенням теорії держави і

права, згідно з якими функції держави розуміються як напрями, сторони або види державної діяльності.

З метою окреслення особливостей поняття «забезпечення інформаційної безпеки», пов'язаних зі значенням лексеми «забезпечення» і застосуванням діяльнісного підходу, доцільно акцентувати ось на чому.

Тлумачні словники, здебільшого, наводять подвійне семантичне значення слова «забезпечення»:

1) надання, створення засобів та умов, гарантування, захист;

2) засоби або система засобів [2, с. 375].

Названі аспекти, хоча й відповідають його загальноприйнятому тлумаченню, але, з точки зору теорії діяльності, не є рівнозначними. Засоби діяльності обов'язково виявляються у змістових елементах, що становлять незмінну основу самої діяльності [3, с. 89]. Залежно від широти розгляду конкретного виду діяльності засоби можуть як виступати самостійним елементом її змісту, так і знаходити свій вираз в інших елементах – меті, завданнях та результатах діяльності. Зокрема, організаційну діяльність держави узагальнено можна представити у двох стадіях: перша – створення необхідних засобів та надання їх відповідним суб'єктам, друга – використання засобів суб'єктами у своїй діяльності для вирішення поставлених завдань. У цьому аспекті засоби як такі є завданнями й результатом діяльності, спрямованої на досягнення мети вищого порядку, і перебувають у змістовій єдності із самою діяльністю.

Щодо поняття «забезпечення»: «Забезпечення є сукупністю діяльності із забезпечення, засобів забезпечення та суб'єктів забезпечення. Діяльність із забезпечення полягає в наданні допомоги суб'єктам у досягненні поставлених цілей. Засоби забезпечення утворюють сукупність матеріальних, духовних, фінансових, правових, організаційних і технічних засобів, необхідних для діяльності із забезпечення. Суб'єктами забезпечення є індивіди, організації та органи держави, що здійснюють діяльність із забезпечення» [4].

Отже, діяльнісний підхід, не створюючи термінологічної дисгармонії, нерозривно поєднує обидва аспекти «забезпечення», під чим слід розуміти відповідну діяльність у всій повноті змістових та структурних елементів.

Системність інформаційної безпеки дозволяє визначити її забезпечення як складний, комплексний вид діяльності, що зумовлює її надзвичайну структурну розгалуженість. Сьогодні загальноприйнятого механізму структуризації забезпечення інформаційної безпеки немає. Для виокремлення складових його загальної структури найчастіше використовуються такі термінологічні

конструкції, як «напрями», «механізми» та «шляхи» забезпечення. Однак саме розуміння забезпечення інформаційної безпеки як комплексного виду діяльності дозволяє гармонізувати термінологію і здійснювати не лише структурний, а й глибокий змістовий аналіз, повною мірою застосовуючи потенціал діяльнісного підходу.

Результати аналізу різноманітних джерел свідчать про недостатню розробленість та систематизованість структурних складових забезпечення інформаційної безпеки. На рівні законодавства практично безальтернативним залишається підхід, у межах якого залежно від пріоритетних загроз визначаються напрями забезпечення інформаційної безпеки, об'єднані за традиційними сферами життєдіяльності. Доктрина інформаційної безпеки України, а також фундаментальні нормативно-правові акти у сфері забезпечення національної безпеки використовують саме такий підхід.

У науковій сфері пріоритет надається класифікації загроз як чинників, що зумовлюють основні напрями або шляхи забезпечення інформаційної безпеки. Водночас не менше пізнавальне значення має класифікаційна характеристика самого забезпечення інформаційної безпеки, здійснена на підставі не лише предмета діяльності (загрози), а й інших критеріїв, що дозволить отримати більш повне уявлення щодо його особливостей.

Осмислення забезпечення інформаційної безпеки як функції держави логічно інтегрує окремі компоненти методології дослідження цих явищ. Тому класифікацію забезпечення інформаційної безпеки доцільно здійснити на основі моделі, використаної для класифікації функцій держави в цій роботі. Кожен обраний критерій такої класифікації розглядається не як підстава диференціації, а як ознака, що задає площину розгляду забезпечення інформаційної безпеки. Застосування цього прийому дозволяє створити теоретичну модель забезпечення інформаційної безпеки, не порушуючи системних взаємозв'язків його складових.

Емпіричною базою класифікації забезпечення інформаційної безпеки саме як функції сучасної правової держави, тобто офіційно визнаної діяльності (регламентованої правовими актами), можуть слугувати положення актів законодавства України, що згідно із Законом України «Про основи національної безпеки України» (ст. 2) становлять правову основу забезпечення інформаційної безпеки, а також актів законодавства інших країн.

Серед таких актів, зокрема, закони України «Про Основні засади розвитку інформаційного суспільства в Україні на 2007−2015 роки», «Про Концепцію Національної програми інформатизації», «Про Національну програму

інформатизації», «Про інформацію», «Про державну таємницю», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про доступ до публічної інформації»; проекти законів України «Про Концепцію національної інформаційної політики», «Про Концепцію державної інформаційної політики»; укази Президента України «Про Доктрину інформаційної безпеки України», «Про Стратегію національної безпеки України»; закони.

8.2. Класифікаційна характеристика забезпечення інформаційної безпеки

Зважаючи на окреслені вище методологічні особливості, класифікувати забезпечення інформаційної безпеки можна так.

1. За сферами суспільного (державного) життя:

− забезпечення інформаційної безпеки в економічній сфері;

− забезпечення інформаційної безпеки в політичній сфері; − забезпечення інформаційної безпеки у воєнній сфері;

− забезпечення інформаційної безпеки в науковотехнологічній сфері;

− забезпечення інформаційної безпеки в екологічній сфері;

− забезпечення інформаційної безпеки в соціальній сфері тощо.

Підтвердженням важливості такого розподілу є зосередження на ньому уваги в численних наукових дослідженнях і багатьох нормативно-правових актах доктринального-концептуального рівня, які стосуються інформаційної та національної безпеки. Зокрема українським законодавством інформаційна безпека визначається як невід'ємна складова кожної зі сфер національної безпеки, що закріплено Законом України «Про Концепцію Національної програми інформатизації» та Доктриною інформаційної безпеки України [5; 6].

2. За об'єктами національної безпеки:

− забезпечення інформаційної безпеки особи;

− забезпечення інформаційної безпеки суспільства;

− забезпечення інформаційної безпеки держави [5; 7].

У контексті сприйняття інформаційної безпеки як невід'ємної складової кожної зі сфер національної безпеки проглядається виключна єдність загальних об'єктів національної та інформаційної безпеки. Так, Законом України «Про основи національної безпеки» об'єктами національної безпеки визначено людину й громадянина, суспільство, державу. Доктрина інформаційної безпеки України деталізує особливості цих об'єктів щодо забезпечення інформаційної безпеки, використовуючи поняття життєво важливих інтересів в інформаційній сфері, а саме:

1) особи − забезпечення конституційних прав і свобод людини на збирання, зберігання, використання та поширення інформації; недопущення несанкціонованого втручання в зміст, процеси оброблення, передачі та використання персональних

даних; захищеність від негативного інформаційнопсихологічного впливу;

2) суспільства − збереження і примноження духовних, культурних та моральних цінностей Українського народу; забезпечення суспільно-політичної стабільності, міжетнічної та міжконфесійної злагоди; формування і розвиток демократичних інститутів громадянського суспільства;

3) держави − недопущення інформаційної залежності, інформаційної блокади України, інформаційної експансії інших держав та міжнародних структур; ефективна взаємодія органів державної влади та інститутів громадянського суспільства при формуванні, реалізації й коригуванні державної політики в інформаційній сфері; побудова та розвиток інформаційного суспільства; забезпечення економічного й науково-технологічного розвитку України; формування позитивного іміджу України; інтеграція України у світовий інформаційний простір [5].

3. За сучасними аспектами розуміння інформаційної безпеки:

− забезпечення інформаційно-психологічної безпеки;

− забезпечення інформаційної безпеки у сфері прав і свобод людини;

− забезпечення інформаційно-технічної (технологічної) безпеки.

Незважаючи на умовність, цей контекст розгляду набуває дедалі більшої популярності в роботах українських дослідників, причому особливу увагу останнім часом привертає виокремлення інформаційної безпеки у сфері прав і свобод людини, а також кібернетичної безпеки, яку певною мірою можна вважати складовою інформаційно-технічної (технологічної) безпеки.

Забезпечення інформаційно-психологічної безпеки полягає в мінімізації негативних впливів на свідомість людини (як громадян, так і державних посадових осіб) та суспільства, пов’язаних передусім із маніпулюванням свідомістю з різною метою, зокрема терористичною, і поширенням суспільно небезпечної ідеології (культу насильства та жорстокості, расизму, радикального націоналізму, порнографії тощо).

Основним змістом забезпечення інформаційної безпеки у сфері прав і свобод людини є недопущення розголошення інформації з обмеженим доступом, порушень права власності на інформацію, неправомірного обмеження свободи слова та доступу громадян до публічної інформації й інших прав і свобод, які належать до інформаційної сфери або реалізуються в ній.

До забезпечення інформаційно-технічної (технологічної) безпеки належить створення можливостей для безпечного формування й розвитку інформаційних ресурсів та інформаційної інфраструктури, своєчасного виявлення загроз безпеці держави, суспільства, особи в інформаційній сфері та організація ефективної протидії їм за допомогою технічних засобів.

4. *За основними видами інформаційної діяльності:*

− забезпечення законних можливостей створення, збирання, одержання та використання інформації;

− забезпечення законного порядку поширення інформації;

− забезпечення належного зберігання інформації;

− охорона та захист інформації;

− створення і розвиток інформаційних ресурсів.

Основні види інформаційної діяльності були безпосередньо визначені та розкриті попередніми редакціями Закону України «Про інформацію», а державна діяльність, що відповідає цим видам, згідно зі ст. 3 чинної редакції цього закону становить основу державної інформаційної політики України [8]. Відносини у сфері охорони та захисту інформації, забезпечення належного режиму доступу до інформації, що охороняється законом (державної таємниці, конфіденційної, службової інформації тощо), в Україні вже тривалий час є предметом правового регулювання. При цьому питання використання й отримання відкритої соціально необхідної інформації до недавнього часу залишалися поза увагою законодавця.

Ситуація почала поступово змінюватись із затвердженням у 2009 році Доктрини інформаційної безпеки України, якою серед основних засад визначено: свободу збирання, зберігання, використання та поширення інформації; достовірність, повноту й неупередженість інформації; обмеження доступу до інформації виключно на підставі закону. Крім того, з метою створення механізмів реалізації права кожного на доступ до публічної інформації у 2011 році прийнято Закон України «Про доступ до публічної інформації» і внесено зміни до Закону України «Про інформацію» та деяких інших нормативно-правових актів.

5. *За формами державного забезпечення інформаційної безпеки:*

− забезпечення якісного інформування;

− забезпечення процесів інформатизації;

− правова регламентація сфери інформаційних відносин;

− боротьба з правопорушеннями в інформаційній сфері.

Зміст державного забезпечення інформаційної безпеки може

інтерпретуватися як система державних гарантій в інформаційній сфері, прямо чи опосередковано визначених фундаментальними нормативно-правовими актами, що регламентують інформаційну сферу суспільних відносин.

Інформування, тобто надання суб'єктам необхідної для функціонування й життєдіяльності якісної інформації, є однією із засад розвитку інформаційного і громадянського суспільства. Оскільки інформація виступає засобом осягнення простору існування суб'єктів, то належний рівень їх поінформованості про процеси, що відбуваються в державі та світі, є необхідним підґрунтям для прийняття адекватних рішень. Особливо гостро проблеми інформування виявляються в напрямах: якісного інформаційного забезпечення діяльності державних органів і посадових осіб; ефективного поширення правової інформації як організаційної основи у важливих сферах суспільних відносин, зокрема у сфері забезпечення інформаційної безпеки; надання своєчасної, повної, неупередженої інформації суспільству щодо діяльності державних органів; об'єктивного та оперативного висвітлення подій як державного, так і світового масштабу.

Інформатизація як цілеспрямована діяльність держави полягає в створенні політичних, економічних, технічних та інших умов для інформаційного розвитку суб'єктів, розвитку державного інформаційного ресурсу та оптимізації обміну інформацією шляхом широкого використання інформаційних технологій.

До пріоритетних загальнодержавних проектів інформатизації в Україні згідно з Концепцією Національної програми інформатизації належать: створення національної інформаційнотелекомунікаційної системи; розвиток системи національних інформаційних ресурсів; інформатизація стратегічних напрямів розвитку економіки держави, її безпеки та оборони, соціальної сфери [6]. Відповідно, відставання від провідних країн світу за рівнем інформатизації органів державної влади та місцевого самоврядування, кредитно-фінансової сфери, промисловості, сільського господарства, освіти, охорони здоров'я, сфери послуг і побуту тощо є джерелом загроз інформаційній безпеці.

Правова регламентація сфери інформаційних відносин і боротьба з правопорушеннями в ній є взаємодоповнюючими складовими процесу необхідного унормування «інформаційної» поведінки суб'єктів. Їх правові проблеми мають спільне коріння і зумовлюють розвиток інформаційних правовідносин. Розглядаючи ці питання в контексті розбудови України як правової держави та становлення її правової системи, доцільно звернути увагу на потенційні можливості кодифікації інформаційного законодавства України,

яка може забезпечити одночасне вирішення таких важливих завдань: гармонізація вітчизняного інформаційного законодавства з вимогами міжнародних актів, подолання прогалин щодо реалізації права на інформацію, удосконалення й розвиток інституту юридичної відповідальності за правопорушення в інформаційній сфері тощо.

6. За напрямами пізнавального процесу в галузі забезпечення інформаційної безпеки:

− професійна освіта;

− наукові дослідження;

− інформаційно-просвітницька діяльність.

Комплексність підходів до осягнення інформаційної безпеки зумовлює виділення особливої діяльності, що закладає інтелектуальні підвалини успішного національного інформаційного розвитку. Основними формами такої діяльності є професійна освіта та організація наукових досліджень у сфері інформаційної діяльності, що були безпосередньо визначені ст. 15, 16 однієї з попередніх редакцій Закону України «Про інформацію» (згідно з його останніми змінами і доповненнями від 02.12.2010) [8].

Високому рівню інформаційно-правової культури і професійної підготовки фахівців із забезпечення інформаційної безпеки відводиться одне з фундаментальних місць у системі гарантій інформаційної безпеки. В умовах реформування системи вищої освіти в Україні організація такої підготовки є складним завданням, виконанню якого сприятиме створення консолідованими зусиллями системи цільової підготовки й перепідготовки фахівців у різних галузях забезпечення інформаційної безпеки.

Зокрема до результатів такої діяльності належить створення напряму підготовки фахівців із вищою освітою − «Управління інформаційною безпекою» [9], яка здійснюється деякими провідними вищими навчальними закладами України. Прикладом міжнародної співпраці щодо перепідготовки фахівців є Концепція підготовки суддів і прокурорів із питань кіберзлочинності, розроблена Радою Європи в межах Проекту «Кіберзлочинність» та Лісабонською мережею Ради Європи з підготовки суддів протягом 2009 року [10].

Важливість усебічних наукових досліджень у нових сферах життєдіяльності держави і суспільства не викликає сумнівів. На сучасному етапі входження інформаційних відносин до сфери правового регулювання особливої актуальності набувають правові дослідження, гармонійним предметом яких є інформаційна безпека. З цього приводу слушна думка А. І.

Марущака, який наголошує на доречності застосування класичних напрямів досліджень юридичної науки стосовно проблем, пов'язаних з інформаційною безпекою, а саме:

− науково-теоретичне обґрунтування доцільності правового регулювання суспільних відносин, що виникають із приводу інформаційної безпеки особи, суспільства, держави;

− визначення основних понять та категорій, які застосовуватимуться для унормування відповідних суспільних процесів;

− наукові розробки щодо повноважень суб'єктів суспільних інформаційно-безпекових відносин, форм і методів їх реалізації;

− дослідження питань юридичної відповідальності за правопорушення у сфері інформаційної безпеки [11, с. 37].

Інформаційно-просвітницька діяльність є втіленням такого засобу реалізації державної влади, як переконання, і загалом полягає в підвищенні рівня всіх складових інформаційної культури суспільства, особливо інформаційно-правової. Крім того, важливою складовою цієї діяльності є надання суспільству об'єктивної та всебічної інформації щодо чинників, які зумовлюють основні напрями державної політики, з метою формування консолідованої суспільної думки стосовно них. Так, серед напрямів державної політики у сфері інформаційної безпеки України окремо виділяється посилення інформаційнопросвітницької діяльності серед населення щодо забезпечення національної безпеки України в разі повноправного її партнерства з державами-членами ЄС та НАТО [5].

7. *Залежно від елементів змісту діяльності із забезпечення інформаційної безпеки:*

1) за об'єктами забезпечення інформаційної безпеки:

− розвиток і вдосконалення інформаційно-телекомунікаційної інфраструктури, недопущення доведення її до критичного рівня (захист критичної інформаційно-телекомунікаційної інфраструктури);

− забезпечення законного та ефективного використання національних інформаційних ресурсів (захист національних інформаційних ресурсів від несанкціонованого втручання, інноваційне їх оновлення, впровадження новітніх технологій створення, оброблення та поширення інформації, формування відкритих державних інформаційних ресурсів і забезпечення доступу до них громадян);

− захист інформації (забезпечення якісних характеристик інформації − конфіденційності, цілісності та доступності тощо);

− захист свідомості суб'єктів (особи, групи осіб, суспільства) від деструктивного інформаційного впливу (створення сприятливого психологічного клімату в національному інформаційному просторі задля утвердження загальнолюдських та національних моральних цінностей) [12; 5];

2) за суб'єктами 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) [5];

3) за характером предмета діяльності із забезпечення інформаційної безпеки:

− протидія негативним інформаційним процесам і явищам

(загрозам, небезпекам);

− сприяння посиленню позитивних інформаційних процесів (процесів розвитку суспільства);

− сприяння трансформації нейтральних інформаційних процесів у позитивні;

4) за складовими механізму протидії загрозам інформаційній безпеці:

− моніторинг інформаційної сфери (аналіз факторів впливу на інформаційну сферу, виявлення серед них загроз інформаційній безпеці);

− ранжування загроз (установлення пріоритетності напрямів державної діяльності з протидії загрозам інформаційній безпеці);

− профілактика і попередження негативного впливу загроз;

− нейтралізація загроз;

5) за характером здійснення державного впливу:

− безпосереднє створення необхідних умов життєдіяльності суб'єктів в інформаційній сфері;

− опосередкований вплив шляхом підвищення інформаційного потенціалу суб'єктів і сприяння їх самоорганізації;

6) за засобами забезпечення інформаційної безпеки:

− правове забезпечення (правова регламентація відносин в інформаційній

сфері; контрольно-наглядова діяльність, зокрема шляхом нагляду за дотриманням законності в інформаційній сфері, а також ліцензування, сертифікації, експертизи та ін.);

− техніко-технологічне забезпечення (інженерно-технічне, матеріально-технічне, програмно-апаратне, криптографічне забезпечення тощо).

8. *Залежно від особливостей забезпечення доступу до інформації*:

1) за правовим режимом доступу до інформації:

− забезпечення режиму доступу до інформації з обмеженим доступом;

− забезпечення оптимального обміну відкритою інформацією;

− забезпечення належного розповсюдження публічної інформації;

2) за заходами із захисту секретної інформації:

− інженерно-технічне забезпечення;

− організаційно-правове забезпечення;

− оперативно-розшукове забезпечення; - криптографічне забезпечення [13; 14].

Висновки

Звичайно, наведена структуризація діяльності із забезпечення інформаційної безпеки не є вичерпною [15 – 17]. Міждисциплінарний характер інформаційної безпеки, що охоплює технічні (технологічні), правові, психологічні аспекти, зумовлює надзвичайну складність і багаторівневість системних зв’язків складових забезпечення інформаційної безпеки. Усвідомлення особливостей кожної з них сприятиме процесам осягнення комплексності забезпечення інформаційної безпеки, визначенню тактичних і стратегічних напрямів діяльності у сфері забезпечення інформаційної безпеки, гармонізації національного інформаційного законодавства, що в сукупності створює важливі засади ефективної державної інформаційної політики.