УДК: 34.096+321.01

Тихомиров Олександр Олександрович

ДІЯЛЬНІСНИЙ ПІДХІД У ДОСЛІДЖЕННЯХ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ: ОБ'ЄКТИ І СУБ'ЄКТИ

Постановка проблеми. Своєрідні властивості інформаційної безпеки, особливості її окремих складових, проблеми і шляхи забезпечення дедалі частіше стають актуальним напрямами досліджень у межах різноманітних соціально-гуманітарних і технічних наук, зокрема правових, політологічних, психологічних, соціологічних, економічних, у сфері державного управління й управління персоналом, забезпечення національної та державної безпеки тощо.

Очевидно, що широта наукової сфери, об'єктом якої є інформаційна безпека зумовлює надзвичайну розгалуженість її методології. Часто автори досліджень певних аспектів забезпечення інформаційної безпеки спираються на вузьке розуміння інформаційної безпеки, розроблене окремою галуззю знань, що свідчить про несформованість цілісної методологічної основи, негативно відбивається на комплексності досліджень інформаційної безпеки і, як наслідок, на обґрунтованості і достовірності їх результатів.

Зважаючи на інтенсивність і глибину процесів інформатизації суспільного життя, сучасне уявлення про інформаційну безпеку має базуватись на сприйнятті її як складного динамічного соціально-технічного феномену, як одного з найважливіших чинників подальшого розвитку суспільства. Саме тому вкрай важливим є виважене формування методологічної основи кожного дослідження, яке поряд із використанням загальних і специфічних методів пізнання буде ґрунтуватись на світоглядних, філософських, соціологічних, наукознавчих, теоретичних засадах.

Значний потенціал системоутворювального компоненту методології комплексних досліджень інформаційної безпеки має діяльнісний підхід, адже для гуманітарних досліджень він виступатиме одним із основних за методологічним навантаженням, а для технічних – формуватиме єдині світоглядні, філософські, теоретичні засади.

Аналіз останніх досліджень і публікацій. В умовах розбудови правової держави, особливо значущим для осмислення інформаційної безпеки як виду соціально важливої діяльності стає досвід використання діяльнісного підходу правовою наукою (С.Д.Гусарєва, В.М.Карташова, В.І.Леушина, В.І.Гоймана). Певним чином діяльнісний підхід використовувався і в правових та спеціальних дослідженнях національної, державної, інформаційної безпеки у працях В.П.Горбуліна, Г.В.Іващенка, Б.А.Кормича, М.Б.Левицької, В.А.Ліпкана, В.М.Лопатіна, Ю.Є.Максименко, А.І.Марущака, Г.В.Новицького, А.О.Стрельцова та ін. Проте у сфері комплексних досліджень інформаційної безпеки можливості діяльнісного підходу залишаються не повністю використаними.

Метою статті є теоретичне осмислення забезпечення інформаційної безпеки з використанням діяльнісного підходу, виокремлення і загальна характеристика об'єктів і суб'єктів як змістових елементів діяльності із забезпечення інформаційної безпеки.

Виклад основного матеріалу. Статтею 17 Конституції України забезпечення інформаційної безпеки, поряд із захистом суверенітету і територіальної цілісності, визнається однією із найважливіших функцій держави і справою всього Українського народу. З огляду на це 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 і у повну міру відповідає положенням теорії держави і права, згідно з якими функції держави розуміються як напрями, сторони або види державної діяльності.

Крім того і сама інформаційна безпека обов'язково має діяльнісну складову, що додатково підкреслює доцільність широкого застосування діяльнісного підходу [1; 2].

Енциклопедичні джерела, відображаючи загальнонауковий аспект діяльності, визначають її як спосіб буття людини у світі, як здатність людини вносити зміни у дійсність. При цьому зміст діяльності розкривається за допомогою низки взаємопов'язаних елементів, які становлять незмінну основу діяльності, зберігають її властивості навіть за умов зовнішніх змін, надають діяльності рис сталості [3, с. 89].

Цими елементами є: об'єкт і предмет, на який спрямована діяльність; суб'єкт з його потребами й інтересами; мета, відповідно до якої перетворюється предмет; засоби і методи досягнення мети, принципи і результати діяльності. Саме їх доцільно розглядати як інтегруючу основу змісту діяльності із забезпечення інформаційної безпеки, і зокрема об'єктам та суб'єктам буде приділена увага у цій публікації.

Слід також зазначити, що названі змістові елементи у різних комбінаціях утворюють інші конструкції, які достатньо активно використовуються в наукових дослідженнях сфери національної та інформаційної безпеки, зокрема суб'єкти у поєднанні із засобами та заходами із застосування цих засобів найчастіше асоціюються з системою забезпечення; мета і відповідні їй методи і засоби відображають механізм забезпечення; методи, способи та засоби визначають шляхи забезпечення тощо.

Об'єкти забезпечення інформаційної безпеки. Об'єкт безпеки є однією з фундаментальних категорій теорії безпеки, що визначає змістову спрямованість безпеки, її конкретного виду або складової.

Розглядаючи інформаційну безпеку як особливий елемент системи національної безпеки, важливим є встановлення співвідношення об'єктів інформаційної безпеки з об'єктами безпеки вищого порядку – національної безпеки, якому як вітчизняним законодавством, так і науковими дослідженнями не приділяється належної уваги.

Так, Доктрина інформаційної безпеки України лише розкриває відповідні особливості об'єктів національної безпеки, визначених Законом України "Про основи національної безпеки", як людина і громадянин, суспільство, держава, в ракурсі інформаційної безпеки, безпосередньо не конкретизуючи її об'єкти і користуючись при цьому конструкцією "життєво важливі інтереси в інформаційній сфері". Відносно особи ці інтереси виявляються у забезпеченні конституційних прав і свобод людини на збирання, зберігання, використання та поширення інформації; недопущенні несанкціонованого втручання у зміст, процеси обробки, передачі та використання персональних даних; захищеності від негативного інформаційно-психологічного впливу. Відносно суспільства – у збереженні і примноження духовних, культурних і моральних цінностей Українського народу; забезпеченні суспільно-політичної стабільності, міжетнічної та міжконфесійної злагоди; формуванні і розвитку демократичних інститутів громадянського суспільства. Відносно держави – у недопущенні інформаційної залежності, інформаційної блокади України, інформаційної експансії з боку інших держав та міжнародних структур; ефективній взаємодії органів

державної влади та інститутів громадянського суспільства при формуванні, реалізації та коригуванні державної політики в інформаційній сфері; побудові та розвитку інформаційного суспільства; забезпеченні економічного та науково-технологічного розвитку України; формуванні позитивного іміджу України; інтеграції України у світовий інформаційний простір [4].

Дещо інший підхід обрано законодавцем у Концепції Національної програми інформатизації, прийнятій у 1998 році, яка окреслює об'єкти інформаційної безпеки як елементи інформаційної інфраструктури країни, зокрема інформаційні ресурси, канали інформаційного обміну і телекомунікації, механізми забезпечення функціонування телекомунікаційних систем і мереж тощо [5].

Наукові інтерпретації об'єктів забезпечення інформаційної безпеки більш конкретизовані, ніж нормативні, проте характеризуються значним плюралізмом підходів.

Так, В.І.Полевий об'єктами системи забезпечення інформаційної безпеки визначає: 1) засоби комунікації та масиви інформації, відображені на матеріальних носіях (технічна складова інформаційної безпеки); 2) свідомість особи, групи осіб або масова свідомість (психологічна складова); 3) інформація з обмеженим доступом, яка є критично важливою для держави або інших суб'єктів (змістова складова) [6].

Подібної позиції дотримується і О.М.Солодка, яка до елементів захисту інформаційної безпеки України у процесі євроатлантичної інтеграції, які по суті і є об'єктами інформаційної безпеки, відносить: інформаційні права суб'єктів; інформацію з обмеженим доступом; інформаційний простір; системи і засоби передачі і зберігання інформації [7].

А.Б.Качинський об'єктами інформаційної безпеки вважає інформацію та її інфраструктуру [8, с. 20].

В.А.Ліпкан, Ю.Є.Максименко, В.М.Желіховський визначають об'єкти системи забезпечення інформаційної безпеки України як: 1) інтереси органів державного управління в інформаційній сфері; 2) систему органів державного управління, а також їх компетентних осіб і відносини між ними (суспільні відносини в інформаційній сфері); 3) власне систему забезпечення інформаційної безпеки України [9, с. 162].

Наведене вище свідчить про відсутність загальновизнаного уявлення щодо об'єктів забезпечення інформаційної безпеки і необхідність певного переосмислення існуючих підходів, що може бути здійснено ґрунтуючись на таких теоретичних позиціях.

По-перше, система національної безпеки і система забезпечення національної безпеки не є тотожними поняттями, і, відповідно, об'єкти національної безпеки та об'єкти забезпечення кожної із її складових, зокрема і інформаційної, повинні розглядатися як різнопорядкові явища. Виходячи з гуманітарної парадигми національної безпеки та певної суб'єктивності поняття "безпека" [2], об'єкти національної безпеки визначені як особа, суспільство і держава, можна сприймати як родові відносно об'єктів забезпечення кожної окремої складової національної безпеки. З цієї позиції підхід до розкриття об'єктів забезпечення інформаційної безпеки, використаний у Доктрині інформаційної безпеки України, не виглядає як недолік, адже в сутності безпека об'єкта виявляється через захищеність його найважливіших якостей (якостей його структурних складових), якими у вітчизняному законодавстві є життєво важливі інтереси.

По-друге, об'єктом забезпечення інформаційної безпеки є будь-яка соціальна, технічна або соціотехнічна система, функціонування якої визначально залежить від її інформаційної інфраструктури.

По-третє, загальним об'єктом забезпечення інформаційної безпеки може розглядатися сама інформаційна безпека як система умов функціонування і розвитку суб'єктів в інформаційній сфері. Тоді конкретизованими об'єктами забезпечення інформаційної безпеки виступатимуть об'єкти та явища матеріального і нематеріального світу, які повинні створювати або забезпечувати оптимальні

умови функціонування суб'єктів в інформаційній сфері. Їх доцільно розглядати в правовому, психологічному та інженерно-технічному (технологічному) контекстах, тобто відповідно до сучасного уявлення про складові інформаційної безпеки.

Отже, загальними об'єктами національної та інформаційної безпеки є особа, суспільство, держава. Тоді узагальненими об'єктами забезпечення інформаційної безпеки можна вважати інформаційну інфраструктуру (держави, суспільства), яка має технічні і правові компоненти, і свідомість (особи, суспільства), що загалом інтерпретується таким чином:

– технічні компоненти інформаційної інфраструктури: технічні канали інформаційного обміну і телекомунікації, а також технічні системи оброблення та збереження інформації (інженерно-технічний контекст);

– правові компоненти інформаційної інфраструктури: інформаційні права та обов'язки суб'єктів; правові механізми забезпечення функціонування інформаційних ресурсів, телекомунікаційних систем і мереж; правовий порядок збереження конфіденційності, цілісності та доступності інформації (правовий контекст);

– свідомість особи, групи осіб, суспільства (психологічний клімат у національному інформаційному просторі); змістові характеристики соціально важливої інформації (психологічний контекст).

Розглядаючи об'єкти, окрему увагу доцільно приділити і *предмету забезпечення інформаційної безпеки*, оскільки саме ним зумовлюються окремі напрями діяльності суб'єктів забезпечення інформаційної безпеки, які прийнято називати їх функціями (функціями системи забезпечення інформаційної безпеки).

У системі об'єкт-предмет діяльності, предмет – це та складова або компонент об'єкта діяльності (певна цілісність, виділена з об'єкта діяльності), на яку суб'єкт спрямовує свою діяльність і яка підлягає трансформації.

Як уже зазначалося, об'єктом забезпечення інформаційної безпеки є власне сама інформаційна безпека як сукупність різноманітних умов життєдіяльності суб'єктів в інформаційній сфері. Процеси, якими створюються ці умови, можуть мати як позитивний (конструктивний), так і негативний (деструктивний) характер. Відповідно, виокремлюються дві сфери предметної спрямованості діяльності із забезпечення інформаційної безпеки: сприяння позитивним процесам; протидія негативним процесам.

Негативні процеси у своїй сутності становлять загрози (небезпеки, виклики, ризики тощо), які гальмують розвиток або сприяють деградації, у той час як позитивні процеси, що можуть сприйматися через нормативно-правову конструкцію "життєво важливі інтереси", стимулюють і забезпечують розвиток.

Проте слід звернути увагу на деякі важливі діалектичні особливості цих явищ. Так, загрози або інші негативні чинники, що не спричиняють дестабілізуючого ефекту, але усвідомлюються суб'єктом, є стимулом його еволюції у напрямі набуття якостей, які протиставляються негативному впливу, виробляючи тим самим певний рівень імунітету. І навпаки, наявність лише позитивних процесів або тривала відсутність окремих загроз може призвести до послаблення та атрофії захисних механізмів. Це означає, що оптимальне середовище функціонування суб'єктів, зокрема й інформаційне, повинно сприйматися не ідеалістично, а як об'єктивно необхідна сукупність позитивних і негативних недестабілізуючих чинників, які загалом забезпечують бажаний розвиток. Такі роздуми підкреслюють обов'язкову наявність синергетичної складової процесу забезпечення інформаційної безпеки, що у повну міру відповідає тенденціям розвитку сучасного суспільства (громадянського, інформаційного), яке ґрунтуються на самоорганізації.

У наукових джерелах досить детально розкриті питання класифікації та змісту загроз і життєво важливих інтересів у сферах забезпечення національної та інформаційної безпеки. Знайшли вони своє закріплення та змістове наповнення і на концептуально-доктринальному рівні законодавства сучасних

держав, а також у міжнародних актах. У вітчизняному законодавстві загрози і життєво важливі інтереси в інформаційній сфері та похідні від них "напрями забезпечення національної (інформаційної) безпеки", "напрями державної політики у сфері інформаційної безпеки", "напрями державної інформаційної політики" безпосередньо чи опосередковано відображені у законах України "Про основи національної безпеки", "Про стратегію національної безпеки України", "Про основи державної політики у сфері науки і науково-технічної діяльності", "Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки", "Про Концепцію Національної програми інформатизації", "Про Національну програму інформатизації", "Про інформацію", "Про доступ до публічної інформації", а також у Доктрині інформаційної безпеки України.

Суб'єкти забезпечення інформаційної безпеки. З філософського погляду суб'єкт діяльності – це носій діяльності, те, що уособлює активний творчий початок діяльності. У контексті забезпечення безпеки важливим є розгляд суб'єкта діяльності в нерозривному зв'язку з тим, на що саме спрямована ця діяльність, тобто з об'єктом діяльності, оскільки в реальності суб'єкти й об'єкти забезпечення безпеки можуть бути одночасно тим і іншим.

Суб'єкт забезпечення безпеки – одна із 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 у сучасній правовій державі є засобом визначення повноважень суб'єктів державної діяльності та окреслення сфери їх компетенції.

Теорія національної безпеки відносить до суб'єктів забезпечення всі державні та суспільні інституції, які є учасниками процесу забезпечення національної безпеки, а саме: апарат держави як систему державних органів, органи місцевого самоврядування, громадян та їх об'єднання. З цього переліку виокремлюються дві групи суб'єктів – ті, що наділені державно-владними повноваженнями, і ті, що ними не наділені, хоча в окремих випадках можуть мати певний обсяг делегованих державно-владних повноважень. Тобто формально виділяються дві взаємодоповнюючі складові забезпечення національної безпеки: державне забезпечення і недержавне забезпечення.

Аналогічний підхід доцільно застосовувати і до розгляду суб'єктів забезпечення інформаційної безпеки, причому виділення суб'єктів недержавного забезпечення є особливо актуальним, зважаючи на складність, динамічність та синергетичність процесів інформаційного розвитку суспільства. Як зазначає колектив авторів під керівництвом Ю.С.Шемшученка та І.С.Чижа, "політика інформаційної безпеки має реалізовуватися як системою інститутів публічної влади, так і інститутами громадянського суспільства, до компетенції яких належить вирішення питань створення безпечних умов функціонування і розвитку інформаційної сфери" [10, с. 79].

Крім того, в умовах сучасних світових глобалізаційних процесів, коли і національна, і тим більше інформаційна безпека держави розглядаються як явища наднаціонального (наддержавного) характеру, модель ефективного винятково самостійного забезпечення власної інформаційної безпеки окремою державою виглядає недосконалою. Сьогодні науковці стверджують про необхідність формування системи забезпечення міжнародної безпеки, а значну частину концептуальних положень національних законодавств провідних країн світу у сфері безпеки, зокрема й інформаційної, визначають домовленості, що містяться у відповідних міжнародних актах, які є результатом діяльності міжнародних організацій.

Таким чином, серед суб'єктів забезпечення інформаційної безпеки узагальнено можна виокремити три групи:

– міжнародні організації;

– держава в особі державних організацій;

– недержавні організації, громадяни та їх об'єднання.

Звичайно держава, яка безпосередньо здійснює державне забезпечення інформаційної безпеки, посідає особливе місце серед цих суб'єктів, оскільки тільки вона, виступаючи повноважним представником свого народу, в тісній взаємодії з міжнародними організаціями та інститутами громадянського та інформаційного суспільства здатна сформувати цілісну національну політику забезпечення інформаційної безпеки, що враховуватиме наявні та потенційні інтереси суспільства й особливості міжнародного становища держави.

Кожна державна організація у межах своєї діяльності, реалізуючи функції держави, певною мірою виступає суб'єктом державного забезпечення інформаційної безпеки. Крім того, в сучасній державі існує система органів, для яких окремі напрями забезпечення інформаційної безпеки є безпосередньою функцією. В Україні до них належать: Служба безпеки України, Служба зовнішньої розвідки України, Міністерство оборони України, Міністерство закордонних справ України, Державна служба спеціального зв'язку та захисту інформації України, Національна комісія з питань регулювання зв'язку України, Національна експертна комісія України з питань захисту суспільної моралі, Державна адміністрація зв'язку Міністерства транспорту та зв'язку України, Державна служба України з питань захисту персональних даних, Міжвідомча комісія з питань інформаційної політики та інформаційної безпеки при Раді національної безпеки і оборони України, Національна рада України з питань телебачення і радіомовлення, а також Головне управління з питань безпекової та оборонної політики, Головне управління забезпечення доступу до публічної інформації, Управління з питань комунікацій Адміністрації Президента України.

Серед міжнародних організацій, рішення яких відіграють важливу роль у формуванні системи забезпечення інформаційної безпеки як регіонального та світового масштабу, так і окремих держав, доцільно виділити: Європейський Союз (ЄС); Організацію Об'єднаних Націй (ООН); Організацію Об'єднаних Націй з питань освіти, науки і культури (ЮНЕСКО); Шанхайську організацію співробітництва (ШОС); Євразійське економічне співтовариство (ЄврАзЕС); Північноатлантичний Альянс (НАТО).

Недержавне забезпечення інформаційної безпеки може здійснюватися численними недержавними інституціями, зокрема засобами масової інформації; провайдерами телекомунікаційних послуг; комерційними підприємствами, які надають послуги з технічного захисту інформації; різноманітними об'єднаннями громадян, які здійснюють громадський контроль державного забезпечення інформаційної безпеки та сприяння йому, тощо.

Висновки. Забезпечення інформаційної безпеки є визначальною для майбутнього суспільства, комплексною діяльністю, що потребує особливої виваженості методології її наукових досліджень. Діяльнісний підхід у цій методології має значний системоутворювальний потенціал, оскільки він інтерпретується в науці як пояснювальний принцип, парадигма, теоретична модель або метод наукових досліджень, що дає змогу йому стати органічною складовою методологічної бази наукових досліджень багатьох напрямів. Використання діяльнісного підходу дозволяє виявити своєрідність об'єктів і суб'єктів, їх природу, діалектичні особливості, у взаємозв'язку один із одним, а також іншими компонентами діяльності із забезпечення інформаційної безпеки – метою, методами і засобами, принципами, результатами, яким буде приділено увагу в наступній публікації.

Список використаних джерел

1. Тихомиров О.О. Перспективні зміни поняття інформаційної безпеки / О.О.Тихомиров // Правова інформатика. – 2010. – № 4 (28). – С. 68-75.

2. Тихомиров О.О. Забезпечення інформаційної безпеки: теоретико-правовий аспект / О.О.Тихомиров // Право України. – 2011. – № 4. – С. 252-259.

3. Гусарєв С.Д. Юридична діяльність: методологічні та теоретичні аспекти / С.Д.Гусарєв. − К. : Знання, 2005. − 375 с.

4. Указ Президента України від 8 липня 2009 р. № 514/2009 "Про Доктрину інформаційної безпеки України" [Електронний ресурс]. − Режим доступу : http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=514%2F2009.

5. Закон України від 4 лютого 1998 р. № 75/98-ВР "Про Концепцію Національної програми інформатизації" [Електронний ресурс]. − Режим доступу : http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=75%2F98-%E2%F0.

6. Полевий В.І. Система забезпечення інформаційної безпеки України в контексті системності інформаційних загроз / В.І.Полевий // Науковий вісник НА СБ України. − 2006. − № 24. − С. 153-162.

7. Солодка О.М. Забезпечення інформаційної безпеки у процесі євроатлантичної інтеграції України / О.М.Солодка // Інформаційна безпека людини, суспільства, держави − 2009. − № 1 (1). − С. 52-56.

8. Качинський А.Б. Безпека, загрози і ризик: наукові концепції та математичні методи / А.Б.Качинський. − К., 2003. − 472 с.

9. Ліпкан В.А. Інформаційна безпека України в умовах євроінтеграції : навч. посіб. / В.А.Ліпкан, Ю.Є.Максименко, В.М.Желіховський. − К. : КНТ, 2006. − 280 с.

10. Правове забезпечення інформаційної діяльності в Україні / [заг. ред. Ю.С.Шемшученко, І.С.Чиж]. − К. : ТОВ "Вид-во "Юридична думка", 2006. − 384 с.

Аннотация: Статья посвящена теоретическому осмыслению обеспечения информационной безопасности в рамках деятельностного подхода, выделению и общей характеристике объектов и субъектов как содержательных элементов такого обеспечения.

Ключевые слова: информационная безопасность, деятельность, объект, субъект.

Abstract: The article is devoted to the theoretical comprehension of information security within the framework of the activity approach, the allocation and common characterization of objects and subjects as elements of the content of such security.

Key words: information security, activity, object, subject.