Аннотация: В статье рассматриваются проблемы определения роли государства в обеспечении информационной безопасности в условиях глобализации.

Ключевые слова: информационная безопасность, стратегия национальной безопасности, государство, задачи, мероприятия, перспективы.

Abstract: The issues of defining the role of the state in ensuring information security in the age of globalization are considered in the article.

Key words: information security, national security strategy, state, tasks, measures, perspectives.

УДК: 34.096+321.01

ТИХОМИРОВ Олександр Олександрович

ДІЯЛЬНІСНИЙ ПІДХІД У ДОСЛІДЖЕННЯХ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ: МЕТА, ЗАСОБИ І МЕТОДИ, ПРИНЦИПИ, РЕЗУЛЬТАТИ

Постановка проблеми. Сучасні дослідження інформаційної безпеки мають широкий спектр напрямів у межах як технічних, так і соціально-гуманітарних, зокрема правових наук. Це висуває особливі вимоги до формування методологічних основ досліджень, які повинні забезпечувати розвиток цілісної галузі знань про інформаційну безпеку, повноту та об'єктивність її наповнення, що сприятиме втіленню принципів науковості і професіоналізму у практичній складовій забезпечення інформаційної безпеки і наближатиме його до оптимальності.

Аналіз останніх досліджень і публікацій. Незважаючи на інтенсивність досліджень інформаційної сфери, увага науковців до змістових елементів діяльності із забезпечення інформаційної безпеки найчастіше залишається фрагментарною, що об'єктивно зумовлено широтою цієї сфери і специфікою наукових завдань окремих досліджень, але негативно позначається на комплексності досліджень інформаційної безпеки і достовірності їх результатів.

Як вже зазначалося у попередній статті, присвяченій суб'єктам і об'єктам забезпечення інформаційної безпеки, значний потенціал системоутворювального компоненту методології комплексних досліджень інформаційної безпеки має діяльнісний підхід – комплекс методів, серед яких об'єднуючим і домінуючим є діяльнісний. Проте його можливості сьогодні залишаються не достатньо використаними [1].

Метою статті є теоретичне осмислення забезпечення інформаційної безпеки з використанням діяльнісного підходу, виокремлення мети, засобів і методів, принципів, результатів як змістових елементів діяльності із забезпечення інформаційної безпеки та їх загальна характеристика.

Виклад основного матеріалу. *Мета забезпечення інформаційної безпеки.* Мета є постійно присутнім фактором, обов'язковим та необхідним елементом будь-якої цілеспрямованої діяльності. З одного боку, мета діяльності може розглядатися як вихідний, детермінуючий компонент не лише змісту, а й структури діяльності. З іншого, мета діяльності зумовлюється низкою зовнішніх факторів, що присутні у межах соціального середовища, і передусім такими факторами, як

потреби та інтереси. Водночас мета діяльності формується під впливом інших факторів: режиму законності, стану правопорядку, політичної обстановки або економічної ситуації в країні, рівня правової культури тощо [2, с. 97].

Рівень визначеності мети залежить від характеристик суб'єкта, особливостей сфери його діяльності і може бути різним. Очевидно, що мета масштабної консолідуючої діяльності, якою є забезпечення національної безпеки, має найвищий рівень узагальненості і сталості, а мета забезпечення інформаційної безпеки як складової національної – більш конкретизована і розкривається завданнями діяльності, що постають на певному етапі розвитку і змінюються із часом.

На загальнотеоретичному рівні мета забезпечення інформаційної безпеки також може розглядатися достатньо абстрактно, зокрема як досягнення такого стану інформаційної безпеки, який забезпечує оптимальне задоволення інформаційних потреб і інтересів суб'єктів. Або ж, у соціологічному аспекті, – як формування системи суспільних відносин, у межах яких певним чином задовольняються національні інтереси й об'єктом яких є інформація, інформаційна діяльність, інформаційна інфраструктура тощо.

Мета забезпечення національної безпеки України визначається пріоритетами національних інтересів (ст. 6 Закону України "Про основи національної безпеки"), що розкривають конституційну модель України (ст. 1 Конституції України) як суверенної і незалежної, демократичної, соціальної, правової держави.

У свою чергу, мета забезпечення інформаційної безпеки України опосередковано відображається у пріоритетах національних інтересів, але безпосередньо закріплена Доктриною інформаційної безпеки України як "створення в Україні розвиненого національного інформаційного простору і захист її інформаційного суверенітету" [3]. Проте таке визначення дещо зміщує акцент із соціально-гуманітарної складової пріоритетної для національної безпеки (забезпечення реалізації прав, свобод та життєво важливих інтересів, і особливо інтелектуального, духовного і культурного розвитку людини і громадянина) на технологічну і не відбиває синергетичні та субсидіарні особливості інформаційної безпеки, її взаємозв'язки з інформаційним суспільством.

Із цих позицій більш досконалою виглядає інтерпретація мети забезпечення інформаційної безпеки на основі Окінавської хартії глобального інформаційного суспільства та відповідних їй загальних положень Закону України "Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки" через пріоритетність розбудови орієнтованого на інтереси людей, відкритого для всіх і спрямованого на розвиток інформаційного суспільства, в якому кожен має можливість створювати і накопичувати інформацію та знання, вільно їх отримувати, користуватися й обмінюватися ними, тим самим у повній мірі реалізовувати свій потенціал, сприяючи суспільному й особистому розвитку та підвищуючи якість життя [4; 5].

Подальша деталізація мети забезпечення інформаційної безпеки може здійснюватись основними завданнями, що стоять перед Україною на сучасному етапі розвитку, до яких в інформаційній сфері належать:

– інформатизація процесів управління державою;

– формування доступних національних інформаційних ресурсів;

– інтеграція у світовий інформаційний простір;

– збереження національної ідентичності та популяризація національної культури;

– розвиток інтелектуального потенціалу країни;

– створення позитивного морально-психологічного клімату у національному інформаційному просторі;

– формування позитивного іміджу України на світовій арені;

– протидія кіберзлочинності та кібертероризму тощо.

Засоби і методи забезпечення інформаційної безпеки. Вибір методів і засобів у

будь-якій сфері діяльності загалом визначається метою та завданнями. Забезпечення інформаційної безпеки є комплексним видом діяльності, що зумовлює наявність в її арсеналі широкого кола методів та засобів, притаманних різним галузям, сферам діяльності. Ці засоби та методи, визначаючи один одного та об'єднуючись на різних рівнях забезпечення у системи, утворюють механізми забезпечення інформаційної безпеки.

Концепції систематизації механізмів забезпечення інформаційної безпеки можуть бути різними. Так, у сфері управління інформаційною безпекою (серія стандартів ISO/IEC 27000) традиційно окреслюють кілька рівнів: 1) фізичний; 2) програмно-технічний; 3) управлінський; 4) технологічний; 5) рівень користувача; 6) мережевий; 7) процедурний [6]. Ці рівні відображають визнану систему забезпечення інформаційної безпеки окремих організацій (органів, підприємств, установ тощо) та створення безпечних каналів обміну інформацією між ними. Проте не охоплюють усієї багатоаспектності інформаційної безпеки, оскільки згадана діяльність орієнтована переважно на захист інформації необхідної окремим суб'єктам у процесі здійснення ними певних видів діяльності.

Для правильного розуміння системи засобів та методів забезпечення інформаційної безпеки пропонуємо розглядати їх крізь гіпотетичну трирівневу модель, яка відображає особливості їх використання з урахуванням предметної і гуманітарної спрямованості:

1) рівень загального сприяння (регулятивний рівень);

2) рівень індивідуального сприяння (рівень стимулювання самозахисту суб'єктів);

3) рівень захисту (охоронний рівень).

Першому рівню відповідають методи та засоби, які відносно другого і третього рівня мають загальний характер. Вони притаманні багатьом сферам діяльності (політичній, правовій, економічній, освітній, науково-технологічній тощо) і використовуються для створення загальних умов задоволення потреб і інтересів суб'єктів в інформаційній сфері, що загалом виражається у розвитку інформаційної інфраструктури держави та національних інформаційних ресурсів, а також загальному інтелектуальному та культурному розвитку населення.

Другому рівню відповідають методи та засоби освітньо-виховного індивідуального впливу, спрямованого на формування здатностей самостійного забезпечення власної інформаційної безпеки, зокрема підвищення рівня культури використання засобів оброблення інформації, критичного ставлення до інформації, а також сприяння розвитку механізмів внутрішньоособистісного психологічного захисту.

Третьому рівню відповідають спеціальні методи та засоби, які загалом утворюють: механізми організаційно-правового та технічного збереження якісних характеристик інформації (захисту інформації), механізми протидії маніпулюванню свідомістю суспільства шляхом викривленої, недостовірної, неповної інформації або шляхом використання сугестивних технологій і, зокрема, нейролінгвістичного програмування; механізми контролю застосування спеціальних методів та засобів.

Слід зазначити, що запропонована модель є лише альтернативним виміром, який не применшує цінності існуючих варіацій систематизації засобів та методів, що використовуються у сфері інформаційної безпеки.

Зокрема їх систему можна інтерпретувати й іншим способом: 1) правові; 2) управлінсько-організаційні; 3) інформаційно-аналітичні, прогностичні; 4) психологічного захисту особистості; 5) технічного і криптографічного захисту інформації тощо.

Окремо слід акцентувати увагу на важливості адекватного використання правових засобів і методів. Право як загальновизнаний соціальний регулятор має водночас і переваги, і недоліки, які зумовлюються його природними властивостями, зокрема універсальністю. Правові норми є єдиним забезпеченим сучасною державою засобом регулювання різних сфер діяльності, для чого використовують достатньо універсальну систему

засобів і методів (методи: переконання, стимулювання, примус; засоби: суб'єктивні права, юридичні обов'язки, юридична відповідальність, правосуддя тощо). Крім того правові норми є способом закріплення концептуальних основ життя суспільства та напрямів його подальшого розвитку, зокрема в інформаційній сфері та сфері інформаційної безпеки, а також регламентації діяльності (визначення повноважень) різноманітних державних інституцій. Тому оптимальність правового регулювання, адекватність вибору правових засобів і методів безпосередньо визначає ефективність соціально важливих проявів інформаційної діяльності і, як наслідок, якість організаційного підґрунтя забезпечення інформаційної безпеки.

Принципи забезпечення інформаційної безпеки. Принципи будь-якої діяльності людини відіграють важливу роль, оскільки встановлюють її вихідні, основоположні засади. Забезпечення інформаційної безпеки не є винятком. Сьогодні до нього висуваються особливі вимоги не тільки щодо відповідності принципам, притаманним власне сфері національної та інформаційної безпеки, а й відповідності конституційним принципам розбудови держави.

У межах діяльнісного підходу важливим є зосередження уваги на принципах, що відображають концепцію забезпечення інформаційної безпеки як комплексного виду діяльності у контексті розбудови правової держави, громадянського та інформаційного суспільства, а також глобалізаційних та інтеграційних процесів. Ці принципи можна поділити на дві групи.

Першу групу становлять принципи, які відображають загальносистемні засади державної політики забезпечення інформаційної безпеки:

– комплексність підходів до забезпечення інформаційної безпеки;

– оптимальність системи забезпечення інформаційної безпеки;

– всебічна виваженість державної політики інформаційної безпеки;

– єдність та цілісність законодавчих підходів до забезпечення інформаційної безпеки;

– об'єктивність оцінки загроз та адекватність і своєчасність заходів із забезпечення інформаційної безпеки;

– чітке розмежування повноважень та взаємодія органів державної влади у забезпеченні національної безпеки;

– використання в інтересах країни міждержавних систем та механізмів міжнародної колективної безпеки.

До другої групи належать принципи, що закладають правові та демократичні основи діяльності із забезпечення інформаційної безпеки і які на фоні сучасних перетворень суспільства привертають все більшу увагу дослідників інформаційної сфери:

– свобода збирання, зберігання, використання та поширення інформації;

– гарантованість достовірності, повноти та неупередженості інформації;

– доступність інформації та законність обмеження доступу до інформації;

– інформаційна рівність;

– збалансованість особистих, суспільних і державних інтересів в інформаційній сфері;

– невідворотність юридичної відповідальності за правопорушення в інформаційній сфері та адекватність її міри;

– гармонійність між національним і міжнародним законодавством в інформаційній сфері;

– пріоритетність національної інформаційної продукції;

– взаємна відповідальність особи, суспільства і держави;

– гласність і демократичний контроль забезпечення інформаційної безпеки тощо.

Окремо доцільно виділити низку принципів, що стосуються забезпечення інформаційно-психологічної безпеки. Характер деяких із них є достатньо суперечливим, проте вони у майбутньому можуть набути законодавчого закріплення, чому вже є реальні підтвердження [7]:

– державна монополія на розробку й виробництво спеціальних засобів інформаційно-психологічного впливу;

– законність використання спеціальних

засобів інформаційно-психологічного впливу;

– обов'язковість участі громадських організацій у діяльності із забезпечення інформаційно-психологічної безпеки;

– організованість міжнародного співробітництва у сфері забезпечення інформаційно-психологічної безпеки;

– скоординованість діяльності органів державної влади і громадських об'єднань щодо забезпечення інформаційно-психологічної безпеки;

– захищеність традиційних засад суспільства і суспільної моральності.

Результат забезпечення інформаційної безпеки. Очевидно, що результат діяльності із забезпечення інформаційної безпеки має корелюватися із інформаційною безпекою, а точніше – з її станом на момент оцінки результатів, інакше ця діяльність втрачає сенс.

Необхідним і логічним є оцінювання стану забезпечення інформаційної безпеки на підставі положень законодавства, що визначають мету, об'єкти, напрями забезпечення інформаційної безпеки, а також життєво важливі інтереси особи, суспільства, держави в інформаційній сфері.

Це оцінювання має водночас характер практичного і науково-теоретичного пізнання та повинне ґрунтуватися на таких методологічних принципи, як об'єктивність і реалістичність, всебічність і комплексність аналізу тощо. Однак реалізація цих принципів вимагає розробки обґрунтованих методичних підходів і прийомів визначення реального стану та перспектив розвитку суспільних відносин в інформаційній сфері і, зокрема у сфері забезпечення інформаційної безпеки, яких на сьогодні не існує. Слід зазначити, що в науковому світі активізувалася робота із оцінювання рівня інформаційної безпеки із застосуванням математичних методів. Проте існуючі моделі, методи і методики, які ґрунтуються на інформації з відкритих джерел, потребують розвитку і вдосконалення [8; 9]. Навіть у практично орієнтованій, стандартизованій сфері управління інформаційною безпекою комплексна оцінка результатів управління залишається поза увагою.

Отже актуальним науковим і практичним завданням у сфері інформаційної безпеки залишається формування загальновизнаних підходів до визначення оптимальних моделей і шляхів її забезпечення на основі виявлення найважливіших якісних і кількісних властивостей та параметрів цього явища. Важливість такого завдання підтверджується і вітчизняним законодавством, яке визначає розроблення та впровадження системи індикаторів інформаційного розвитку суспільства та узгодженням їх із міжнародними стандартами і методологією, одним із основних напрямів розвитку інформаційного суспільства в Україні [5; 10].

Певною мірою вирішенню цього завдання може сприяти застосування методів критеріального аналізу, які все частіше використовуються в дослідженнях явищ соціальної сфери [11; 12].

У міжнародній практиці поширене оцінювання рівня розвитку інформаційного суспільства або його структурних елементів, що опосередковано відображає і стан інформаційної безпеки, адже він безпосередньо залежить від здатностей і можливостей суб'єктів інформаційних відносин. Оцінювання здійснюється на основі е-індексів, вибір та методика побудови яких визначається обраними державою пріоритетами. До основних індикаторів експерти включають зокрема індикатори стану доступу до телекомунікаційної інфраструктури (радіо, телебачення, телефону, персональних комп'ютерів, Інтернету) населення взагалі і окремо в освітніх закладах, установах, державних організаціях тощо. Найбільш поширеними є е-індекси: цифрової спроможності або цифрової перспективи (Digital Opportunity Index – DOI), цифрового доступу (Digital Access Index – DAI), мережевої готовності (The World Economic Forum's Networked Readiness Index – NRI), інформаційного суспільства (Informational Society Index – ISI) [13]. За цими індексами Україна посідає далеко не перші місця, що свідчить про не близькі перспективи високого рівня інформаційної безпеки в широкому її розумінні.

Таким чином, інформаційна безпека як

результат комплексної діяльності і як стан оптимального функціонування і розвитку суб'єктів в інформаційній сфері потребує комплексної оцінки через систему показників інформаційної безпеки – найбільш значущих параметрів, що надають загальне уявлення щодо інформаційної системи держави і суспільства, її стійкості, ефективності, здатності до розвитку тощо. Систему показників доцільно розділити на два логічних блока: 1) критерії та показники, що відображають технологічну сторону інформаційної безпеки (рівень розвитку та захищеності інформаційної інфраструктури); 2) критерії та показники, що відображають рівень інформаційного розвитку суб'єктів (зокрема держави, суспільства), а також наявні та потенційні можливості до забезпечення власної інформаційної безпеки.

Належне місце в комплексній оцінці забезпечення інформаційної безпеки повинна зайняти правова оцінка, яка відображатиме рівень реалізованості правових засад інформаційної безпеки особи, суспільства, держави, тобто ефективність існуючих правових механізмів безпечного функціонування суб'єктів в інформаційній сфері. На загальному рівні таку оцінку можна здійснювати через систему показників стану законності та правопорядку в інформаційній сфері [12].

Висновки. Широке використання діяльнісного підходу у ході наукових досліджень різних аспектів інформаційної безпеки сприятиме формуванню цілісної галузі знань про інформаційну безпеку та її забезпечення, яка характеризуватиметься органічністю і гармонійною поєднаністю всіх складових та відображатиме природні властивості феномену "інформаційна безпека", серед яких:

– багатогранність сучасного уявлення про інформаційну безпеку, зокрема невід'ємність таких її складових, як інформаційно-технічна, інформаційно-правова, інформаційно-психологічна, що забезпечує адекватність формування методології досліджень і, відповідно, об'єктивність і обґрунтованість їх результатів;

– зверхність гуманістичної парадигми інформаційної безпеки над техніко-технологічною, що орієнтує на пріоритетність задоволення потреб і інтересів людини і суспільства;

– діалектичність інформаційного середовища, що відображає суб'єктивність оптимального поєднання позитивних і негативних чинників впливу, необхідних для стабільного інформаційного розвитку;

– нерозривність взаємозв'язку з інформаційним суспільством як метою і результатом діяльності із забезпечення інформаційної безпеки;

– синергетичні властивості інформаційної безпеки, тобто безпрецедентну важливість самоорганізаційної складової забезпечення інформаційної безпеки;

– субсидіарність у співвідношенні державного і недержавного забезпечення, яка визначає межі втручання держави у процеси забезпечення інформаційної безпеки людини і суспільства;

– комплексність у виборі засобів і методів забезпечення інформаційної безпеки, що забезпечує повноту забезпечення оптимальність його результатів;

– глобальність, транснаціональність, консолідованість забезпечення інформаційної безпеки у процесі розбудови глобального інформаційного суспільства і повноцінного входження всіх членів світового суспільства у світовий інформаційний простір.

Список використаних джерел

1. Тихомиров О.О. Діяльнісний підхід у дослідженнях забезпечення інформаційної безпеки: об'єкти і суб'єкти / О.О.Тихомиров // Інформаційна безпека людини, суспільства, держави. – 2012. – № 2 (9). – С. 18-24.

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

3. 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.

4. Міжнародний документ від 22 липня 2000 р. "Окінавська хартія глобального інформаційного суспільства" [Електронний ресурс]. – Режим доступу : http://zakon1.rada. gov.ua/cgi-bin/laws/main.cgi?nreg=998_163.

5. Закон України від 9 січня 2007 р. № 537-V "Про Основні засади розвитку інформаційного суспільства в Україні на 2007-2015 роки" [Електронний ресурс]. − Режим доступу : http://zakon. rada.gov.ua/cgi-bin/laws/main.cgi?nreg=537-16.

6. ISO/IEC 27002:2005 Information technology. Security techniques. Code of practice for information security management [Електронний ресурс]. – Режим доступу : http://www.iso. org/iso/catalogue_detail?csnumber=50297.

7. Проект Федерального Закона "Об информационно-психологической безопасности" [Электронный ресурс]. – Режим доступа : http:// www.medialaw.ru/publications/zip/68/lopatin.htm.

8. Хорошко В.О. Методика кількісно-якісного аналізу та визначення рівня інформаційної безпеки [Електронний ресурс] / В.О.Хорошко, В.С.Чередниченко // Інформаційні технології та комп'ютерна інженерія. – Режим доступу : http://www.nbuv.gov.ua/portal/ natural/Itki/2008_3/08hvafis.pdf.

9. Панченко В.М. Методика виявлення ознак інформаційного впливу в засобах масової інформації / В.М.Панченко, В.І.Полевий // Інформаційна безпека людини, суспільства, держави. – 2011. – №3 (7). – С. 70-77.

10. Морозов О.Л. Інформаційна безпека в умовах сучасного стану і перспектив розвитку державності [Електронний ресурс] / О.Л.Морозов // Віче. – Режим доступу : http://www.viche.info/journal/598/.

11. Тихомиров О.О. Критеріальний метод у правових дослідженнях / О.О.Тихомиров // Філософські, методологічні і психологічні проблеми права : тези доп. III Всеукр. наук.-практ. конф. (Київ, 23 квітня 2010 р.) / [редкол. : В.В.Коваленко, М.В.Костицький, О.М.Джужа та ін.]. – К. : Київ. нац. ун-т внутр. справ, 2010. – С. 206-207.

12. Тихомиров О.О. Критеріальна оцінка інформаційного розвитку суспільства та інформаційної безпеки / О.О.Тихомиров // Бюлетень Міністерства юстиції України. – 2010. – № 4-5. – С. 250-254.

13. Гурковський В.І. Державне управління розбудовою інформаційного суспільства в Україні (історія, теорія, практика) / В.І.Гурковський. – К. : Вид-во "Науковий світ" та МНДЦ з проблем боротьби з організованою злочинністю при РНБО України, 2010. – 396 с.

Аннотация: Статья посвящена теоретическому осмыслению обеспечения информационной безопасности в рамках деятельностного подхода, выделению и общей характеристике цели, средств и методов, принципов, результатов как содержательных элементов такого обеспечения.

Ключевые слова: информационная безопасность, деятельность, цель, средства и методы, принципы, результаты.

Abstract: The article is devoted to the theoretical comprehension of information security ensuring within the framework of the activity approach, the highlighting and common characterization of aim, means and methods, principles, results as conceptual elements of such ensuring.

Key words: information security, activity, aim, means and methods, principles, results.