УДК 35:354:303:001.8

В. В. Антонюк,
аспірант, Національна академія державного управління при Президентові України, м. Київ

ОСНОВНІ НАУКОВО-МЕТОДОЛОГІЧНІ ПІДХОДИ ДО ДОСЛІДЖЕННЯ ДЕРЖАВНОЇ ПОЛІТИКИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

V. Antoniuk,
graduate student, National Academy of Public Administration the President of Ukraine, Kiev

THE MAIN SCIENTIFIC AND METHODOLOGICAL APPROACHES TO THE STUDY OF THE STATE OF INFORMATION SECURITY POLICY

Досліджено сутність науково-методологічних підходів до дослідження державної політики інформаційної безпеки; здійснено класифікацію етапів дослідження проблем безпеки у науковому дискурсі; показано особливості застосування системного підходу у дослідженні проблем інформаційної безпеки.

The essence of scientific and methodological approaches to the study of the state of information security policy, and to classify stages of the study of security problems in scientific discourse, showing features of a systems approach to the study of information security problems.

Ключові слова: державна політика, державне управління, інформаційна безпека, система забезпечення національної безпеки, системний підхід.
Key words: public policy, public administration, information security, the system of national security, system approach.

ПОСТАНОВКА ПРОБЛЕМИ

Становлення сучасної парадигми інформаційної безпеки відбувалося через переосмислення наукової спадщини видатних мислителів Європи, США та інших країн. Проблема забезпечення безпеки людини, суспільства і держави та отримання про це достовірної інформації переважно розглядалась у контексті війни та миру. Погляди на роль держави у забезпеченні безпеки в суспільстві, а також знаннєві (інформаційні) аспекти даної проблеми були близькими, спорідненими. Але поступово, з розвитком суспільства сила первісної єдності потроху руйнується, починається послідовне виокремлення різних життєвих сфер та елементів.

АНАЛІЗ ОСТАННІХ ДОСЛІДЖЕНЬ І ПУБЛІКАЦІЙ

Концептуальні ідеї державного управління інформаційною безпекою сягають сивої давнини. Мислителі різних епох засуджували насильство, мріяли про вічний мир і безпеку пропонували різні моделі здійснення своїх задумів.

Одні з них звертали увагу переважно на інформаційно-етичний бік проблеми (Августин Блаженний, І. Кант, Р. Оуен, А. Бергсон, А. Швейцер). Вони вважали, що агресія, війна є породженням аморальності, що безпечного стану можна досягти тільки в результаті морального перевиховання людей у дусі взаєморозуміння, терпимості до різних віросповідань, усунення націоналістичних пережитків, виховання людей у дусі принципу "всі люди брати". У цих процесах вони приділяли визначальну роль державі як соціальному інституту [5, с. 29].

Інші вбачали головну перешкоду для досягнення безпечного суспільного стану в господарській розрусі, в порушенні нормального функціонування всієї економічної та інформаційної структури (Ціцерон), в колізії природного й громадянського станів особистості (Т. Гоббс, Дж. Локк) [2,с.194]. У зв'язку з цим вони намагалися схилити людство до миру й безпеки, малюючи картини загального процвітання в суспільстві без воєн, у якому пріоритет надаватиметься розвитку науки, техніки, мистецтва, літератури, інформації, а не вдосконаленню засобів знищення. Вони вважали, що міждержавна безпека може бути встановлена в результаті розумної політики освіченого правителя[2, с. 201].

Треті розробляли правові аспекти проблеми безпеки, досягти якої вони прагнули шляхом договору між урядами, створенням регіональних або всесвітніх федерацій держав (Г. Іроцій, А. Сен-Сімон, К. Ясперс, А. Тойнбі).

Четверті вважали, що коріння небезпек має соціальний характер, що усунути їх можна лише змінивши структуру суспільства (Е. Роттердамський, С. Франк).

ФОРМУЛЮВАННЯ ЦІЛЕЙ СТАТІ

Мета статті — основні науково-методологічні підходи до дослідження державної політики інформаційної безпеки.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ ДОСЛІДЖЕННЯ

Сучасні методологічні підходи до філософського аналізу феномену інформаційної безпеки мають увібрати в себе якомога більше позитивних аспектів проаналізованої історичної спадщини. Історико-ретроспективний аналіз даної проблеми є необхідним для вибору перспективної методологи дослідження проблем забезпечення інформаційної безпеки.

У системі національної безпеки держави поряд зі стійкістю суспільства, його соціально-економічною стабільністю, неабияке значення має інформаційна безпека, під якою зазвичай розуміється стан відсутності інформаційних небезпек і загроз або, в разі їх наявності, стан стійкості основних сфер життєдіяльності (політики, економіки, науки, техніки, сфери державного управління, суспільної свідомості військової справи тощо) стосовно небезпечних інформаційних впливів (як упровадження, так і вилучення інформації).

Переважна більшість сучасних дослідників характеризують інформаційну безпеку як стан захищеності інформаційного середовища, що відповідає інтересам держави, за якого забезпечується формування використання і можливості розвитку незалежно від дії внутрішніх і зовнішніх інформаційних загроз. Аналогічної точки зору дотримується російський дослідник І. Панарін, але з акцентом на вирішальну роль політичної еліти суспільства, яка, на його думку, реально може протистояти інформаційним впливам.

Інше визначення дає А. Тер-Акопов [6, с.175]. Він пропонує розуміти під інформаційною безпекою суб'єкта стан захищеності інформації, що забезпечує життєво важливі інтереси людини.

Існують також визначення інформаційної безпеки як стану, тенденції розвитку, умови життєдіяльності соціальних суб'єктів, інститутів, за яких забезпечується збереження їх якісної визначеності з об'єктивно зумовленими інноваціями. Представники цього напряму (О. Возженніков, В. Калайда, Ю. Максименко, О. Прохожев, Т. Філіпенко, А. Юричко) розглядають інформаційну безпеку як стан, що характеризується відсутністю загроз, тобто чинників і умов, котрі несуть загрозу безпосередньо індивідові, суспільству, державі з боку інформаційного середовища. У цьому разі поняття "стан" істотно відрізняється від поняття "процес" оскільки означає послідовність станів, зв'язаність їх стадій зміни і розвитку. Поняття "процес" на відміну від поняття "стан" акцентує увагу на моменті спрямованості в зміні об'єкта, тимчасовості, цілепокладенні.

Представник третього напряму Я. Серебрянніков визначає безпеку як "діяльність людей, суспільства, держави, світової спільноти із виявлення (вивчення), попередження, ослаблення, усунення (ліквідації) викликів і загроз, здатних знищити їх, позбавити фундаментальних матеріальних і духовних цінностей, завдати неприйнятної (неприпустимої об'єктивно і суб'єктивно) шкоди, закрити шлях для прогресивного розвитку".

З наведеного вище випливає, що стан безпеки залежить тільки від інтересів суб'єктів суспільної взаємодії в інформаційній сфері, збалансованість яких і визначає рівень загроз, але не вказується, на те, що ці інтереси є життєво важливими, а також на існування і зовнішніх загроз.

О. Левін вважає, що визначати інформаційну безпеку через захищеність не зовсім коректно. На його думку, дотримуючись загальновідомої тези "краща оборона — це напад", треба діяти активно, знищувати джерела інформаційної небезпеки. При цьому стосовно змісту інформаційної безпеки доцільно вживати не поняття "інтереси", а набагато фундаментальніше поняття — "цінності". З погляду О. Левіна, в цінностях виражаються інтереси суб'єктів суспільних відносин, зіткнення яких і породжують загрози [4, с. 67].

Крім зазначеного вище, існує точка зору, що в найзагальнішому вигляді під інформаційною безпекою можна розуміти здатність суб'єкта безпеки зберігати свої системотворчі властивості, основні характеристики при дезорганізуючих, деструктивних, руйнівних діях на кіберпростір, інформаційно-комунікативні технології. Рівень та інтенсивність цих дій з позицій забезпечення інформаційної безпеки мають певні межі. Їх перевищення може викликати часткові, істотні або незворотні негативні зміни. Якщо мову вести про інформаційну безпеку держави, то мається на увазі її здатність протистояти негативним, руйнівним діям, спрямованим на завдання шкоди її національним інтересам. Вона реалізується в конкретній діяльності держави та її інститутів, що дало змогу ввести до наукового обігу поняття "забезпечення інформаційної безпеки", котре характеризує функціонування соціальної системи, спрямованої на досягнення стабільності .

На думку прихильників останньої точки зору, "інформаційна безпека" і "забезпечення інформаційної безпеки" є різними поняттями. Перше дає насамперед істотну характеристику стану соціальної спільноти, тоді як друге — діяльнісну характеристику, тобто висвітлює діяльність суб'єктів даного соціуму стосовно підтримання безпеки. У цьому сенсі "безпека" усвідомлюється як мета життєдіяльності, а "забезпечення безпеки" — як діяльність із досягнення безпечного стану.

Аналогічних поглядів дотримується й чимало західних філософів, соціологів та політологів, які вважають, що інформаційна безпека — це здатність держави ефективно захистити національні інтереси та цінності на основі виявлення загроз і намірів супротивника. Інакше кажучи, це здатність системи забезпечити безпечний рівень життєдіяльності своєї нації та її конкурентноспроможність з метою надійного існування і сталого розвитку.

Відомі російські дослідники М. Дзлієв і А. Урсул вважають, що забезпечення безпеки не зводиться тільки до захисту; ідея національної безпеки тісно пов'язана з концепцією стійкого демократичного розвитку, є її невід'ємною частиною і водночас умов її реалізації. Такий підхід значно розширює поняття "інформаційна безпека" за рахунок включення в нього "здатності держави ефективно захищати національні інтереси і цінності" [2, с. 321—322].

Отже, інформаційна безпека є складною категорією, різноманіття розглянутих концепцій пов'язане з тим, що інформаційна безпека як соціокультурне явище є складною багаторівневою функціональною системою.

Основними структурними елементами системи інформаційної безпеки є особа, суспільство і держава, їх життєво важливі інтереси, загрози в інформаційній сфері. Різні підходи, доповнюючи один одного, дозволяють поглянути на проблему забезпечення інформаційної безпеки з позиції комплексного підходу, що дає змогу доповнити наявні знання.

Автор дотримується такого розуміння поняття "інформаційна безпека": стан захищеності життєво важливих інтересів людини, суспільства і державив інформаційній сфері від зовнішніх та внутрішніх викликів і загроз, що забезпечує їх сталий розвиток.

Водночас, інформаційна безпека — це і процес, оскільки найтіснішим чином пов'язана з культурним середовищем і є невід'ємною частиною соціокультурного життя суспільства, в якому діють політична влада, суспільно-політичні сили і рухи, беруть участь особистості, соціальні групи, котрі спонукаються економічними й соціально-політичними потребами, інтересами і цілями. Ця обставина передбачає розкриття наявних зв'язків серед суб'єктів і об'єктів безпеки, їх інтересів, а також тенденцій і закономірностей їх розвитку, понять, за допомогою яких вичленяють загрози із сукупності різних чинників і явищ навколишньої дійсності.

Інформаційна безпека є важливим і дуже складним різноплановим напрямом у загальній системі національної безпеки і стосується військової, економічної, політичної, етнічної, демографічної, ідеологічної, продовольчої та інших видів безпеки. Кожен із зазначених вище видів безпеки, кожна така підсистема у свою чергу виявляється системою стосовно своїх складових елементів.

Основними об'єктами загроз інформаційній безпеці є економічні, технічні, соціальні тощо, вважаємо, що у сучасних умовах саме інформаційно-психологічні джерела загроз є найбільш актуальними і значущими в контексті даної проблематики.

Важливим науковим завданням при дослідженні державного управління інформаційною безпекою є методологія даного питання. На нашу думку, до дослідження цієї проблеми необхідно підходити з урахуванням цивілізаційних, міжнародних і внутрішніх умов, пов'язаних з особливостями трансформації українського суспільства в сучасних умовах поширення глобалізаційних тенденцій.

Однією з найважливіших методологічних проблем дослідження національної безпеки взагалі й інформаційної безпеки зокрема є досягнення правильного співвіднесення теоретичного й емпіричного рівнів наукового пізнання, їх інтеграція з метою отримання узагальненого знання про предмет. У розв'язанні практичних завдань функціонування тих чи інших сфер національної безпеки та системи безпеки в цілому необхідне застосування конкретних методологічних принципів дослідження, які є універсальними для наукового пізнання усіх предметних сторін об'єкта — соціокультурних процесів, які віддзеркалюють розвиток і стан національної безпеки.

Інформаційна безпека також може бути досліджена в межах діалектичного, структурно-функціонального, синергетичного, системного, інформаційно-ціннісного та інших підходів. Убачається за доцільне застосування деяких із цих підходів стосовно інформаційної безпеки охарактеризувати докладніше.

Основи структурно-функціонального аналізу були закладені Т. Парсонсом, Р. Мертоном, їх учнями й послідовниками. Згідно з цим підходом (якщо інтерпретувати його основні положення до контексту досліджуваної проблеми) систему забезпечення інформаційної безпеки будь-якої держави можна розглядати як функціональну систему. Вперше поняття "функціональна система" у вітчизняній науці сформулював П. Анохін, який під ним розумів динамічні саморегулятивні структури, діяльність яких спрямована на забезпечення корисних для існування систем і організацій, до яких вони входять як складові. П. Анохін зазначав, що жодна організація, якою б просторою вона не була за кількістю елементів, не може бути названа саморегульованою системою, якщо її функціонування, тобто взаємодія частин цієї організації, не закінчується якимось корисним для системи результатом і якщо відсутня зворотна інформація в керівний центр про ступінь корисності цього результату [1, с. 121].

Для функціональних систем багатозв'язкового регулювання (а система забезпечення інформаційної безпеки є саме такою) характерним є якісно інший принцип саморегуляції: відхилення від оптимального рівня того чи іншого параметра зумовлює спрямований перерозподіл у певних співвідношеннях значень усіх інших параметрів.

Нашу думку, відповідно до принципу взаємодоповнюваності краще зрозуміти процеси, що відбуваються в системі інформаційної безпеки як у відкритій системі, проблеми взаємодії елементів (підсистем) даної системи та суспільства допомагає (у поєднанні з іншими методами й підходами) синергетичний підхід. Адаптовано сфери інформаційної безпеки синергетичну парадигму можна представити такою проблематикою: неврівноваженість і нестійкість як загальний стан компонентів системи; врівноваженість і тривалість як глухий кут еволюції; роль випадковості у загальному ході подій; відкритість системи, обмін інформацією з соціумом у кожній її точці (за винятком сфери державної таємниці); нелінійність розвитку; вибір напряму розвитку; альтернативність напрямів розвитку як загальний принцип; власні тенденції розвитку інформаційних систем; керований розвиток в умовах самоорганізації.

Для розвитку системи забезпечення інформаційної безпеки характерними є два взаємопов'язаних процеси: збереження стійкості, підтримання цілісності та їх тимчасове порушення. Збереження цілісності, тобто спроможності протистояти зовнішнім впливам (загрозам), забезпечує спадкоємність в її розвитку. При цьому новий склад елементів і тип інформаційних структур дають початок новому цілому. Вони є вторинними стосовно попереднього складу елементів і структур, є їх продуктом і стають первинними щодо нових процесів і явищ.

Тимчасове порушення цілісності, що виникає, нестійкість інформаційних систем відбувається у певних

точках біфуркації, які виникають під впливом нелінійних процесів, що трапляються як у соціумі, так і в самих інформаційних системах та їх окремих елементах. Усе це супроводжується певними змінами, які охоплюють окремі сфери чи інформаційну систему в цілому, внутрішню чи зовнішню структуру, окремі функції чи всю їх систему. На цій основі виникає нова дисипативна структура, з якої розпочинається новий процес інформаційних систем. Нова дисипативна структура забезпечує стійкість системи в якісно іншому стані, на якісно новому рівні організованості.

Прогнозування, планування та визначення напрямів і засобів зміцнення стану інформаційної безпеки у зв'язку зі складністю та суперечливістю розвитку міжнародних відносин у світі не можуть здійснюватися без координації та узгодженості. Тільки синхронний розвиток усіх елементів (підсистем) системи національної безпеки забезпечить її найвищу ефективність. Взаємодоповнюваність структурно-функціональної та синергетичної методології дає цілісне уявлення про систему забезпечення інформаційної безпеки, її функціонування, взаємодію елементів і генезис. Особливо важливим є практичний вихід такого поєднання методологій на розуміння механізму забезпечення інформаційної безпеки.

На наш погляд, системний підхід при аналізі феномену інформаційної безпеки означав, що всі суспільні зв'язки і опосередковування елементи і складові суспільства й держави, функції і проблеми, котрі стосуються забезпечення інформаційної безпеки, розглядаються як взаємопов'язане ціле. Завданням системного підходу при дослідженні проблем інформаційної безпеки буде вираження на рівні спеціальної методології науки загальнонаукових принципів, положень понять, форм і методів системних досліджень, згідно з якими кожний об'єкт, що представляється як система, розглядається не тільки як певне самостійне ціле, а і як складова системи більш високого рівня організації з усіма її суттєвими взаємозв'язками з іншими об'єктами, які входять до її складу.

Сьогодні є всі підстави вважати, що застосування системного підходу дозволить установити загальну орієнтацію досліджень проблем інформаційної безпеки й зафіксувати науковими засобами цілісність, організованість об'єкта (системи, проблеми, соціального явища, процесу тощо), що досліджується, в усій його повноті та в усій багатоманітності й поліаспектності зв'язків в об'єкті.

Загалом особливості системного підходу, які відрізняють його як методологічну концепцію в соціально-філософському дослідженні інформаційно-суспільних феноменів, можна звести до таких:

— при визначенні інформаційного феномену як системи опис його елементів не є визначальним, оскільки кожен з елементів суспільної системи розглядається і аналізується не як ізольований, а з урахуванням його "місця" в цілому;

— дослідження інформаційного феномену як системи виявляється невід'ємним від дослідження його взаємозв'язків із зовнішнім середовищем, оскільки об'єкт вивчається як підсистема більшої системи, утвореної об'єднанням об'єкта із середовищем;

— специфічною особливістю є врахування нових властивостей, якостей, котрі виникають при об'єднанні елементів у систему і які не зводяться до простої суми властивостей елементів, що утворюють таку систему (емерджентність);

— між складовими інформаційного феномену як системи існують відношення взаємозалежності і взаємопідпорядкування, які виражаються в тому, що зміни або модифікація одного з цих складових (елементів) зумовлюють певні зміни усіх інших; до складу системи входять елементи, які перебувають у відношенні структурного, каузального, генетичного, функціонального та інших зв'язків;

— у системі можна виділити закономірний тип зв'язку, що утворює її структуру, яка у свою чергу, забезпечує стійкість системи і зміни, які призводять до радикального її перетворення або до зникнення.

У силу високого ступеня спільності системний підхід базуються на ряді принципів діалектики, а саме: взаємозв'язок і розвиток, залежність і незалежність (автономність), якісна відмінність частини і цілого. Однак системний підхід навіть у реалізації цих принципів вужчий, аніж діалектика. Для підтвердження цього можна вказати, зокрема, на принцип розвитку який у системному підході представлений лише через рух і зміни, тоді як принцип заперечення в розвитку, який притаманний діалектиці, конструктивно не входить у системний підхід.

Аспекти системного підходу стосовно проблеми забезпечення інформаційної безпеки у своїй єдності та взаємодії перетворюють системний підхід у ефективний засіб пізнання. Як правило, окремі аспекти при філософському аналізі інформаційної безпеки найбільш доцільно застосовувати у поєднанні, в комплексі, оскільки всебічне дослідження будь-якої системи, процесу чи проблеми може бути забезпечене тільки сукупним застосуванням усіх аспектів системного підходу.

Вираженню інтегративних властивостей і якостей системи забезпечення інформаційної безпеки у системному дослідженні служать такі поняття, як "елемент", "структура", "система", "середовище", "функції", "розвиток", "управління" тощо. Розглянемо їх методологічне значення для соціально-філософського аналізу системи забезпечення інформаційної безпеки.

Структура системи забезпечення інформаційної безпеки — це сукупність закономірних системотворчих зв'язків-відносин, яка здатна до перетворення та саморегуляції. Завдяки зв'язкам елементів утворюється цілісність і упорядкованість системи. Структура досліджуваної системи, згідно із законом існування елементів, характеризується типом суспільних відносин конкретного суспільства. Кожний вид відносин створює відносно самостійну сферу, тому можна вважати, що структура системи інформаційної безпеки — це її елементи, представлені їх функціональною властивістю.

Система інформаційної безпеки має внутрішню і зовнішню структури. Перша спрямована на збереження й зміцнення, а друга забезпечує її комунікацію із оточуючим середовищем. Перебудова структури спричиняє якісну зміну системи інформаційної безпеки, однак усі такі зміни структури здійснюються для збереження функцій, необхідних суспільству, державі й особистості. Отже, виявлення структури дає змогу зв'язати елементи систе-

ми інформаційної безпеки в цілому, визначити систему відносин між ними і такий спосіб їх взаємодії, який детермінований парадигмою суспільного розвитку.

Система інформаційної безпеки характеризується певними законами функціонування й розвитку її елементів. Вона формується, виникає та існує в процесі практичної діяльності суб'єктів і реалізуються через неї. Це дозволяє зрозуміти джерело причинних зв'язків і спрямованість процесів, які відбуваються в системі безпеки тієї чи іншої держави. У системі інформаційної безпеки виявляються як закони, притаманні їй як цілому, так і закони окремих її сфер.

Дослідження функцій системи дозволяє дати відповідь на питання: "Для чого діє та утримується державою система забезпечення інформаційної безпеки?" Функціонування даної системи — це прояв її внутрішньої активності, за якої функції елементів виступають засобом розв'язання протиріч, пристосування системи до внутрішніх змін і середовища, досягнення загальної мети системи і збереження її цілісності, забезпечення умов для її розвитку. Розуміння функцій системи інформаційної безпеки дає змогу сформулювати закони їх функціонування. Вони характеризують зміни, спрямовані на збереження динамічної тривалості системи в межах певного типу, внаслідок чого зміни в елементах системи інформаційної безпеки є завжди постійними. Однак такі зміни не виводять систему інформаційної безпеки за межі досягнутого рівня організації, не спричиняють її глобальних змін.

На певному етапі функціонування системи забезпечення інформаційної безпеки, коли закони її функціонування починають ускладнювати прояв структурних відносин, визрівають умови для переходу системи до іншого типу зв'язків, що дозволяє зберегти цілісність системи. З утворенням нових зв'язків у системі інформаційної безпеки починають виявлятися закони розвитку; розвиток системи інформаційної безпеки — це процес, що приводить систему до структури іншого рівня розвитку. Він відрізняється від функціонування системи інформаційної безпеки як простої зміни стану в рамках старої структури. Разом з тим, жорстке розмежування розвитку і функціонування є неприпустимим. Розвиток системи інформаційної безпеки відбувається в єдності протилежностей — зміни й збереження, де збереження виступає синонімом незмінності, оскільки зберігаються зміни. Тому закони функціонування й закони розвитку системи інформаційної безпеки є нерозривними.

У процесі реалізації державного управління формуванням системи інформаційної безпеки, вона стає цілісною системою, яка має нові якості, не притаманні окремим її елементам. Система забезпечення інформаційної безпеки — це діалектична єдність її елементів, які взаємодіють із середовищем і протистоять йому, пов'язаних між собою певним типом структури, що забезпечує цілісність системи інформаційної безпеки. Вони (елементи) отримують можливість виступати як ціле завдяки відтворенню своїх передумов. Але це може відбуватися тільки тоді, коли система виступає внутрішньо суперечливим утворенням. Тому система інформаційної безпеки певного типу характеризується своїм специфічним характером змін і своїм історичним часом.

ВИСНОВКИ

Підсумовуючи сказане вище, доходимо висновків, що з позицій системного підходу система забезпечення інформаційної безпеки являє собою відкриту систему зі специфічними структурними і функціональними елементами. Вона має власні внутрішні зв'язки і зв'язки з навколишнім середовищем, функціонує й розвивається під впливом численних факторів (як природних, так і соціальних).

Подальші наукові дослідження автора будуть присвячені дослідженню інформаційної безпеки у системно-функціональному вимірі.

Література:

1. Анохин П.К. Узловые вопросы функциональной системы. — М.: Наука,1980 — 196 с.

2. Дзлиев М.И. Основы обеспечения безопасности Росии: учеб. пос. // М.И. Дзлиев, А.Д. Урсул; Рос. Гос. Торгово-экон. ун-т, НИИ проблем безопасности и устойчивого развития. — М.: ЗАО "Издательство"Экономика", 2003. — 423 с.

3. Дзьобань О.П. Проблема індивідуальної та колективної безпеки у творчості Томаса Гоббса та Іммануїла Канта (філософсько-правовий аспект) / О.П. Дзьобань, Ю.С. Размєтаєва // Проблеми філософії права. — Том III. — №1—2. — Київ-Чернівці: Рута, 2005.

4. Левин А.А. Приоритетные направления деятельности государства по обеспечению информационной безопасности Российской Федерации: дисс. ... канд. полит. наук: 20.01.02. — М., 2004. — 150 с.

5. Соловьев В.С. Философские начала цельного знания /В.С. Соловьев. — Соч. У 2-х т. — Т. 2. — М.: Политиздат, 1989. — 321 с.

6. Тер-Акопов А.А. Безопасность человека. Социальные и правовые основы /А.А.Тер-Акопов. — М.: Норма, 2005. — 272 с.

References:

1. Anohin, P.K. (1980), Uzlovye voprosy funkcional'noj sistemy. [Key issues of the functional system], Nauka, Moscow Russia.

2. Dzliev, M.I. and Ursul, A.D. (2003), Osnovy obespechenija bezopasnosti Rosii: Uchebnoe posobie [Fundamentals of Russia's security: a training manual], Moscow Russia.

3. Dz'oban', O.P. and Ju.S. Razmjetajeva (2005), "The problem of individual and collective security in the work of Hobbes and Kant (philosophical and legal aspects)", Problemy filosofii' prava. Vol.1—2.

4. Levin A.A. (2004) " Priority directions of the state to ensure the information security of the Russian Federation", Abstract of Ph.D. Russian Academy of Public Service under the President of the Russian Federation of Moscow, Moscow Russia.

5. Solov'ev, V.S. (1989), Filosofskie nachala cel'nogo znanija. [Philosophical Principles of Integral Knowledge], Politizdat, Moscow Russia.

6. Ter-Akopov, A.A. (2005), Bezopasnost' cheloveka. Social'nye i pravovye osnovy. [Human security. Social and legal framework], Norma, Moscow Russia.

Стаття надійшла до редакції 17.09.2013 р.