УДК 1:316.4

Дзьобань О. П., Панфілов О. Ю., Чемчикаленко Р. А.

МЕТОДОЛОГІЧНИЙ КОНТЕКСТ ДОСЛІДЖЕННЯ ПРОБЛЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

У статті робиться спроба визначити методологічні засади щодо дослідження феномену інформаційної безпеки суспільства. Обґрунтовується доцільність застосування діалектичного, структурно-функціонального, синергетичного, системного та інших підходів у науковому пізнанні інформаційної безпеки як характеристики стану соціуму

***Ключові слова**: інформаційна безпека, система інформаційної безпеки, методологічна концепція, системний підхід, принцип взаємодоповнюваності методів.*

Постановка проблеми. 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 нового узагальненого знання про предмет. У розв'язанні практичних завдань стосовно функціонування тих чи інших сфер безпеки суспільства необхідно використовувати конкретні методологічні принципи дослідження, які є універсальними для наукового пізнання усіх предметних сторін об'єкта – суспільно-політичних процесів, які віддзеркалюють розвиток і стан інформаційної безпеки.

Для визначення провідних тенденцій у розвитку інформаційної безпеки в умовах глобалізації необхідно визначити рівень культурно-політичної організації нації в конкретний історичний момент, у певних соціокультурних умовах, апелюючи при цьому і до історичного минулого, порівнюючи з ним сьогоднішню ситуацію в різноманітних сферах соціального життя. Необхідним у даному контексті є встановлення діалектичного взаємозв'язку між чинниками, які визначають безпеку особи, суспільства й держави, виявлення ступеня їх стійкості й варіативності під впливом динамічних змін соціокультурного середовища.

Більш того, інформаційна безпека є складною категорією і не може бути вичерпно проаналізована тільки під кутом одного методологічного підходу. Різноманіття концепцій, що пояснюють природу і сутність інформаційної безпеки, доводить, що інформаційна безпека є складною багаторівневою функціональною системою. Основними структурними елементами системи інформаційної безпеки є особа, суспільство і держава, їх життєво важливі інтереси, загрози в інформаційній сфері. Отже, пошук різних методологічних підходів, що будуть доповнювати один одного, дозволить поглянути на проблему інформаційної безпеки комплексно, розкрити усі змістовні складові даного явища.

Аналіз останніх досліджень. Проблема інформаційної безпеки є предметом дослідження багатьох вчених, спеціальних інститутів та центрів, що представляють різні наукові галузі знання, причому як гуманітарні, так і технічні. За останні роки у вітчизняній та зарубіжній науці в цілому накопичено потенціал для поглибленого дослідження проблеми інформаційної безпеки.

Зокрема, характеристикам інформатизації як об'єктивної закономірності розвитку суспільства, проблемам становлення інформаційної цивілізації та прогнозам її розвитку, технічним й гуманітарним фактори цього процесу присвячені праці Д. Белла, Зб. Бжезинського, Е. Дайсона, М. Кастельса, Й. Масуди, А. Мінка, Дж. Нейсбіта, Е. Паркера, Е. Тоффлера, Р. Абдєєва, В. Афанасьєва, Т. Березі, В. Глушкова, В. Лекторського, В. Лисицького, Е. Моргунова, Б. Парахонського, Г. Почепцова, А. Ракітова та інших.

Дослідженням сутнісних та змістовних основ інформаційної безпеки присвячені праці Е. Бєляєва, М. Бусленка, С. Гриняєва, О. Данильяна, О. Дзьобаня, Г. Ємельянова, В. Лопатіна, О. Позднякова, Л. Сергієнка, В. Циганкова, М. Чеснокова та інших дослідників. Однак, незважаючи на те, що існує велика кількість наукових праць з проблем інформаційної безпеки, варто підкреслити той факт, що їхній зміст часто має полемічний характер, сутність інформаційної безпеки та підходи до її дослідження надано у фрагментарному вигляді, а комплексний методологічний підхід до дослідження даного явища практично відсутній.

Метою статті є спроба визначання основних методологічних підходів у дослідженні феномену інформаційної безпеки.

Основні результати дослідження. Інформаційна безпека розуміється у даній статті як стан захищеності життєво важливих інтересів людини, суспільства і держави в інформаційній сфері від зовнішніх та внутрішніх викликів і загроз, що забезпечує їхній 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 й рухи, соціальні групи, індивіди, котрі спонукаються економічними й соціально-політичними потребами, інтересами і цілями. Така обставина передбачає розкриття наявних зв'язків серед суб'єктів і об'єктів безпеки, їхніх інтересів, а також тенденцій і закономірностей їхнього розвитку.

Виходячи з цього, на нашу думку, інформаційна безпека може бути досліджена в межах діалектичного, структурно-функціонального, синергетичного, системного та інших підходів. Охарактеризуємо їх докладніше.

Основи структурно-функціонального аналізу були закладені Т. Парсонсом, Р. Мертоном, їх учнями й послідовниками. Згідно з даним підходом (якщо інтерпретувати його основні положення до контексту даної проблеми) систему забезпечення інформаційної безпеки будь-якої держави можна розглядати як функціональну систему [1]. Вперше поняття «функціональна система» у вітчизняній науці було сформульоване П. Анохіним, який під цим поняттям розумів уявлення про динамічні саморегулятивні організації, діяльність яких спрямована на забезпечення корисних для існування самих систем і організацій, до яких вони входять як складові, результатів більш високого рівня [2, с. 67; 3, с. 32]. П. Анохін зазначав, що жодна організація, якою б просторою вона не була за кількістю елементів, що її складають, не може бути названа самокерованою, саморегульованою системою, якщо її функціонування, тобто взаємодія частин цієї організації, не закінчується якимось корисним для системи результатом і якщо буде відсутня зворотна інформація в керуючий центр про ступінь корисності цього результату. Він також стверджує, що системою можна назвати тільки комплекс таких вибірково втягнутих компонентів, у яких взаємодія і взаємовідносини набувають характеру взаємодії компонентів для отримання фокусованого корисного результату [2 с. 107; 3 с. 74]. Погоджуючись з думкою К. Судакова [4, с. 73–78], можна стверджувати, що система інформаційної безпеки, як і будь-яка функціональна система будується на основі таких принципів: результат діяльності як провідний, системотворчий чинник; саморегуляція як загальний принцип організації функціональних систем; виборча мобілізація окремих органів і закладів в цілісну організацію функціональної системи, взаємодія окремих елементів для досягнення кінцевих результатів діяльності системи; ієрархія функціональних систем; мультипараметрична взаємодія функціональних систем за кінцевими результатами; системогенез – виборче формування функціональних систем у процесі онтогенетичного розвитку соціуму.

Провідним системотворчим чинником, що організує функціональну систему будь-якого рівня складності, є корисний для системи та соціуму в цілому результат. Саме кінцевий результат діяльності визначає конфігурацію тієї чи іншої функціональної системи.

Онтологічна різноманітність соціуму визначає численні функціональні системи, що складають різні аспекти життя суспільства як складної функціональної системи. Одні функціональні системи генетично детерміновані, інші зумовлюються мірою розвитку соціуму, мірою його просування шляхом соціального прогресу. Кожна функціональна система будується на основі принципу саморегуляції: відхилення результату діяльності системи від рівня, що забезпечує нормальну життєдіяльність соціуму, обов'язково спричиняє ланцюг процесів, спрямованих на відновлення оптимального рівня цього результату [90, с. 27-33]. Завдяки динамічній саморегулятивній діяльності різні функціональні системи визначають необхідну для нормальної життєдіяльності соціуму тривалість суспільних процесів.

Процес саморегуляції системи інформаційної безпеки може розглядатися в різних аспектах. Якщо розглядати його з точки зору управління даною системою, то доцільно погодитися з точкою зору М. Требіна стосовно важливості аналізу ініціативи та ретельності в діяльності керівних державних кадрів при функціонуванні системи [5]. При аналізі саморегулятивної діяльності системи інформаційної безпеки слід виходити з того, що межі цієї саморегуляції задаються суспільством. Саморегуляція необхідна даній системі при організації своєї життєдіяльності, структуруванні сил і засобів для вирішення завдань, що перед нею ставить соціум.

Домінування функціональних систем у соціумі визначається їх суспільною значущістю. Відповідно до кожної домінуючої в певному ієрархічному порядку вибудовуються всі інші функціональні системи. Мультипараметричний принцип взаємодії різних функціональних систем визначає їх узагальнену діяльність. Як правило, зміна одного показника результату діяльності однієї функціональної системи в соціумі негайно відбивається на результатах діяльності інших.

Для функціональних систем багатозв'язкового регулювання (а система 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 всіх інших параметрів результату їх показників [6; 7]. Суспільство як цілісний організм у кожний момент часу являє собою взаємодію – інтеграцію (по горизонталі і вертикалі) – різних функціональних систем, які визначають його нормальне функціонування. Якщо порівнювати функціональні системи

різного класу, що діють в межах соціуму, можна виділити їх спільні властивості: тривалість результату їх діяльності, що досягається відповідними механізмами саморегуляції; постійну оцінку досягнутого результату системою; наявність великої кількості виконавчих механізмів активного впливу на результат; взаємодію окремих елементів системи з досягнення корисного для неї результату; загальну функціональну архітектоніку [1]. Це все стосується і системи інформаційної безпеки держави.

На нашу думку, відповідно до принципу взаємодоповнюваності методів, краще зрозуміти процеси, які 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 до сфери безпеки синергетичну парадигму можна представити такою проблематикою: неврівноваженість і нестійкість як загальний стан компонентів системи (армії, міліції, інших військових формувань тощо); врівноваженість і тривалість як тупик еволюції і окремий випадок загального стану системи; роль випадковості в загальному ході подій; роль одиничного впливу на хід природних подій, що відбуваються в суспільних структурах; відкритість системи, обмін інформацією з соціумом в кожній її точці (за винятком сфери державної таємниці); нелінійність розвитку; вибір напряму розвитку; альтернативність напрямів розвитку як загальний принцип; власні тенденції розвитку системи безпеки як самоорганізованої системи; керований розвиток в умовах самоорганізації.

Розвиток системи інформаційної безпеки, який відбувається внаслідок внутрішньої взаємодії її підсистем та елементів, пов'язаний з упорядкованістю або дезорганізацією внаслідок внутрішніх процесів і активного впливу суспільного оточення, що призводить до зміни структури й функцій елементів системи. Отже, причина розвитку системи інформаційної безпеки багато в чому пов'язана із саморозвитком суспільства. Сутність цього явища полягає в тому, що зміна функцій елементів, яка відбувається в результаті флуктуацій різної природи, спричиняє зміну функцій системи та її структури. Перебудова структури обумовлює нову зміну функцій елементів. Кожний з них починає характеризуватися функціями, не притаманними їм раніше. Структура, поєднавши елементи системи безпеки, стає джерелом нових способів і форм реалізації її функцій. З іншого боку, оскільки система інформаційної безпеки характеризується достатньо конкретними функціями, структура постійно перебудовується для їх збереження. Отже, якісні зміни в функціях вказують на зміну типу структурних взаємовідносин в системі. Тому нова структура і функції – це продукт розвитку системи, а не її функціонування. Зміст саморозвитку – це істотні зміни стану системи безпеки, що призводять до заміни елементів, змін її устрою і форм функціонування.

Для розвитку системи інформаційної безпеки характерними є два взаємопов'язані 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 структури дають початок новому цілому. Вони є вторинними по відношенню до колишнього складу елементів і структур, є їх продуктом і стають первинними відносно нових процесів і явищ.

Тимчасове порушення цілісності, що виникає, нестійкість системи безпеки відбувається у певних точках біфуркації, які виникають під впливом нелінійних процесів, що трапляються як у соціумі, так і в самій системі та її окремих елементах. Усе це супроводжується певними змінами, які охоплюють окремі сфери чи 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 розвитку системи безпеки. Нова дисипативна структура забезпечує стійкість системи безпеки в якісно іншому стані, на якісно новому рівні організованості.

Історія розвитку систем безпеки різних рівнів і ступенів складності являє собою процес розвитку засобів, техніки, науки, персоналу, управління й зміни взаємозв'язків між ними. Це вказує на те, що система інформаційної безпеки існує не лише як певний тип, рід чи вид, але й як історична реальність, що поєднує в собі всі досягнення суспільного розвитку. Весь цикл розвитку системи безпеки складається з певних стадій – виникнення, становлення, зрілість і перетворення. Причому на кожній з них дану систему можна розглядати як систему, що постійно розвивається.

Розвиток систем інформаційної безпеки характеризується єдністю минулого, сучасного й майбутнього. Тому його аналіз включає генетичний і прогностичний аспекти. Перший аспект припускає аналіз розвитку системи безпеки до нинішнього часу. На цьому етапі з'ясовуються: історія виникнення даної системи, її сутність, процес становлення, зміна функцій, що являє собою система в розвиненому стані тощо. Другий аспект включає розгляд перспектив подальшого розвитку системи та очікуваного функціонування. Він базується на розумінні тенденцій минулого, законів нинішнього, що дає основу для прогнозування майбутнього. Разом з тим і майбутній стан системи інформаційної безпеки

перехідних соціальних систем важко передбачити. Спектр можливих напрямів подальшого їх розвитку задається самою її природою, яка зазнає еволюції, і характером зовнішнього середовища. Іншими словами, він визначається біфуркацією – розгалуженням старої якості на кінцеву множину цілком певних потенційно нових якостей. Це так звана нелінійність першого порядку, що надає процесу самоорганізації з самого початку неоднозначного (стохастичного) характеру. Перехід системи безпеки від одного стану до іншого вимагає вибору з безлічі можливих нових структур лише однієї. Тому на місце традиційного динамічного детермінізму приходить «стохастичний», або ймовірний детермінізм (ланцюжок біфуркацій та послідовність актів вибору). Ланцюжок біфуркацій може не лише відвести систему інформаційної безпеки від первісного стану, але й повернути її в цей стан. Для такої системи як конкретної системи, що взаємодіє з конкретним середовищем, існує свій атрактор – граничний стан, досягнувши якого, вона вже не може повернутися в жоден з колишніх станів [8; 9; 10].

З точки зору синергетики, досвід історії розвитку різноманітних систем безпеки свідчить про те, що роль спонукальної сили, відповідальної за самоорганізацію цілісної системи, відіграє спеціальний відбір. Щоб визначити, яким чином це досягається, є сенс дослідити основні чинники відбору: тезаурус, детектор і селектор. Тезаурус складає безліч можливих дисипативних структур, які виникають потенційно в надрах актуально існуючої структури як результат відповідної біфуркації. У ролі детектора, що обирає з тезаурусу певну біфуркаційну структуру і завдяки цьому перетворює її з імовірної в дійсну, виступає внутрішня взаємодія елементів системи безпеки. При цьому важливо звернути увагу на його подвійний (суперечливий) характер: це не просто конкуренція (боротьба) протидіючих один одному елементів, але й кооперація елементів, що сприяють один одному в цій боротьбі. Закон відносин внутрішньої взаємодії в системі безпеки з її зовнішньою взаємодією з середовищем визначає той принцип стійкості, на підставі якого детектор повинен обирати з безлічі можливих біфуркаційних структур найбільш стійку в даному середовищі [9; 11]. Цей принцип залежатиме від специфічного відношення внутрішньої взаємодії в системі безпеки до характеру оточуючого середовища. Один і той же детектор при різних зовнішніх умовах може «користуватися» різними селекторами. Таким чином, тільки взаємодія всіх трьох факторів – тезаурусу, детектора й селектора – робить зрозумілою творчу силу спеціального відбору та його спроможність (здебільшого феноменальну) кардинально впливати на інформаційну безпеку. Ця спроможність виявляється в нелінійності другого порядку – диспропорційності наслідку і причини (на відміну від лінійних процесів, для яких характерна пропорційність наслідку причині).

В контексті проблем інформаційної безпеки виникає важливе питання: чи існує зворотний зв'язок між результатами відбору та його факторами? Всупереч діалектиці Георга Гегеля, синергетика дає на це питання позитивну відповідь. Справа в тому, що окрім відбору існує ще супервідбір, тобто відбір самих факторів відбору. В цьому виявляється нелінійність третього порядку (спроможність самоорганізованої системи до самодії). Щоб зробити відбір більш конструктивним, треба зробити його більш радикальним (сміливим), а для цього – створити істотно новий тезаурус. Однак створити останній можна лише створюючи новий хаос. Таким чином, використання синергетичного підходу до аналізу системи інформаційної безпеки дозволяє дещо інакше уявити процес її розвитку й саморозвитку, її можливу подальшу перспективу.

Прогнозування, планування та визначення напрямів і засобів зміцнення інформаційної безпеки у сучасних умовах 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 інформаційної безпеки забезпечить її найвищу ефективність. Взаємодоповнюваність структурно-функціональної та синергетичної методології дає цілісне уявлення про сутність інформаційної безпеки, її функціонування, взаємодію елементів і генезис. Є всі підстави стверджувати, що при аналізі процесів, що відбуваються в системі інформаційного безпеки, доцільно використовувати методологію системного дослідження, розроблену У. Баклі, К. Белі, Н. Луманом та ін. [12; 13; 14]. Якщо взяти до уваги, що Н. Луман розуміє суспільство як «всеосяжну соціальну систему, що включає всі інші соціетальні системи» [14, с. 126], то як одну з соціетальних систем можна розглядати й систему інформаційної безпеки.

Прикметник «системний» стосовно цілого ряду понять (метод, дослідження, особливість, модель тощо) означає в даному контексті урахування в даних поняттях принципів системного підходу.

Сутність системних досліджень в рамках філософського аналізу інформаційної безпеки полягає в використанні фундаментального методологічного поняття системи як єдиного абстрактного образу конкретних складових суспільства, у виділенні провідних, визначальних сторін (аспектів), тенденцій та протиріч розвитку системи, у представленні проблеми, що вирішується, як своєрідної концептуальної системи.

На нашу думку можна стверджувати, що системний підхід при філософському аналізі феномена інформаційної безпеки – це підхід, при якому всі суспільні зв'язки і опосередковування, елементи і складові суспільства й держави, функції і проблеми стосовно забезпечення інформаційної безпеки розглядаються у вигляді взаємопов'язаного цілого. Завданням системного підходу при дослідженнях 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 (суспільне утворення, суспільний інститут тощо), що представляється як система, розглядається не тільки як деяке самостійне ціле, а також і як складова системи більш високого рівня організації з усіма її суттєвими взаємозв'язками з іншими об'єктами, які входять до складу цієї більш складної системи [15].

Сьогодні є всі підстави вважати, що застосування системного підходу дозволить встановити загальну орієнтацію філософських досліджень суспільства як системи, держави, проблем інформаційної безпеки і зафіксувати науковими засобами цілісність, організованість об'єкта (системи, проблеми, соціального явища, процесу тощо), що досліджується, в усій його повноті і в усій багатоманітності й поліаспектності зв'язків в об'єкті. Тут, очевидно, доцільно вказати на розбіжності системного і комплексного підходів до розгляду об'єкта дослідження, які досить часто ототожнюються в науковій літературі завдяки перекладу з латини слова «комплексний» (complexus – зв'язок, поєднання).

Комплексний підхід – це підхід, який передбачає одночасне урахування всіх аспектів, особливостей і факторів, які прямо чи опосередковано впливають на вирішення проблеми, але не такий, що випливає безпосередньо з ідеї їх взаємопов'язаного єдиного цілого. Комплексний підхід у філософському аналізі інформаційної безпеки як складної багаторівневої системи означає всебічне вивчення об'єкта або проблеми у тісній взаємодії із найрізноманітнішими науками і науковими напрямками, із залученням різноманітних наукових теорій і методів. Сама по собі комплексність недостатня для виявлення повноти картини суспільного утворення чи явища, її обов'язково повинна доповнювати системність [1; 14; 16].

Системний підхід в аналізі інформаційної безпеки є своєрідним розвитком комплексного підходу, оскільки при ньому більш глибоко, більш точно відображаються внутрішні і суттєві зв'язки й відношення компонентів суспільної системи, закономірності її функціонування, що є основою створення більш повної теорії об'єкта, що досліджується. Поняття «системність» у деякому смислі ширше, глибше, аніж «комплексність». Воно охоплює зв'язки всередині одного рівня (горизонтальні) і між різними рівнями (вертикальні), в той час як поняття «комплексність» охоплює переважно зв'язки одного або суміжних рівнів ієрархічної структури системи.

В цілому особливості системного підходу, які відрізняють його як методологічну концепцію в дослідженні суспільних феноменів, можна звести до наступних:

- при визначенні суспільного утворення (об'єкта, феномена) як системи опис його елементів не є визначним, оскільки кожний із елементів суспільної системи розглядається і аналізується не як ізольований, а з урахуванням його «місця» в цілому;
- дослідження суспільного утворення (об'єкта, феномена) як системи виявляється невід'ємним від дослідження його взаємозв'язків із зовнішнім середовищем, оскільки об'єкт вивчається як підсистема більш крупної системи, утвореної об'єднанням об'єкта із середовищем;
- специфічною особливістю є урахування нових властивостей, якостей, які виникають при об'єднанні елементів у систему і які не зводяться до простої суми властивостей елементів, що утворюють таку систему (емерджентність);
- між складовими (елементами) суспільного феномена 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 знаходяться у відношенні структурного, каузального, генетичного, функціонального та інших зв'язків;
- у системі можна виділити закономірний тип зв'язку, що утворює її структуру, яка, в свою чергу, забезпечує стійкість системи і зміни якої призводять до радикального її перетворення або до зникнення, причому ці зв'язки не дані безпосередньо, явно, а відкриваються за допомогою особливих епістемологічних процедур.

В силу високого ступеня спільності системний підхід базується на ряді принципів діалектики, таких, як взаємозв'язок і розвиток, залежність і незалежність (автономність), якісна відмінність частки і цілого. Однак, системний підхід навіть в реалізації цих принципів вужчий, аніж діалектика. Для підтвердження цього можна вказати, зокрема, на принцип розвитку, який у системному підході пред-

ставлений лише через рух і зміни, в той час як принцип заперечення в розвитку, який притаманний діалектиці, конструктивно не входить у системний підхід.

Другим принципом є принцип кінцевої мети: абсолютний пріоритет кінцевої (глобальної) мети. Це означає, що все повинно бути підкорене глобальній меті (основній функції, основному призначенню) цілеспрямованої суспільної системи. Будь-яка спроба змін, удосконалення і управління у такій системі повинна оцінюватись з точки зору того, допомагає чи зашкоджує вона досягненню кінцевої мети. Це покладає особливу відповідальність на вибір мети і її чітке тлумачення. Розпливчаті, не повністю визначені кінцеві цілі тягнуть за собою неясності в структурі і управлінні соціальною системою, далеко не сприяють забезпеченню її безпеки. Крім того, нехтування цим принципом призводить до досить суттєвих негативних наслідків у суспільстві (перебудова, «рішуча» боротьба з пияцтвом і алкоголізмом, непродумана приватизація, конверсія тощо).

Наступний принцип – це принцип ієрархічності пізнання, який вимагає багаторівневого (а саме трьохрівневого) вивчення об'єкта дослідження: вивчення самого об'єкта – «власний» рівень; вивчення цього ж об'єкта як елемента більш широкої системи – «зовнішній» рівень, і, в кінці кінців, вивчення вказаного об'єкта у співвідношенні із компонентами, що утворюють даний об'єкт – «нижній» рівень. Принцип ієрархічності досить ефективний як при філософській рефлексії інформаційної безпеки держави в цілому, так і її окремих складових (політичної, економічної, воєнної, демографічної, духовної, правової тощо).

Ще одним принципом – принципом інтеграції – віддзеркалюється та особливість системного підходу, що він спрямований на вивчення інтегративних властивостей і закономірностей соціальних систем, розкриття базисних механізмів інтеграції цілого.

Важливим принципом системного підходу при аналізі соціальних систем, зокрема інформаційної безпеки та її складових, є принцип функціональності: спільний розгляд структури безпеки та її функцій з пріоритетом функцій над структурою. Згідно з цим принципом будь-яка структура суспільного утворення тісно пов'язана з функціями системи і її складових і досліджувати (створювати, реформувати) структуру необхідно після усвідомлення її функцій в системі. На практиці принцип функціональності, зокрема, означає, що у випадку надання системі інформаційної безпеки нових функцій корисно переглянути її структуру, а не пробувати втиснути нову функцію в стару систему.

Таким чином, на нашу думку, основні проблеми системного підходу, як свідчить практика й аналіз наукової літератури, пов'язані з розвитком методів практичної реалізації вказаних принципів і, зокрема, виявленням законів об'єднання частин в ціле, законів, які визначають характер структури, функціонування і розвитку, зв'язку з умовами і середовищем функціонування, граничних характеристик систем; з розробкою змістовних і формальних засобів представлення суспільних утворень як систем; з дослідженням методологічного підґрунтя різноманітних системних теорій.

Всебічне вивчення соціальної системи будь-якого рівня організації (особливо з точки зору її інформаційної безпеки) передбачає встановлення складу її компонентів, структури і функцій як системи в цілому, так і її складових, а також факторів, які забезпечують цілісність і відносну самостійність системи. Відповідно до цього наукова література виділяє системно-компонентний, системно-структурний, системно-функціональний та системно-інтегративний аспекти, які повною мірою можливо і доцільно застосовувати при аналізі суспільних утворень (систем) з точки зору забезпечення їх безпеки [6; 17].

Системно-компонентний аспект системного підходу передбачає вивчення елементного складу соціальної системи та її безпеки як початковий етап її дослідження. Він пов'язаний з пошуком відповіді на питання про те, з чого, з яких компонентів утворене ціле. При цьому вважається, що компоненти суспільної системи – це ті структурні одиниці, взаємодія яких забезпечує притаманні системі якісні особливості.

На наш погляд компоненти системи забезпечення інформаційної безпеки можуть різними способами пов'язуватись в ціле. А саме відповідь на питання про те, як утворені ці зв'язки, тобто відповідь на питання про структуру системи інформаційної безпеки може дати системно-структурний аспект системного підходу. Для здійснення цього, очевидно, необхідно передбачити вивчення різнотипних зв'язків, що об'єднують складові елементи у систему. Структура безпеки як системи відіграє визначну роль у даному контексті. Вона пов'язує компоненти, надаючи системі інформаційної безпеки деяку досить певну визначеність, цілісність, зумовлює виникнення нових властивостей і якостей, не притаманних жодному з її компонентів окремо [15].

Особливо велике значення для збереження основ інформаційної безпеки як системи має відносна її самостійність, стійкість структури, причому як на рівні вертикальних зв'язків (система державного управління від президента до місцевих органів влади, включаючи як законодавчу, так і виконав-

чу гілки), так і на рівні зв'язків горизонтальних (система взаємовідносин між елементами суспільства: соціальними інститутами, колективами тощо). Без стійких зв'язків, взаємодії компонентів, тобто без структури, інформаційна безпека соціальної системи, очевидно, перестає існувати як конкретне ціле.

Третім, важливим аспектом системного підходу при аналізі сутності інформаційної безпеки є системно-функціональний аспект. У науковій літературі він зазвичай пов'язується з аналізом поведінки окремих складових системи і розглядом функціонування системи в цілому. Система забезпечення безпеки держави, як і кожна реальна система, виконує певні функції, які являють собою інтегративний результат функціонування складових компонентів. Функції компонентів по відношенню до системи повинні носити доцільний характер, інакше даний компонент може випасти із системи, стати для неї чужорідним елементом. Функції складових компонентів системи забезпечення інформаційної безпеки, очевидно, повинні узгоджуватись в часі і просторі і у випадку життєздатної соціальної системи є переважно результатом впливу на них загальносистемних (загальносуспільних) функцій.

Одним із кардинальних аспектів системного підходу сучасна наукова література виділяє питання про фактори системності, тобто про ті механізми, які забезпечують збереження якісної специфіки системи. Найбільш загальним, універсальним підґрунтям системності з точки зору філософії є матеріальна єдність світу і притаманні дійсності діалектичні принципи взаємозв'язку і руху. Разом з тим, у різних сферах дійсності і в кожному конкретному типі систем ці принципи набувають специфічних форм. Особливо це стосується безпеки суспільства (держави) як особливого різновиду складних, багаторівневих систем.

Розглянуті аспекти системного підходу стосовно проблеми дослідження інформаційної безпеки як системи у своїй єдності і взаємодії перетворюють системний підхід у ефективний засіб пізнання. Як правило, описані вище аспекти при науковому аналізі безпеки як системи 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 [7; 15; 17].

На сучасному етапі розвитку світової наукової думки системний підхід розвивається, головним чином, у напрямку розширення і розгалуження його додатків, тобто застосування його для розв'язання конкретних теоретичних і практичних проблем у різних галузях науки, техніки, управління соціально-економічними та політичними процесами тощо. Сьогодні системний підхід дозволяє органічно поєднувати аналіз і синтез, кількісне і якісне в дослідженні різноманітних субстанцій, об'єктів, процесів та соціальних феноменів, що, в свою чергу, відкриває надзвичайно широкі можливості для застосування евристичних, логіко-математичних та багатьох інших методів при вивченні і аналізі сучасних соціальних систем та методів і способів забезпечення їх стійкості, стабільності й безпеки.

Системний підхід нерозривно взаємопов'язаний з принципом діалектичної взаємообумовленості, який передбачає розгляд соціальних феноменів в їх цілісності й розвитку. Даний принцип стосовно методології безпеки всебічно й глибоко опрацювали російські дослідники М. Моісеєв, М. Михалка [18; 19]. В їхніх працях міститься обґрунтування вимог до духовного світу особистості, необхідності цілепокладення в діяльності людини стосовно безпеки, концепції керованого розвитку та кооперативної взаємодії в контексті безпеки.

Поряд з принципом діалектичної взаємообумовленості доцільно застосовувати принцип доповнюваності, оскільки при дослідженні проблем інформаційної безпеки у перехідних умовах часто виникають проблеми інтерпретації фактів, гносеологічні труднощі співвіднесення дискретного й безперервного. Даний принцип свого часу розробив Нільс Бор стосовно атомної фізики. Зміст ідеї доповнюваності знаходить своє застосування у найрізноманітніших галузях наукового знання. В ній міститься важливий момент і для розуміння об'єкта безпеки, який полягає в ствердженні того, що висновки про особливості буття об'єкта залежать від умов і способів наукового дослідження. Даний аспект концепції доповнюваності Н. Бора необхідно враховувати при виявленні найвпливовіших факторів, які впливають на безпеку різних сферах життєдіяльності.

Положення теорії доповнюваності про можливість опису й інтерпретації соціального чи природного явища за допомогою різних мов також є важливим для аналізу процесів у сфері інформаційної безпеки (логічний, математичний та ін. описи). Особливо важливим тут є ствердження російського дослідника М. Моісеєва (послідовника й інтерпретатора думок Н. Бора стосовно соціальної реальності) про те, що жодне складне явище неможливо описати за допомогою однієї мови [19; 20], оскільки теорія безпеки – міждисциплінарна галузь знань, яка базується і на суспільствознавстві, і на природознавстві.

Принцип доповнюваності реалізується в дослідженні інформаційної безпеки не тільки в загальнотеоретичному, а й у прикладному сенсі; не тільки для опису й пояснення доповнюваності сфер і видів безпеки, а й для отримання нового знання, яке має значно наближатися до адекватної рефлексії об'єктивного стану речей. Важливість застосування принципу доповнюваності підтверджується ще й тим, що система забезпечення інформаційної безпеки (особливо в перехідних умовах) складається з численних підсистем, які постійно змінюються як за складом, так і за кількістю і вимагають самостійного аналізу. Виникає необхідність інтегрувати показники безпеки на різних її рівнях і в різних сферах життєдіяльності суспільства, синтезувати узагальнені критерії безпеки, що є можливим лише на основі принципу доповнюваності знання.

Інформаційна безпека є тим об'єктом наукового дослідження, де очевидним є широке застосування діалектичної методології. Органічним є застосування закону єдності й боротьби протилежностей, який представлений у даному контексті як своєрідне відношення доповнюваності, що пронизує усі сфери людської життєдіяльності. Таким же органічним є розуміння боротьби протилежностей як основи розвитку об'єкта дослідження. Стосовно співвідношення стійкого розвитку нації [21, с. 33] з її безпекою важливим є не аморфний розвиток «сам по собі», а спрямованість і динаміка розвитку. Так же важливою є не безпека «сама по собі», а як умова стійкого розвитку і досягнення національних цілей.

Стійкий розвиток нації і міжнародної спільноти обов'язково передбачає створення безпечних умов життєдіяльності у планетарному масштабі. Інтерпретація соціального розвитку у виді діалектичного процесу сприяє відшуканню тих протилежних сторін об'єкта дослідження, або, при конкретному аналізі, ті соціальні інтереси, які вступають у протиріччя з національними інтересами і тим самим негативно впливають на інформаційну безпеку, гальмують розвиток.

Діалектика соціального розвитку в перехідних умовах є такою, що в процесі інтенсивної взаємодії дві форми розвитку, кількісна й якісна, являються нам у діалектичній єдності. Під впливом соціальних факторів відбувається динамічне повторення кількісних змін безпеки життєдіяльності в якісні. Механізм такого переходу також пов'язаний з реалізацією ідей доповнюваності, як одного з основних принципів наукового пізнання інформаційної безпеки. Діалектичні зміни у парадигмі інформаційної безпеки є завжди відображення протиріччя старого й нового. Поза розв'язанням цього протиріччя передусім у свідомості немає й розвитку безпечних умов життєдіяльності й розвитку.

В цілому аналіз різноманітних методологічних підходів до розгляду забезпечення інформаційної безпеки зокрема як особливого соціокультурного феномена дозволяє краще визначити особливості та функції даної системи, осмислити принципи її життєдіяльності в умовах соціальних трансформацій. Однак максимальній ефективності реалізації описаних методів у практиці життєдіяльності перехідних суспільств сприятиме співставлення сучасних підходів до розуміння даного феномена з класичними, які є дійсним теоретичним підґрунтям усвідомлення даної проблематики. Таке співставлення дає можливість визначити сутність основних джерел загроз і факторів впливу на стан інформаційної безпеки опрацювати найоптимальніші шляхи й напрямки забезпечення інформаційної безпеки в сучасних суспільствах перехідного типу.

Висновки: Результати проведеного аналізу надають підстав стверджувати, що системний підхід у дозволяє:

- розвинути, специфічно інтерпретувати абстрактні принципи та категорії філософії і безпосередньо застосувати їх для аналізу інформаційної безпеки суспільства;
- виявити недоліки в системі наявних знань про інформаційну безпеку, визначити новий підхід до її розгляду як цілісного об'єкта;
- розгорнути проблему інформаційної безпеки в формі системи понять і методів дослідження.

Таким чином, успіхи пізнання пов'язані не з описом елементів системи інформаційної безпеки, а з відкриттям в них специфічних якостей, які роблять їх цілим. Отже, предметом системного дослідження інформаційної безпеки виступає виявлення типів зв'язків і, передусім, системотворчих зв'язків цілісності, виокремлення об'єктивної структури даного системного утворення та її характеру. Такий підхід дає значно більше можливостей і для пошуку внутрішніх механізмів зміни й діяльності системи безпеки, аніж її опис та «розклад» на складові елементи.

Література

1. Парсонс Т. Функциональная теория изменения / Т. Прасонс // Американская социологическая мысль : Тексты / [под ред. В. И. Добренькова]. – М. : Изд-во МГУ, 1994. – С. 464–480.
2. Анохин П. К. Узловые вопросы функциональной системы / П. К. Анохин. – М. : Наука, 1980. – 198 с.

3. Анохин П. К. Философские аспекты теории функциональной системы / П. К. Анохин. – М. : Наука, 1978. – 128 с.
4. Судаков К В. Функциональная система / К. В. Судаков // Вопросы философии. – 1984. – № 10. – С. 73–78.
5. Требін М. П. Армія та суспільство: соціально філософський аналіз взаємодії в умовах трансформації: Монографія / М. П. Требін. – Х. : Видавничий Дім «ІНЖЕК», 2004. – 404 с.
6. Богданович В. Ю. Методологические основы системных исследований проблем военной безопасности и государства / В. Ю. Богданович, А. Я. Маначинский. – К. : НІСД, 2001. – 172 с.
7. Волкова В. И. Основы теории систем и системного анализа / В. И. Волкова, А. А. Денисов – СПб. : ГТУ, 1999. – 510 с.
8. Бранский В. П. Теоретические основания социальной синергетики / В. П. Бранский // Вопросы философии. – 2000. – № 4. – С. 112–129.
9. Василькова В. В. Порядок и хаос в развитии социальных систем: Синергетика и теория социальной самоорганизации / В. В. Василькова – СПб. : Лань, 1999. – 480 с.
10. Делокаров К. Х. Системная парадигма современной науки и синергетика / К. Х. Делокаров // Общественные науки и современность. – 2000. – № 6. – С. 110–118.
11. Ліпкан В. А. Національна безпека України: нормативно-правові аспекти забезпечення : монографія / А. А. Липкан. – К. : Текст, 2003. – 180 с.
12. Buckley W. Sociology and Modern Systems Theory / W. Buckley. – Englewood Cliffs, N. J. : Prentice-Hall, 1967. – 624 p.
13. Bailey K. D. Sociology and the New Systems Theory: Toward a Theoretical Synthesis / K. D. Bailey. – Albany. State University of New York Press, 1994. – 568 p.
14. Luhmann N. Social Systems: Outline of a General Theory. – Stanford, Calif : Stanford University Press, 1995. – 492 p.
15. Дзьобань О. П. До питання про застосування системного підходу у соціально-філософському аналізі національної безпеки держави / О. П. Дзьобань, В. О. Чернієнко // Наукові записки Харківського військового університету. Соціальна філософія, педагогіка, психологія. – Х. : ХВУ, 2002.– Вип. XIV. – С. 75–82.
16. Systems and «Systems theory [Електроний ресурс]. – Режим доступу: http://www.outbacksoftware.com/.
17. Берталанфи Л. фон. История и статус общей теории систем / Л. Берталанафи // Системное исследование. Ежегодник – М. : Наука, 1973. – С. 20–36.
18. Михалка М. Концепции кооперативной безопасности / М. Михалка // Вестник Московского университета. – Серия 18 : «Социология и политология». – 2001. – № 1. – С. 104–119.
19. Моисеев Н. Н. Еще раз о проблеме коэволюции / Н. Н. Моисеев // Вопросы философии. – 1998. – № 8. – С. 26–32.
20. Моисеев Н. Информационное общество как этап новейшей истории / Н. Моисеев // Свободная мисль. – 1996. – № 1. – С. 76–82.
21. Романович А. Л. Проблема безопасности в контексте устойчивого развития / А. Л. Романович // Социально-гуманитарные знания. – 2003. – № 1. – С. 3–18.

О. П. Дзьобань, А.Ю. Панфілов, Р.А. Чемчикаленко

В статье осуществлена попытка определить методологические основания исследования феномена информационной безопасности. Обосновывается целесообразность применения диалектического, структурно-функционального, синергетического, системного и других подходов в научном познании информационной безопасности как характеристики состояния социума.

Ключевые слова: *информационная безопасность, система информационной безопасности, методологическая концепция, системный подход, принцип дополняемости.*

Dzoban A., Panfilov O., Chemchykalenko R.

METHODOLOGICAL CONTEXT OF STUDYING THE PROBLEM OF INFORMATION SECURITY.

Annotation. The article attempts to identify the methodological basis of research concerning the phenomenon of communities information security. Information security is understood as a state of protection of human vital interests, society and the state in the information sphere from internal and external threats and challenges that ensures their sustainability. However, information security – is a process, as closely linked to the cultural environment and is an integral part of social and cultural life of society, which operate with political power, social and political forces and movements, social groups and individuals who urged economic and socio-political needs, interests and goals.

Information security can be studied within the dialectic, structural-functional, synergistic, systematic and other approaches

From the standpoint of structural and functional analysis of information security, as well as any functional system is based on the following principles: result of the activity as a wired, backbone facto; self-regulation as a general principle of functional systems; electoral mobilization of individual organs and institutions into a coherent organization of functional systems, cooperation of individual elements to achieve the outcomes of the system; hierarchy of functional systems; multi parametric interaction of functional systems on outcome; system-genesis – selective formation of functional systems during ontogenetic development of society.

To understand the processes that occur in the information security system as in an open system problems of interaction elements (subsystems) this system and the society helps in combination with other methods and approaches – synergistic approach. Been adapted to the security sector synergistic paradigm can be represented by the following issues: imbalance and instability as the general state of the system components; balance and length as the impasse of evolution and the special case of the general state of the system; role of randomness in the general course of events; role of the individual impact on the course of natural events, occurring in social structures; system openness, sharing with society in its every point (except the scope of state secrets); nonlinearity of development; choice of direction; alternative development strategy as a general principle; own tendencies of development of the security as a self-organizing system; managed development in terms of self-organization.

The complementarity of structural and functional and synergetic methodology provides a holistic view of the nature of information security, its functioning, interaction elements and genesis. Along the analysis processes, occurring in the system of information security, appropriate to use the methodology of systems research.

Systematic approach to analyzing the phenomenon of information security – an approach in which all public relations and mediation elements and components of society and the state , functions and problems concerning information security are considered as interconnected whole. The objective of a systematic approach in the research of information security problems is the expression level of a special methodology of science general principles, regulations, concepts, forms and methods of systematic research, according to which each object (public education, social institution , etc.) that is represented as a system considered not just as some independent entity, but also as a component of a higher level of organization, with all its significant relationships with other objects that are part of a complex system.

The systems approach is closely correlated with the principle of dialectical interdependence which involves consideration of social phenomena in their integrity and development. Alongside with the principle of dialectical interdependence is advisable to apply the principle of subsidiarity, as in the study of information security issues in transitional conditions often have trouble interpreting facts epistemological difficulties correlation of discrete and continuous. The subsidiarity principle is implemented in the study of information security not only in the general theoretical, but also in terms of the application; not only for the description and explanation of the complementarity of activities and the types of security, but also to generate new knowledge, which is much closer to an adequate reflection of the objective state of affairs

***Keywords**: information security, system of information security, methodological concept, system approach, principle of complementarity methods.*

Надійшла до редакції 20.02.2014