

УДК 316.32(477)



Костянтин ЗАХАРЕНКО
здобувач НПУ імені М. П. Драгоманова

РОЗВИТОК СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ: ДОСВІД ЗАРУБІЖНИХ КРАЇН

© Захаренко К., 2018

Ключові слова: людина, інформація, культура, інформаційний простір, інформаційна безпека, політика інформаційної безпеки.

У різних державах розроблені основні принципи та інструментальні засоби формування ефективного інформаційного захисту національного безпекового простору. Застосовуючи різні засоби, країни-лідери достатньо ефективно здійснюють національну політику інформаційної безпеки. Україні необхідно вивчити й адекватно застосувати закордонний досвід, трансформуючи його відповідно до національної специфіки й унікальної ролі держави в сучасній геополітиці. В нашій країні наявна низка складних проблем у сфері інформаційної безпеки, що потребують нагального і кардинального вирішення. Водночас їх розв'язання передбачає не тільки концептуально-теоретичне осягнення питань інформаційної безпеки, але й створення такого національного законодавства, яке підводило б нормативно-правове підґрунтя під діяльність різних

суб'єктів інформаційного простору. Адже успішний розвиток демократично-правової держави та громадянського суспільства можливий лише за умови належного використання інформаційних ресурсів та реалізації такої державної політики, яка б забезпечувала високий рівень національної інформаційної безпеки.



ля розбудови ефективної системи національної інформаційної безпеки, особливо в умовах гібридної війни, яку веде проти України російський агресор, необхідне детальне вивчення досвіду провідних країн світу, які здійснюють ефективний інформаційний захист своїх держав і громадян. Сьогодні існують національні системи інформаційної безпеки, що реально довели свою ефективність та структурно-функціональну довершеність. «Найбільш розвинуті системи інформаційної безпеки функці-

онують у США, Великій Британії, Ізраїлі, ФРН, Російській Федерації, Китаї, тобто у тих країнах, які постійно знаходяться під потужним зовнішнім інформаційним впливом, а тому змушені створювати національні системи інформаційного захисту. Притому зазначені системи цих країн мають і достатню активну складову, завдяки чому існує можливість проведення інформаційно-психологічних заходів та кібернетичних атак проти країн-супротивників» [7, с. 168]. У сучасному світі вже розроблені основні принципи та інструментальні засоби формування ефективного інформаційного захисту національного безпекового простору. Водночас Україні необхідно лише адекватно застосувати закордонний досвід найуспішніших в цьому плані країн, коректно трансформуючи його з урахуванням національної специфіки й унікальної ролі України в сучасній геополітиці.

Особливою багатовимірністю та ефективністю система інформаційної безпеки вирізняється у такого глобального геополітичного гравця, як Сполучені Штати Америки. Необхідно наголосити, що система інформаційної безпеки в США є надзвичайно розмаїтою й складною, а також спирається на достатньо деталізоване, але підпорядковане єдиній стратегії федеральне та місцеве законодавство. «Законодавство США у сфері забезпечення інформаційної безпеки – це сукупність федеральних законів та законів штатів, які створюють правову основу для здійснення державної політики у цій сфері. Досить ґрунтовно в законодавстві врегульовано питання щодо забезпечення безпеки інформації в державних комп'ютерних системах (Закон «Про комп'ютерну безпеку», Закон «Про удосконалення інформаційної безпеки»), боротьби з комп'ютерною злочинністю та зловживання», Закон «Про зловживання комп'ютерами»), регулювання співвідношення прав громадян на отримання інформації (Закон «Про свободу інформації», Закон «Про висвітлення діяльності уряду») та конфіденційність їх приват-

ного життя (Закон «Про охорону особистих таємниць»). Адміністративно-організаційне забезпечення інформаційної безпеки в США спрямоване на координацію всіх дій щодо захисту інформації та проведення єдиної державної політики інформаційної безпеки. Президент США є основною відповідальною особою за забезпечення національної безпеки загалом та інформаційної безпеки зокрема» [6, с. 9–10]. Зрозуміло, що США як наддержава ставить перед собою зовсім інші цілі, аніж Україна в межах власної безпекової політики. Ми не можемо розраховувати на ті матеріальні і технологічні ресурси, що використовуються в Сполучених Штатах з метою гарантування національної та громадської інформаційної безпеки. Водночас українські спеціалісти можуть сприйняти окремі технологічний досвід, а законодавці мають вивчати ті способи нормативного забезпечення інформаційної політики держави, що зарекомендували себе в США як універсальні та доволі ефективні.

Розвинені країни Європи також велику увагу приділяють усебічному забезпеченню в межах національної політики, економіки, безпеки, громадянського суспільства інформаційного захисту від загроз, що постають в сучасному глобальному інформаційному суспільстві. Так, у Франції інформаційний сектор функціонування національного суспільства визначається одним з головних, поряд з економікою, політикою, культурою. Захист інформаційного простору визнається одним з найважливіших напрямів гарантування національної безпеки Французької Республіки. «Франція вважає, що у низці основних секторів, які потребують державного захисту, поряд з енергетикою, транспортом, фінансами є інформаційна сфера, зокрема системи забезпечення безпеки інформації обмеженого користування, насамперед державної таємниці, та телекомунікаційні служби. Можна зробити висновок, що саме в цьому виявляється новий елемент у понятті сучасної багатовекторності геостратегії французької правлячої еліти, що безпосередньо впли-

ває на особливості вибору способів використання оперативних можливостей національних спецслужб, ЗМІ та інших державних і неурядових структур, залучених до реалізації політики інформаційної безпеки французького суспільства і держави. Як наслідок, національний інформаційний простір Французької Республіки стає основним об'єктом захисту під час формування відповідних завдань, структури механізму та сучасного поняття тактики реалізації його сил і засобів у розвідувально-інформаційних та розвідувально-підкривних заходах, зокрема у діяльності спецслужб щодо проведення спеціальних заходів, пов'язаних із захистом французького інформаційного простору від негативних зовнішніх проявів і здійснення вигідних легальних та таємних вигідних впливів на іноземних партнерів і/або опонентів» [3, с. 343–344]. Отже, інформаційний простір у Франції розглядається як один з пріоритетних об'єктів спеціального захисту, який здійснюється всіма можливими законотворчими, організаційно-управлінськими, силовими та інформаційно-технологічними засобами. Принагідно французький уряд та громадянське суспільство постійно проводять моніторингові заходи, всіляко запобігаючи можливим спробам з боку державних функціонерів обмежувати демократію, виправдовуючись необхідністю здійснення певних заходів по контролю над національним інформаційним простором.

Менш демократично в цьому питанні поводить себе уряд Китайської Народної Республіки. В інформаційній політиці Китаю домінують принципи втілення достатньо моноцентричних оборонних і наступальних доктрин. У політичному та безпековому дискурсі КНР інформація, як в її соціально-культурному, так і в технологічно-інноваційному вимірах, розглядається насамперед як збройний ресурс, як засіб впливу на власних громадян та активного захисту і протидії зовнішнім інформаційним впливам. Використання могутньої та широкої ресурсної бази дозволяє Китаю проводити

достатньо ефективну інформаційну політику, навіть незважаючи на її недемократичну спрямованість. «Політика інформаційної безпеки визначає пріоритетними напрямками діяльності держави розробку національних стратегій, які поєднують оборонні і наступальні доктрини для забезпечення національних інтересів і захисту внутрішнього інформаційного середовища та інформаційної інфраструктури, подолання асиметричності інформаційного розвитку щодо інформаційно розвинених країн як потенційних супротивників в інформаційному протистоянні. Всі структурні складові державної інформаційної політики зумовлені потребою забезпечення національних інтересів шляхом реалізації китайської моделі інформаційного суспільства та специфіки інтеграції КНР у глобальне інформаційне середовище. Включення стратегії державної інформаційної політики в урядові програми дає Китаю можливість реформувати політичну ідеологію в контексті сучасних тенденцій міжнародного розвитку. Участь КНР в процесах міжнародної регіональної інтеграції формує стратегію інформаційної політики держави, яка полягає в одночасній інтеграції до світової системи міжнародних відносин і практичній реалізації національної моделі інформаціоналізму як чинника модернізації політичної системи КНР та її потенційного лідерства на регіональному та міжнародному рівнях» [9, с. 8–9]. Тож можна побачити успішні спроби Китаю в реалізації власної моделі інформаційної політики, яка охоплює як внутрішні проблеми країни, так і її регіональні та глобальні геополітичні зазіхання. Багато в чому саме завдяки розробці власної моделі інформаціоналізму КНР поступово досягає успіху, виконуючи завдання щодо перетворення на одного з ключових гравців на глобальній геополітичній «шахівниці», створюючи значну конкуренцію не тільки Європі, але й Сполученим Штатам Америки.

Отже, у світі існують країни з різними традиціями державного управління, які достатньо ефективно здійснюють національну політику інформаційної безпеки, засто-

совуючи різні засоби: від створення систематизованої нормативно-правової бази до використання значних матеріально-технологічних ресурсів. Успішний досвід країн-лідерів став у пригоді та позитивно вплинув на вирішення багатьох проблем, що існують сьогодні в інформаційно-безпековому полі України. «Політико-правовий аналіз стану управління захистом безпекових інтересів в Україні свідчить, що його рівень не задовольняє потреби суспільства та держави. Серед чинників, які це спричиняють, необхідно визначити: відсутність організаційної системи розроблення й реалізації єдиної державної політики в галузі забезпечення інформаційно-психологічної безпеки; нерозуміння інформаційно-психологічної боротьби як механізму протидії експансії та агресії стосовно країни в будь-якій формі її прояву та забезпечення власних національних інтересів; недостатня розвиненість науково-методичної бази забезпечення інформаційно-психологічної безпеки, стратегії й тактики ведення інформаційно-психологічної боротьби; відсутність підготовки фахівців з комплексним баченням проблем інформаційно-психологічної безпеки країни, а також організації та ведення інформаційно-психологічної боротьби. За таких умов держава не спроможна протистояти масованому інформаційно-психологічному впливу з боку інших країн та ефективно виконувати завдання інформаційно-психологічної боротьби для забезпечення національних інтересів» [5, с. 11]. Як бачимо, в нашій державі існує ціла низка складних проблем у сфері інформаційної безпеки, що потребують нагального і кардинального вирішення. Саме тому особливої актуальності сьогодні набуває теоретико-методологічне та філософсько-політологічне дослідження проблем національної інформаційної безпеки в Україні, що переживає кризовий етап свого розвитку.

Актуальності цій проблематиці надає й те, що перед українською державою і суспільством постійно постають нові виклики, пов'язані як з динамічною глобальною ситуацією, що постійно змінюється через

бурхливий розвиток інформаційної цивілізації, так і з агресивною політикою Російської Федерації на регіональному рівні. Складаються такі обставини, коли Україна змушена формувати власну систему інформаційної безпеки, не стільки вибудовуючи стратегію, скільки реагуючи на все нові й нові виклики. «За цих обставин перед керівництвом України постає проблема необхідності усвідомлення нового характеру викликів та загроз, що стоять перед країною і набувають значних масштабів. Відповідно інтереси України вимагають формування системи, що дозволить їй адекватно реагувати на негативні зовнішні та внутрішні впливи, зберігати цілісність суспільства та держави» [8, с. 3]. Для побудови такої системи першочергово необхідно провести значну аналітичну підготовку, на основі якої чітко визначитись із пріоритетами та орієнтирами подальшої державної інформаційної політики. Окрім того, важливо обирати такі засоби інформаційного захисту, які б були достатньо ефективними на даний момент і при цьому потребували б адекватних ресурсних та технологічних затрат. Це також вимагає серйозного концептуально-теоретичного пошуку у сфері визначення основних засад державної інформаційно-безпекової політики.

Продовженням концептуально-теоретичних пошуків в галузі інформаційної безпеки має стати створення систематизованого національного законодавства, що підвело б нормативно-правове підґрунтя під діяльність різних суб'єктів, у тому числі й держави, у сфері забезпечення різних рівнів інформаційної безпеки суспільства. Особливо важливо, з нашого погляду, врахувати при цьому успішний досвід європейських країн, що ефективно захищають свій інформаційний простір від шкідливих зовнішніх впливів. «Назріла нагальна потреба здійснення кодифікації інформаційного законодавства України, зокрема шляхом прийняття Інформаційного кодексу України. Існує необхідності врахування під час практичної розробки дієвого Інформаційного кодексу України європейських стандартів у сфері захисту

інформації та забезпечення інформаційної безпеки людини, суспільства і держави. Визначено доцільність включення до проекту Інформаційного кодексу норм комп'ютерної етики, морально-етичних основ регулювання взаємовідносин між комп'ютером та людиною в міжнародному мережевому просторі. Увага акцентується на необхідності прийняття такого нормативно-правового акта, положеннями якого буде передбачено основні засади інформаційного розвитку держави, врегульовано діяльність органів державної влади України щодо забезпечення інформаційної безпеки (у тому числі протидії інформаційним війнам), визначено ключові принципи забезпечення інформаційної безпеки людини, суспільства, держави та подальшого інформаційного розвитку України, закріплено систему заходів, своєчасне виконання яких сприятиме зміцненню інформаційної безпеки (у тому числі у сфері протидії інформаційним війнам) та виведенню діяльності щодо її зміцнення на якісно новий рівень» [1, с. 12]. Отже, кодифікація національного законодавства в галузі інформаційної безпеки може вирішити проблему систематизації даної сфери державної та суспільної життєдіяльності. Важливо лише, щоб така кодифікація відбувалася на основі чітко розроблених та структурно вибудованих теоретико-методологічних засад дослідження інформаційно-безпекового сегменту діяльності української держави і громадянського суспільства.

Проте теоретична проблематика інформаційної безпеки, що досліджується в межах сучасного філософсько-політологічного дискурсу, переконливо доводить свою актуальність і в питаннях державного та громадянського управління. Саме інформація стає інклюзивним, інтегративним, наскрізним ресурсом, що дозволяє максимально ефективно управляти тією чи іншою спільнотою в межах сучасної інформаційної цивілізації. «Ефективне управління сучасним інформаційним суспільством має обов'язково передбачати формування державної інформаційної політики та створення належних умов її реалізації, а метою цієї

діяльності повинне стати узгодження системно-функціональної та інформаційної складових в умовах стрімкого поширення процесів глобалізації. Звідси зрозуміло, чому проблема забезпечення інформаційної безпеки увійшла до числа найбільш значущих і пріоритетних завдань, вирішення яких необхідне для існування й подальшого розвитку нашого суспільства. Інформаційна безпека важлива тому, що ми захищаємо свій інформаційний простір, а отже, свої інформаційні ресурси, свою національну культуру. Зрештою, ми захищаємо себе, своє право на життя, своє місце в історії» [2, с. 207]. Тож, філософська специфіка проблематики інформаційної безпеки полягає в тому, що інформація сьогодні стала ресурсом глобального об'єднання людства, що несе багато нових можливостей, але ставить перед окремими спільнотами і людством в цілому нові виклики і ризики. Від того чи зможемо ми відповісти на ці виклики максимально адекватно, захистивши свій інформаційний простір від багатьох небезпек і шкідливих впливів, багато в чому залежить успіх та своєчасність національно-будівничих та державотворчих зусиль, що здійснюються українським народом в складних геополітичних та глобально-цивілізаційних умовах.

Сьогодні успішний розвиток демократично-правової держави та громадянського суспільства можливий лише за умов повноцінного використання інформаційних ресурсів, а також встановлення чіткої державної політики, що забезпечувала б високий рівень національної інформаційної безпеки. Фактично, інформаційна безпека держави і національного соціуму стає ключовим чинником демократизаційних перетворень всередині країни, а також її виходу на конкурентоспроможний рівень в регіональному та глобальному масштабі. «Національна інформаційна безпека України нині постає як одне з найважливіших завдань, від успішного розв'язання якого залежить цілісність, суверенітет, суспільний прогрес України. Практичне забезпечення національної інформаційної безпеки мож-

ливе за рахунок єдності усіх факторів політичного, економічного, правового, організаційного та ін. Національна інформаційна безпека реальний фактор успішної геостратегічної політики України, водночас з демократичним суспільним розвитком українського соціуму» [4, с. 62]. Це й зумовлює значний рівень актуальності концептуально-теоретичних досліджень філософсько-політологічного характеру, спрямованих на вивчення всієї повноти можливостей, які дозволяють сучасним державам і суспільствам захищати свій інформаційний простір від величезної кількості викликів і проблем, що постають у межах глобальної інформаційної цивілізації. Цим зумовлена й актуальність і важливість визначення теоретико-методологічних засад дослідження інформаційної безпеки держави.

Отже, визначивши актуальні проблеми інформаційної безпеки й розглянувши різні дискурсивні традиції та способи визначення категорії «інформаційна безпека», що існують в українському та іноземному філософсько-політологічному дискурсі, а також здійснивши компаративний аналіз проблеми інформаційної безпеки в системі інформаційної політики України та провідних країн світу, можемо зробити такі **висновки**.

По-перше, доведено актуальність і багатовимірність концептуально-теоретичного вивчення та аналізу даної проблеми в сучасному філософсько-політологічному та національно-безпековому дискурсі. Насамперед, основною детермінантою актуальності проблематики інформаційної безпеки є значне зростання інформаційних потоків і обмінів на глобальному рівні. Таке зростання ставить перед національними безпековими просторами багато викликів і труднощів, які вимагають постійного дослідження і вирішення. Додаткової небезпеки додають інформаційні втручання, що здійснюються на регіональному рівні. При цьому інформаційні виклики постають як перед людиною, громадянином, так і суспільством, народом, державою. Це й створює надзвичайну складність концептуально-теоретичного дослідження проблем інформа-

ційної безпеки. Одним з основних методів вивчення проблем інформаційної безпеки, що постають і перед людиною, і перед суспільством, і перед державою, є комплексно-системний підхід. Така полісуб'єктність інформаційно-безпекового поля зумовлює її складність, важливість і актуальність з погляду філософсько-світоглядної рефлексії та політологічно-безпекової аналітики.

По-друге, проаналізувавши основні принципи та критерії визначення поняття «інформаційна безпека» суспільства в контексті сучасного філософсько-політологічного дискурсу, показано різноманітність та поліваріантність таких визначень. Українські та закордонні дослідники даної проблематики, визначаючи категорію інформаційної безпеки, звертаються до таких її аспектів, як глобально-цивілізаційна значущість, гарантування національної безпеки і оборони, визначення інформаційно-технологічних параметрів безпеки, гарантування інформаційної безпеки кожної окремої особистості чи конкретних соціальних спільнот. З огляду на таке різноманіття підходів, ключовим теоретико-методологічним принципом нашого дослідження обрано принцип системності, на основі якого робиться комплексний, структурно-функціональний аналіз категорії «інформаційна безпека» з урахуванням її індивідуальних, соціальних, державних і глобальних вимірів. При такому розгляді особливо важливо формулювати інтегративні чинники, що поєднують інформаційну безпеку держави і суспільства з інформаційно-психологічною та світоглядно-феноменологічною безпекою кожної людини. Зважаючи на теоретико-методологічні засади дослідження проблеми інформаційної безпеки, ми визначаємо дане поняття як вид національної безпеки, спрямований на забезпечення прав і свобод людини щодо вільного доступу до інформації, створення і впровадження безпечних інформаційних технологій та захист прав власності всіх учасників інформаційної діяльності.

По-третє, здійснивши компаративний аналіз проблеми інформаційної безпеки в

системі інформаційної політики України та провідних країн світу, доведено необхідність розробки систематизованої стратегії формування інформаційно-безпекової політики в нашій державі. На сьогодні в нашій державі ще не сформовано відповідної сучасним цивілізаційним та геополітичним викликам системи інформаційної безпеки. Існує необхідність її посилення буквально на всіх напрямках: нормативно-правовому, організаційно-управлінському, інформаційно-технологічному. Але насамперед існує нагальна необхідність вироблен-

ня чіткої стратегії здійснення перетворень у секторі інформаційної безпеки держави і суспільства. Така стратегія має ґрунтуватися на міцному концептуально-теоретичному, науково-практичному базисі, який має сформуватися в межах національного філософсько-політологічного дискурсу. Саме тому дослідження багатоаспектної проблематики інформаційної безпеки держави, соціуму і людини є сьогодні надзвичайно актуальним і важливим завданням, що постає перед науковою спільнотою нашої країни.

ЛІТЕРАТУРА

1. **Абакумов В.М.** Правове регулювання протидії інформаційним війнам в Україні: автореф. дис. ... канд. юр. наук: спец. 12.00.07 «Адміністративне право і процес; фінансове право; інформаційне право». Запоріжжя, 2011. 22 с.
2. **Дзьобань О.П., Пилипчук В.Г.** Інформаційне насильство та безпека: світоглядно-правові аспекти: монографія. Харків: Майдан, 2011. 244 с.
3. Інформаційна безпека (соціально-правові аспекти): підручник / Б.В. Остроухой, Б.М. Петрик, М.М. Присяжнюк та ін. Київ: КНТ, 2010. 776 с.
4. **Кирильчук Є.О.** Проблеми національної інформаційної безпеки України в контексті сучасних національних державотворчих процесів та світової інтеграції // Наукові праці МАУП. Київ: Вид. дім «Персонал», 2013. Вип. 1 (36). С. 60–63.
5. **Коваль З.В.** Політико-правові механізми державного управління інформаційно-психологічною безпекою України: автореф. дис. ... канд. наук з державного управління: спец. 25.00.02 «Механізми державного управління». Одеса, 2011. 22 с.
6. **Конах В.К.** Забезпечення інформаційної безпеки держави як складової системи національної безпеки (приклад США): автореф. дис. ... канд. політ. наук: пец. 21.01.01 «Основи національної безпеки держави». Київ, 2005. 20 с.
7. **Левченко О.В.** Проблеми і шляхи формування системи інформаційної безпеки держави // Збірник наукових праць Харківського університету Повітряних Сил. Харків: ХУПС ім. Івана Кожедуба, 2014. Вип. 2 (39). С. 166–168.
8. **Смола Л.Є.** Інформаційно-психологічні детермінанти сучасного політичного процесу (світовий та вітчизняний контексти): автореф. дис. ... д-ра політ. наук: спец. 23.00.01 «Теорія та історія політичної науки». Львів, 2011. 34 с.
9. **Хуан Цинь.** Інформаційна політика Китайської Народної Республіки в сучасних міжнародних відносинах: автореф. дис. ... канд. політ. наук: спец. 23.00.03 «Політична культура та ідеологія». Київ, 2007. 14 с.

REFERENCES

1. **Abakumov V.M.** Legal regulation of counteraction to informational wars in Ukraine: author's abstract. dis ... Candidate jur Sciences: special 12.00.07 "Administrative law and process; finance law; information law". Zaporozhye, 2011. 22 p.
2. **Dzobanov O.P., Pylpuchuk V.G.** Information Violence and Security: Worldview Issues: Monograph. Kharkiv: Maydan, 2011. 244 p.
3. Information security (socio-legal aspects): textbook / B.V. Ostroukoy, B.M. Petryk, M.M. Prisyajnyuk and others. Kiev: CST, 2010. 776 p.
4. **Kyrylchuk E.O.** Problems of National Information Security of Ukraine in the Context of Contemporary National State-Building Processes and World Integration // Scientific Papers of MAUP. Kiev: Publish. House "Personnel", 2013. 1 (36). PP. 60–63.
5. **Koval Z.V.** Political-legal mechanisms of state management of information-psychological safety of Ukraine: author's abstract. diss ... Candidate Sciences in Public Administration: Speciality 25.00.02 "Mechanisms of public administration". Odessa, 2011. 22 p.
6. **Konakh V.K.** Providing information security of the state as a component of the national security system (US example): author's abstract. diss ... Candidate Politic. Sciences: Speciality 21.01.01 "Fundamentals of National Security of the State". Kyiv, 2005. 20 p.
7. **Levchenko O.V.** Problems and ways of formation of information security system of the state // Collection of scientific works of Kharkiv University of Air Forces. Kharkiv: HUPPS them. Ivana Kozheduba, 2014. 2 (39). PP. 166–168.
8. **Resin L. E.** Information-psychological determinants of the modern political process (world and domestic contexts): author's abstract. diss ... doctor in Political Sciences: Speciality 23.00.01 "Theory and History of Political Science". Lviv, 2011. 34 p.
9. **Juan Qin.** Information policy of the People's Republic of China in modern international relations: author's abstract. diss ... Candidate Political Sciences: Speciality 23.00.03 "Political culture and ideology". Kyiv, 2007. 14 p.