

## РОЗДІЛ III

### СОЦІАЛЬНА ФІЛОСОФІЯ

УДК 351.746.1:004

<http://orcid.org/0000-0003-0980-7313>

#### ДО ПИТАННЯ ПРО РОЗВИТОК НАЦІОНАЛЬНОЇ СИСТЕМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ: ДОСВІД СУСІДІВ

К.В. Захаренко, кандидат філософських наук,  
здобувач НПУ імені М.П. Драгоманова

*В різних державах розроблені основні принципи та інструментальні засоби формування ефективного інформаційного захисту національного простору. Застосовуючи різні засоби, країни-лідери достатньо ефективно здійснюють національну політику інформаційної безпеки. Україні необхідно вивчити й адекватно застосувати при цьому успішний закордонний досвід країн, що ефективно захищають свій інформаційний простір від шкідливих зовнішніх впливів, трансформуючи його відповідно до національної специфіки й унікальної ролі держави в сучасній геополітиці. В нашій країні наявна низка складних проблем в сфері інформаційної безпеки, що потребують нагального і кардинального вирішення. Водночас їх розв'язання передбачає не тільки теоретико-методологічне та філософсько-політологічне осягнення питань інформаційної безпеки, але й створення такого національного законодавства, яке підводило б нормативно-правове підґрунтя під діяльність різних суб'єктів інформаційного простору, що переживає кризовий етап свого розвитку. 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. Автор звертає увагу на українських спеціалістів, які можуть сприйняти окремий технологічний досвід та матеріальні ресурси, а законодавці мають вивчати способи нормативного забезпечення інформаційної політики держави, що зарекомендували себе в США як універсальні та доволі ефективні з метою забезпечення національної та громадської інформаційної безпеки. Акцентовується увага на кодифікації національного законодавства в галузі інформаційної безпеки, яка 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.*

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

**Актуальність проблеми.** Для розбудови ефективної системи національної інформаційної безпеки 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 функціонують у США, Великій Британії, Ізраїлі, ФРН, Російській Федерації, Китаї, тобто у тих країнах, які постійно знаходяться під потужним зовнішнім інформаційним впливом, а тому вимушені 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» [1, с. 168]. В 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.

**Мета статті** розглянути розвиток національної системи інформаційної безпеки та проаналізувати досвід і високий рівень сусідніх країн та країн-лідерів.

**Виклад основного матеріалу.** Особливою багатою вимірністю та ефективністю система інформаційної безпеки вирізняється у такого глобального геополітичного гравця, як Сполучені Штати Америки. Необхідно відзначити, що система інформаційної безпеки в США є надзвичайно багатомірною і 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 (Закон «Про комп'ютерне шахрайство 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 приватного життя (Закон «Про охорону особистих таємниць»). Адміністративно-організаційне забезпечення інформаційної безпеки в США спрямоване на координацію всіх дій по захисту інформації та проведення єдиної державної політики інформаційної безпеки. Президент США є основною відповідальною особою за забезпечення національної безпеки загалом та інформаційної безпеки зокрема» [2, с. 9-10]. Зрозуміло, що США як наддержава ставить перед собою зовсім інші цілі, ніж Україна в рамках власної безпекової політики. Ми не можемо розраховувати на ті матеріальні і технологічні ресурси, що використовуються в Сполучених Штатах з метою забезпечення національної та громадської інформаційної безпеки. В той же час, українські спеціалісти можуть сприйняти окремий 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 всебічному забезпеченню в рамках 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 ключових, поряд з економікою, політикою, культурою. Захист інформаційного простору визнається одним з ключових і найважливіших напрямів забезпечення національної безпеки Французької Республіки. «Франція вважає, що у низці основних секторів, які потребують державного захисту, поряд з енергетикою, транспортом, фінансами є інформаційна сфери, 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 впливає 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-підбивних 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]. Таким чином, 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. В 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» [4, с. 8-9]. Таким чином, можна зазначити 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 по перетворенню на одного з ключових гравців на глобальній геополітичній «шахівниці», створюючи значну конкуренцію не тільки Європі, але й Сполученим Штатам Америки.

Таким чином, в світі існують країни з різними традиціями державного управління, які достатньо ефективно здійснюють національну політику інформаційної безпеки, застосовуючи різні засоби: від створення система-

тизованої нормативно-правової бази до використання значних матеріально-технологічних ресурсів. Вивчаючи успішний досвід країн-лідерів, можна залучати певні моменти, що спричинили б позитивний вплив 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 в 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 і те, що перед українською державою і суспільством постійно постають нові виклики, збуджувані як динамічною глобальною ситуацією, що постійно змінюється через бурхливий розвиток інформаційної цивілізації, так агресивною політикою Російської Федерації на регіональному геополітичному 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» [6, 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 в сфері визначення основних засад державної інформаційно-безпекової політики.

Продовженням концептуально-теоретичних пошуків в галузі інформаційної безпеки має стати створення систематизованого національного законодавства, що підводило б нормативно-правове підґрунтя під діяльність різних суб'єктів, в тому числі й держави, в сфері забезпечення різних рівнів інформаційної безпеки суспільства. Особливо важливо, з нашої точки зору, 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 необхідність 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» [7, с. 12]. Таким чином, 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 вибудуваних теоретико-методологічних засад дослідження інформаційно-безпекового сегменту діяльності української держави і громадянського суспільства.

Окрім того, теоретична проблематика інформаційної безпеки, що досліджується в рамках сучасного філософсько-політологічного дискурсу, переконливо доводить свою актуальність і в питаннях державного та громадського управління. Саме інформація стає інклюзивним, інтегративним, наскрізним ресурсом, що дозволяє максимально ефективно управляти тією чи іншою спільнотою в рамках 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» [8, с. 207]. Таким чином, 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 демократичних 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 можливе 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» [9, 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 в рамках глобальної інформаційної цивілізації. Цим зумовлена й актуальність і важливість визначення теоретико-методологічних засад дослідження інформаційної безпеки, що проводиться в нашому дисертаційному дослідженні.

**Висновки.** Таким чином, визначившись з основними витоками та детермінантами актуальності проблеми інформаційної безпеки, розглянувши різні дискурсивні традиції та способи визначення категорії «інформаційна безпека», що існують в українському та іноземному філософсько-політологічному дискурсі, а також здійснивши компаративний аналіз відображення проблеми інформаційної безпеки в системі інформаційної політики України та провідних країн світу, можемо зробити низку взаємопов'язаних висновків про основні принципи та теоретико-методологічні засади нашого дослідження поставленої проблематики.

По-перше, визначивши основні витoki та детермінанти проблеми інформаційної безпеки, доведено значну актуальність та 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 геополітичному рівні. При цьому інформаційні виклики постають перед усіма: людиною, громадянином, суспільством, народом, державою. Це й створює надзвичайну складність концептуально-теоретичного дослідження проблем інформаційної безпеки. В нашому дослідженні одним з основних методів визначено комплексно-системний підхід, на основі якого здійснюється цілісне вивчення проблем інформаційної безпеки, що постають і перед людиною, і перед суспільством, і перед державою. Полісуб'єктність інформаційно-безпекового

поля зумовлює складність, важливість і актуальність дослідження поставленої проблематики з точки зору 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, підкреслено значну різноманітність та поліваріантність таких визначень. Українські та закордонні дослідники даної проблематики, визначаючи категорію інформаційної безпеки, звертаються до таких її аспектів, як глобально-цивілізаційна значимість, роль у забезпеченні національної безпеки і оборони, визначення інформаційно-технологічних параметрів безпеки, значення забезпечення 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. З огляду на такі 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 огляд відображення 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 посилення буквально на всіх напрямках: нормативно-правовому, організаційно-управлінському, інформаційно-технологічному. Але насамперед існує нагальна необхідність вироблення чіткої стратегії здійснення перетворень в секторі інформаційної безпеки держави і національного суспільства. Така стратегія має ґрунтуватися на міцному концептуально-теоретичному, науково-практичному базисі, який має сформуватися в рамках 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. Левченко О.В. Проблеми і шляхи формування системи інформаційної безпеки держави / О.В. Левченко //Збірник наукових праць Харківського університету Повітряних Сил. – Харків: ХУПС ім. Івана Кожедуба, 2014. – Випуск 2 (39). – С. 166-168.
2. Конах В.К. Забезпечення інформаційної безпеки держави як складової системи національної безпеки (приклад США). Автореферат дисертації на здобуття наукового ступеня кандидата політичних наук. Спеціальність: 21.01.01 – основи національної безпеки держави / Вікторія Конах. – К., 2005. – 20 с.
3. Інформаційна безпека (соціально-правові аспекти): підручник / Б.В. Остроухой, Б.М. Петрик, М.М. Присяжнюк та ін. – К.: КНТ, 2010. – 776 с.
4. Хуан Цинь. Інформаційна політика Китайської Народної Республіки в сучасних міжнародних відносинах. Автореферат дисертації на здобуття наукового ступеня кандидата політичних наук. Спеціальність: 23.00.03 – політична культура та ідеологія / Хуан Цинь. – К., 2007. – 14 с.
5. Коваль З.В. Політико-правові механізми державного управління інформаційно-психологічною безпекою України. Автореферат дисертації на здобуття наукового ступеня кандидата наук з державного управління. Спеціальність: 25.00.02 – механізми державного управління / Зіновій Коваль. – Одеса, 2011. – 22 с.
6. Смола Л.Є. Інформаційно-психологічні детермінанти сучасного політичного процесу (світовий та вітчизняний контексти). Автореферат дисертації на здобуття наукового ступеня доктора політичних наук. Спеціальність: 23.00.01 – теорія та історія політичної науки / Лідія Смола. – Львів, 2011. – 34 с.
7. Абакумов В.М. Правове регулювання протидії інформаційним війнам в Україні. Автореферат дисертації на здобуття наукового ступеня кандидата юридичних наук. Спеціальність: 12.00.07 – адміністративне право і процес; фінансове право; інформаційне право / Віктор Абакумов. – Запоріжжя, 2011. – 22 с.
8. Дзьобань О.П. Інформаційне насильство та безпека: світоглядно-правові аспекти: Монографія / О.П. Дзьобань, В.Г. Пилипчук. – Харків: Майдан, 2011. – 244 с.
9. Кирильчук Є.О. Проблеми національної інформаційної безпеки України в контексті сучасних національних державотворчих процесів та світової інтеграції / Є.О. Кирильчук // Наукові праці МАУП. – К.: ДП Видавничий дім «Персонал», 2013. – Випуск 1 (36). – С. 60-63.

## К ВОПРОСУ О РАЗВИТИИ НАЦИОНАЛЬНОЙ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ: ОПЫТ СОСЕДЕЙ

К.В. Захаренко

В разных государствах разработаны основные принципы и инструментальные средства формирования эффективного информационного защиты национального пространства. Применяя различные средства, страны-лидеры достаточно эффективно осуществляют национальную политику информационной безопасности. Украине необходимо изучить и адекватно применить при этом успешный зарубежный опыт стран, эффективно защищают свое информационное пространство от вредных внешних воздействий, трансформируя его в соответствии с национальной специфики и уникальной роли государства в современной геополитике. В нашей стране есть ряд сложных проблем в сфере информационной безопасности, требующих неотложного и кардинального решения. В то же время их решение предполагает не только теоретико-методологическое и философско-политологическое постижения вопросам информационной безопасности, но и создание такого национального законодательства, подводило бы нормативно-правовую основу под деятельность различных субъектов информационного пространства, переживает кризисный этап своего развития. Ведь развитие демократически правового государства и гражданского общества возможно лишь при условии надлежащего использования информационных ресурсов и реализации такой государственной политики, которая бы обеспечивала высокий уровень национальной информационной безопасности. Автор обращает внимание на украинских специалистов, которые могут принять отдельный технологический опыт и материальные ресурсы, а законодатели должны изучать способы нормативного обеспечения информационной политики государства, зарекомендовавших себя в США как универсальные и довольно эффективные с целью обеспечения национальной и общественной информационной безопасности. Акцентируется внимание на кодификации национального законодательства в области информационной безопасности, которая может решить проблему систематизации данной сферы государственной и общественной жизнедеятельности. Важно только, чтобы такая кодификация происходила на основе четко разработанных и структурно выстроенных теоретико-методологических основ исследования информационно-безопасности сегмента деятельности украинского государства и гражданского общества.

**Ключевые понятия:** человек, политика, информация, культура, информационное пространство, информационная безопасность, политика информационной безопасности.

## AS TO THE QUESTION OF THE DEVELOPMENT OF THE NATIONAL SYSTEM OF INFORMATION SECURITY: THE NEIGHBOURINSEXPERIENCE

Kostyantyn V. Zakharenko

In different countries, the basic principles and tools for the formation of effective information protection of the national space have been developed. By applying various means, the countries-leaders are effectively implementing the national information security policy. Ukraine needs to study and adequately apply the successful foreign experience of countries that effectively protect their information space from harmful external influences, transforming it in accordance with the national specificity and the unique role of the state in modern geopolitics. In our country there is a number of complex issues in the field of information security that require urgent and radical solutions. At the same time, their solution involves not only theoretical, methodological, philosophical and political comprehension of information security of issues, but also the creation of such a national legislation that would set the legal basis for the activities of various subjects of the information space, experiencing a crisis stage of its development. Indeed, the successful development of a democratic state and civil society is only possible if the information resources are properly used and the

---

implementation of such a state policy that would ensure a high level of national information security. The author draws attention to Ukrainian specialists who can perceive individual technological experience and material resources, and legislators should study the ways of normative maintenance of information policy of the state that have proven themselves in the USA as universal and quite effective in order to ensure national and public information security. The emphasis is on codification of national legislation in the field of information security, which can solve the problem of systematization of this sphere of state and social life. It is important only that such codification takes place on the basis of well-developed and structurally constructed theoretical and methodological foundations of the research of the information security segment of the activity of the Ukrainian state and civil society.

**Key notions:** person, politics, information, culture, information space, information security, information security policy.