УДК 1:316.3+340.12

Є. М. Мануйлов, доктор філософії, професор;
Ю. Ю. Калиновський, доктор філософських наук, професор

АКСІОЛОГІЧНИЙ ВИМІР ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНСЬКОЇ ДЕРЖАВИ

Досліджено ціннісні аспекти інформаційної безпеки Української держави. Проаналізовано закордонний досвід стратегічного планування у сфері інформаційної безпеки. Визначено сутнісні характеристики інформаційного суверенітету України. Розкрито роль суб'єктів громадянського суспільства в забезпеченні аксіологічної підойми інформаційної безпеки.

Ключові слова: *інформаційна безпека, цінності, державотворення, інформаційний суверенітет, інформаційний простір.*

Актуальність проблеми. В умовах «гібридної війни», розв'язаної проти України, важливість зміцнення інформаційної безпеки нашої держави не викликає сумнівів. Як відомо, інформаційна безпека має декілька базових вимірів, одним із найважливіших з яких є аксіологічний. Формування та розвиток ціннісного підґрунтя інформаційної безпеки нашої країни є необхідною умовою спротиву інформаційній агресії, що здійснюється проти України.

У нашому дослідженні ми зосередимо увагу на ролі та значенні ціннісних детермінант у формуванні соціокультурних засад інформаційної безпеки України, що й буде ***метою*** цієї наукової розвідки.

Аналіз наукових джерел і публікацій. У сучасних глобальних процесах інформація є потужним ресурсом, який сприяє національному прогресу. Саме тому набуття якісної (достовірної) інформації, її зберігання, захист та швидкість оброблення становлять необхідні передумови стабільного існування будь-якої держави. У свою чергу, реалізація права людини на достовірну інформацію є необхідною складовою демократичного поступу суспільства.

Очевидно, право людини на інформацію є базовою правовою цінністю, яку має захищати демократична держава. Як зауважують фахівці, право на інформацію – це право особистості на комунікацію, тобто вираження своєї індивідуальності в суспільстві, яке є одним із найважливіших прав людини. Можна розрізнити щонайменше три аспекти сучасних інформаційно-комунікативних відносин:

– ідеологічний – створення, поширення та закріплення в масовій свідомості певних ціннісних настанов, послань-меседжів, пояснень та обґрунтувань політичних рішень і дій влади;

– інформаційний – процеси обміну інформацією між учасниками комунікативних відносин;

– технологічний – регулювання техніко-технологічних процесів розвитку різних сегментів інформаційної сфери [1, с. 82].

Виходячи з вищезазначеного, можна стверджувати, що забезпечення права на інформацію й гарантування інформаційної безпеки людини та суспільства в усіх її вимірах є надактуальним завданням сьогодення. На думку фахівців, інформаційна безпека (як складова національної безпеки) – це захищеність життєво важливих інтересів людини і громадянина, суспільства і держави, за якої забезпечуються сталий розвиток суспільства, своєчасне виявлення, запобігання та нейтралізація реальних і потенційних загроз національним інтересам у сферах науково-технічної та інноваційної політики, культурного розвитку населення, забезпечення свободи слова та інформаційної безпеки, захисту інформації, зв'язку, інформаційних технологій при виникненні негативних тенденцій до створення потенційних або реальних загроз національним інтересам [2, с. 231–232].

Отже, інформація є стратегічним ресурсом держави, а захист права людини та суспільства на достовірну інформацію становить ціннісний імператив демократичного державотворення.

З розвитком інформаційного суспільства світова спільнота стикнулась з необхідністю захисту інформаційних прав людини, протидії інформаційним атакам, формування національних систем інформаційної безпеки. Так, у 1986 р. країни Європи спільно розробили загальні «Європейські критерії безпеки інформаційних технологій», на основі яких були сформульовані завдання у сфері інформаційної безпеки:

– захист інформаційних ресурсів від несанкціонованого доступу з метою забезпечення конфіденційності;

– забезпечення цілісності інформаційних ресурсів шляхом їх захисту від несанкціонованої модифікації або знищення;

– забезпечення працездатності систем за допомогою протидії загрозам відмови в обслуговуванні [3, с. 390].

Розмірковуючи над сутністю аксіологічного підґрунтя інформаційної безпеки, фахівці визначають низку аспектів розгляду цієї проблеми. Зокрема, науковець І. Зязюн своєрідно інтерпретує вищеозначену проблему, зазначаючи, що як ніколи постає питання про аксіологічну безпеку, один із важливих аспектів інформаційної безпеки – своєрідної психологічної складової так званого «соціального почуття» (за А. Адлером – «співпричетності до життя суспільства, невідчуженості від колективного буття і прагнення до кооперації та співробітництва із собі подібними»). Автор переконаний, що дуже мало

людей реально уявляють справжню небезпеку аксіологічної війни. Лише цінності структурно конституюють саму громадянськість, саму суб'єктивність індивідуума, а тому їх зруйнування впливає на всі без винятку напрями життя людини і суспільства виключно знищуюче [4, с. 11].

Вищеозначений дослідник переконливо доводить, що основою процвітання і благополуччя держави має бути не інформаційна агресія проти інших країн, а сильна внутрішня політика, розвиток моральних принципів і моральних норм, комфортна психологічна обстановка в державі. Незнання практичних шляхів відтворення ціннісного світу громадян і ефективного забезпечення аксіобезпеки пов'язано з нерозумінням масштабу і причин аксіокатастрофи, що, у свою чергу, визначається причиною нерозуміння організуючої, конструюючої і системоутворюючої ролі цінностей у внутрішньому світі людини і в міжособистісному просторі співтовариств [4, с. 14–15].

У сучасних умовах особливу роль у формуванні ціннісного підґрунтя суспільного й державного буття відіграють мережеві спільноти та організації, які відповідно є суб'єктами інформаційної безпеки держави.

Узагальнюючи різноманітні джерела, Т. Кравченко зауважує, що сьогодні вже існує мережева організація соціального життя, заснована на залученні багатьох людей до мережевих спільнот, комунікативною основою яких є Інтернет. У мережевих спільнотах проявляються негативні риси, які впливають на ціннісний світ людини та суспільства, що, у свою чергу, відбивається на якісних показниках інформаційної безпеки держави. До таких негативних рис фахівці відносять такі:

– невпевненість в інформаційній безпеці особистих даних у мережі;

– право державних структур на перегляд інформації акаунтів соціальних мереж;

– інформаційні технології створюють можливість руйнування життєвого світу людей і їх життєвих пріоритетів і цінностей, залучення свідомості людей в небезпечну для психіки віртуальну реальність, у той час як інформація набуває статусу всезагальної цивілізаційної цінності, значного, життєво важливого ресурсу суспільства і держави [5, с. 57].

Таким чином, існує нагальна потреба у розповсюдженні та утвердженні гуманістичних цінностей серед користувачів мережі Інтернет шляхом поширення просвітницького, науково-популярного, релігійного, літературного, етичного контенту в прийнятній та привабливій формі для різних груп населення. Така діяльність, безумовно, буде зміцнювати ціннісні підвалини інформаційної безпеки нашої країни.

Наступним чинником, що негативно впливає на аксіосферу інформаційної безпеки, є намагання окремих суб'єктів інформаційного простору поставити

власні приватні інтереси вище загальнодержавних, бажання використовувати інформаційні технології для маніпулювання суспільною свідомістю.

Розмірковуючи над вищеозначеною проблемою, О. Литвиненко зауважує, що оскільки лобіювання приватних інтересів становить загрозу національній інформаційній безпеці, то потрібно на державному рівні проводити ефективні та дієві заходи з метою захисту національного інформаційного простору. Це, зокрема, такі:

– збільшення бюджетного фінансування державних інформаційних агентств та інших ЗМІ з метою підвищення рівня стимулювання і мотивування співробітників;

– удосконалення законодавства у сфері інформаційної діяльності, прийняття закону, за яким лише 20% приватних інформаційних агентств та ЗМІ можуть належати іноземним громадянам і містити у статутному фонді іноземний капітал, а 80% – громадянам України;

– проведення рекламних кампаній для збільшення престижу державних та власне українських інформаційних агентств [6, с. 204].

Негативний вплив окремих суб'єктів медіа-простору на інформаційну та духовну безпеку нашої країни обумовлений до певної міри несистемним законодавством у цій царині. У цьому контексті Ю. Дмитерко стверджує, що інформаційне законодавство України й досі значною мірою залишається фрагментарним і несистематизованим, на рівні підзаконних нормативних актів є доволі суперечливим. Правові норми, які регулюють інформаційний простір, розпорошені по різних законах та підзаконних нормативних актах, що ускладнює їх практичне застосування. Інформаційне законодавство містить значний масив протиріч та неузгодженостей, оперує недосконалим термінологічним апаратом. Неврегульованою з правового боку залишається діяльність інтернет-видань. Крім того, потрібно відзначити, що судові та правоохоронні органи не приділяють достатньо серйозної уваги боротьбі з порушеннями інформаційного законодавства [7, с. 366].

У стратегічному плані державі варто зміцнювати аксіосферу суспільства шляхом відтворення цінностей через освіту та виховання, дбати про інформаційну безпеку та захищеність культурно-інформаційного поля країни від зовнішніх впливів. Інформаційна стабільність та втілення чітких ціннісних пріоритетів демократичного розвитку держави забезпечуватиме їй конкурентоспроможність у глобальних процесах сучасності.

Як влучно зауважує дослідник І. Поліщук, демократія як спосіб правління є притаманним історичній державності українського народу, тому повернення до власної демократичної суверенної державотворчої традиції та модернізація політичного життя на засадах функціонування сучасних

поліархій є запорукою нашого прогресу в епоху постмодерну XXI ст. [8, с. 354].

На переконання науковців, стабільність вітчизняного суспільства передбачає розробку та утвердження стійкої системи демократично орієнтованих пріоритетних цінностей. Необхідно визначити базові цінності, довкола яких згрупуються інші цінності та ідеї, утворюючи безпечні умови для існування людини та суспільства в цілому. Відповідна новітня система цінностей спрямована на об'єднання суспільств та людей, на забезпечення гідних та безпечних умов життя людини (особи) в сучасному суспільстві. Зрозуміло, що аналіз ціннісних основ безпеки особи є основою для формулювання політики регулювання ціннісної системи українського суспільства, насамперед через політичну дію особи та суспільних груп. Синтез процесів соціокультурної та національної самоідентифікації українського народу, що здійснюється в ході будівництва незалежної держави, означає реалізацію специфічного соціокультурного проекту, складовими якого слід вважати в першу чергу відродження культурної історичної пам'яті, рефлексію всього без винятку попереднього культурно-історичного досвіду та його реконструкцію на основі нової системи цінностей та орієнтації [9, с. 203].

Очевидно, розуміння інформаційної безпеки має включати в себе не тільки захист інформаційних ресурсів суспільства, держави та людини, а й збереження ціннісних аспектів історичної пам'яті, культурних традицій, специфічного національно-етнічного способу життя українського народу. У цьому контексті дослідники ведуть мову про захист інформаційного суверенітету нашої країни, розуміння якого вбирає в себе правові, політичні, ціннісно-культурні, безпекові й інформаційні процеси в державі. Цілком логічно, що програми з інформаційної безпеки спрямовані в першу чергу на захист інформаційного суверенітету держави.

Так, О. Олійник, О. Соснін, Л. Шиманський констатують, що інформаційний суверенітет Української держави – це виключне право України відповідно до Конституції, законодавства України та норм міжнародного права самостійно і незалежно з додержанням балансу інтересів особи, суспільства і держави визначати й здійснювати внутрішні та геополітичні національні інтереси в інформаційній сфері, державну внутрішню і зовнішню інформаційну політику, розпоряджатися власними інформаційними ресурсами, формувати інфраструктуру національного інформаційного простору, створювати умови для його інтегрування у світовий інформаційний простір та гарантувати інформаційну безпеку держави [10].

Інформаційний суверенітет України має забезпечуватися за рахунок:

а) виняткового права власності України на інформаційні ресурси, що формуються за рахунок коштів з державного бюджету;

б) створення відповідних національних систем інформації;

в) встановлення режиму доступу інших держав до інформаційних ресурсів України;

г) використання інформаційних ресурсів на засадах рівноправного співробітництва з іншими державами [11, с. 62].

Як справедливо зазначає О. Олійник, система забезпечення інформаційної безпеки безпосередньо впливає на забезпечення інформаційного суверенітету та є відповідним комплексом правових механізмів реалізації конституційних принципів суверенності і незалежності України. Інформаційний суверенітет є важливою умовою забезпечення інформаційної безпеки, вони взаємно пов'язані. Їх взаємозв'язки виявляються в такому:

– головною метою забезпечення як інформаційного суверенітету, так і інформаційної безпеки є захист національних інтересів;

– реалізація функцій держави в цих сферах має здійснюватися за загальними принципами, визначеними Конституцією України і законами України;

– забезпечення інформаційної безпеки безпосередньо пов'язано із суверенним правом держави, що випливає із засад інформаційного суверенітету як важливої складової державного суверенітету;

– державна політика у сфері забезпечення інформаційного суверенітету й інформаційної безпеки має як загальні напрями діяльності, так і такі, що реалізуються на властивих їм напрямах, котрі доповнюють один одного та підвищують рівень гарантій щодо досягнення позитивних результатів [12, с. 58].

На сьогоднішній день захист інформаційного суверенітету країни та забезпечення інформаційної безпеки є справою не тільки державних органів, але й приватних структур, суб'єктів громадянського суспільства. Саме останні в демократичному суспільстві беруть активну участь у формуванні й популяризації різноманітних цінностей, які є підґрунтям розвитку інституту інформаційної безпеки.

На переконання О. Гіда, недостатньо активно в країні формується громадська думка про те, що питання інформаційної безпеки не можуть забезпечуватись лише на урядовому рівні. Тому для ефективного вирішення цієї проблеми необхідно постійно поглиблювати партнерство держави з приватним сектором, оскільки багато стратегічних об'єктів нині знаходяться в його управлінні. У той же час українські компанії неохоче надають відомості про кількість і характер атак на їхні інформаційно-комунікаційні системи та наслідки і збитки від їх впливів. Вони також не повідомляють правоохоронні органи про наявні загрози вторгнення в роботу їхніх об'єктів інформаційної сфери. Компетентні органи також не володіють даними щодо наявності на цих об'єктах досконалих систем захисту від негативних інформаційних і кіберне-

тичних впливів. У результаті спостерігається надвисока латентність порушень в інформаційному просторі, що є одним із вагомих факторів процвітання кіберзлочинності в Україні [13, с. 233].

Практика свідчить, що окремі приватні компанії, які навіть мають потужні ресурси, не можуть комплексно та ефективно протидіяти кіберзлочинності. Тому існує потреба у плідній співпраці комерційних та державних структур у спільному захисті інформаційних інтересів держави.

Як доводять фахівці, в останні роки спостерігається різка активізація діяльності різного роду організованих кримінальних угруповань, а також екстремістських і терористичних організацій, які втручаються в інформаційний простір для реалізації своїх, далеких від благородних, намірів. Це і вчинення злочинів у різних сферах господарювання та управління, і хакерські атаки на урядові сайти і портали та банківські бази даних, і спроби дестабілізувати діяльність об'єктів критичної інфраструктури та суспільно-політичну обстановку в певному регіоні чи державі в цілому тощо. Усе більшого поширення набуває кібершпигунство. У багатьох випадках кібератаки чітко вмотивовані. Одні з них переслідують суто економічні чи фінансові інтереси або спрямовані на завдання людям фізичної шкоди, інші – мають яскраво виражене політичне забарвлення і спрямовані на посилення деструктивних настроїв у суспільстві. Немало випадків, коли кіберпростір використовується з хуліганських спонукань [14, с. 260].

Відповідно кіберзлочини здійснюють руйнівний вплив і на аксіологічне підґрунтя інформаційної безпеки держави та суспільства, порушуючи такі базові цінності, як справедливість у користуванні інформаційними ресурсами, рівність у доступі до інформаційних баз даних, правова захищеність індивідуальної та авторської інформації, підміна правової свободи анархією в інформаційному просторі тощо.

Можна констатувати, що ціннісна складова є обов'язковим елементом різноманітних рамкових та нормативних документів щодо регулювання діяльності суб'єктів у інформаційній сфері, захисту її від кіберзлочинів. Так, головна зовнішньополітична ініціатива США щодо перспектив розвитку кіберпростору, яка була оприлюднена 16 травня 2011 р. під назвою «Міжнародна стратегія для кіберпростору» (International Strategy for Cyberspace), містить низку «базових принципів», які відображають ціннісно-світоглядну спрямованість даного документа. Згідно із цією Стратегією такими принципами є:

– «фундаментальні свободи» (можливість шукати, отримувати й передавати інформацію та ідеї через будь-які засоби зв'язку та незважаючи на кордони);

– «прайвесі» (люди мають бути обізнані із загрозами їхній персональній інформації та про можливість здійснення проти них кіберзлочинів);

– «вільні потоки інформації» (рух інформації не має обмежуватися фільтрами, міжмережевими екранами, оскільки вони створюють видимість безпеки, кіберпростір має бути місцем інновацій та співпраці держави й бізнесу задля більшої безпеки) [15, с. 4–5].

У свою чергу, в Доктрині інформаційної безпеки України від 25 лютого 2017 р. чітко визначені національні інтереси України в інформаційній сфері, в основу яких покладені життєво важливі цінності існування людини, суспільства та держави. Такими національними інтересами в інформаційній сфері, зокрема, є:

1) життєво важливі інтереси особи: забезпечення конституційних прав і свобод людини на збирання, зберігання, використання та поширення інформації; забезпечення конституційних прав людини на захист приватного життя; захищеність від руйнівних інформаційно-психологічних впливів;

2) життєво важливі інтереси суспільства і держави:

– захист українського суспільства від агресивного впливу деструктивної пропаганди, передусім з боку Російської Федерації;

– захист українського суспільства від агресивного інформаційного впливу Російської Федерації, спрямованого на пропаганду війни, розпалювання національної і релігійної ворожнечі, зміну конституційного ладу насильницьким шляхом або порушення суверенітету і територіальної цілісності України;

– всебічне задоволення потреб громадян, підприємств, установ і організацій усіх форм власності в доступі до достовірної та об'єктивної інформації;

– забезпечення вільного обігу інформації, крім випадків, передбачених законом;

– розвиток та захист національної інформаційної інфраструктури;

– збереження і примноження духовних, культурних і моральних цінностей Українського народу;

– забезпечення всебічного розвитку і функціонування української мови в усіх сферах суспільного життя на всій території України;

– вільний розвиток, використання і захист мов національних меншин та сприяння вивченню мов міжнародного спілкування;

– зміцнення інформаційних зв'язків з українською діаспорою, сприяння збереженню її етнокультурної ідентичності;

– розвиток медіа-культури суспільства та соціально відповідального медіа-середовища;

– формування ефективної правової системи захисту особи, суспільства та держави від деструктивних пропагандистських впливів;

– створення з урахуванням норм міжнародного права системи і механізмів захисту від негативних зовнішніх інформаційно-психологічних впливів, передусім пропаганди;

– розвиток інформаційного суспільства, зокрема його технологічної інфраструктури;

– безпечне функціонування і розвиток національного інформаційного простору та його інтеграція у європейський і світовий інформаційний простір;

– розвиток системи стратегічних комунікацій України;

– ефективна взаємодія органів державної влади та інститутів громадянського суспільства під час формування, реалізації державної політики в інформаційній сфері;

– забезпечення розвитку інформаційно-комунікаційних технологій та інформаційних ресурсів України;

– захищеність державної таємниці та іншої інформації, вимоги щодо захисту якої встановлені законом;

– формування позитивного іміджу України у світі, донесення оперативної, достовірної і об'єктивної інформації про події в Україні до міжнародної спільноти;

– розбудова системи іномовлення України та забезпечення наявності іншомовного українського каналу в кабельних мережах та в супутниковому мовленні за межами України [16].

Як зазначалося вище, важливу роль у забезпеченні інформаційної безпеки держави, відтворення її ціннісної складової відіграють суб'єкти громадянського суспільства – аналітичні та наукові центри, громадські організації та рухи.

З цього приводу Ю. Лісовська стверджує, що включення інститутів громадянського суспільства в систему захисту інформаційної безпеки забезпечує вирішення низки важливих завдань. По-перше, забезпечується участь громадськості у прийнятті рішень з питань інформаційної безпеки. По-друге, введення інститутів громадянського суспільства у механізм політики інформаційної безпеки забезпечує процес залучення громадян у розв'язання проблем інформаційної безпеки, їхню активну позицію з відповідних питань [17, с. 110].

За класифікацією дослідника А. Головка, інститути громадянського суспільства, які виступають суб'єктами забезпечення інформаційної безпеки України, варто поділити на такі групи:

1) до першої групи слід віднести громадські об'єднання, тобто різного роду організації, спілки, асоціації та ін. Прикладом тут можуть слугувати ГО «Академія національної безпеки», Всеукраїнська асоціація «Інформаційна безпека та інформаційні технології», Центр військово-політичних досліджень (більш відома завдяки своєму проекту «Інформаційний опір»);

2) другу групу складають неурядові аналітичні центри як позадержавні експертні та наукові установи. До них варто віднести Український центр економічних і політичних досліджень ім. Олександра Разумкова (або просто

Центр Разумкова), Український інститут публічної політики, Центр політико-правових реформ;

3) третя група об'єднує всі недержавні засоби масової інформації, що діють на території України, а саме друковані джерела (журнали, газети), телевізійні канали, радіостанції, інтернет-ресурси. Тут можна згадати газету «Інформаційний бюлетень», інтернет-видання «Українська правда», телевізійні канали «112.ua», «Перший український інформаційний – 5 канал», телевізійний канал «24» та ін. [18, с. 104].

Залучаючи громадян до заходів з інформаційної безпеки, громадські організації здійснюють аксіологічну та просвітницько-виховну функції, формують суспільну думку щодо важливих питань захисту національних інформаційних інтересів.

Сучасні демократичні країни демонструють стабільну практику співпраці державних та недержавних суб'єктів інформаційної безпеки, що знайшло своє відображення і на законодавчому рівні. Наприклад, 26 листопада 2003 р. Конгресом США ухвалено закон «Про внутрішню безпеку» (Home Security Act), відповідно до якого створено Міністерство внутрішньої безпеки (Department of Homeland Security), на яке покладено координацію діяльності державних органів і всіх приватних структур з питань забезпечення інформаційної безпеки. Цим законом передбачено розробку Національної стратегії із забезпечення безпеки у кіберпросторі (National Strategy to Secure Cyberspace) та Національної стратегії фізичного захисту об'єктів життєзабезпечення населення (The National Strategy for the Physical Protection of Critical Infrastructures). Зазначеними документами передбачено створення єдиної національної системи протидії кібернетичному тероризму, в рамках якої ініційовано створення територіальних, відомчих і приватних центрів протидії, визначено їхні функції та порядок взаємодії [19, с. 93–94].

Європейські країни рухаються у схожому напрямі. Так, у лютому 2011 р. уряд Нідерландів ухвалив Національну стратегію кібербезпеки «Сила через співпрацю», якою передбачено створення Національної ради з кібербезпеки. Завданням цього органу буде забезпечення реалізації підходу, в основу якого покладено співробітництво державного та приватного секторів, а також різного роду наукових центрів. Передбачено також створення Національного центру з питань кібербезпеки, завданням якого є виявлення тенденцій та загроз інформаційній безпеці, а також сприяння подоланню наслідків інцидентів і кризових ситуацій у цій сфері [20, с. 30–31].

Аналіз нормативно-правової бази, що регламентує участь недержавних суб'єктів як структурних елементів системи забезпечення інформаційної безпеки, дає підстави виокремити такі її основні форми:

– участь у роботі консультативно-дорадчих органів при органах державного управління в інформаційній сфері;

– участь у публічних громадських обговореннях, що проводяться органами державного управління в інформаційній сфері;

– участь у вивченні громадської думки, що проводиться органами державного управління в інформаційній сфері;

– направлення органам державного управління в інформаційній сфері інформаційних запитів та скарг у ході громадського контролю за їх діяльністю, а також скарг та заяв про інформаційні правопорушення в процесі громадського контролю за дотриманням законності в інформаційній сфері;

– направлення органам державного управління в інформаційній сфері заяв (клопотань) про задоволення прав та законних інтересів у цій сфері [21, с. 34].

Вищенаведене свідчить, що недержавні суб'єкти інформаційної безпеки мають можливості публічно обговорювати політичні, правові, моральні та інші цінності, утверджувати їх значення в суспільному житті, впливати на формування ціннісної підойми суспільної свідомості, а, як наслідок, прямо та опосередковано брати участь у захисті інформаційного суверенітету держави.

Як справедливо стверджує К. Захаренко, впливовим недержавним суб'єктом інформаційної безпеки країни є неурядові аналітичні центри. Роль неурядових аналітичних центрів як генераторів нових ідей та альтернативних підходів є особливо важливою на перехідних етапах, коли відбуваються глибокі внутрішні трансформації в усіх сферах суспільного життя, у сфері інформаційної безпеки зокрема. Неурядові аналітичні центри є також інструментом громадського контролю, вони впливають і на визначення цілей та цінностей суспільства, формують суспільну думку, яка є основним об'єктом інформаційних атак з боку інших держав. Їх потенціал як посередника та ефективного каналу зв'язку між інтелектуальним середовищем і державними органами та суспільством важко переоцінити. Неурядові аналітичні центри – це потужний інструмент громадського контролю за діями влади. Важлива їхня роль і у визначенні цілей та цінностей суспільства, формуванні громадської думки з актуальних для країни питань. Як правило, неурядові аналітичні центри представлені у медіа-просторі країни: їх спеціалісти виступають у ЗМІ, фахівці аналітичних центрів надають коментарі із суспільно важливих питань, попереджають про загрози у сфері національної безпеки, інформаційної зокрема [22, с. 59–60].

Разом з тим у роботі аналітичних центрів України (як державних, так і недержавних) сьогодні існує безліч проблем, які негативно впливають на їх можливості щодо протидії інформаційним загрозам перед суспільством та державою. Перш за все це відсутність бюджетного фінансування аналітичних

структур (окрім деяких урядових закладів). Щодо неурядових (які є найбільш професійними аналітичними структурами в Україні), то через відсутність попиту з боку органів державної влади на послуги незалежних аналітичних структур їх фінансове, організаційне й матеріальне забезпечення беруть на себе зарубіжні спонсори, а це, у свою чергу, формує в Україні професійне аналітичне середовище, яке, з одного боку, незалежне від діючої влади, а з іншого – може реалізовувати цілі, не завжди прийнятні для інтересів держави. Другою проблемою є неготовність органів державної влади співпрацювати із зовнішніми джерелами інформації й проектами, а це спричиняє закритість та непрозорість процедури підготовки й ухвалення рішень вищим політичним керівництвом держави. Щодо роботи партійних та ділових структур, то тут також спостерігається їх неготовність працювати в режимі прикладних політичних досліджень, нових ділових і політичних стратегій, нестандартних рішень. Проблему складає й кадрове питання через низький рівень інтелектуальної підготовки політичних аналітиків, що не дозволяє українським «фабрикам думки» конкурувати із закордонними аналогами [23, с. 380].

Отже, аналітичні центри (як урядові, так і неурядові) здатні значно посилити ціннісно-знаннєві підвалини інформаційної безпеки нашої держави, запропонувати науково обґрунтоване вирішення складних проблем у цій царині, здійснювати інтелектуальну підтримку інформаційного спротиву України у «гібридній війні». На жаль, можливості цих структур не завжди раціонально використовуються державними органами, які відповідають за інформаційну безпеку, зокрема їх аналітичні розробки часто-густо не знаходять свого практичного втілення.

Підсумовуючи вищенаведене, варто зауважити, що низка проблем у інформаційній безпеці нашої держави в її аксіологічному вимірі обумовлена деформаціями інформаційного простору під впливом різноманітних чинників об'єктивного та суб'єктивного характеру.

Зокрема, до головних негативних чинників, які зумовлюють сучасний стан українського інформаційного простору, фахівці відносять такі:

– відсутність чіткої скоординованої державної інформаційної політики за умов наявності й активного виконання кількох, на жаль, недостатньо скоординованих державних програм за такими напрямами, як інформатизація, формування і захист національного інформаційного ресурсу і простору тощо;

– інвестування інформаційних структур (як державних, так і приватних) за «залишковим принципом» унаслідок економічних причин;

– експансія в Україну зарубіжних виробників інформаційної продукції, що об'єктивно переважають національних за якістю продукції, економічними можливостями, а також застосовують агресивну ринкову стратегію;

– недостатній професійний рівень працівників інформаційної сфери, недоліки вітчизняної системи їхньої підготовки (особливо це стосується електронних ЗМІ та нових інформаційних, зокрема глобальних, систем);

– технічне відставання інформаційної інфраструктури і її повна залежність від постачання іноземної техніки, занепад вітчизняної телекомунікаційної промисловості [24, с. 130].

Висновки. Таким чином, аксіологічне підґрунтя інформаційної безпеки України є квінтесенцією ментальних, цивілізаційних, політичних, правових, культурно-історичних цінностей та традицій, які мають забезпечувати сталість суспільного розвитку й збереження національно-культурної самобутності нашого народу. Важливою складовою забезпечення інформаційного суверенітету нашої держави є відтворення загальнолюдських та національних цінностей як державними інститутами, так і суб'єктами громадянського суспільства. Держава має стимулювати громадянську ініціативу щодо зміцнення інформаційної безпеки, створювати належні правові та економічні умови для діяльності суб'єктів громадянського суспільства в цій царині.

ЛІТЕРАТУРА

1. Радченко О. Моделювання державної комунікативної політики в умовах сучасної України / О. Радченко, О. Бухтатий // Публ. упр.: теорія та практика. – 2014. – Вип. 3. – С. 80–91.
2. Зайцев М. М. Суб'єкти забезпечення інформаційної безпеки України / М. М. Зайцев // Форум права. – 2013. – № 3. – С. 231–238.
3. Чічановський А. А. Інформаційні процеси в структурі світових комунікаційних систем : підручник / А. А. Чічановський, О. Г. Старіш. – Київ : Грамота, 2010. – 568 с.
4. Зязюн І. Криза цінностей – катастрофа суспільств і держав / І. Зязюн // Освіта дорослих: теорія, досвід, перспективи. – 2010. – № 2. – С. 7–19.
5. Кравченко Т. О. Аксіологічний аспект інформаційно-мережевої парадигми / Т. О. Кравченко // Філософія науки: традиції та інновації. – 2014. – № 1. – С. 53–63.
6. Литвиненко О. Проблема інформаційної безпеки в контексті сучасного українознавства / О. Литвиненко // Українознавчий альманах. – 2011. – Вип. 5. – С. 202–205.
7. Дмитерко Ю. Ю. Відображення дійсності у ЗМІ: державно-правовий аспект журналістики / Ю. Ю. Дмитерко // Ефективність держ. упр. – 2014. – Вип. 38. – С. 361–367.
8. Поліщук І. О. Державотворча традиція України: політико-культурний вимір : наук. монографія / І. О. Поліщук, В. І. Чигрінов. – Харків : ХІБМ, 2006. – 380 с.
9. Бушман І. О. Ціннісні орієнтири сучасного суспільства / І. О. Бушман // Гілея : наук. вісн. – 2015. – Вип. 102. – С. 201–205.

10. Олійник О. В. Політико-правові аспекти формування інформаційного суспільства суверенної і незалежної держави [Електронний ресурс] / О. В. Олійник, О. В. Соснін, Л. Є. Шиманський. – Режим доступу: http://www.niss.gov.ua/book/Sosnin_2.htm.
11. Кирильчук Є. О. Проблеми національної інформаційної безпеки України в контексті сучасних національних державотворчих процесів та світової інтеграції / Є. О. Кирильчук // Наук. пр. МАУП. – 2013. – Вип. 1. – С. 60–63.
12. Олійник О. Інформаційний суверенітет як важлива умова забезпечення інформаційної безпеки України / О. Олійник // Наук. зап. Ін-ту законодавства Верхов. Ради України. – 2015. – № 1. – С. 54–59.
13. Гіда О. Ф. Фактори, що впливають на формування викликів національним інтересам України в інформаційному просторі / О. Ф. Гіда // Боротьба з організ. злочинністю і корупцією (теорія і практика). – 2013. – № 2. – С. 228–236.
14. Гіда О. Ф. Міжнародні ініціативи у сфері посилення інформаційної безпеки та протидії організованій злочинності / О. Ф. Гіда // Боротьба з організ. злочинністю і корупцією (теорія і практика). – 2012. – Вип. 1. – С. 258–266.
15. Дубов Д. В. Майбутнє кіберпростору та національні інтереси України: нові міжнародні ініціативи провідних геополітичних гравців : аналіт. доп. / Д. В. Дубов, М. А. Ожеван. – Київ : НІСД, 2012. – 32 с.
16. Доктрина інформаційної безпеки України від 25 лютого 2017 р. [Електронний ресурс]. – Режим доступу: http://www.president.gov.ua/documents/472017–21374.
17. Лісовська Ю. П. Адміністративно-правова діяльність недержавних органів та організацій як структурних елементів системи забезпечення інформаційної безпеки / Ю. П. Лісовська // Наук. пр. МАУП. – 2014. – Вип. 2 (41). – С. 108–113.
18. Головка А. А. Громадянське суспільство як суб'єкт забезпечення інформаційної безпеки України / А. А. Головка // Україна в процесах глобального інформаційного обміну : матеріали наук.-практ. конф. (м. Львів, 26–27 трав. 2016 р.). – Львів : Нац. ун-т «Львів. політехніка», 2016. – С. 103–105.
19. Алямкін Р. В. Правове забезпечення національної інформаційної безпеки / Р. В. Алямкін, М. П. Федорін // Наук. зап. Ін-ту законодавства Верхов. Ради України. – 2013. – № 4. – С. 91–96.
20. Доклад Группы правительственных экспертов по достижениям в сфере информатизации и телекоммуникаций в контексте международной безопасности (A/65/201). – Нью-Йорк : Организация Объединенных Наций, 2012. – 57 с.
21. Бурило Ю. П. Участь недержавних суб'єктів у здійсненні державного управління інформаційною сферою / Ю. П. Бурило // Прав. інформатика. – 2007. – № 4. – С. 31–41.
22. Захаренко К. Ефективність використання потенціалу недержавних суб'єктів інформаційної безпеки / К. Захаренко // Мультиверсум : філос. альманах. – 2016. – Вип. 1–2. – С. 58–70.
23. Лисак В. Ф. Сучасні українські «мозкові центри» як суб'єкти суспільно-політичного процесу в державі / В. Ф. Лисак, О. Л. Агєєва // Гілея : наук. вісн. – 2015. – Вип. 95. – С. 377–382.

24. Хімей В. Основні сучасні проблеми інформаційної безпеки України / В. Хімей // Теле- та радіожурналістика. – 2014. – Вип. 13. – С. 127–132.

REFERENCES

1. Radchenko, O., Bukhtatyy, O. (2014). Modelyuvannya derzhavnoyi komunikatyvnoyi polityky v umovakh suchasnoyi Ukrayiny. *Publichne upravlinnya: teoriya ta praktyka – Public administration: theory and practice, issue 3, 80–91* [in Ukrainian].
2. Zaytsev, M. M. (2013). Subyekty zabezpechennya informatsiynoyi bezpeky Ukrayiny. *Forum prava –Law forum, 3, 231–238* [in Ukrainian].
3. Informatsiyni protsesy v strukturi svitovykh komunikatsiynykh system. A.A. Chichanovskyy, O.H. Starish (Eds.). (2010). Kyiv: Hramota [in Ukrainian].
4. Zyazyun, I. (2010). Kryza tsinnostey – katastrofa suspilstv i derzhav. *Osvita doroslykh: teoriya, dosvid, perspektyvy – Adult education: theory, experience and perspectives*, *2, 7–19* [in Ukrainian].
5. Kravchenko, T. O. (2014). Aksiolohichnyy aspekt informatsiyno-merezhevoyi paradyhmy. *Filosofiya nauky: tradytsiyi ta innovatsiyi – Philosophy of science: traditions and innovations*, *1, 53–63* [in Ukrainian].
6. Lytvynenko, O. (2011). Problema informatsiynoyi bezpeky v konteksti suchasnoho ukrayinoznavstva. *Ukrayinoznavchyy al'manakh – Almanac of Ukraine*, *issue 5, 202–205* [in Ukrainian].
7. Dmyterko, Yu.Yu. (2014). Vidobrazhennya diysnosti u zmi: derzhavno-pravovyy aspekt zhurnalistyky. *Efektyvnist' derzhavnoho upravlinnya – The effectiveness of public administration*, *issue 38, 361–367* [in Ukrainian].
8. Polishchuk, I. O., Chyhrinov, V. I. (2006). Derzhavotvorcha tradytsiya Ukrayiny: polityko-kul'turnyy vymir: Naukova monohrafiya. Kharkiv: KhIBM [in Ukrainian].
9. Bushman, I. O. (2015). Tsinnisni oriyentyry suchasnoho suspil'stva. *Hileya: naukovyy visnyk – Hilea: scientific journal, issue 102, 201–205* [in Ukrainian].
10. Oliynyk, O. V., Sosnin, O. V., Shymans'kyy, L. Ye. (2010). Polityko-pravovi aspekty formuvannya informatsiynoho suspil'stva suverennoyi i nezalezhnoyi derzhavy. URL: http://www. niss. gov.ua/book/Sosnin_2.htm [in Ukrainian].
11. Kyryl'chuk, Ye. O. (2013). Problemy natsional'noyi informatsiynoyi bezpeky Ukrayiny v konteksti suchasnykh natsional'nykh derzhavotvorchykh protsesiv ta svitovoyi intehratsiyi. *Naukovi pratsi MAUP –Proceedings AIDP, issue 1, 60–63* [in Ukrainian].
12. Oliynyk, O. (2015). Informatsiynyy suverenitet yak vazhlyva umova zabezpechennya informatsiynoyi bezpeky Ukrayiny. *Naukovi zapysky Instytutu zakonodavstva Verkhovnoyi Rady Ukrayiny. –Scientific notes the Institute of Legislation Verkhovna Rada of Ukraine, 1, 54–59* [in Ukrainian].
13. Hida, O. F. (2013). Faktory, shcho vplyvayut' na formuvannya vyklykiv natsional'nym interesam Ukrayiny v informatsiynomu prostori. *Borot'ba z orhanizovanoyu zlochynnistyu i koruptsiyeyu (teoriya i praktyka) – The fight against organized crime and corruption (theory and practice), 2, 228–236* [in Ukrainian].
14. Hida, O. F. (2012). Mizhnarodni initsiatyvy u sferi posylennyainformatsiynoyi bezpeky ta protydiyi orhanizovaniy zlochynnosti. *Borot'ba z orhanizovanoyu zlochynnistyu*

i koruptsiyeyu (teoriya i praktyka) – The fight against organized crime and corruption (theory and practice), issue 1, 258–266 [in Ukrainian].
15. Dubov, D. V., Ozhevan M.A. (2012). Maybutnye kiberprostoru ta natsional'ni interesy Ukrayiny: novi mizhnarodni initsiatyvy providnykh heopolitychnykh hravtsiv : analit. dop. Kyiv: NISD [in Ukrainian].
16. Doktryna informatsiynoyi bezpeky Ukrayiny vid 25 lyutoho 2017. URL: http://www.president.gov.ua/documents/472017–21374
17. Lisovs'ka, Yu.P. (2014). Administratyvno-pravova diyal'nist' nederzhavnykh orhaniv ta orhanizatsiy yak strukturnykh elementiv systemy zabezpechennya informatsiynoyi bezpeky. *Naukovi pratsi MAUP – Scientific works IAPM, issue 2 (№ 41), 108–113* [in Ukrainian].
18. Holovka, A. A. (2016). Hromadyans'ke suspil'stvo yak sub»yekt zabezpechennya informatsiynoyi bezpeky Ukrayiny. *Ukrayina v protsesakh hlobal'noho informatsiynoho obminu* : proceedings of the Scientifik and Practical Conference. L'viv: Natsional'nyy universytet «L'vivs'ka politekhnika», *103–105* [in Ukrainian].
19. Alyamkin, R. V., Fedorin, M. P. (2013). Pravove zabezpechennya natsional'noyi informatsiynoyi bezpeky. *Naukovi zapysky Instytutu zakonodavstva Verkhovnoyi Rady Ukrayiny – Scientific notes of the Institute of Legislation of Supreme Council of Ukraine, 4, 91–96* [in Ukrainian].
20. Doklad Hruppu pravytel'stvennukh ekspertov po dostyzhenyyam v sfere ynformatyzatsyy y telekommunykatsyy v kontekste mezhdunarodnoy bezopasnosty (A/65/201). (2012). N'yu-York, Orhanyzatsyya Obedynennukh Natsyy.
21. Burylo, Yu.P. (2007). Uchast' nederzhavnykh sub»yektiv u zdiysnenni derzhavnoho upravlinnya informatsiynoyu sferoyu. *Pravova informatyka – Law informatics*, *4, 31–41* [in Ukrainian].
22. Zakharenko, K. (2016). Efektyvnist' vykorystannya potentsialu nederzhavnykh sub»yektiv informatsiynoyi bezpeky. *Mul'tyversum. Filosofs'kyy al'manakh – Multiverse. Philosophical almanac, issue 1–2, 58–70* [in Ukrainian].
23. Lysak, V.F. Ahyeyeva, O. L. (2015). Suchasni ukrayins'ki «mozkovi tsentry» yak sub»yekty suspil'no-politychnoho protsesu v derzhavi. *Hileya: naukovyy visnyk – Hilea: scientific journal, issue 95, 377–382* [in Ukrainian].
24. Khimey, V. (2014). Osnovni suchasni problemy informatsiynoyi bezpeky Ukrayiny. *Tele- ta radiozhurnalistyka – Tele- and radio journalism, issue 13, 127–132* [in Ukrainian].

АКСИОЛОГИЧЕСКОЕ ИЗМЕРЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ УКРАИНСКОГО ГОСУДАРСТВА

Мануйлов Е. Н., Калиновский Ю. Ю.

Исследованы ценностные аспекты информационной безопасности Украинского государства. Проанализирован зарубежный опыт стратегического планиро-

вания в сфере информационной безопасности. Определены сущностные характеристики информационного суверенитета Украины. Раскрыта роль субъектов гражданского общества в обеспечении аксиологической основы информационной безопасности.

Ключевые слова: *информационная безопасность, ценности, государственное строительство, информационный суверенитет, информационное пространство.*

AXIOLOGICAL DIMENSION OF UKRAINIAN INFORMATION SECURITY

Manuylov E. M., Kalinowski Y. Y.

Investigated the value of information security aspects of the Ukrainian state. It is alleged that in today's global processes, information is a powerful resource that contributes to national progress. Therefore, acquiring accurate information, storage, protection and processing speed are prerequisites of stable existence of any state. In turn, the realization of the human right to get an accurate information is a necessary part of the democratic development of society. Today there is an urgent need for consolidation and dissemination of humanistic values through various communication media, particularly among Internet users by promoting educational, scientific, popular, religious, literary, ethical content in an affordable and compelling form for different population groups. Such activities will surely enhance the value of information security foundations of our country.

Determined intrinsic characteristics of information sovereignty of Ukraine. Proved that an understanding of information security should include not only the protection of information resources of society, the state and the person, but also preserving of valuable aspects of historical memory, cultural traditions, and specific national and ethnic lifestyle of Ukrainian people. In this context, researchers are talking about the protection of information sovereignty of our country which understanding includes legal, political, and cultural values, security and information processes in the country.

Revealed the role of subjects of civil society in providing of axiological levers of information security. Research shows that non-subject of information security have the opportunity to publicly discuss the political, legal, moral and other values, to assert their importance in public life, to influence the value levers of social consciousness and as a result directly or indirectly participate in the protection of information sovereignty state. Specifically, analytical centers (both governmental and non-governmental) can greatly enhance the value and knowledge of information security foundations of our state, to offer scientifically grounded solutions to complex problems in this area, to make information supporting the intellectual opposition of our country in «hybrid warfare». Unfortunately, the possibilities of these structures are not always used efficiently by authorities that in charge of information security, in particular their analytical development often do not find their practical implementation.

Proved that the state should strategically strengthen the axio-sphere of society by playing values through education and training and take care of information security and protection of cultural and information fields of the country from external influences. Information stability and implementing clear value priorities of democratic state will ensure competitiveness in the current global processes.

Key words: *information security, values, state-building, information sovereignty, information space.*