

УДК 303.8

К. В. Захаренко, к. філос. н.,
здобувач**ПРОБЛЕМИ КОНСОЛІДАЦІЇ СУБ'ЄКТІВ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ**

Анотація. Аналізуються проблеми, суперечності та технології консолідації діяльності суб'єктів інформаційної безпеки. В статті розглядається вплив як внутрішніх, так і зовнішніх інформаційно-ідеологічних суб'єктів. Автор доводить, що під тиском інформаційної революції виникають загрози, які спричиняють необхідність запровадження різних засобів і технологій інформаційної безпеки. Їх функціонування покликані забезпечувати суб'єкти інформаційної безпеки – від окремих індивідів до соціальних інститутів, між якими має бути налагоджена належна взаємодія.

Ключові слова: людина; політика; інформація; культура; інформаційна безпека; суб'єкти інформаційної безпеки.

К. В. Захаренко, к. филос. н.,
соискатель**ПРОБЛЕМЫ КОНСОЛИДАЦИИ СУБЪЕКТОВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ**

Аннотация. Анализируются проблемы, противоречия и технологии консолидации деятельности субъектов информационной безопасности. В статье рассматривается влияние как внутренних, так и внешних субъектов. Автор доказывает, что под влиянием информационной революции возникают угрозы, которые обуславливают необходимость внедрения различных методов и технологий информационной безопасности. Их функционирование должны обеспечивать субъекты информационной безопасности – от отдельных индивидов до социальных институтов, между которыми должно быть налажено соответствующее взаимодействие.

Ключевые слова: человек; политика; информация; культура; информационная безопасность; субъекты информационной безопасности.

К. V. Zakharenko, Candidate of Philosophical Sciences,
Degree Seeker**ISSUES OF INFORMATION SECURITY SUBJECTS CONSOLIDATION**

Urgency of the research. Analyzing subject-object interactions in the field of information security, it is necessary to focus on the essential characteristics of information security ideological subjects first of all.

Target setting. In the context of our study, it is important to find out how relations between party structures, mass media and the state are developing, since it is with the help of the media that ideological actors influence the country's information security.

Actual scientific researches and issues analysis. The studies by such foreign and domestic experts are quite interesting: D. C. Hallin, P. Mancini, V. Madison, O. Boichenko, V. Bryzhko, V. Vakulych, O. Hida, O. Dzoban, Ya. Malyk, Yu. Nesteriako, Yu. Ruban and others. Experts agree that the development analysis of the main domestic media sectors gives grounds for asserting that the model of "Polarized pluralism" exists in Ukraine is highly probable.

Uninvestigated parts of general matters defining. Excepting internal ideological subjects of Ukraine information security, it is important to analyze the impact on it and external ideological actors.

The research objective. It is necessary to consider the problems, contradictions and technologies of the information security actors' activities consolidation.

The statement of basic materials. Problems, contradictions and technologies of consolidation of information security subjects activity are analyzed. The article examines the influence of both internal and external informational and ideological subjects.

Conclusions. The author proves that under the pressure of the information revolution there are threats that necessitate the introduction of various information security means and technologies. Their functioning is intended to provide the subjects of information security - from individuals to social institutions, between which proper interaction should be established.

Keywords: human; policy; information; culture; information security; information security subjects.

DOI: 10.25140/2412-1185-2018-1(11)-36-43

Актуальність теми дослідження. Аналізуючи суб'єкт-об'єктні взаємодії у сфері інформаційної безпеки необхідно насамперед зосередити увагу на сутнісних характеристиках ідеологічних суб'єктах інформаційної безпеки.

В залежності від типу політичної системи роль ідеологічних суб'єктів інформаційної безпеки, а саме партій, громадських рухів тощо, може бути багатоаспектною за формами прояву та силі впливу на загальнодержавну систему інформаційної безпеки. Так, у тоталітарних країнах ідеологічні суб'єкти інформаційної безпеки (партії, державний апарат) не допускають інших суб'єктів – колективи, етнонаціональні групи, до діяльності у цій сфері. Інформаційна безпека при тоталітаризмі спрямована, перш за все, на захист інтересів держави. Інформаційні потреби людини й суспільства в таких системах мають другорядний характер. Необхідно зазначити, що інформаційна політика у тоталітарній країні передбачає захист “провладних” ідеологічних постулатів та критику інших ідеологій, які характеризуються як реакційні. Відповідно, у тоталітарних країнах всі засоби масової інформації знаходяться під жорстким контролем держави і являють собою систему не тільки агітації й пропаганди, а є також знаряддям маніпулювання суспільною свідомістю.

Як відомо, у демократичних політичних системах не існує однієї державницької ідеології. Держава забезпечує конкуренцію ідеологій, які є ненасильницькими за своєю суттю, на відміну, скажімо, від фашизму або комунізму. Інформаційна безпека у демократичних країнах спрямована на захист інтересів і громадянина, і держави, і суспільства як рівноправних об'єктів. У системі забезпечення інформаційної безпеки демократичної країни гармонізуються інтереси та відносини у трикутнику „людина – держава – суспільство”. В свою чергу ідеологічні суб'єкти інформаційної безпеки, а це перш за все, партії та їх представники в органах влади всіх рівнів й громадських організаціях впливають на вироблення інформаційної політики держави.

Постановка проблеми. В контексті нашого дослідження важливо з'ясувати як вибудовуються відносини між партійними структурами, мас-медіа та державою, оскільки саме за допомогою ЗМІ ідеологічні суб'єкти впливають на інформаційну безпеку країни. Вочевидь, що засоби масової інформації відіграють не останню роль у здійсненні інформаційної політики держави та у її інформаційній безпеці через це ідеологічне (партійне) спрямування медіа набуває стратегічного значення щодо захисту національних інформаційних інтересів.

Аналіз останніх досліджень і публікацій. Західні дослідники Д. Галлін та П. Манчіні у своїй науковій праці “Чотири теорії преси” проаналізували три моделі взаємодії засобів масової інформації та держави, визначивши також і роль ідеологічних суб'єктів (партій) у цих взаємовідносинах.

Перша – це модель “Поляризованого плюралізму”, що характеризується низьким рівнем тиражів газет, низькою фактичною (часом на відміну від декларованої) професіоналізацією медіа-спільноти, високим рівнем пов'язаності ЗМІ з політичними партіями та фінансово-промисловими групами, в тому числі регіональними; ця система розвинулася у країнах Південної Європи (Іспанія, Італія, Греція, Португалія).

Друга модель отримала назву “Демократичного корпоративізму” і характеризується високим рівнем розвитку наступних чотирьох параметрів: масової преси, політичного паралелізму, журналістської професіоналізації та втручання держави у діяльність ЗМІ. Вона характерна переважно для країн Центральної і Північної Європи (Німеччина, Австрія, Швейцарія, Бельгія,

Голландія, Данія, Фінляндія, Норвегія, Швеція), а її назва пов'язана з визначальною роллю у діяльності ЗМІ стабільних соціальних груп-корпорацій.

Третя модель – “Ліберальна”. Вона має високий ступінь журналістської професіоналізації, середній рівень тиражів масових газет, низький рівень політичного паралелізму, низький рівень втручання держави у діяльність засобів масової інформації. Така модель характерна для держав Північно-Атлантичного регіону (Великобританія, Канада, США) [1].

Досить цікавими, у цьому контексті, є дослідження О. Бойченка, В. Брижка, В. Вакулича, О. Гіда, О. Дзьобаня, Я. Малика, Ю. Нестеряка, Ю. Рубана та інших. Фахівці сходяться на думці, що аналіз розвитку основних вітчизняних галузей засобів масової інформації (телебачення, радіомовлення, преса, інформаційні агентства) дає підстави стверджувати щодо високої імовірності існування в Україні моделі “Поляризованого плюралізму”. Зокрема, за інформацією відповідних державних установ (Державної статистичної служби України, Книжкової палати ім. І. Федорова) та органів (Державний комітет телебачення і радіомовлення, Національна рада України з питань телебачення і радіомовлення) галузь засобів масової інформації характеризується низьким рівнем тиражів газет та високим рівнем пов'язаності з політичними партіями та фінансово-промисловими групами [2, с. 105].

На думку дослідників В. Шахова та В. Мадіссона, в умовах глобалізації виникає багато питань стосовно змісту та ролі національного інтересу в житті країни. Адже зрозуміло, що в умовах тотального розвитку інтеграційних процесів, подальшої інтернаціоналізації політики і зростання ролі міжнародних організацій об'єктивно відбувається процес звуження національно-державного суверенітету, оскільки посилюється втручання міжнародних організацій у внутрішні справи країни, яка прагне взяти участь в тих чи інших інтеграційних проектах [3, с. 48].

Виділення недосліджених частин загальної проблеми. З нашої точки зору, окрім внутрішніх ідеологічних суб'єктів інформаційної безпеки України, варто аналізувати вплив на неї й зовнішніх ідеологічних суб'єктів.

Постановка завдання. Необхідно розглянути проблеми, суперечності та технології консолідації діяльності суб'єктів інформаційної безпеки.

Виклад основного матеріалу. Дослідники розрізняють внутрішні та зовнішні джерела інформаційної безпеки.

До зовнішніх джерел інформаційної безпеки належить діяльність іноземних політичних, військових, економічних та розвідувальних структур в інформаційній сфері; політика домінування деяких країн в інформаційній сфері; діяльність міжнародних терористичних груп; розробка концепцій інформаційних війн будь-якими структурами; культурна експансія у відношенні до конкретної країни [5, с. 24].

Наслідки їх діяльності можуть бути як позитивними, так і негативними. Позитивні наслідки проявляються тоді, коли зовнішні ідеологічні суб'єкти (партії, громадські організації, наднаціональні структури) підтримують ідеологічні настанови певної країни, наприклад, сприяють утвердженню ліберальних (демократичних) цінностей в Україні, діляться досвідом проведення певних реформ та ін. Негативний вплив зовнішніх ідеологічних суб'єктів проявляється у нав'язуванні тим або іншим країнам ціннісно-світоглядних настанов не сумісних з їх культурою, політичними традиціями, правовою системою тощо.

Як свідчить світова практика зовнішні ідеологічні суб'єкти можуть бути задіяні у інформаційних війнах. У сучасних умовах розповсюдження інформаційних технологій об'єктом таких війн може стати будь-яка держава. Найбільш вразливими для інформаційно-психологічної експансії виявляються держави, які характеризуються:

а) відносною політичною відкритістю та включеністю у глобальні процеси обміну капіталами та інформацією;

б) етнічною, расовою, конфесійною, ідеологічною строкатістю;

в) слабкими та/або нерозвиненими політичними інститутами й інститутами сектора безпеки [4, с. 6].

В наш час Україна постає типовим об'єктом впливу зовнішніх інформаційно-ідеологічних суб'єктів. Предметом цих впливів є національна єдність, територіальна цілісність, мова, культура, релігія, зовнішньополітичний вектор розвитку української держави. Проте зовнішні руйнівні дії певних суб'єктів не мали б значного впливу на суспільну свідомість та громадську думку, якби їх не підтримували політичні сили або окремі політики в самій Україні.

Таким чином, чим розвиненішими є внутрішні ідеологічні суб'єкти інформаційної безпеки та структури, що з ними взаємодіють, тим меншим є вплив зовнішніх ідеологічних суб'єктів. Основне завдання внутрішніх ідеологічних суб'єктів інформаційної безпеки полягає у захисті національних інтересів та пріоритетів, а також у чіткому розумінні політико-ідеологічних цілей зовнішніх ідеологічних суб'єктів.

Інтеграційні процеси, розвиток ринкової економіки та інтернаціоналізація ринку капіталу й праці актуалізують проблему ролі суб'єкта комерційної діяльності як агента інформаційної безпеки (небезпеки) суспільства (якщо комерційна мета суперечить інтересам держави і суспільства, можливі його деструктивні інформаційні впливи на суспільство).

Суб'єкт комерційної діяльності у XXI сторіччі не може обійтись без застосування інформаційних технологій у різний спосіб: рекламна компанія, збереження та обробка інформації, продаж певної інформації іншим комерційним структурам, захист персональних даних співробітників, захист новітніх технологічних розробок тощо. Разом з тим, існує постійна небезпека несанкціонованого втручання у інформаційні ресурси комерційних суб'єктів з боку інших держав, іноземних комерційних структур (промисловий та комерційний шпіонаж, знищення баз даних задля перемоги у конкурентній боротьбі тощо).

Саме тому від якісного захисту власних інформаційних ресурсів суб'єктами комерційної діяльності залежить і загальносуспільна та загальнодержавна інформаційна безпека, перш за все, у сфері економічної діяльності. Вищезначені суб'єкти повинні дбати про власну інформаційну безпеку, прогнозуючи та нівелюючи можливі загрози, оскільки захист комерційної інформації є важливим чинником безпеки суспільства та держави в цілому та інформаційної зокрема.

Як зазначають фахівці, у сфері інформаційної безпеки комерційних структур, основні загрози, що відносяться до порушення можливості використання комп'ютерних систем або обробленої інформації, становлять загрози доступності. Ідентифікація і контроль за діями користувачів, керованість комп'ютерною системою становлять предмет спостереження й керованості. Як правило, інформаційні системи аналізуються в трьох головних секторах: технічних засобах, програмному забезпеченні і комунікаціях для ідентифікування і застосування промислових стандартів інформаційної безпеки, як механізми захисту і запобігання на трьох рівнях: фізичному, особистому і організаційному [6, с. 64].

З нашої точки зору, особливу роль у забезпеченні інформаційної безпеки суспільства і держави відіграють такі комерційні суб'єкти як ІТ-компанії: співробітництво з державою у розробці нового програмного продукту для всіх сфер життєдіяльності суспільства, розробка систем захисту інформаційних ресурсів держави, участь у створенні загальнодержавних стратегій та програм розвитку інформаційної сфери, протидії кіберзлочинності тощо.

В інформаційному суспільстві й комерційні структури, і держава, і громадський сектор повинні об'єднати зусилля щодо подолання небезпек у інформаційній сфері: комп'ютерні злочини, кіберзлочинність, кібертероризм тощо. Найбільшою проблемою сьогодення в діяльності правоохоронних органів щодо протидії злочинності є суттєве зростання комп'ютерних злочинів внаслідок широкого розповсюдження комп'ютерних систем і технологій у всіх сферах життєдіяльності суспільства. В свою чергу кіберзлочинність за своєю суттю набагато ширша за комп'ютерну злочинність і включає цілий спектр протиправних діянь. Під кіберзлочинністю розуміється сукупність злочинів, що здійснюються в кіберпросторі за допомогою комп'ютерних систем або комп'ютерних мереж, а також інших засобів доступу до кіберпростору, в рамках комп'ютерних систем або мереж, і проти комп'ютерних систем, комп'ютерних мереж і комп'ютерних даних. Аналіз статистичних даних свідчить про швидке зростання кіберзлочинності, про можливість спричинення цими злочинами значного фінансового збитку громадянам і організаціям при мінімальному ризику для злочинця, а також про зростання взаємозв'язку кіберзлочинності з організованою злочинністю [7, с. 57-58].

З метою забезпечення інформаційної безпеки держави важливо також прийняти правові норми для тих комерційних суб'єктів, які надають інформаційні послуги та працюють на ринку телекомунікаційних технологій. Зокрема, необхідно чітко прописати на законодавчому рівні не тільки права, але й обов'язки операторів та провайдерів телекомунікацій, які б відповідали положенням Декларації про свободу комунікацій в мережі Інтернет, затвердженої Комітетом Міністрів на засіданні заступників міністрів Ради Європи 28 травня 2003 року в м. Страсбурзі (Франція) [8], Конвенції Ради Європи про кіберзлочинність [9].

На нашу думку, для посилення відповідальності комерційних суб'єктів у галузі інформаційної безпеки варто імплементувати положення Конвенції Ради Європи про кіберзлочинність:

- надання органам дізнання та слідства повноважень щодо видачі обов'язкових до виконання приписів про термінове фіксування та подальше зберігання комп'ютерних даних, які необхідні для розкриття злочину (ч. 1 ст. 16 та ст. 17 Конвенції про кіберзлочинність);
- збереження провайдерськими установами даних про трафік інформації на термін до 90 днів з можливістю подальшого продовження цього строку (ч. 2 ст. 16 Конвенції про кіберзлочинність);
- встановлення для суб'єктів, які зберігають комп'ютерні дані, зобов'язань не розголошувати факт проведення оперативно-розшукових та процесуальних дій протягом періоду, який визначається законодавством держави (ч. 3 ст. 16, ч. 3 ст. 20, ч. 3 ст. 21 Конвенції про кіберзлочинність);
- розкриття провайдером в інтересах органу дізнання або слідства технічної інформації, достатньої для ідентифікації підприємств чи фізичних осіб, що надавали послуги, та шлях, яким інформація передавалась (ч. 1 ст. 17 Конвенції про кіберзлочинність);
- надання органам дізнання та слідства права терміново здійснити обшук (огляд, виїмку) комп'ютерної інформації [9].

Таким чином, суб'єкти комерційної діяльності можуть співробітничати з державними структурами у сфері інформаційної безпеки за такими напрямками як технологічний, консультативний, безпековий, науковий, інформаційно-аналітичний та ін.

Разом з тим, суб'єкти комерційної діяльності можуть створювати певні небезпеки у інформаційній сфері для суспільства та держави. Яскравим прикладом вищезначеного явища є діяльність певних ЗМК (засобів масової комунікації), зокрема окремих каналів комерційного телебачення. Так, нажаль, певні телеканали можуть закупати низькопробну продукцію, яка руйнує морально-психологічний клімат у суспільстві, пропагує насильство та нездоровий спосіб життя. Як справедливо підкреслюють фахівці, основний потік телематеріалів прямує з крупних промислово розвинених країн Заходу (США, Англія, Франція, ФРН) в менш розвинені. Тільки США щорічно продають телевізійним організаціям інших країн телематеріалів на 100-200 тис. годин віщання. Другий найбільший експортер телепрограм Велика Британія реалізує таких матеріалів на порядок менше (на 20-30 тис. годин віщання), далі слідують Франція (15-20 тис. годин) і ФРН (5-6 тис. годин). У 80-х роках ХХ сторіччя чимало європейських газет почали писати про "культурний геноцид" і "американський телевізійний десант в Європі". Тоді ж у Франції та інших європейських країнах, стала складатися протекціоністська політика щодо національного кіно та телебачення [10, с. 190-191].

Отже, Україна повинна захищати національний інформаційний простір від закордонного (західного та східного) інформаційного впливу, який забезпечується місцевими комерційними структурами задля отримання прибутку. Необхідно напрацювати чіткі критерії для визначення характеру діяльності комерційних суб'єктів різного ґатунку згідно з якими можна визначати їхній позитивний або негативний вплив на інформаційну безпеку держави та суспільства.

Підводячи підсумки щодо суб'єкт-об'єктних характеристик у сфері інформаційної безпеки, варто проаналізувати проблему консолідації суб'єкта задля підвищення ефективності інформаційної політики та інформаційної безпеки.

Консолідація суб'єктів інформаційної безпеки є нагальною потребою в Україні від вирішення якої в наш час залежить не тільки захист національно-культурної ідентичності, але й збереження та розвиток держави. В умовах розв'язаної проти України інформаційної війни консолідація суб'єктів інформаційної безпеки повинна відбуватися навколо єдиної стратегії розвитку інформаційної сфери, ціннісних констант, виваженої та ефективною інформаційної політики.

На думку О. Гада, інформаційна безпека нерозривно пов'язана з необхідністю зміцнення ідеологічної платформи держави. Іншими словами, щоб бути захищеними інформаційно, необхідно мати контрольовану державою медію структуру (Інтернет-ресурси, ЗМІ, телебачення), власну систему пропаганди для здійснення інформаційних атак і контратак стосовно спроб посилення зовнішніх впливів на суспільно-політичну обстановку в країні [11, с. 232].

Не сприяє консолідації суб'єктів інформаційної безпеки той факт, що за роки незалежності Україна не виробила сталої стратегії національної безпеки в питаннях захисту її інформацій-

ного суверенітету від деструктивних впливів. Недостатньо чітко прописані повноваження основних державних структур – МВС, СБУ, Державної служби захисту зв'язку та захисту інформації щодо протидії викликам в інформаційній сфері. Багато проблем виникає і через незнання користувачами основ мережевої безпеки та відсутність в органах державної влади і місцевого самоврядування спеціально підготовлених кадрів, здатних оперативно та ефективно вирішувати ці проблеми. 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 [11, с. 233].

Партії як ідеологічні суб'єкти інформаційної безпеки України також повинні дбати про загальнонаціональні інтереси: у своїй інформаційно-просвітницькій діяльності популяризувати демократичні цінності, сприяти єдності українського народу, відмовитись від політичних технологій протиставлення та розколу різних соціальних груп, етнонаціональних утворень у вітчизняному соціумі. Партії та їх лідери повинні усвідомлювати свою відповідальність щодо захисту національних інтересів, в тому числі й у сфері інформаційної безпеки, брати участь у створенні та реалізації інформаційної політики держави.

Одним з ключових суб'єктів забезпечення інформаційної безпеки та інформаційної політики суспільства й держави є різноманітні ЗМІ. Більш активне залучення медіа-спільноти до обговорення та реалізації інформаційної політики держави буде сприяти підвищенню її ефективності. В цьому контексті, на особливу увагу заслуговує розвиток співпраці держави з мас-медіа, оскільки ЗМІ найчастіше є первинними джерелами інформації і виконують роль важливої соціальної інституції в реалізації державної інформаційної політики. Зокрема, необхідно широко використовувати їх можливості для регулярного інформування населення про політичну та соціально-економічну ситуацію в країні, роз'яснення владою змісту реформ та очікуваних результатів від їх реалізації, оперативного реагування на світові й внутрішні події, які торкаються національних інтересів України. Слід також орієнтувати медіа ресурси на нейтралізацію негативних впливів з боку різного роду деструктивних сил, спроб маніпулювання свідомістю людей через інформаційний простір. Цьому сприятиме створення національних медіа-ресурсів, метою яких буде відстоювання інтересів держави в глобальному інформаційному просторі через аргументоване доведення до широкого кола користувачів соціальних мереж як у країні, так і за її межами, альтернативних поглядів на значущі соціальні й політичні події [12, с. 337].

Консолідація суб'єктів інформаційної політики та інформаційної безпеки в Україні визначається низкою законодавчих актів: Конституцією України (1996), Законами України "Про наукову і науково-технічну діяльність" (1991), "Про інформацію" (1992), "Про науково-технічну інформацію" (1993), "Про захист інформації в автоматизованих системах" (1994), "Про друковані засоби масової інформації" (1992), "Про авторське право та суміжні права" (1993), "Про національний архівний фонд і архівні установи" (1993), "Про телебачення і радіомовлення" (1995), "Про Концепцію Національної програми інформатизації" (1998), "Про Національну програму інформатизації" (1998), "Про основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки" (2007), а також іншими чинними нормативними актами загального і спеціального змісту, в яких визначено співвідношення міжнародних норм і національних пріоритетів.

Головними напрямками та принципами інформаційної політики в Україні, навколо яких повинна відбуватися консолідація всіх суб'єктів інформаційної безпеки, є такі: забезпечення доступу громадян до інформації; створення національних систем і мереж інформації; зміцнення матеріально-технічних, фінансових, організаційних, правових і наукових основ інформаційної діяльності; забезпечення ефективного використання інформації; сприяння постійному оновленню, збагаченню та зберіганню національних інформаційних ресурсів; створення загальної системи охорони інформації; сприяння міжнародному співробітництву в галузі інформації і гарантування інформаційного суверенітету України; сприяння задоволенню інформаційних потреб українців за кордоном [13, с. 38-40].

Важливе значення у формуванні соціокультурного й виховного консолідуючого підґрунтя суб'єктів інформаційної політики та безпеки відіграють заклади освіти. В контексті нашої наукової розвідки можна виокремити наступні напрямки освітньо-інформаційної політики: а) за-

безпечення єдності процесів управління освітою за допомогою автоматизованих засобів управління і пов'язаних з ними комплексів із використанням технічних і програмних засобів нових поколінь; б) створення інформаційних систем Міністерства освіти і науки України на користь забезпечення процесів (у тому числі й інтелектуальних) освітньої діяльності; в) використання сучасних інформаційних технологій для досліджень і запровадження в життя якісно нових засобів інформаційних технологій і форм їх застосування та ін. [14, с. 127].

Висновки. Суб'єкт-об'єктні характеристики інформаційної безпеки мають багатоплановий й різноманітний характер. Системоутворюючим суб'єктом інформаційної безпеки є держава, але її діяльність у демократичних країнах не може повною мірою забезпечити багатоаспектні інтереси й потреби об'єктів у цій сфері. Саме тому виникає необхідність залучення до забезпечення інформаційної безпеки країни недержавних суб'єктів, а також різноманітних колективів, етнопатристичних утворень, комерційних структур тощо.

Література

1. Галлін Деніел С. Сучасні медіасистеми: три моделі відносин ЗМІ та політики / Деніел С. Галлін, Паоло Манчіні ; [пер. з англ. О. Насика]. – К. : Наука, 2008. – 320 с.
2. Вакулич, В. Державна інформаційна політика як механізм реалізації інформаційної функції сучасної держави / В. Вакулич, О. Бухтатий // Публічне управління: теорія та практика. – 2014. – Вип. 1. – С. 97-107.
3. Шахов, В. Національний інтерес і національна безпека в геостратегії України / В. Шахов, В. Мадіссон // Вісник Національної академії державного управління при Президентові України. – 2013. – № 2. – С. 44-56.
4. Рубан, Ю. Г. Україна як суб'єкт і об'єкт сучасних міжнародних інформаційних воєн / Ю. Г. Рубан // Стратегічні пріоритети. – 2009. – № 2(11). – С. 5-9.
5. Малик, Я. Й. Забезпечення інформаційної безпеки України у контексті світового досвіду / Я. Й. Малик, О. І. Береза // Ефективність державного управління. – 2012. – Вип. 32. – С. 20-27.
6. Нестеряк, Ю. В. Міжнародні критерії інформаційної безпеки держави: теоретико-методологічний аналіз / Ю. В. Нестеряк // Публічне управління: теорія та практика. – 2014. – Вип. 1. – С. 62-67.
7. Бойченко, О. В. Міжнародне співробітництво правоохоронних органів держав в галузі забезпечення інформаційної безпеки / О. В. Бойченко // Форум права. – 2009. – № 2. – С. 56-62.
8. Інформаційне законодавство: Збірник законодавчих актів: У 6 т. / За заг. ред. Ю. С. Шемшученка, І. С. Чиж. – Т. 5. Міжнародно-правові акти в інформаційній сфері. – К.: ТОВ "Видавництво "Юридична думка", 2005. – 328 с.
9. Конвенція Ради Європи про кіберзлочинність. – Режим доступу: http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?page=1&nreg=994_575.
10. Дзьобань, О. П., Пилипчук, В. Г. Інформаційне насильство та безпека: світоглядно-правові аспекти: Монографія / За заг. ред. проф. В. Г. Пилипчука. – Харків : Майдан, 2011. – 244 с.
11. Гіда, О. Ф. Фактори, що впливають на формування викликів національним інтересам України в інформаційному просторі / О. Ф. Гіда // Боротьба з організованою злочинністю і корупцією (теорія і практика). – 2013. – № 2. – С. 228-236.
12. Гіда, О. Ф. Щодо основних засад формування державної інформаційної політики / О. Ф. Гіда // Боротьба з організованою злочинністю і корупцією (теорія і практика). – 2013. – № 1. – С. 333-341.
13. Брижко, В. До питання сучасної інформаційної політики / В. Брижко // Вісник Академії управління МВС. – 2009. – № 2. – С. 27-47.
14. Ярошенко, А. О. Напрями модернізації української освітньо-інформаційної політики / А. О. Ярошенко // Міжнародний науковий форум: соціологія, психологія, педагогіка, менеджмент. – 2010. – Вип. 3. – С. 122-130.

References

1. Hallin, D. C. & Mancini P. (2008). *Suchasni mediasystemy: try modeli vidnosyn ZMI ta polityky [Comparing Media Systems: Three Models of Media and Politics (Communication, Society and Politics)]*. (O. Nasyko, Trans). Kyiv: Nauka [in Ukrainian].
2. Vakulych, V. & Bukhtatyi O. (2014). Derzhavna informatsiina polityka yak mekhanizm realizatsii informatsiinoi funktsii suchasnoi derzhavy [State information policy as a mechanism for the implementation of the information function of the modern state]. *Publichne upravlinnia: teoriia ta praktyka – Public Administration: Theory and Practice*, 1, 97-107 [in Ukrainian].
3. Shakhov, V. & Madisson, V. (2013). Natsionalnyi interes i natsionalna bezpeka v heostrategii Ukrainy [National interest and national security in the geostrategy of Ukraine]. *Visnyk Natsionalnoi akademii derzhavnoho upravlinnia pry Prezydentovi Ukrainy – Bulletin of the National Academy of Public Administration under the President of Ukraine*, 2, 44-56 [in Ukrainian].
4. Ruban, Yu. H. (2009). Ukraina yak subiekt i obiekt suchasnykh mizhnarodnykh informatsiinykh voien [Ukraine as the subject and object of contemporary international information wars]. *Stratehichni priorytety – Strategic Priorities*, 2 (11), 5-9 [in Ukrainian].
5. Malyk, Ya. Y. & Bereza, O. I. (2012). Zabezpechennia informatsiinoi bezpeky Ukrainy u konteksti svitovoho dosvidu [Providing information security of Ukraine in the context of world experience]. *Efektivnist derzhavnoho upravlinnia – Efficiency of public administration*, 32, 20-27 [in Ukrainian].
6. Nesteriak, Yu. V. (2014). Mizhnarodni kryterii informatsiinoi bezpeky derzhavy: teoretiko-metodolohichni analiz [International criteria for information security of the state: theoretical and methodological analysis]. *Publichne upravlinnia: teoriia ta praktyka – Public administration: theory and practice*, 1, 62-67 [in Ukrainian].
7. Boichenko, O. V. (2009). Mizhnarodne spivrobitnytstvo pravookhoronnykh orhaniv derzhav v haluzi zabezpechennia informatsiinoi bezpeky [International cooperation of law enforcement bodies in the field of information security provision]. *Forum prava – Law of the forum*, 2, 56-62 [in Ukrainian].

8. Shemshuchenko, Yu. S. & Chyzh, I. S. (Eds.). (2005). *Informatsiine zakonodavstvo: Zbirnyk zakonodavchyykh aktiv T. 5.: Mizhnarodno-pravovi akty v informatsiinii sferi. [Information Law: Collection of Legislative Acts. Vol. 5. International legal acts in the field of information]*. Kyiv: TOV "Vydavnytstvo "Yurydychna dumka" [in Ukrainian].
9. Konventsia Rady Yevropy pro kiberzlochynnist : vid 23 lystopada 2001 [Council of Europe Convention on Cybercrime from November 23 2001]. *zakon.rada.gov.ua*. Retrieved from http://zakon0.rada.gov.ua/laws/show/994_575 [in Ukrainian].
10. Dzoban, O. P. & Pylypchuk, V. H. (2011). *Informatsiine nasylstvo ta bezpeka: svitohliadno-pravovi aspekty [Information Violence and Security: Worldview Aspects]*. Kharkiv : Maidan [in Ukrainian].
11. Hida, O. F. (2013). Faktory, shcho vplyvaiut na formuvannia vykykiv natsionalnym interesam Ukrainy v informatsiinomu prostori [Factors Influencing the Challenges to the National Interests of Ukraine in the Information Space]. *Borotba z orhanizovanoi zlochynnistiu i koruptsiieiu (teoriia i praktyka) - Fighting Organized Crime and Corruption (theory and practice)*, 2, 228-236 [in Ukrainian].
12. Hida, O. F. (2013). Shchodo osnovnykh zasad formuvannia derzhavnoi informatsiinoi polityky [On the Basic Principles of the Formation of State Information Policy]. *Borotba z orhanizovanoi zlochynnistiu i koruptsiieiu (teoriia i praktyka) – Fighting Organized Crime and Corruption (theory and practice)*, 1, 333-341 [in Ukrainian].
13. Bryzhko, V. (2009). Do pytannia suchasnoi informatsiinoi polityky [On the issue of modern information policy]. *Visnyk Akademii upravlinnia MVS - Bulletin of the Academy of Management of the Ministry of Internal Affairs*, 2, 27-47 [in Ukrainian].
14. Yaroshenko, A. O. (2010). Napriamy modernizatsii ukrainskoi osvithno-informatsiinoi polityky [Directions of modernization of the Ukrainian educational and informational policy]. *Mizhnarodnyi naukovyi forum: sotsiologhiia, psykholohiia, pedahohika, menedzhment - International scientific forum: sociology, psychology, pedagogy, management*, 3, 122-130 [in Ukrainian].

Надійшла 22.03.2018

Бібліографічний опис для цитування:

Захаренко, К. В. Проблеми консолідації суб'єктів інформаційної безпеки / К. В. Захаренко // Проблеми соціальної роботи: філософія, психологія, соціологія. – 2018. – № 1 (11). – С. 36-43.