УДК 327.8: 15
DOI: 10.33663/1563-3349-2021-90-190

А. П. ДЕМАРТИНО

ПРОТИДІЯ ЗОВНІШНІМ ІНФОРМАЦІЙНИМ ВПЛИВАМ: ОБҐРУНТУВАННЯ УКРАЇНСЬКОЇ ВЕРСІЇ

На основі систематизації здобутків українських учених і практичного досвіду протистояння зовнішнім інформаційним впливам визначаються основні напрями формування розвиненої системи інформаційної безпеки як важливої складової національної безпеки країни в цілому. До таких напрямів віднесені: кадрове забезпечення, електронне урядування, оцінка інформаційних ризиків; інституційне, технологічне й нормативно-правове забезпечення належного функціонування інформації. З'ясовано, що забезпечення визначених напрямів діяльності потребує вироблення державної інформаційної політики, здатної до стратегічного поетапного розв'язання ключових державотворчих проблем.

Ключові слова: *зовнішній інформаційний вплив, інформаційна безпека, електронне урядування, інформаційні ризики, політична пропаганда, інформаційний простір.*

Demartyno Andriy. **Combating external information influences: justification of the ukrainian version**

The article, based on the systematization of the achievements of Ukrainian scientists and practical experience of resisting external information influences, identifies the main directions of formation of a developed information security system as an important component of national security in general. Such areas include: staffing, e-government, information risk assessment; institutional, technological and regulatory support for the proper functioning of information. It was found that the provision of certain areas of activity requires the development of state information policy, capable of strategic phased solution of key state-building problems.

Key words: *external information influence, information security, e-government, information risks, political propaganda, information space.*

У сучасних умовах підвищеної динаміки світового розвитку захист інформаційного середовища є одним із вагомих чинників розвитку сфери національної безпеки. І саме цей чинник дедалі

© *ДЕМАРТИНО Андрій Павлович* – кандидат історичних наук, керівник служби з питань стратегічного планування і аналізу Апарату Ради національної безпеки і оборони України; ORCID: 0000-0002-2647-0129; e-mail: andrede17@gmail.com

активніше впливає на стан політичної, економічної та інших складових суспільного розвитку України. Відповідно безпека суспільства характеризується ступенем його захищеності, стійкості головних сфер життєдіяльності до небезпечних інформаційних впливів. Томуде майбутнє України має будуватися з урахуванням того, що в сучасному світі інформація стала одним із найважливіших ресурсів неприхованого й гібридного силового протиборства.

В. Степанов вважає, що увага до проблем інформаційної безпеки держави викликана такими причинами: інформаційна інфраструктура й інформаційні ресурси стають ареною міждержавної боротьби за світове лідерство; процеси глобалізації, що особливо яскраво виявляються в інформаційній сфері, істотно підсилили залежність ефективності функціонування суспільства та держави від стану інформаційної сфери; рух України до створення інформаційної інфраструктури й інтеграції її в європейську інфраструктуру призводить до посилення небезпеки несанкціонованого втручання в роботу інформаційних і телекомунікаційних систем держави; дедалі зростаюча економічна залежність операторів зв'язку від іноземних інвесторів, а також поява на території України мереж і систем зв'язку, що належать акціонерним товариствам і приватним особам; необхідність координації зусиль щодо створення й розвитку мереж зв'язку з урахуванням потреби зміцнення обороноздатності держави та забезпечення її інформаційної безпеки тощо [1]. Звідси особливо актуальною постає проблема наукового дослідження інформаційної експансії, тобто зовнішніх інформаційних впливів та пропаганди, механізмів їх реалізації та формування належної протидії цьому явищу. Дієвими повинні стати як засоби убезпечення (інформаційне протиборство, інформаційна боротьба, спеціальні інформаційні операції), так і правила та процедури захисту (контрпропаганда, контрсугестія – опір інформаційним впливам, інформаційна політика, нормативно-правові рамки функціонування інформації). Саме інформаційна безпека визначається здатністю нейтралізувати такі впливи.

Визначенням механізмів забезпечення інформаційної безпеки України присвятили свої праці такі вчені, як В. Горбатенко, Н. Грицяк, Т. Гузенко, В. Гурковський, У. Ільницька, І. Кресіна, В. Марков, Р. Марутян, В. Остроухов, В. Петрик, Г. Почепцов, О. Радченко, Е. Рижков, Ю. Рубан, А. Семенченко, В. Степанов,

О. Стойко, В. Тарасюк, О. Тихомиров та ін. Названі науковці аналізують поняття «інформаційне суспільство», «інформаційна політика», «інформаційна безпека», «інформаційна війна», «інформаційне законодавство» й пропонують на цій основі систематизацію чинників інформаційної безпеки. Однак ще не можна вважати, що наявні наукові дослідження дають змогу виробити прийнятну систему практичної реалізації завдань щодо забезпечення належного рівня інформаційної безпеки. Для виокремлення складових її загальної структури найчастіше використовуються такі вербальні конструкції, як «напрями», «механізми», «шляхи» забезпечення [2]. Подібна риторика виправдана в умовах недостатньої визначеності й постійного оновлення зовнішніх інформаційних впливів. Водночас це означає необхідність постійної, підвищеної уваги до проблеми протидії останнім, оскільки зовнішня інформаційна експансія в майбутньому, вірогідно, лише зростатиме.

Виходячи із зазначеного, метою пропонованої статті є з'ясування характеру зовнішніх інформаційних впливів та визначення основних напрямів протидії їм у сучасній Україні. До завдань статті віднесено: виявлення особливостей зовнішніх деструктивних інформаційних впливів; визначення можливостей, засобів, технологій в рамках основних напрямів протидії інформаційній експансії.

Аналіз наукових досліджень зарубіжних та українських учених засвідчує відсутність однозначного тлумачення поняття «інформаційний вплив» та його найбільш поширених форм. Наукового узагальнення та систематизації потребують також методи оцінки матеріалів ЗМІ для формування заходів протидії інформаційному впливу. За визначенням В. Остроухова і В. Петрика, під «інформаційним впливом» слід розуміти «організоване, цілеспрямоване застосування спеціальних інформаційних засобів і технологій для внесення змін у свідомість населення (корекція поведінки) та (або) інформаційно-технічну інфраструктуру об'єкта» [3, с. 136]. Об'єктами небезпечного інформаційного впливу можуть бути: свідомість, психіка людей, інформаційно-технічні системи різного масштабу і призначення тощо. До них також можна віднести особистість, колектив, суспільство, державу, світове співтовариство [4]. Характер деструктивних впливів на інформаційний простір, тобто на процеси отримання, опрацювання, збереження й поши-

рення інформації будь-якого виду, засвідчує три форми впливу: 1) вплив на форму повідомлень, механізми їх передачі, зберігання, опрацювання даних тощо; 2) блокування передачі повідомлень; 3) вплив на зміст повідомлень.

В Україні загальною проблемою слід вважати, на нашу думку, насамперед відсутність дієвих механізмів забезпечення інформаційної безпеки, їх неспівмірність із загрозами, що постали в останнє десятиліття. Відповідно до Доктрини інформаційної безпеки України основним суб'єктом деструктивного інформаційного впливу на Україну є Російська Федерація як держава-агресор. Відповідно загрозами національним інтересам та національній безпеці України в інформаційній сфері є:

– деструктивна діяльність, спрямована на підрив обороноздатності, деморалізацію особового складу Збройних Сил України та інших військових формувань, провокування екстремістських проявів, підживлення панічних настроїв, загострення і дестабілізацію суспільно-політичної та соціально-економічної ситуації, розпалювання міжетнічних і міжконфесійних конфліктів в Україні;

– проведення державою-агресором спеціальних інформаційних операцій в інших державах з метою створення негативного іміджу України у світі;

– інформаційна експансія держави-агресора та контрольованих нею структур, зокрема шляхом розширення власної інформаційної інфраструктури на території України та в інших державах;

– інформаційне домінування держави-агресора на тимчасово окупованих територіях;

– недостатня розвиненість національної інформаційної інфраструктури, що обмежує можливості України ефективно протидіяти інформаційній агресії та активно діяти в інформаційній сфері для реалізації національних інтересів України;

– неефективність державної інформаційної політики, недосконаліть законодавства стосовно регулювання суспільних відносин в інформаційній сфері, невизначеність стратегічного наративу, недостатній рівень медіа-культури суспільства; поширення закликів до радикальних дій, пропаганда ізоляціоністських та автономістських концепцій співіснування регіонів в Україні [5].

Серед найсерйозніших загроз, які постали останнім часом, в умовах застосування різноманітних елементів гібридної війни,

слід виділити пропаганду з використанням новітніх інформаційних можливостей і технічних засобів. Негативний вплив пропаганди з цілеспрямованим використанням засобів масової інформації визначається такими ознаками: створення атмосфери бездуховності й аморальності, негативного ставлення до культурної спадщини; маніпулювання суспільною свідомістю різних соціальних груп з метою створення політичної напруженості та хаосу; дестабілізація політичних відносин між партіями, об'єднаннями й рухами з метою провокації конфліктів, розпалювання недовіри, підозрілості, загострення політичної боротьби, провокування репресій проти опозиції і навіть громадянської війни; зниження рівня інформаційного забезпечення органів влади й управління, інспірація помилкових управлінських рішень; дезінформування населення про роботу державних органів, підрив їхнього авторитету, дискредитація органів управління; підрив міжнародного авторитету держави, її співробітництва з іншими країнами; завдання шкоди та збитків життєво важливим інтересам держави в політичній, економічній, оборонній та інших сферах тощо.

Загальною метою такого впливу є ослаблення моральних і матеріальних сил противника. Він передбачає різноманітні заходи пропагандистського впливу на свідомість людини, насамперед в ідеологічній та емоційній галузях. Специфічною особливістю такого впливу є те, що він не призводить безпосередньо до кровопролиття, руйнувань, реальних жертв, ніхто не позбавляється їжі, даху над головою тощо. І це може породжувати неналежне ставлення до нього. А втім руйнування, якого завдає інформаційний вплив у суспільній психології, психології особистості, за масштабами і значенням цілком співмірні, а часом і перевищують наслідки збройних воєн.

Як зазначає Р. Марутян, суттєвою загрозою національній безпеці України в інформаційній сфері є здійснення іноземними державами негативного інформаційно-психологічного впливу на суспільну свідомість громадян України та світову громадськість через проведення інформаційних акцій та кампаній, спеціальних інформаційних операцій. Це відбувається через систематичне поширення тенденційної, неповної або упередженої інформації про Україну та політичні процеси, що відбуваються на її теренах. Усе це впливає на зовнішню та внутрішню політику держави, що виступає

об'єктом інформаційного впливу, знижує її міжнародний імідж [6]. В якості інформаційних засобів, що їх використовує керівництво окремих держав, здійснюючи інформаційну експансію, застосовуються: внесення у суспільну та індивідуальну свідомість ворожих, шкідливих ідей та поглядів; дезорієнтація та дезінформація громадян; ослаблення певних переконань, устоїв; залякування громадян образом ворога; демонстрація противнику своєї могутності.

За характером здійснення зовнішнього інформаційно-психологічного впливу на Україну іноземні держави можна поділити на дві групи: групу ситуативного впливу та групу постійного впливу. До групи ситуативного впливу можна віднести більшість західних держав, інформаційні впливи яких на Україну здебільшого стосуються євроінтеграційних перспектив України, внутрішньополітичної та економічної ситуації в нашій державі, російсько-українських відносин, деяких аспектів трактування історії тощо. До країн, які здійснюють постійний і найбільш інтенсивний інформаційно-психологічний вплив на Україну, дослідник відносить насамперед Російську Федерацію, а також Румунію та Угорщину [7].

В контексті з'ясування інформаційної експансії Російської Федерації важливою проблемою є вивчення її інформаційної присутності та поширення дезінформації в країнах Євросоюзу. Активний медіа-супровід світових та європейських подій з боку РФ виник задовго до анексії АР Крим та військової агресії на Сході України. Телебачення і друковані ЗМІ, підконтрольні РФ, використовувалися ще із середини 2000-х років, а особливого поширення набули напередодні та під час грузинсько-російського збройного конфлікту в серпні 2008 року. Найбільш вразливими щодо впливу російської пропаганди виявилися Чеська Республіка, Австрія й Угорщина. Найменш вразливими – Велика Британія, Естонія, Данія. Росія свідомо проштовхує пропаганду і сприяє розвитку тих політичних сил усередині ЄС, які налаштовані скептично щодо майбутнього Євросоюзу. Кількість країн, які підпадають під кампанію з дезінформації з боку Російської Федерації, з кожним роком зростає. З огляду на масові повідомлення російською мовою стає очевидним, що російська кампанія з дезінформації спрямована насамперед на російськомовні меншини в різних країнах. Окрім дискредитації Євросоюзу, значні зусилля Росія спрямовує на негативне висвітлення подій в Україні, спроби легалізації так званих ДНР та ЛНР.

Характерним напрямом інформаційно-психологічного впливу Румунії та Угорщини є зазіхання на частину територій України – Північну Буковину та Південну Бессарабію (Румунія) та частину українського Закарпаття (Угорщина). Зокрема, подібні заяви значно посилилися з боку Угорщини після перемоги на виборах у 2010 р. ультраправих партій «Фідес» (понад 60 %) та «Йоббік» (12 %). Щодо Румунії варто зауважити, що ідеї відновлення «Великої Румунії» не тільки підтримуються лідерами правлячої коаліції (зокрема, консервативною та націонал-ліберальною партіями), а й користуються великим соціальним попитом серед румунського населення.

Зважаючи на вищезазначені загрози, протидія негативним інформаційним впливом, як видається, потребує системної діяльності за такими напрямами.

1. Підготовка якісного кадрового складу в сфері забезпечення інформаційної безпеки. Необхідність вирішення цієї проблеми пов'язана з тим, що людський ресурс є основою у прийнятті та реалізації будь-яких управлінських рішень. Відповідно потребує формування на державному рівні нового складу державних службовців, які вирішуватимуть проблеми забезпечення інформаційної безпеки системи публічного управління. Компетентні управлінці зазвичай виявляють здатність щодо розроблення механізмів реалізації прав громадян на інформацію загального користування; визначення основних положень стратегії держави у сфері використання засобів масової інформації на засадах досліджень процесів формування суспільної свідомості; удосконалення та розвитку індустрії інформування населення країни.

2. Налагодження дієвого механізму функціонування системи електронного урядування. Нині вже існують розроблені системи електронного документообігу в органах державної влади та органах місцевого самоврядування, однак єдиної системи у цій сфері в Україні досі не існує. Відповідно важливою складовою процесу політичної модернізації українського суспільства «повинна бути комунікативна політика, що передбачає не лише надання суспільству певної інформації про органи влади, їх діяльність, а й отримання від суспільства зворотної інформації про інтереси і потреби громадян, рівень їх забезпечення, а також пропозиції щодо ефективнішого управління суспільними справами» [8, с. 273]. Елек-

тронне урядування, як засвідчує світовий досвід, є однією з найважливіших складових процесів інформатизації, що відбуваються в нашій країні. Зрештою воно сприятиме істотному ослабленню російського інформаційного впливу на інформаційний простір України і спрямуванню на західні інформаційні орієнтири. А це, в свою чергу, зумовлюватиме зростання суспільного інтересу до західної моделі соціально-економічного й суспільно-політичного розвитку.

3. Формування бази даних інформаційних ризиків, які потребують термінового та ефективного реагування. Чинником впливу інформаційних загроз на соціальну спільноту є ускладнення соціальних процесів, що виявляється в загостренні суперечностей між різними соціальними прошарками, напруженні політичної боротьби, розпалюванні релігійних та етнічних суперечностей, зниженні загальної культури населення, розвитку бездуховності, зростанні злочинності, розповсюдженні антигуманних ідей [9]. Слід зважати й на те, що сам по собі розвиток та впровадження у різні сфери життя суспільства новітніх інформаційних технологій, як і будь-яких інших науково-технічних досягнень, не тільки забезпечує комфортність, а й нерідко приховує певні небезпеки.

4. Створення інституцій, які комплексно забезпечуватимуть систему інформаційної безпеки в публічному управлінні, захист національного інформаційного простору. Головна мета розвитку цього напряму – забезпечення медійної переваги в інформаційному просторі. Крім того, пріоритетними завданнями інформаційних структур органів влади мають стати: контроль за інформаційними потоками; надання об'єктивної, вичерпної інформації, фахових коментарів та оперативних пояснень щодо тих чи інших подій; систематичне висвітлення офіційної позиції посадових осіб та політичних лідерів [10]. Якомога повніше освоєння вітчизняних і світових наукових надбань у перетворенні наукової інформації і знань на органічну частину власного національного інтелектуального і духовного потенціалу, національної наукової культури сприятиме європейській інтеграції України. Важливою ознакою самодостатності національного науково-інформаційного простору є його здатність до якомога повнішого забезпечення потреб внутрішніх інформаційних комунікацій у національному науковому і освітньому середовищі. Цьому теж мають слугувати належний

розвиток його інституційної структури, наявність різноманітних вертикальних і горизонтальних зв'язків між окремими учасниками комунікацій, необхідних для вільного обміну інформаційними потоками.

5. Забезпечення конкурентоспроможності національного інформаційного контенту. Наповнений значущим змістом, національний науково-інформаційний простір набуває самодостатності лише за умови своєї конкурентоспроможності у світовому просторі. Це означає, крім усього іншого, що зарубіжну наукову інформацію, здобутки світової науки він має опановувати безпосередньо, а не через опосередковану рецепцію інформації з третіх країн, як це відбувалося в минулому. Адже раніше вся зарубіжна науково-технічна інформація доходила до України вже опрацьованою російськими інформаційними установами. У цьому контексті В. Тарасюк слушно зазначає: «Інформатизація суспільства, розвиток й популяризація критичного ставлення до інформації, до невідомих джерел інформації – перші кроки до захисту національного інформаційного простору. Протидіяти агресивним інформаційним проявам слід, застосовуючи аналогічні інструменти інформаційних технологій: працювати з тими ж соціальними групами, вести активний діалог у соцмережах, Інтернет-спільнотах, використовувати можливості соціальної реклами, підтримувати діяльність громадських організацій відповідного спрямування. Медіаграмотність та критичне ставлення до інформації мають стати загальнонаціональним трендом» [11, с. 186]. Зазначене вимагає організації значних зусиль із моніторингу, інтеграції та опрацювання інформації, залучення фахівців, які добре орієнтуються в загальній картині розвитку наукових досліджень, функціонування світової науки. Здійснення такої роботи потребує широкого доступу до світових баз науково-аналітичної, бібліометричної, наукометричної інформації.

6. Створення технологічної і нормативно-правової бази забезпечення інформаційної безпеки. Йдеться про налагодження розподілу й використання персональної інформації з метою створення умов для інформаційних взаємовідносин між органами державної влади і суспільством; розвиток науково-практичних основ інформаційної безпеки, а саме: визначення основних положень стратегії держави в сфері створення і забезпечення умов формування і використання інформаційного ресурсу, підтримки високих темпів його

наповнення і заданих критеріїв якості (доступність, достовірність, своєчасність, повнота); розробку методів і засобів оцінки ефективності систем і засобів інформаційної безпеки та їх сертифікація.

Як висновок, слід зазначити, що забезпечення означених напрямів діяльності потребує вироблення державної інформаційної політики, здатної до стратегічного поетапного вирішення ключових державотворчих проблем: протидія масштабним негативним інформаційно-психологічним впливам, операціям та війнам; інтеграція України до світового та регіонального європейського інформаційного просторів через входження в міжнародні інформаційні та інформаційно-телекомунікаційні системи та організації; створення власної національної моделі інформаційного простору з відповідною інфраструктурою та забезпечення розвитку інформаційного суспільства за зразком розвинених західних держав; модернізація системи інформаційної безпеки держави шляхом удосконалення національного законодавства в цій сфері та узгодження його з міжнародними стандартами й дієве правове регулювання інформаційних процесів; підвищення конкурентоспроможності вітчизняної інформаційної продукції та інформаційних послуг; впровадження сучасних інформаційно-комунікативних технологій у процеси державного управління.

1. Степанов В. Ю. Інформаційна безпека в інформаційній сфері державного управління. *Теорія та практика державного управління.* 2016. Вип. 4. С. 24–28. URL: http://nbuv.gov.ua/UJRN/Tpdu_2016_4_5. **2.** Тихомиров О. О. Класифікації забезпечення інформаційної безпеки. URL: http://www.law.journalsofznu.zp.ua/archive/visnik-1-2011/29.pdf. **3.** Остроухов В., Петрик В. До проблеми забезпечення інформаційної безпеки України. *Політичний менеджмент.* 2008. № 4. С. 135–141. **4.** Марков В. В. Актуальні проблеми інформаційної безпеки України в системі міжнародної координації. *Право і безпека.* 2013. № 1. С. 78–80. **5.** Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України»: Указ Президента України № 47/2017. URL: https://www.president.gov.ua/documents/472017-21374. **6.** Марутян Р. Р. Рекомендації щодо вдосконалення політики забезпечення інформаційної безпеки України. URL: http://www.dsaua.org/index. php?option=com_content&view=article&id=198%3A2014-08-13-12-55-48&catid=66%3A2010-12-13-08-48-53&Itemid=90&lang=uk. **7.** Щодо окремих напрямів вдосконалення державної інформаційної політики України. Національний інститут стратегіч-

них досліджень Аналітична записка. URL: http://old2.niss.gov.ua/articles/1489/. **8.** Правовий вимір державної інформаційної політики України в умовах глобальних викликів: монографія. Кресіна І. О., Горбатенко В. П., Коваленко А. А., Стойко О. М., Явір В. А., Батанова Н. М., Кукуруз О. В., Тарасюк В. М., Ходаківський М. Д. За ред. І. О. Кресіної. Київ: Інститут держави і права ім. В. М. Корецького НАН України, 2018. 282 с. **9.** Рыжков Э. В. Энергоинформационная безопасность общества и государства с позиции деятельности правоохранительных органов. *Злочини проти особистої волі людини:* зб. матер. міжнар. наук.-практ. семінару (19–20 вересня 2000 р.). Харків, 2002. С. 83–88. **10.** Ільницька У. Інформаційна безпека Украаини: сучасні виклики, загрози та механізми протидії негативним інформаційно-психологічним впливам. URL: file:///Users/1/Downloads/hv_2016_2_1_7.pdf. **11.** Тарасюк В. Застосування інформаційних технологій в умовах гібридної війни: монографія. Київ: GlobeEdit, 2020. 226 с.

Referens

1. Stepanov V. Yu. Informatsiina bezpeka v informatsiinii sferi derzhavnoho upravlinnia. *Teoriia ta praktyka derzhavnoho upravlinnia.* 2016. Vyp. 4. S. 24–28. URL: http://nbuv.gov.ua/UJRN/Tpdu_2016_4_5. **2.** Tykhomyrov O. O. Klasyfikatsiї zabezpechennia informatsiyŋoї bezpeky. URL: http://www.law.journalsofznu.zp.ua/archive/visnik-1-2011/29.pdf. **3.** Ostroukhov V., Petryk V. Do problemy zabezpechennia informatsiinoi bezpeky Ukrainy. *Politychnyi menedzhment.* 2008. №4. S. 135–141. **4.** Markov V. V. Aktualni problemy informatsiyŋoї bezpeky Ukraïny v systemi mizhnarodnoї koordynatsiї. *Pravo i bezpeka.* 2013. №1. S. 78–80. **5.** Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 29 hrudnia 2016 roku «Pro Doktrynu informatsiinoi bezpeky Ukrainy»: Ukaz Prezydenta Ukrainy № 47/2017. URL: https://www.president.gov.ua/documents/472017-21374. **6.** Marutian R. R. Rekomendatsii shchodo vdoskonalennia polityky zabezpechennia informatsiinoi bezpeky Ukrainy. URL: http://www.dsaua.org/index. php?option=com_content&view=article&id=198%3A2014-08-13-12-55-48&catid=66%3A2010-12-13-08-48-53&Itemid=90&lang=uk. **7.** Shchodo okremykh napriamiv vdoskonalennia derzhavnoi informatsiinoi polityky Ukrainy. Natsionalnyi instytut stratehichnykh doslidzhen Analitychna zapyska. URL: http://old2.niss.gov.ua/articles/1489/. **8.** Pravovyi vymir derzhavnoi informatsiinoi polityky Ukrainy v umovakh hlobalnykh vyklykiv: monohrafiia. Kresina I. O., Horbatenko V. P., Kovalenko A. A., Stoiko O. M., Yavir V. A., Batanova N. M., Kukuruz O. V., Tarasiuk V. M., Khodakivskyi M. D. Za red. I. O. Kresinoi. Kyiv: Instytut derzhavy i prava im. V. M. Koretskoho NAN Ukrainy, 2018. 282 s. **9.** Rыzhkov Э. V. Эnerhoynformatsyonnaia bezopasnost obshchestva y hosudarstva s pozytsyy deiatelnosty pravookhranytelnыkh orhanov. *Zlochyny proty osobystoї voli liudyny:* zb. mater. mizhnar. nauk.-prakt. seminaru (19–20 veresnia 2000 r.). Kharkiv, 2002. S. 83–88. **10.** Ilnytska U. Informatsiina bezpeka Ukrayny: suchasni vyklyky, zahrozy ta mekhanizmy protydii nehatyvnym informatsiino-

psykholohichnym vplyvam. URL: file:///Users/1/Downloads/hv_2016_2_1_7.pdf. **11.** Tarasiuk V. Zastosuvannia informatsiinykh tekhnolohii v umovakh hibrydnoi viiny: monohrafiia. Kyiv: GlobeEdit, 2020. 226 s.

Demartyno Andriy. **Combating external information influences: Justification of the Ukrainian version**

The article, based on the systematization of the achievements of Ukrainian scientists and practical experience of resisting external information influences, identifies the main directions of formation of a developed information security system as an important component of national security in general. Such areas include: staffing, e-government, information risk assessment; institutional, technological and regulatory support for the proper functioning of information. It was found that the provision of certain areas of activity requires the development of state information policy, capable of strategic phased solution of key state-building problems.

The author finds out that counteraction to negative information influences requires systematic activity in Ukraine in the following areas: training of high-quality personnel in the field of information security; establishing an effective mechanism for the functioning of the e-government system; formation of a database of information risks that require urgent and effective response; creation of institutions that will comprehensively ensure the information security system in public administration, protection of the national information space; ensuring the competitiveness of national information content; creation of technological and normative-legal base of information security.

Ensuring these areas of activity requires the development of state information policy, capable of strategic gradual solution of key state-building problems, such as: counteraction to large-scale negative information and psychological influences, operations and wars; integration of Ukraine into the world and regional European information space through entry into international information and information and telecommunication systems and organizations; creation of own national model of information space with the corresponding infrastructure and maintenance of development of an information society on a model of the developed western states; modernization of the information security system of the state by improving national legislation in this area and harmonizing it with international standards and effective legal regulation of information processes; increasing the competitiveness of domestic information products and information services; introduction of modern information and communication technologies in public administration processes.

Key words: external information influence, information security, e-government, information risks, political propaganda, information space.