УДК 323

ОРГАНІЗАЦІЙНО-ПРАВОВИЙ МЕХАНІЗМ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ УКРАЇНИ В УМОВАХ ЗОВНІШНЬОЇ АГРЕСІЇ: НАПРЯМИ ВДОСКОНАЛЕННЯ

Пашковський В. Ф.,
аспірант
Національного інституту стратегічних досліджень

У статті аналізується проблема формування організаційно-правового механізму забезпечення інформаційної безпеки України в умовах російської агресії. Обґрунтовано доцільність вироблення цілісної державної інформаційної політики та запропоновано напрями її вдосконалення задля належного захисту й нейтралізації загроз в інформаційні сфері.

В статье анализируется проблема формирования организационно-правового механизма обеспечения информационной безопасности Украины в условиях российской агрессии. Обоснована целесообразность выработки целостной государственной информационной политики и предложены направления ее усовершенствования для надлежащей защиты и нейтрализации угроз в информационной сфере.

The article analyzes the problem of forming an organizational and legal mechanism for ensuring information security of Ukraine in the conditions of Russian aggression. The expediency of developing a holistic state information policy is substantiated. The directions for improving information security are proposed for proper protection and neutralization of threats in the information sphere.

Ключові слова: гібридна війна, інформаційна безпека, організаційно-правовий механізм.

Постановка проблеми. Російська агресія проти України, яка порушила встановлений світопорядок і продовжує загрожувати глобальній безпеці, актуалізує наукове осмислення проблем політики національної безпеки. На нинішньому етапі розвитку суспільства багато конфліктів з категорії «збройні зіткнення» переходять до інформаційного простору, який стає новою ареною протиборства. Це явище можна пов'язати, насамперед, зі зміною змісту та структури інформації, яка сьогодні вважається головним продуктом постіндустріального суспільства. У сучасну епоху комп'ютеризації суспільства і запровадження нових інформаційних технологій відбуваються якісні зміни інформації за змістом та структурою. У контексті змін змісту інформації виокремлюються такі аспекти: збільшення інформаційних ресурсів суспільства, поява нових інформаційних продуктів та послуг, процеси інтернаціоналізації та глобалізації інформації, зростання швидкості старіння та оновлення інформації, збільшення диференціації та спеціалізації інформації. Ера комп'ютерних і цифрових технологій наділяє інформацію фіксованістю, інваріантністю, запам'ятовуванням, передаванням, перетворюванням, відтворюванням, стиранням. Найважливішим результатом формування інформаційного суспільства стало виникнення глобального інформаційного простору, в якому розгорнулася гостра боротьба за досягнення інформаційної переваги. Інформаційне суспільство сформувало нові форми конфліктів – інформаційні, з якими люди не стикалися в індустріальному суспільстві, які не мали такої інтенсивності, не діяли так масштабно й не представляли такої загрози для безпеки громадян, суспільства та держави. Досвід розвинених країн показує, що потужний захист від викликів інформаційних війн може бути реалізований тільки за умов ефективної та обґрунтованої стратегії інформаційної безпеки, наявності дієвої системи інформаційної безпеки та відповідних механізмів управління нею.

З огляду на зазначене, **актуальність теми статті** зумовлена необхідністю наукового осмислення сутності інформаційної безпеки України в умовах зовнішньої агресії та пошуку належних механізмів її забезпечення.

Аналіз останніх досліджень та публікацій. Проблематика з'ясування сутності інформаційної безпеки держави, а також пошуків механізмів її забезпечення відображена у наукових працях таких вчених, як В. Горбулін, О. Литвиненко, Д. Дубов, М. Ожеван, М. Розумний, С. Пирожков, А. Качинський та інших. Водночас сучасний контекст державної політики національної безпеки потребує комплексного дослідження інформаційної безпеки у контексті забезпечення національних інтересів, вироблення дієвих механізмів захисту інформаційного простору держави, дослідження політико-правових

механізмів побудови системи інформаційної безпеки. Саме у вирішенні цього наукового завдання й полягає теоретичне та прикладне значення даного дослідження.

Метою статті є виявлення особливостей забезпечення інформаційної безпеки України як іманентної складової частини її національної безпеки в умовах гібридної війни.

Виклад основного матеріалу. Відповідно до класичного визначення «національна безпека (безпека нації) – це захищеність життєво важливих інтересів особистості, суспільства, держави та довкілля в різних сферах життєдіяльності від внутрішніх і зовнішніх загроз, що забезпечує сталий і поступальний розвиток країни» [1, с. 25]. У науковій літературі інформаційна безпека конституюється як важлива складова частина національної безпеки. Крім того, така теоретична кореляція не лише емпірично підтверджуються, а й суттєво посилюється в умовах ведення гібридних війн, зокрема російської агресії проти Української держави.

Інформаційна війна є безумовною складовою частиною та передумовою гібридних війн. В умовах гібридних війн використовують всі основні інформаційні методи та інструменти, які застосовуються в звичайних війнах. Гібридна війна містить як військові, так і цивільні складові. Безумовно, поява гібридної війни як нової форми конфлікту принципово змінює усталену архітектуру безпеки та ставить під сумнів можливості наявних гарантій безпеки [2, с. 18].

Роль інформаційної війни у складі гібридної, на нашу думку, надзвичайно важлива та ще неоцінена вченими, не досліджена військовими експертами тощо. Без інформаційної складової можна відхилити саму можливість появи гібридної війни.

Успішність гібридної та інформаційної війни Російської Федерації пов'язана із анексією АР Крим. Серед основних переваг інформаційної війни під час анексії АР Крим В.П. Горбуліним виокремлюються такі:

– слабка центральна влада та часткове безвладдя на тлі зміни влади;

– актуалізація суперечностей між державною владою України і регіонами. Паралельно відбувається невдоволення населенням регіонів діями центральної влади;

– незадовільний матеріально-технічний та психологічний стан структур національної безпеки, органів правопорядку як по всій Україні, так і в більшості регіонів країни;

– існування антагонізму між різними силовими структурами України, відсутність злагодженості у співпраці між ними;

– високий рівень активної інформаційно-пропагандистської роботи Росії саме в Криму протягом 1990–2014 рр. [3].

Інформаційна війна Російської Федерації проти України на певних етапах мала свої переваги та поразки. Зокрема, під час підготовчого етапу до гібридної війни інформаційні психологічно-пропагандистські заходи мали найбільший вплив на населення АР Крим, частини Луганської та Донецької областей. Це забезпечило РФ успішну анексію АР Крим, подальше розгортання гібридної війни на території Луганської та Донецької областей. Із розвитком протидії з боку України РФ почала втрачати переможні позиції в інформаційній війні. З огляду на те, що Україна не мала потужної армії, належної стратегії, не була готова до агресії з боку сусідньої держави, протидія інформаційній війні розвивалась дуже повільно, із вагомими втратами для української сторони.

Варто також зауважити, що успішність агресора в інформаційній війні проти України забезпечило і те, що Росія – єдина у світі держава, яка залучила скільки організаційних та фінансових ресурсів до підготовки інформаційно-пропагандистських кампаній, що є невід'ємною складовою частиною стратегічної культури РФ [4, с. 39].

Методи обробки, передавання, накопичення інформації, які використовуються на сучасному етапі розвитку, сприяли появі загроз, які пов'язані із можливістю втрати, викривлення, спотворення та розкриття даних, які належать кінцевим споживачам, зокрема державі. Тобто різні операції із інформацією впливають на появу загроз інформаційної безпеки на національному рівні. Від стану та рівня протидії інформаційним загрозам залежить інформаційна безпека в країні.

Аналіз стану протидії інформаційним загрозам в Україні показує, що на національному рівні відсутня чітка скоординована політика та стратегія щодо забезпечення інформаційної безпеки. Усі нормативно-правові акти, які стосуються цього напряму, не пов'язані між собою. У кожному із документів визначаються різні види загроз інформаційній безпеці та напрями їх подолання.

Через відсутність державної програми відсутній чіткий організаційний механізм, не визначено відповідальність за порушення інформаційної безпеки держави. Поява окремих рішень щодо забезпечення інформаційної безпеки свідчить про те, що цей напрям національної безпеки в Україні тільки починає формуватись. Тобто можна зазначити, що однією із найважливіших проблем у сфері забезпечення інформаційної безпеки є відсутність державної інформаційної політики, яка включає наявність нормативно-правової бази та визначеного в ній організаційного механізму захисту, проблему експансії зарубіжних виробників інформаційної продукції та технічного забезпечення, яка може вплинути на появу різноманітних ризиків, економічні проблеми, проблеми підготовки персоналу в інфор-

маційній інфраструктурі, відсутність визначення точного кола загроз інформаційній безпеці в Україні, проблему низької культури та рівня знань користувачів інформаційних ресурсів.

На нинішньому етапі розвитку стан протидії інформаційним загрозам в Україні перебуває на стадії формування та розвитку. Діяльність із інформаційного захисту в Україні почала формуватись безпосередньо під час російського військового вторгнення в Україну. Основну роль у забезпеченні інформаційного захисту країни відіграють активні громадяни, волонтери, політики, які захищають національні інтереси України.

До заходів із протидії гібридній війні РФ проти України, які здійснюють на державному рівні, можна віднести такі: заборона трансляції телеканалів РФ в ефірних та кабельних мережах на території України і контроль виконання цього заходу; заборона в'їзду на територію України радикально налаштованих осіб, що прямують через державний кордон та можуть брати участь в акціях антиукраїнської спрямованості; заборона в'їзду на територію України відомих осіб, які в інформаційному просторі чинять дії, що підпадають під статті Кримінального кодексу України стосовно посягань на територіальну цілісність та недоторканість України, державну безпеку країни.

Захист та протидія інформаційним війнам повинні здійснюватись виключно в межах розробленої стратегії щодо захисту від інформаційних загроз та протидії інформаційним війнам в Україні. Відповідна стратегія зможе забезпечити як нормативно-правову, так і організаційну базу формування інформаційної безпеки в Україні.

На рівні держави існує нормативно-правова база, яка регулює основні напрямки забезпечення та розвитку системи інформаційної безпеки України, яка складається з Конституції України, Закону України «Про основи національної безпеки України», Концепції розвитку сектору безпеки і оборони України, Стратегії національної безпеки України, Воєнної доктрини України, Закону України «Про інформацію», інших актів. Вказані нормативно-правові акти регулюють основні засади інформаційної безпеки на державному рівні.

Стратегія національної безпеки України у сфері протидії інформаційним викликам на національному рівні визначає:

– основні загрози інформаційної безпеки;
– основні види загроз кібербезпеці та інформаційним ресурсам;
– пріоритети забезпечення безпеки за визначеними видами загроз [5].

Національні пріоритети забезпечення інформаційної безпеки, визначені Стратегією національної безпеки України, передбачають боротьбу та протидію певним видам інформаційних війн, які сьогодні впливають на інформаційний простір країни.

Закон України «Про основи національної безпеки України» регламентує основні реальні та потенційні загрози національній безпеці України, стабільності в суспільстві та в інформаційній сфері. Також в цьому нормативно-правовому документі виокремлено основні напрями державної політики з питань національної безпеки України у досліджуваній сфері. Цей закон основні загрози інформаційної безпеки класифікує за напрямками:

– хакерських загроз (загрози комп'ютерної злочинності та комп'ютерного тероризму);
– розвідувальних загроз (загроза розголошення інформації, яка пов'язана із державною таємницею або з обмеженим доступом, орієнтованої на забезпечення потреб та захисту національних інтересів суспільства та держави);
– психологічних загроз (загрози проявів обмеження свободи слова та доступу до публічної інформації, поширення ЗМІ культу насильства, жорстокості, загрози спроб маніпулювання суспільною свідомістю, зокрема під час спроб розповсюдження неповної, упередженої або недостовірної інформації) [6].

Закон України «Про інформацію» регламентує відносини стосовно формування, накопичення, отримання, зберігання, поширення, використання, захисту та охорони інформації. Цей Закон визначає загальні норми щодо операцій з інформацією в Україні [7].

Варто зазначити, що у контексті дослідження протидії інформаційним загрозам в Україні в цьому Законі регламентуються основи захисту інформації. Відповідно до законодавчих норм захист інформації визначено сукупністю адміністративних, правових, технічних, організаційних та інших заходів, які забезпечують цілісність, збереження інформації та відповідний порядок доступу до інформації.

Розглянута нормативно-правова база визначає основні засади протидії інформаційним загрозам в Україні.

Головним центральним органом виконавчої влади щодо забезпечення інформаційного суверенітету України є Міністерство інформаційної політики України, яке функціонує відповідно до Положення про Міністерство інформаційної політики України, затвердженого постановою Кабінету Міністрів України від 14 січня 2015 р. № 2 [8].

З огляду на нормативно-правові засади можна резюмувати, що діяльність Міністерства інформаційної політики України також орієнтована на організацію протидії інформаційним загрозам в Україні. Згідно з правовими нормами ця діяльність повинна бути направлена на такі дії:

– захист інформаційного простору України від зовнішнього інформаційного впливу. Це досить широкий масштаб роботи, який включає протидію інформаційним загрозам основних видів інформаційних війн;

– навчання державних службовців з питань комунікацій. Цей напрям діяльності націлений на попередження загрози командно-управлінських війн як складової частини інформаційних війн;

– нормативно-правове регулювання у сфері забезпечення інформаційного суверенітету України.

Концепція розвитку сектору безпеки і оборони України зазначає, що безпековими викликами, які можуть посилювати загрозу застосування воєнної сили проти України, є такі:

– цілеспрямований інформаційний (інформаційно-психологічний) вплив на формування негативного міжнародного іміджу України, дестабілізація внутрішньої суспільно-політичної обстановки, загострення міжетнічних та міжконфесійних відносин в Україні або її окремих регіонах і місцях компактного проживання національних меншин;

– реалізація іноземними державами, міжнародними злочинними угрупованнями кіберзагроз щодо автоматизованих систем державного та військового управління, об'єктів критичної інформаційної інфраструктури [9].

Серед основних завдань, визначених цим документом для сектору безпеки та оборони, є забезпечення охорони державної таємниці, іншої інформації з обмеженим доступом, а також інформаційної та кібербезпеки. Пріоритетними напрямами удосконалення системи інформаційної безпеки вважаються такі: створення єдиної платформи захищених електронних комунікацій органів державної влади; створення національної системи кібербезпеки; удосконалення державного управління та керівництва сектором безпеки і оборони, системою забезпечення інформаційної та кібербезпеки, системою захисту інформації та безпеки інформаційних ресурсів тощо.

Сьогодні діяльність міністерства щодо діяльності в напрямку вирішення питання протидії інформаційним загрозам в Україні перебуває лише на рівні загальних нормативно-правових засад.

На Державне агентство з питань електронного урядування України також покладено завдання протидії інформаційним загрозам та забезпечення інформаційної безпеки в країні. Зокрема, Положенням про Державне агентство з питань електронного урядування України визначається, що основними пріоритетами діяльності у сфері забезпечення інформаційної безпеки є такі:

– сприяння виробництву конкурентоспроможних національних інформаційних продуктів;

– сприяння виробництву в Україні засобів захисту інформації, розробці захищених інформаційних та телекомунікаційних систем, впровадження сучасних захищених інформаційних технологій для захисту інтересів державного керівництва;

– розроблення ефективної системи запобігання та виявлення загроз державних електронних інформаційних ресурсів стосовно протидії розповсюдженню комп'ютерних вірусів, апаратних та програмних закладок, а також витоку інформації за допомогою технічних каналів і шляхом несанкціонованих дій;

– забезпечення цілісності, конфіденційності, доступності інформаційних ресурсів України, які формують передумови розвитку особистості, стабільного функціонування держави та суспільства, захисту інформації та персональних даних, якими володіють юридичні, фізичні особи та держава, від внутрішніх та зовнішніх інформаційних загроз, зокрема за допомогою протидії комп'ютерним злочинам;

– забезпечення безпеки інформаційно-телекомунікаційних систем органів місцевого самоврядування та органів державної влади, інформаційно-телекомунікаційних систем, що функціонують для захисту інтересів державного управління, для задоволення потреб безпеки та оборони країни, банківських та кредитних сфер, інших сфер економіки держави, систем управління критичною інфраструктурою;

– удосконалення нормативно-правової бази з метою забезпечення інформаційної безпеки, зокрема і кібербезпеки на національному рівні;

– впровадження захищених та надійних механізмів ідентифікації учасників електронної взаємодії в країні;

– створення системи моніторингу безпеки інформаційних систем та ресурсів [10].

Нормативне визначення пріоритетів у сфері забезпечення інформаційної безпеки висвітлює широкий спектр діяльності у цій сфері. У Положенні не визначено схему та напрями впровадження основних пріоритетів забезпечення інформаційної безпеки в Україні, що не дозволяє оцінити фактичні результати.

Окрім протидії інформаційним загрозам в Україні на державному рівні, в країні сформувався активний громадський спротив, який виражається у такі способи:

– бойкот російських товарів та послуг. У багатьох торгових мережах товари з РФ позначаються написом «зроблено в РФ». Цей захід має важливе значення у питанні захисту інформаційного

простору України, формуванні у громадян думки про недопустимість фінансування ворожої сторони через купівлю в РФ товарів та послуг;

– миттєва реакція на брехню, помилки, неточності в матеріалах проросійських ЗМІ. Цей захід здійснюється на рівні блогерів, волонтерів, політиків, звичайних громадян, він має достатньо вагомий вплив на інформаційний простір.

Стан протидії інформаційним загрозам в Україні сьогодні перебуває на стадії розвитку. Фактичний інформаційний захист на національному рівні почав формуватись саме під час російського вторгнення в Україну. Вагома роль у забезпеченні інформаційного захисту країни належить активним громадянам, волонтерам, політикам, які захищають національні інтереси України.

Висновки. З огляду на загрозу посилення інформаційного складника гібридної війни в Україні з боку РФ у стратегії щодо захисту від інформаційних загроз та протидії інформаційним війнам в Україні необхідно окремо виокремити напрями загроз та протидій стосовно Російської Федерації. Необхідно на рівні органів державної влади, правоохоронних органів різних рівнів закріпити основні заходи щодо поетапного інформаційного протистояння РФ як по всій території України, за її межами, так і на території анексованої АР Крим, на окупованих територіях Донецької та Луганської областей, прифронтових територіях, територіях, що межують з окупованими.

Серед цих заходів можна виокремити такі: забезпечення окупованих територій каналами інформування та доведення до населення цих територій проукраїнської позиції; моніторинг, контроль засобів масової інформації на прифронтових територіях, територіях, що межують з окупованими, для виявлення негативного інформаційного впливу з боку РФ; поширення трансляції проукраїнських теле- і радіоканалів; психологічна підтримка населення на окупованих територіях, прифронтових територіях, територіях, що межують з окупованими; психологічно-пропагандистська підтримка військових у зоні ведення бойових дій повинна здійснюватись на стратегічних та професійних засадах.

Література:

1. Горбулін В.П., Качинський А.Б. Системно-концептуальні засади стратегії національної безпеки України. К.: ДП «НВЦ «Євроатлантикінформ»», 2007. 592 с.
2. Parulua A. Hybrid Warfare – Contemporary Concept in Georgia's External Security. URL: file:///C:/Users/%D0%92%D0%B0%D0%B4%D1%96%D0%BB%D0%B5%D0%BD/Desktop/H%C3%BCbriids%C3%B5japidamine+-+kaasaegsed+Gruusia+v%C3%A4lisjulgeoleku+kontseptsioonid.pdf.
3. Горбулін В.П. «Гібридна війна» як ключовий інструмент російської геостратегії реваншу. Стратегічні пріоритети. К.: НІСД, 2014. № 4. С. 5–12.
4. Darczewska J. The Devil is in the Details. Information Warfare in the Light of Russia's Military Doctrine, Point of View no. 50, Warsaw: Centre for Eastern Studies. 2015.
5. Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України»: Указ Президента України від 26.05.2015 р. № 287/2015 URL: http://zakon2.rada.gov.ua/laws/show/287/2015.
6. Про основи національної безпеки України: Закон України від 19.06.2003 р. № 964-IV / Верховна Рада України. Відомості Верховної Ради України. 2003. № 39. Ст. 351.
7. Про інформацію: Закон України від 02.10.1992 р. № 2657-XII / Верховна Рада України. Відомості Верховної Ради України. 1992. № 48. Ст. 650.
8. Питання діяльності Міністерства інформаційної політики України: постанова Кабінету Міністрів України від 14.01.2015 р. № 2 URL: http://zakon2.rada.gov.ua/laws/show/2-2015-%D0%BF.
9. Про рішення Ради національної безпеки і оборони України від 4 березня 2016 року «Про Концепцію розвитку сектору безпеки і оборони України»: Указ Президента України від 14.03.2016 р. № 92/2016. URL: http://zakon5.rada.gov.ua/laws/show/92/2016.
10. Про затвердження Положення про Державне агентство з питань електронного урядування України: постанова Кабінету Міністрів України від 01.10.2014 р. № 492. URL: http://zakon3.rada.gov.ua/laws/show/492-2014-%D0%BF.