DOI: 10.5281/zenodo.3532664
УДК 351.75

Бєльська Т. В., д.держ.упр., доц., ХНУМГ ім. О. М. Бекетова, м. Харків,
Крюков О. І., д.держ. упр., проф., ННВЦ НУЦЗУ, м. Харків

Bielska T., Doctor of Science in Public Administration, Associate Professor, Associate Professor of the Department of Management and Public Administration, O.M. Beketov National University of Urban Economy in Kharkiv, Kharkiv,
Kryukov O., Doctor of Sciences in Public Administration, professor, professor of the department of public administration in the field of civil protection of the Educational-Scientific-Production Center of the National University of Civil Protection of Ukraine, Kharkiv

ІНФОРМАЦІЙНІ ВІЙНИ ТА ІНФОРМАЦІЙНА БЕЗПЕКА: ЗАГРОЗИ ТА ВИКЛИКИ ДЛЯ ДЕМОКРАТІЇ

INFORMATION WARS AND INFORMATION SECURITY: THREATS AND CHALLENGES FOR DEMOCRACY

У статті констатується, що неконтрольована інформація може стимулювати різні інформаційні небезпеки. Визначено, що потреба пристосування управління до умов зовнішнього середовища породжує необхідність вироблення ефективних стратегій управління інформацією. Встановлено, що інформаційні війни тісно пов'язані з громадянським суспільство.

Ключові слова: *інформаційна політика, інформаційна безпека, гібридна війна, кібер-війна, інфологеми, фейки, тролі.*

The article states that uncontrolled information can stimulate various informational dangers. It is determined that the need to adapt management to environmental conditions necessitates the development of effective information management strategies. It has been established that information wars are closely related to civil society.

Keywords: *information policy, information security, hybrid war, cyber war, infologues, fakes, trolls.*

Постановка проблеми. Глобальне громадянське суспільство, крім по-

зитивного впливу на демократизацію процесу ухвалення міжнародно-політичних рішень, може становити певну загрозу для демократії. Загрозою, зокрема, можуть стати антидемократичні цілі, засоби та наслідки дій. І все ж таки ризики демократії не є підставою для гальмування розвитку глобального громадянського суспільства – вони є спонукою ставитися до нього зважено.

Аналіз останніх досліджень і публікацій. Наукова лексика збагатилася цілою низкою понять, які відображають принципово новий характер відносин у світовій політиці, економіці та соціальних стосунках. У науці з'явився термін "інформаційна війна", який передбачає створення нових засобів протиборства, нового виду зброї – інформаційної, що зазвичай і розуміють, говорячи про війни Шостого покоління. Учені Г. Почепцов, С. Гриняєв, А. Манойло інтерпретують інформаційну війну як соціальне явище, породжене суспільством, як інструмент міждержавного військового протиборства, як складову системи регулювання політичного конфлікту, як інструмент державної політики і (на нашу думку, найбільш точно) як консцієнтальну війну (від латинського conscientia – свідомість). Всі вищевикладені процеси спричинені особливостями сучасного періоду глобалізації та неврегульованістю правових питань у глобальному інформаційному просторі.

Аналіз наукових публікацій із зазначеної проблеми підтверджує, що громадянського суспільства залучається в процес інформаційних воєн, спотворюючи сутність і зміст гегелівської концепції громадянського суспільства. Відзначаючи неперевершені можливості інформаційних і комунікаційних процесів у глобалізованому світі, слід звернути увагу на зростання обсягу інформації, яку почали отримувати громадяни без контролю своїх національних урядів.

Постановка завдання. Метою статті є аналіз інформаційної політики держави і вироблення рекомендацій для забезпечення інформаційної безпеки суспільства.

Виклад основного матеріалу. У реальному житті участь громадянського суспільства в інформаційних війнах виражається в роботі найрізноманітніших формальних і неформальних організацій і груп, що активно працюють у напрямку боротьби з тероризмом і беруть участь у полеміці з питань протидії терору. Громадянське суспільство надає можливість організувати суспільну полеміку, обговорювати різні питання, наприклад чинити інформаційну протидію негативним публікаціям у зарубіжних ЗМІ через газети, спеціальні журнали, зібрання громадськості та через інші засоби пропаганди. Участь громадянського суспільства в обговоренні практичних питань боротьби з тероризмом є важливою складовою забезпечення національної безпеки.

Інтернет і мережеві технології стали ключовим механізмом для просування нової моделі свідомості [1].

Процеси глобалізації й інформатизації спонукають до переміщення

активності суспільства в Інтернет.

У процесі інформаційної війни здійснюється вплив на цивільне населення та (або) військовослужбовців іноземної держави шляхом поширення певної інформації; здійснюються цілеспрямовані дії, розпочаті для досягнення інформаційної переваги шляхом заподіяння шкоди інформаційним процесам і системам супротивника з одночасним захистом власних інформаційних процесів і систем. Об'єктом інформаційної війни є як масова, так і індивідуальна свідомість. Засобами ведення інформаційної війни є будь-які засоби передання інформації – від ЗМІ до поширення чуток. [2, с. 119].

За кожним інформаційним повідомленням стоять ті чи інші фінансово-політичні групи впливу, між якими не існує ні ідеологічного, ні політичного, ні світоглядного консенсусу. Актив телеканалів складають лояльні до вигідної їм точки зору блогери, активісти громадських організацій, члени партій і нечисленні експерти-аналітики. До зазначених організацій та установ належать також різні місіонерські релігійні структури, які нав'язують ідеї, нерідко навіть протиправним шляхом із використанням методик і технологій нейропсихічного програмування та гіпнозу, які пригнічують волю людини. У зоні бойових дій і в тилу нарощують активність агітатори й організатори акцій, що працюють під прикриттям деяких партій і громадських організацій. Таким чином, громадськість втягується в інформаційну війну

Інформаційні війни, які також називають війнами Шостого покоління, переслідують мету встановити контроль над свідомістю громадян держави потенційного супротивника.

Інформаційна війна передбачає проведення заходів, спрямованих проти систем управління, а також проти комп'ютерних та інформаційних мереж і систем. Деструктивний вплив на системи управління досягається шляхом застосування інформаційної зброї та проведення системи інформаційних операцій.

Як інформаційна зброя використовуються інфологеми. Інфологема – це хибна, перекручена або неповна інформація, що зображує реальні події, наповнені ідеологічними міфами, політичними пропагандистськими вигадками [3, с. 284; 4]. Вони формують громадську думку, стійкі стереотипи індивідуального та соціальної поведінки, ціннісні установки й орієнтації населення та соціально-психологічні стандарти поведінки громадян. Як і будь-які ідеологічні міфи, інфологеми є активними й агресивними. Вони витісняють достовірну інформацію, залишаючись нерідко правдоподібними. Вони лягають на благодатний ґрунт напруженої психології мас, миттєво вводяться в інформаційні канали й легко перетікають в різні галузі політичного та духовного життя.

Інфологеми є головним продуктом діяльності політтехнологів. Особливо ефективним застосування інфологем стає під час виборів, революцій,

громадянських війн і збройних конфліктів.

До інфологем належать чутки, фейки, тролі, повторення гасел чи шаблонних фраз і збудження іншими прийомами запланованого психологічного впливу на поведінку населення.

Під чутками узвичаєно розуміти неперевірену усну інформацію, дані, достовірність яких не встановлено, але і не спростовано. Політичні чутки використовують для: 1) компрометації союзників; 2) перевірки прийнятності тієї чи іншої пропозиції для громадськості; 3) дискредитації противника; провокування населення на здійснення дій, які є вигідними для одного з двох політичних противників. Для профілактики та спростування чуток, з одого боку, треба відкрито і детально повідомляти про всі події, навіть якщо вони мають негативний аспект, але з іншого – інформацію все ж таки доцільно фільтрувати й коригувати, що породжує дилему.

На практиці ця дилема вирішується шляхом установлення таких форм контролю над чутками: 1) спростування чуток важливими персонами; 2) запровадження цензури; 3) створення спеціальних урядових установ, що займаються вивченням чуток і наданням достовірної інформації (колонка чуток в газеті, різні соціологічні центри) [5, с. 42–43].

Дуже поширеними інфологемами є фейки. Це поняття увійшло в наше життя відносно недавно, воно походить від англійського *fake* – "підроблений, фальшивий, липовий". До фейків належать: фотографії, підроблені в фотошопі, відеороліки, змонтовані у відеоредакторі або зняті зовсім в інший час і в іншому місці, фальшиві новини, які неможливо відрізнити від правди, так звані в слов'янському світі "газетні качки", сторінки в соціальних мережах, створені від імені інших, як правило, відомих людей, фальшиві акаунти.

Деякі матеріали мають відеопідкріплення, тому на їх тлі фейки виглядають як справжні новини. Згодом правда з'ясовується, але інформація вже була кинута в мережу й зробила свою справу. Коли емоції вщухають, на зміну одній неправдивій інформації надходить інший фейк. Над тим, щоб чергова інформаційна бомба накрила максимальну кількість людей і стала популярною за лічені хвилини, працюють сотні кореспондентів. У зв'язку з цим з'явився ще один термін – "тролінг".

Троль, тролінг (від англ. Trolling) – розміщення в Інтернеті провокаційних повідомлень із метою викликати конфлікти між учасниками, образи, "війну правок", марнослів'я тощо.

Психологічний вплив на противника, що ґрунтується на комунікативних процесах із використанням сучасних інформаційних технологій, передбачає зміну громадської думки в заданому напрямку, що досягається за допомогою інформаційних операцій.

Інформаційні операції – це сплановані дії, спрямовані на ворога, дружню або нейтральну аудиторію шляхом впливу на його свідомість і поведінку за допомогою використання певним чином організованої

інформації та інформаційних технологій для досягнення певної мети. Вони застосовуються на макро- та мікрорівні. Інформаційні операції макрорівня – це будь-яка агітаційно-пропагандистська та розвідувально-організаційна діяльність, орієнтована на конкретні соціальні групи людей і здійснювана головним чином через засоби масової інформації та каналами комунікацій.

Інформаційні операції мікрорівня мають прицільно персоналізовану спрямованість і здійснюються переважно через міжособистісне спілкування.

Таким чином, інформаційні операції передбачають заподіяння шкоди в політичній, економічній, науково-технічній, соціальній чи будь-який інший суспільній сфері життя держави-противника і на цій основі – чинення вигідного впливу для отримання переваг у тій чи іншій галузі.

У різні часи до здійснення операцій інформаційної боротьби залучалися різні сили з різним ступенем організації та стосунку до державних структур. Зокрема, відомо, що спеціальні підрозділи інформаційної (психологічної) боротьби в структурі державних органів з'явилися тільки під час Першої світової війни. Подальший досвід організації інформаційної боротьби показав, що сили, які залучаються до реалізації політичних та військових заходів, можуть, з метою зовнішнього впливу на державну політику, цілеспрямовано впливати на певні організації та їх підрозділи. Прикладом можуть служити спеціальні підрозділи психологічної війни.

На озброєнні зазначених підрозділів перебувають пересувні теле- та радіоцентри, друкарні, обладнання для проведення усних агітаційних програм щодо особового складу й населення іноземної держави, відповідні технічні засоби: так звані "агітаційні" снаряди, бомби, повітряні кулі тощо, за допомогою яких закидаються на територію противника й розпорошуються пропагандистські матеріали. Наявність таких засобів дозволяє зазначеним підрозділам за короткий проміжок часу налагодити цілеспрямовану роботу по здійсненню ідеологічного та психологічного впливу на противника в рамках проведення різних спеціальних або безпосередньо військових операцій. Доцільно зазначити, що останнім часом спостерігається постійно зростаюча активність неурядових структур, також задіяних у здійсненні психологічного впливу.

Інформаційні війни періодично ведуться у різних країнах світу. Для організації протидії інформаційним операціям необхідно знати фактори, які сприяють виникненню загроз і небезпек в інформаційній сфері держави, з'ясувати їх сутність, вміти оцінювати й визначати реальність і рівень негативного впливу на суспільство та державу.

В. Ковальов, Ю. Матвієнко, Г. Почепцов зробили спробу окреслити деструктивний аспект соціальних мереж, стверджуючи, що "під руйнівною діяльністю соціальних мереж слід розуміти специфічну людську форму активного ставлення до світу, основним змістом якої є знищення або порушення функціонування існуючих об'єктів і систем, що забезпечують нормальне функціонування особистості, суспільства та держави" [6]. Визнання за-

коном діяльності соціальних мереж руйнівною, з точки зору права, є можливим тільки після виконання особами в реальному світі певних дій як наслідку віртуального мережевого ефекту [там же].

Е. Ларіна та В. Овчинський в доповіді "Електронні війни XXI століття" пропонують такий спосіб розділити інформаційніі кібер-війни: "Інформаційні війни є контентом війни, спрямованим на зміну масової та індивідуальної свідомості, боротьбою за свідомості, цінності, установки, моделі поведінки. Інформаційні війни існували задовго до появи Інтернет. Інтернет перевів ці війни на якісно інший рівень інтенсивності, масштабу та ефективності, а кібер-війни спрямовано на руйнівні наслідки інформаційних потоків у вигляді програмних кодів до матеріальних об'єктів та їх систем" [7].

К. Черемних і М. Восканян у доповіді "Anonymous війна" пояснюють недавнє збільшення масових протестів впливом механізмів інформаційної війни [8]. Акції позиціонуються як "ненасильницькі", хоча в деяких країнах, зокрема в Україні, вони переходять у "гібридні війни". Гібридна війна (англ. hybrid warfare) – різновид війни із поєднанням принципово різних типів і способів її ведення, які скоординовано застосовуються задля досягнення спільних цілей. Гібридна війна використовує класичні прийоми ведення війни (із військовослужбовцями в уніформах, військовою технікою та ін.), нерегулярні збройні формування (повстанців, терористів, партизан та ін.) і такі типи війни, як інформаційна та кібервійна. Гібридна війна комбінує партизанську та громадянську війни, а також заколот і тероризм. Визначення "гібридна війна" в міжнародно-правових документах відсутнє [9, с. 52–53]. У зоні бойових дій і в тилу нарощують активність агітатори й організатори акцій, що працюють за сприяння деяких партій і громадських організацій.

На зміну "кольоровим революціям" прийшли "революції 2.0", відмінна риса яких – ключова роль Інтернету та соціальних мереж. "Революція 2.0" не може існувати без мережевих ресурсів – це її повітря, її простір, її інструмент.

У країнах, що мають значний наукомісткий сектор економіки й високотехнологічну виробничу сферу та характеризуються високим рівнем впровадження Інтернету в повсякденне життя, соціум є набагато більш уразливим для застосування інформаційних і кібер-воєн. Одна з провідних американських організацій з вивчення громадської думки Pew Internet & American Life Project провела опитування, хто найбільшою мірою загрожує конфіденційності особистої та корпоративної інформації. Підсумки виявилися такими: 4 % – силові структури, 5 % – уряд, 11 % – інші бізнес-структури, 28 % – рекламодавці та Інтернет-гіганти й 33 % – хакери [7]. Протистояти інформаційним і кібер-війнам держави намагаються у різні способи. Тому важливими та своєчасними були б аналіз соціальних і психологічних наслідків впливів на суспільство інформації, проведення комплексних наукових досліджень із проблем протидії інформаційним війнам та інформаційним атакам, вироблення заходів збереження психологічної стійко-

сті громадян, розробка заходів щодо зниження рівня агресивності та насильства в суспільстві, що охоплюють “блокування” матеріалів, які пропагують культ жорстокості.

Процеси глобалізації, інформатизації й переміщення активності суспільства в Інтернет потребують чіткого осмислення державами необхідних змін та активних дій для створення правового поля, в якому зацікавлені суспільство, особа й держава. Крім відсутності правового поля, Інтернет-спільноти мають ще один недолік – відносну нестабільність утворення, оскільки навіть спільнота з найкращими ідеями ризикує дуже швидко зникнути після втрати цікавості ключових учасників [10].

Із появою нових технологій перед суспільством, особою та державою постають нові виклики. Переміщення активності суспільства в Інтернет потребує створення правового поля для Інтернет-середовища.

Висновки. Отже, інформаційний розрив може стимулювати різні інформаційні небезпеки, починаючи від хакерських атак на приватні сайти і закінчуючи викраденням або оприлюдненням стратегічно важливих відомостей національного характеру. Потреба пристосування управління до умов зовнішнього середовища породжує необхідність вироблення ефективних стратегій управління змінами.

Глобальне громадянське суспільство окрім позитивного впливу на демократизацію процесу прийняття міжнародно-політичних рішень може нести певну загрозу для демократії, однак ризики демократії не є підставою для гальмування розвитку глобального громадянського суспільства, вони є стимулом ставитися до нього зважено. Встановлено, що інформаційні війни тісно пов’язані з глобальним громадянським суспільством. Сьогодні в світі розгортаються спеціальні інформаційні операції та війни, спрямовані проти суверенітету держав, за допомогою міжнародних неурядових організацій, які є інститутами глобального громадянського суспільства. Інформаційні війни періодично ведуться в різних країнах світу напередодні реальних воєн і в процесі їх ведення, тому завданням державної влади є просвіта громадськості для захисту від інформаційних атак та консолідація громадянського суспільства на протидію інформаційним впливам.

Список використаних джерел:

1. Мазур Л. Антропологічний вимір відношення людини до віртуальної реальності [Електронний ресурс] / Любов Мазур // Людина і світ: способи та аспекти взаємовпливів : тези міжнародної наукової конференції “XXIV Читання, присвячені пам’яті засновника Львівсько-Варшавської філософської школи К. Твардовського” (10–11.02.2012 року). – Львів : Ліга-Прес, 2012. – С. 74–76. – Режим доступа : http://ena.lp.edu.ua:8080/bitstream/ntb/27836/1/028_074_076.pdf.

2. Сучасна політична лексика // Вдовичин І., Угрин Л., Шипунов Г. та ін.; за ред. В. Хоми Н. М. – Львів: Новий Світ-2000, 2015. – 395 с.

3. Крысько В. Г. Секреты психологической войны (цели, задачи, методы, формы, опыт) / В. Г. Крысько ; под общ. ред. А. Е. Тараса. – Мн. : Харвест, 1999. –

448 с.

4. Петик М. Україна в сучасних глобалізаційних процесах / М. Петик // Формування ринкової економіки в Україні. – 2009. – Вип. 19. – С. 530–539.

5. Шульга М. А. Соціально-політичне управління / М. А. Шульга – К. : Центр учбової літератури, 2008. – 248 с.

6. Почепцов Г. Информационная война-2013 в представлениях российских экспертов [Електронний ресурс] / Г. Почепцов // Медіапросвіта. – 2014. – Режим доступу : http://osvita.mediasapiens.ua/ethics/manipulation/informatsionnaya_voyna2013_v_predstavleniyakh_rossiyskikh_ekspertov/.

7. Ларина Е. Цифровые войны XXI века [Електронний ресурс] / Е. Ларина, В. Овчинский.– Режим доступа : dynacon.ru/content/articles/2321/#a1.

8. Черемных К. Анонимная война. “новый 1968 год”: мировозренческое содержание и механизмы революций 2.0 (доклад Изборскому клубу) [Електронний ресурс] / К. Черемных, М. Восканян. – Режим доступу : www.dynacon.ru/content/articles/1468/#1.

9. Сучасна політична лексика // Вдовичин І., Угрин Л., Шипунов Г. та ін.; за ред. В. Хоми Н. М. – Львів: Новий Світ-2000, 2015. – 395 с.

10. Bielska Tetiana. Information warfare as a way of implementing the state policy in the modern world / Tetiana Bielska // Regional Development and Public Administration in the Context of General Tendencies of 21 century. – Eds . V . Szymańska. – Słupsk : Publishing House “ADNDU”. – 2015 . – P. 141–152.

References:

1. Mazur, L. Anthropological measurement of the relation of man to virtual reality [Antropolohichnyi vymir vidnoshennia liudyny do virtualnoi realnosti]. Web. <http://ena.lp.edu.ua:8080/bitstream/ntb/27836/1/028_074_076.pdf>/.

2. Vdovychyn, I., Ugryn, L. and Shipunov, G. *Modern political vocabulary. [Suchasna politychna leksika]*. Lviv. 2015. Print.

3. Krysko, V. *Secrets of psychological warfare (goals, objectives, methods, forms, experience). [Sekrety psykholohycheskoi voiny (tsely, zadachy, metody, formy, opyt)]*. 1999. Print.

4. Petyk, M. "Ukraine in modern globalization processes. [Ukrayina v suchasnykh globalizaciynyh processah]". *Formuvannya rynkovoyi ekonomiky v Ukrayini* 19 (2009): 530-539. Print.

5. Shulga, M. *Socio-political management. [Sotsialno-politychne upravlinnya]*. 2008. Print.

6. Pochepcov, G. "Information war 2013 in the views of Russian experts. [Informatsiina viina-2013 uiavlenniakh rosiiskykh ekspertiv]". *Mediaprosvita* (2014). Web. <
http://osvita.mediasapiens.ua/ethics/manipulation/informatsionnaya_voyna2013_v_predstavleniyakh_rossiyskikh_ekspertov>.

7. Larina, Ye. and Ovchinskij, V. *21st Century Digital Wars. [Tsyfrovi viiny XXI stolittia]*. Web. <dynacon.ru/content/articles/2321/#a1>.

8. Cheremnyh, *K. Anonymous war. “The new 1968 year”: worldview content and mechanisms of revolutions 2.0 (report to the Izborsk Club). [Anonimna viina. "Novyi 1968 rik": svitohliadno zmist i mekhanizmy revoliutsii 2.0 (dopovid Izborskomu klubu)]*. Web. <www.dynacon.ru/content/articles/1468/#1>.

9. Vdovychyn, I., Ugryn, L. and Shipunov, G. *Modern political vocabulary. [Suchasna politychna leksika]*. Lviv. 2015. Print.

10. Bielska, T. "Information warfare as a way of implementing the state policy in the modern world". *Regional Development and Public Administration in the Context of General Tendencies of 21 century*. Eds . V . Szymańska. Słupsk : Publishing House "ADNDU" (2015): 141–152. Print.

DOI: 10.5281/zenodo.3532666
УДК 623:355.

Білозір О. В., к.ю.н., докторант МАУП, м. Київ

Bilozir O., PhD, Associate Professor, Department of Public Administration, Interregional Academy of Personnel Management, Kyiv

ТЕОРЕТИКО-МЕТОДОЛОГІЧНІ АСПЕКТИ ФОРМУВАННЯ ДЕРЖАВНОЇ СОЦІАЛЬНОЇ ПОЛІТИКИ

THEORETICAL-METHODOLOGICAL ASPECTS OF FORMATION OF STATE SOCIAL POLICY

Зазначено, що поняття «соціальне» відображає спільний, колективний характер життєдіяльності людей, коли об'єднують їх соціальні зв'язки і спільні інтереси виявляються в рамках різних спільнот: соціальних груп, верств населення, поселень, регіонів та тощо. Взаємодія інтересів цих груп-важлива складова частина життя суспільства. Соціальна політика як інструмент управління має своєю загальною метою усунення соціальних антагонізмів в суспільстві, реалізацію за допомогою спеціальних заходів завдань динамічного розвитку і вдосконалення всієї системи соціальних відносин.

Визначено, що характер відносин між груповими і загальнодержавними інтересами може бути різним. Відносини можуть будуватися на взаємній компромісі і консенсусі, можуть грунтуватися на прямому домінуванні однієї групи і виключення інших зі сфери прийняття рішень, на придушенні інших груп. Люди страждають як від надмірного тиску влади, так і від безвладдя, тому дуже важливим є питання про зміну форм влади, панування і підпорядкування, про участь у владі і в способах реалізації громадянських прав всіх груп населення. Необхідно підкреслити також, що інтереси різних груп в періоди швидких змін суспільства не є заданими, незмінними і раціонально осмисленими, що збільшує необхідність їх наукової рефлексії, громадського обговорення та узгодження. Більш того, значення державної влади для суспільства багато в чому полягає в тому, що вона задає певну інтерпретацію подій і процесів, формує певні уявлення та інтереси.