Вісник Львівського університету. Серія філос.-політолог. студії. 2023. Випуск 51, с. 208–215
Visnyk of the Lviv University. Series Philos.-Political Studies. Issue 51, p. 208–215

УДК (32:001.891.3)
DOI https://doi.org/10.30970/PPS.2023.51.24

ІНСТИТУЦІЙНЕ УПРАВЛІННЯ ІНФОРМАЦІЙНИМИ ПОТОКАМИ ЯК ЧИННИК ПРОТИДІЇ РОСІЙСЬКІЙ КІБЕР-ВІЙНІ

Ольга Свідерська
Національний університет «Львівська політехніка»,
Інститут права, психології та інноваційної освіти,
кафедра теоретичної та практичної психології
вул. Степана Бандери, 12, 79000, м. Львів, Україна

У статті актуалізовано питання, яке безпосередньо пов'язане із національною безпекою та політикою протидії дезінформації. Йдеться про можливість регулювати інформаційні повідомлення ключових суб'єктів політики, не виходячи за рамки демократичних принципів існування суспільства. Важливим також є й обмеження негативного інформаційного впливу з боку держави-агресора РФ. Виокремлено ключові напрями за якими РФ працює проти України: деморалізація українського населення та ЗСУ, дестабілізація українського соціуму, кібер-атаки на критичну інфраструктуру країни, дискредитація України та політичної волі ключових акторів на міжнародній арені, культура «канселінгу» – спроби затерти цифрові сліди воєнних злочинів в Україні.

Акцентовано на вагомості інформаційних потоків для сучасної суспільно-політичної дійсності через розуміння набуття інформацією статусу головного ресурсу й управлінського важеля впливу на комунікації та трансформацію політичних інститутів, практик і форм політичної активності. Визначено: інформаційна війна – це цілеспрямована злочинна діяльність, метою якої є дезінформація, деморалізація, вибудовування «мовчазної покірності населення», що реалізується державою-агресором за допомогою хакерських атак, зламів систем внутрішньо-державного забезпечення життєдіяльності та обороноздатності країни, дискредитації політичного керівництва й збройних сил, проведення стратегічних, кризових та бойових інформаційно-психологічних спецоперацій на території держави, яка стала об'єктом інформаційної чи гібридної агресії.

Доведено, усі категорії суб'єктів політики можуть як послаблювати ефективність ворожих інформаційних атак, так і підсилити їхню дію. Найважливішою умовою ефективного управління інформаційними потоками є консолідоване суспільство, яке поруч із ключовими політичними акторами дбатиме про інформаційну гігієну, поважатиме закон та нестиме свідому відповідальність за розповсюдження певного контенту.

Ключові слова: інформаційна війна, інформаційне суспільство, дезінформація, кібер-злочини, астротерфінг.

Буремне XXI століття можна вважати переломним моментом у віртуалізації політичного життя. Сьогодні не існує жодної політичної сфери реалізації політики, яка не була б доступною сучасному користувачу: події, новини із приватного життя політиків, дебати, політична аналітика, ток-шоу, новини із фронту, обговорення виборів у ключових країнах-партнерах, усе разом нагадує один суцільний політичний мейнстрим, у якому звичайній людині все важче і важче відокремити правдиву інформацію від симулякру, фейку, пропаганди, дезінформації чи добре спланованої інформаційної спецоперації. Давно уже доведено, що алгоритми соціальних мереж не здатні розрізняти правду, а основними показниками істини є популярність певного повідомлення, що відображається у кількості like, коментарів, ретвітів чи переглядів публічного відео [1, с. 13]. Таким чином, постає нагальне питання, яке безпосередньо пов'язане із національною безпекою та політикою протидії

дезінформації, закріпленою на рівні інституційних правил та норм. Зокрема йдеться про можливість регулювати інформаційні повідомлення ключових суб'єктів політики, не виходячи за рамки демократичних принципів існування суспільства. Важливим також є й обмеження негативного інформаційного впливу з боку держави-агресора РФ.

Перебуваючи у активній фазі інформаційного спротиву проти РФ середньостатистичний українець, як і будь-який інший громадянин світу піддається постійному впливу з боку численних інформаційних операцій. У них може бути різна мета, однак найбільш глобальна – перемогти у війні та змусити світ забути про варварські злочини, завдані РФ українському населенню. Сьогодні ми можемо виділити кілька ключових напрямів за якими РФ працює проти України: деморалізація українського населення та ЗСУ, дестабілізація українського соціуму, кібер-атаки на критичну інфраструктуру країни, дискредитація України та політичної волі ключових акторів на міжнародній арені, культура «канселінгу» – спроби затерти цифрові сліди воєнних злочинів в Україні.

Обґрунтовуючи актуальність даної проблеми, варто звернути увагу на особливості функціонування інформаційного суспільства й наслідків його глобалізації для сучасної людини. Як раніше було зазначено: «соціальні мережі, є самі собою нейтральними. Вони лише дають можливість індивіду проявити і виразити свої цілі. Проте вже самі цілі починають забарвлювати ці технології… звідси – застосування «психологічних текстів», вирішення «логічних задач», проведення масштабних політично вмотивованих челенджів, флешмобів тощо» [2, с. 74].

Свого часу М. Кастельс висунув гіпотезу про існування трьох умов глобалізації Мережі: по-перше, її архітектура має бути відкритою, децентралізованою, розповсюдженою і мультикерованою; по-друге важливо дотримуватися відкритих протоколів зв'язку, які мають бути загальнодоступними, поширеними й чутливими до внесення змін; по-третє, установи управління мережею мають відповідати принципам відкритості й співробітництва, які концептуально закладені у понятті Інтернету [3, с. 27]. Розуміння важливості інформаційного суспільства у контексті формування кібер-безпеки зумовлене тим, що під його впливом змінюється політичний процес, формується інша, віртуальна маса та поведінка, яка має ознаки «симулятивності, фрагментарності, нівелювання традиційних інституцій…» [4, с. 68]. Свого часу, перші користувачі комп'ютерних мереж заклали фундамент правил користування віртуальних спільнот, визначивши особливості надсилання повідомлень, загальні правила масових розсилок, поведінки у чатах, онлайн гри з багатьма гравцями, інтернет-конференцій, та ін. [3, с. 50]. На переконання М. Кастельса, особливість цих спільнот полягала у дотримання вільної горизонтальної комунікації й самокерованого створення мережі [3, с. 53]. Можливість зберігати анонімність у соціальній мережі є надзвичайно привабливою: у соціальних мережах не обов'язково використовувати правдиве ім'я, не відчувається ієрархії, витираються поняття про дистанцію чи особисті кордони. Практично кожен користувач може знайти собі людей за спільними інтересами, або ж сформувати нову мережеву спільноту навколо своїх ідей. З іншого боку це сприяє поширенню загального невігластва, адже дозволяє бути «експертом» чи «політичним аналітиком» будь-кому, хто вміє просто користуватися сучасними гаджетами. У контексті інформаційної війни високий рівень віртуалізації суспільства може сприяти здобуттю перемоги, однак з іншого боку, надмірно потужні інформаційні потоки, підкріплені ворожими психологічними спецопераціями, астротерфінгом, кампаніями із дискредитації та дезінформації з боку ворога можуть спричинити формування великої кількості «корисних ідіотів», які підсилять ворожий інформаційний потік, шляхом репостів, суперечок та емоційних реакцій на ті чи інші інформаційні провокації.

Вагомість інформаційних потоків для сучасної суспільно-політичної дійсності підкріплюється й тим, що інформація набула статусу головного ресурсу й управлінського важеля впливу на комунікації та трансформацію політичних інститутів, практик і форм політичної активності [5]. Це дуже добре використовується у астротерфінгу – процесі «створення штучної суспільної думки через застосування сучасного програмного забезпечення для витіснення реальних людей на веб-форумах» [2, с. 75]. Залучення бот-систем сприяє підсиленню обговорення «важливих» для замовника тем та затінення «не зовсім зручних». Таким чином створюється певний інформаційний потік, який вміщує «суспільну думку», сформовану ботами (автоматизованими відповідями програми на ключові слова), візуалізованими образами (мемами), флешмобами (симулятивними кампаніями із поширенням певної інформації мережею), «експертною думкою» (доволі часто сформовану або поширену інфлюенсером у віртуальну масу без відповідних знань та кваліфікацій, але з необхідною кількістю підписників). Отже, як ми вже зауважували: «інформаційне суспільство відображає суспільно-політичну реальність, яка вирізняється суттєвими змінами у структурі ціннісних пріоритетів індивідів, їхньої життєвої стратегії побудови суспільних порядків, нівелювання ролі політичних інституцій у житті суспільства» [6, С. 22–29]. Спостерігаючи за особливістю розвитку світових подій, дуже слушним буде згадати думку С. Ягодзінського про те, що людям не лише подобається користуватися функціоналом соціальних мереж, але й результати використання онлайн інструментарію є доволі видимим та успішними [7, с. 196]. Протягом якогось десятиліття історія налічує достатню кількість безпрецедентних подій, які увійшли в історію завдяки використанню цифрових інструментів.

Отже, згідно загальноприйнятого визначення, інформаційний потік – це рух інформації від її джерела до отримувача, який визначений функціональними зв'язками між ними. Будь-яка інформація складається із знаків, які у свою чергу схожі до речей, що рухаються та зберігають свою форму. На переконання Аль-Федакхі, знаки, які створюють потік інформації піддаються зовнішньому впливу: їх можна «створювати, обробляти, отримувати, випускати та транслювати». Автор вважає, що ці знаки охоплюють більшість комунікативних мовних знаків, за допомогою яких можна передавати інформацію про речі, яких немає (симулякри), речі, які описують явища минулого, теперішнього чи майбутнього [8, с. 304]. Чим більше інформації продукує суспільство, тим більшими і швидшими стають інформаційні потоки. Внаслідок швидкої зміни інформації, збільшення її обсягу формується інформаційне перенасичення, в результаті чого будь-яка фейкова новина перестає бути актуальною практично на наступний день, вона забувається, і забувається бажання її викрити. Цей стан суспільної амнезії створюють не тільки цілеспрямовані маніпуляції свідомістю, але і цілком природні особливості епохи гіперреальності, при якій інформаційні потоки дозволяють людині «ковзати» від однієї новини до іншої, не даючи їй можливості включати критичне мислення і проникнути вглиб політичних проблем. Народжується псевдоінформаційний спам, зростає ентропія, а інформація, котру ми отримуємо від сучасного медіа все більше втрачає ознаки «реальності» [5, с. 182].

Отже, інформаційні потоки є важливими елементами інформаційної війни, а ефективне управляння ними – запорукою її ефективності та протистояння ворогу. У спробі концептуалізувати поняття кібер-війни, Джеймс Віртц підкреслює, що це вишукана технічна тема, в якій домінують інженери, математики та інформатики – люди, які передусім зосереджені на певній програмі, а не на взаємозв'язку між технічною експлуатацією та великою політичною стратегією. У певному сенсі питання, пов'язані з кібервійною, часто розглядаються не просто як щось технічно нове у військовій сфері, а як щось безпрецедентне

[9, с. 29]. Польський дослідник А. Лелонек, під поняттям інформаційної війни, розуміє дії, що здійснюються задля досягнення інформаційної переваги над опонентом, за допомогою процесів опрацювання персональних даних, використання інформаційних систем та комп'ютерних мереж [10, с. 69]. У нашому розумінні «*інформаційна війна* – це цілеспрямована злочинна діяльність, метою якої є дезінформація, деморалізація, вибудовування «мовчазної покірності населення», що реалізується державою-агресором за допомогою хакерських атак, зламів систем внутрішньо-державного забезпечення життєдіяльності та обороноздатності країни, дискредитації політичного керівництва й збройних сил, проведення стратегічних, кризових та бойових інформаційно-психологічних спецоперацій на території держави, яка стала об'єктом інформаційної чи гібридної агресії» [11, с. 62]. Загалом виділяють три рівні дії інформаційної війни: індивідуальний, груповий та глобальний. Ми пропонуємо виділити чотири рівні: індивідуальний, територіальний (регіональний), національний та глобальний [11, с. 62], відповідно до того, як РФ застосовує методи пропаганди у контексті російсько-української війни.

А. Лелонек пропонує додатково виокремити ще два рівні: цивільний і військовий. Особливо цікавим у цьому контексті є «м'які атаки» по відношенню до обох рівнів. Вони не дають миттєвих результатів і є практично невидимими. З одного боку вони виглядатимуть як звичайні кібератаки, з іншого ж через свої особливості впливають на когнітивні процеси [10, с. 70]. Прикладами таких атак можуть бути злами систем, проникнення, руйнування інформаційних систем; використання зовнішніх акторів і корумпованих внутрішніх структур, послаблення можливостей інформаційних системи противника, в т. ч. за допомогою шкідливих програм, використання систему штучного інтелекту [10, с. 71–72]. У контексті російсько-української війни такі м'які атаки відбуваються постійно.

Загалом можемо виокремити кілька ефективних методів управління інформаційними потоками, які можуть використовуватися у кібер-війні:

«Фільтрування інформаційного потоку»: суть методу полягає в обмеженні доступу аудиторії до інформації, руйнуванні інформаційних систем конкурента. Для реалізації цього методу розробляють додаткові засоби фільтрування інформації, які дозволяють знизити ефективність одного чи декількох повідомлень: «парасолька», яка полягає у перешкоджанні отримання адресатом повідомлення; «лійка», коли повідомлення нейтралізується кількісною перевагою інших повідомлень; «колесо», коли у масовій свідомості відбувається підміна одного повідомлення іншим через його «пріоритетність»; «заміна», коли сумніву піддається не сама інформація, а її джерело чи медіатор.

«Вибірковість інформації»: суть методу полягає у спеціальному доборі тільки тих фактів, які є вигідними для інформаційно-психологічного впливу: «відволікання, або копчений оселедець (red herring)» застосовується для відволікання уваги аудиторії від важливої інформації. Метод реалізується через використання іншої інформації, поданої у максимально сенсаційній формі. Тут присутні емоційні гачки, тарґетинг. Як правило реакція суспільства на такі «емоційно підігріті» теми є миттєвою і доволі гострою; «створення фактів» через подання у новинах дійсних правдоподібних, дійсних неправдоподібних і вигаданих, але правдоподібних фактів. Як правило саме «факти» третьої категорії проникають у свідомість автоматично.

«Інформаційний шум»: в основі цієї маніпулятивної стратегії закладений принцип «навішування» на основну інформацію безліч інших матеріалів: велика кількість коментарів, суперечливих думок, складних теоретичних викладів, зарозумілі виступи вузько-профільних «експертів». Таким чином, головна тема губиться у неперервному потоці не пов'язаних між собою повідомлень, які швидко і у великій кількості «падають» на аудиторію.

Серед інших, відомих методів управління інформаційними потоками є: метод *«використання чуток»* – інформації, яка передається під час міжособистісної інтеракції і стосується актуальних явищ й подій у суспільному житті, відображає прагнення людей дофантазувати незрозумілу ситуацію. Чутки часто ґрунтуються на неправдивих свідченнях, і, як правило, є наслідком дефіциту інформації. Людина за своєю природою схильна швидше надати значення інформації, яка подається пошепки, у порівнянні із тією яка є відкритою. Згідно цього переконання, якщо індивід отримує інформацію, яка класифікується як «таємна змова», йому й справді може видатися ніби він володіє унікальними знаннями. Це сприяє запам'ятовуванню поданої інформації, навіть якщо згодом її спростувати.

«Витік секретної інформації» – штучно створені витоки через залучення ЗМІ та анонімних джерел, як правило вони уособлюють «таємну» інформацію, яка стосується ймовірних політичних акцій представників влади, чи тих хто на неї претендує.

«Використання дезінформації та пропаганди». Говорячи про дезінформацію як інструменті управління інформаційними потоками, необхідно зважати що вона може мати декілька форм: приписування комусь чи чомусь певних особливостей та характеристик; спотворення реальних подій; перебільшення значення певної події чи явища; спотворення фактів; відверта брехня. До слова, за словами Девіда Дж. Сміта, РФ має широку концепцію інформаційної війни, яка включає розвідку, контррозвідку, обман, дезінформацію, електронну війну, ослаблення комунікацій, погіршення навігаційної підтримки, психологічний тиск, деградацію інформаційних систем і пропаганду. Комп'ютери є одним із багатьох інструментів російської інформаційної війни, яка ведеться 24 години на добу, сім днів на тиждень, не залежно від того чи перебуває вона у активній війні чи ні, додатково використовуючи медіа, зокрема Russia Today яка є одним із інструментів інформаційної війни [12].

М. Руїз чітко розрізняє дії РФ як на внутрішньодержавному, так і на глобальному рівні, наводячи приклади з доктрини інформаційної безпеки 2016 року, метою якої є «нейтралізація інформаційно-психологічної діяльності, у тому числі й такої, яка спрямована на підрив історичних засад та патріотичних традицій, пов'язаних із захистом Батьківщини». Для реалізації цієї мети необхідно нарощувати можливості, проводити ретельний контроль за населенням, посилювати риторику про західну загрозу та агітацію проти націоналізму. За оцінкою авторки, подібна тактика повинна запевнити громадян РФ у правильності нових кроків (наприклад виправдання повномасштабного вторгнення на територію України) [13].

Джеймс Віртц розглядає РФ як гостру загрозою для США у кіберпросторі. Йдеться зокрема про застосування практики ведення інформаційних кампаній з підриву довіри до США серед міжнародних партнерів, кібер-атаки на критичну інфраструктуру США, а також союзників і партнерів. У війні проти України російські військові та розвідувальні підрозділи використовували низку цифрових можливостей проведення інформаційно-психологічних спецоперацій, зокрема й через глобальну пропаганду. Неодноразово використовувалися кібер-засоби у спробах перешкодити ефективному просуванню української армії, деморалізації ЗСУ, знешкодженні матеріально-технічного забезпечення, атаках на цивільну інфраструктуру та підриві політичної волі українського населення [9, с. 4]. На щастя, поки ці дії мають доволі обмежені результати, зокрема, через стійкість українських мереж та постійну підтримку з боку міжнародних партнерів. З іншого ж боку РФ доволі стійка й захищена у плані інформаційних атак по відношенню до неї. Йдеться у тому числі й про потужну роботу щодо управління інформаційними потоками, які можуть виставити її у негативному світлі передусім перед її громадянами.

Так, за даними Surfshark, опублікованими 20 листопада 2023 року, рекордсменом у запитах урядів країн на видалення вмісту із Google була РФ. Загалом виділяють понад 20 причини, які можуть дозволити керівництву держави вимагати від Google видалення певного контенту. Вважається, що найпопулярнішими запитами є питання, пов'язані із загрозою національній безпеці, екстремізмом, поширенням неправдивої інформації, порушенням авторського права, наклепами, які завдають репутаційної шкоди тощо. Згідно проведеного дослідження на керівництво РФ припадає більшість усіх запитів, пов'язаних із національною безпекою. Цікавим спостереженням є різке збільшення запитів від 2014 року, саме з моменту коли РФ почала війну проти України та анексії Крим. У 2022 році, це ж дослідження вказує, на величезне збільшення запитів РФ (понад 300%): зі 150 урядів, включених у звіт Google, РФ найбільше просить видалити загальнодоступний контент. За останнє десятиліття було подано 215 000 запитів на видалення майже двох мільйонів елементів, які найчастіше стосувалися вмісту YouTube, веб-пошуку та Blogger. Серед причин, які допомагають РФ домогтися видалення певного контенту є інституційні норми країни-агресора, закріплені на рівні законодавства: розширення сфери дії уряду для запитів на видалення URL-адреси із вмістом, забороненим у РФ, із сервісів Google чи ухвалення РФ закону у 2018 році, який забороняє «неповагу» до влади та поширення контенту, який вважається «фейковими новинами» [14].

Також у згаданому дослідженні йдеться, що запити, подані у 2022 році, включають такі випадки, як прохання видалити сайт, який документує російсько-українську війну, зокрема наявність жертв серед цивільного населення в Україні, або відео YouTube і коментарі, пов'язані з частковою військовою мобілізацією в РФ. Водночас відбувається активне формування позитивної думки серед росіян по відношенню до країни-партнера Китаю. До прикладу, знайдені випадки, коли керівництво РФ просило видалити URL-адреси, що ведуть до статей вікіпедії про Сі Цзіньпіна [14]. Звідси можемо зробити висновок, що однією із ключових задач із протидії кібер-війни є розробка стратегічного плану із ефективного інституційного управління інформаційними потоками

Упорядники «Білої книги дезінформації» ключовою проблемою у процесі протидії дезінформації у публічному просторі розглядають існування значної різниці у підходах до розуміння цього процесу у різних суб'єктів політики, яких вони пропонують поділити на чотири ключові кластери: органи державної влади, політичні актори; суб'єкти громадянського суспільства; окремі громадяни; бізнес-корпорації [15, с. 10]. Виокремлення авторами проблем, які пов'язані із протидією дезінформації, це своєрідна спроба знайти спільну точку управління інформаційними потоками, яка б відбивала інституційні правила та норми кібер-безпеки самої держави. Аналізуючи думку авторів щодо проблеми інформаційної національної безпеки, доходимо висновку, що найбільша складність формування державної парадигми протидії пропаганди та дезінформації захована у практиці «подвійних стандартів»: з одного боку органи державної влади і політичні актори «декларують прагнення реалізовувати державну функцію забезпечення захисту держави, суспільства та громадян від загроз в інформаційній сфері», з іншого боку – вони самі можуть вдаватися до інструментів «боротьби з дезінформацією» для просування власних наративів, інформаційного домінування над політичними конкурентами чи придушення свободи слова [15, с. 10], що саме по собі заперечує демократичні принципи функціонування суспільства; схожу ситуацію можна спостерігати й у діяльності суб'єктів громадянського суспільства. Наприклад, автори підкреслюють можливість фінансування громадських організацій чи медіа міжнародними донорськими внесками або грантами, які не завжди надходять від дружніх держав. Оскільки немає державного важелю впливу на функціонування громадянського суспільства, а «громадянське суспільство не має етичних та репутаційних інструментів

впливу на медіа і громадські об'єднання, проблема потенційних зловживань в інформаційному просторі залишається» [15, с. 10]. Йдеться про відсутність механізмів впливу на просування замовних наративів, які відверто можуть працювати на благо ворога.

До третього кластеру суб'єктів політики, які безпосередньо пов'язані із формуванням якості інформаційного потоку відносять інфлюенсерів (лідерів думок), які «під виглядом плюралізму думок та захисту свободи слова … можуть просувати небезпечні для суспільства і держави тези, прикриваючись своїм статусом» [15, с. 11]. Під час ковідної кризи, таких «лідерів думок» було прийнято називати антивакцинаторами, основна діяльність яких була сконцентрована на поширенні паніки, дезінформації, порушенні суспільного порядку, та формуванні відповідних суспільних настроїв та думок. У час повномасштабної війни, такі особи просувають потужні російські наративи та стереотипи щодо ЗСУ, влади, опозиції, церкви, російської мови, необхідності збереження «великої російської культури» тощо. Визначальним маркером такої поведінки є участь окремих індивідів у розповсюдженні наративів держави-агресора, шляхом імпульсивного поширення спожитої інформації за допомогою можливостей соцмереж та месенджерів (ретвіт, репост, ріплей тощо). Найбільша складність у тому, що «лідери думок» як правило мають доволі велику аудиторію підписників, окремі можуть бути й мільйонниками, відповідно кожне обмеження, блокування чи заборона миттєво ними трактується як загроза свободі слова, й відповідні наративи транслюються на користувацьку аудиторію.

Серед бізнес-корпорацій, які беруть участь у розвитку інформаційного простору автори виділяють дві категорії: бізнес, для якого медіа є активом та водночас професійною діяльністю (тут йдеться про наявну мету бізнесу максимізувати прибутки від своєї популярності) або медіамайданчики, що використовуються великим бізнесом для захисту своїх комерційних інтересів у політичній площині. Як правило вони є повному забезпеченні великого бізнесу, який, по суті, може прямо чи опосередковано впливати на редакційну політику [15, с. 11].

Підсумовуючи, вважаємо за доцільне підкреслити вагомість інституційного управління інформаційними потоками та протидії дезінформації з метою збереження національної та кібер-безпеки. У дослідженні неодноразово доведено, що усі категорії суб'єктів політики можуть як послаблювати ефективність ворожих інформаційних атак, так і підсилити їхню дію. Найважливішою умовою, на наше переконання, ефективного управління інформаційними потоками є консолідоване суспільство, яке поруч із ключовими політичними акторами дбатиме про інформаційну гігієну, поважатиме закон та нестиме свідому відповідальність за розповсюдження певного контенту.

Список використаної літератури

1. Вілбер К. Трамп і епоха постправди. Львів: Видавництво Terra Incognita, 2019. 136 с.
2. Свідерська О., Чорній О. Астротерфінг як інструмент психологічного впливу на масову свідомість. Вісник Харківського національного університету імені В. Н. Каразіна. Серія «Питання політології». 2021. Т. 39. С. 71–79.
3. Кастельс М. Інтернет-ґалактика. Міркування щодо Інтернету, бізнесу і суспільства. Київ: Ваклер. 2007. 304 с.
4. Свідерська О. Інституційно-психологічні детермінанти формування віртуальної маси у епоху постправди. Політичне життя, 2020. № 1. С. 68–74.
5. Свідерська О. І. Цифрові наративи формування політичних цінностей в інформаційному суспільстві // Дні науки філософського факультету 2020 : тези щорічної всеукраїнської наукової конференції (Львів, 18 травня 2020 р.). 2020. С. 181–184.
6. Свідерська О., Угрин Л. Інформаційне суспільство: сучасні трансформації: колективна монографія. Трансформація практик політичної активності в інформаційному

суспільстві: теоретико-методологічний аналіз. Вінниця: ФОП Корзун Д.Ю., 2020. 401 с.
7. Ягодзінський С. М. Глобальні інформаційні мережі у соціокультурній перспективі: монографія. Київ: Аграр Медіа Груп. 2015. 275 с.
8. Al-Fedaghi S. Conceptualization of various and conflicting notions of information. Informing Science:the International Journal of an Emerging Transdiscipline №17, 2014. Pp. 295–308.
9. Wirtz J. Cyber War and Strategic Culture: The Russian Integration of Cyber Power into Grand Strategy: NATO Cooperative Cyber Defence Centre of Excellence (the Centre). 2015. Tallinn. 37 p.
10. Lelonek A. Wojna informacyjna, operacje informacyjne i psychologiczne: pojęcia, metody i zastosowanie. Centrum Analiz Propagandy i Dezinformacji. 2017. С. 68–91.
11. Свідерська О. І. Цифрова пропаганда та ризики інформаційної безпеки у контексті російсько-української війни. Політикус. 2022. Вип. 2. С. 60–65.
12. Smith. D. How Russia Harnesses Cyberwarfare. Defense Dossier, Issue 4, August 2012, pp. 7–8.
13. Ruiz M. Venemaa doktriini muutumine. Nr 168. 2017 URL: http://surl.li/nwlac
14. Governments' content removal requests to Google URL: http://surl.li/nvzfu
15. Біденко А., Золотухін Д., Тарабукін О. Біла книга протидії дезінформації. Київ: ГО «Інститут інформаційної безпеки». 2022. 62 с.

INSTITUTIONAL MANAGEMENT OF INFORMATION FLOWS AS A COUNTERMEASURE TO RUSSIAN CYBER WARFARE

Olha Sviderska
Lviv Polytechnic National University,
Institute of Jurisprudence, Psychology and Innovative Education,
Department of Theoretical and Practical Psychology
Stepana Bandery str., 12, 79000, Lviv, Ukraine

The article updates an issue that is directly related to national security and the policy of countering disinformation. It is about the ability to regulate information messages of key political subjects without going beyond the democratic principles of society. It is also important to limit the negative informational influence of the aggressor state of the RF. The key directions in which the RF works against Ukraine are highlighted: demoralization of the Ukrainian population and the Armed Forces, destabilization of Ukrainian society, cyber-attacks on the country's critical infrastructure, discrediting of Ukraine and the political will of key actors on the international arena, the culture of "cancelling" – attempts to erase the digital traces of war crimes in Ukraine.

Emphasis is placed on the importance of information flows for the modern socio-political reality through the understanding of information acquiring the status of the main resource and managerial lever of influence on communications and the transformation of political institutions, practices and forms of political activity. It has been defined: information war is a purposeful criminal activity, the purpose of which is disinformation, demoralization, building "silent obedience of the population", which is implemented by the aggressor state with the help of hacker attacks, hacking of the systems of internal state support for vital activities and defense capabilities of the country, discrediting the political leadership and armed forces, carrying out strategic, crisis and combat informational and psychological special operations on the territory of the state, which has become the object of informational or hybrid aggression.

It has been proven that all categories of political subjects can both weaken the effectiveness of hostile information attacks and strengthen their effect. The most important condition for the effective management of information flows is a consolidated society, which, together with key political actors, will take care of information hygiene, respect the law and bear conscious responsibility for the distribution of certain content.

Key words: information war, information society, disinformation, cyber-crimes, astroturfing.