

УДК 327.88(470+571):323.266:[070+004(477)]

## Методологічні засади інформаційного менеджменту в умовах окупаційно-гібридної війни Росії проти України

Ярослав КАЛАКУРА

д-р іст. н., проф.

Київський національний  
університет імені Тараса  
Шевченка

вул. Володимирська, 60,  
Київ, Україна, 01033

kalajar@ukr.net

ukrainainc@gmail.com

ORCID ID 0000-0001-9007-4991

© Калакура Я., 2021

*З'ясується сутність, принципи, функції та особливості менеджменту інформаційної діяльності в умовах інформатизації і глобалізації сучасного світу, ескаляції окупаційно-гібридної війни Росії проти України як геополітичного реваншу, аналізуються її цілі, форми та методи щодо протидії дезінформації українського суспільства. На основі теорії інформаційного менеджменту, нормативно-правових документів, з урахуванням праць В. Бебика, В. Горбуліна, О. Матвієнко, Д. Дубова, О. Золотаря, І. Кресіної, В. Лизанчука, Є. Магди, Я. Малик, Є. Мануйлова, Ю. Палеха, М. Тимошика та ін. розглянуто методологічний інструментарій вироблення та реалізації єдиної і дійової державної політики в рамках національного та світового інформаційного простору, основоположні принципи, методи та засоби управління інформаційним процесом на загальнонаціональному, регіональному та місцевому рівнях з метою якісного, своєчасного, достовірного і ефективного інформування населення України, включаючи тимчасово окуповані території, а також зарубіжний світ.*

*Звернуто увагу на менеджмент інформаційної безпеки, зокрема «кібербезпеки» — захисту комп'ютерних систем від вірусів і хакерських атак, на забезпечення захищеності систем продукування, обробки і зберігання інформації, її конфіденційності. Значне місце відведено висвітленню діяльності новоствореного Центру протидії дезінформації в умовах активної фази російської окупаційно-гібридної війни, політики «керованого хаосу» в Україні з метою розмивання української ідентичності, почиття нації та народу, консервації стереотипів «молодшого брата», меншовартості та вторинності українців, домінування російської мови, культури та традицій. Обґрунтовано необхідність підвищення ролі традиційних та інноваційних інформаційних технологій, зокрема комп'ютерних і телекомунікаційних на тлі цифровізації країни, удосконалення способів перевірки правдивості інформації, боротьби з інформаційними фейками, кібернетичним тероризмом у державних і комунальних засобах масової інформації, у соціальних мережах та Інтернет.*

*Сформульовано низку пропозицій щодо подальших наукових досліджень у сфері інформаційного менеджменту, підвищення його значення в захисті національного інформаційного простору, розвінчування інформаційно-психологічних маніпуляцій російської пропаганди та її агентури в Україні.*

**Ключові слова:** інформаційний менеджмент, методологія, функції, принципи, методи, російська окупаційно-гібридна агресія, окуповані території, інформаційна війна, свідомість, дезінформація, маніпуляція.

## METHODOLOGICAL PRINCIPLES OF INFORMATION MANAGEMENT IN THE CONDITIONS OF THE OCCUPATION-HYBRID WAR OF RUSSIA AGAINST UKRAINE

**Yaroslav Kalakura**

Doctor of Historical Sciences, Professor  
Taras Shevchenko National University of Kyiv  
60 Volodymyrska St., Kyiv, Ukraine, 01033  
kalajar@ukr.net, ukrainainc@gmail.com  
ORCID ID 0000-0001-9007-4991

*Clarified the essence, principles, functions and features of information activity management in the conditions of informatization and globalization of the modern world, escalation of the occupation-hybrid war of Russia against Ukraine as an act of geopolitical revenge, analyzes its objectives, forms, and methods to counter misinformation Ukrainian society. Based on the theory of information management, legal documents, taking into account the works of V. Bebyk, V. Gorbulin, O. Matvienko, D. Dubov, O. Zolotar, I. Kresina, V. Lizanchuk, E. Magda, Ya. Malyk, E. Manuylov, Yu. Paleh, M. Tymoshyk, etc., considered methodological tools for developing and implementing a unified and effective public policy within the national and world information space, basic principles, methods, and means of managing the information process at the national level, regional and local levels to provide quality, timely, reliable and effective information to the population of Ukraine, including the temporarily occupied territories, as well as the foreign world.*

*Attention is drawn to information security management, in particular "cybersecurity" — protection of computer systems from viruses and hacker attacks, to ensure the security of production systems, processing and storage of information, its confidentiality. A significant place is given to the coverage of the newly created Center for Countering Disinformation in the active phase of the Russian occupation-hybrid war, the policy of "managed chaos" in Ukraine in order to erode Ukrainian identity, feelings of the nation and the people, preservation of stereotypes of the "younger brother", inferiority and secondaries of Ukrainians, dominance of the Russian language, culture and traditions. Grounded the need to increase the role of traditional and innovative information technologies, including computer and telecommunications against the background of digitalization of the country, improving ways to verify the veracity of information, combating information fakes, cyber terrorism in state and municipal media, social networks and the Internet.*

*Formulated a number of proposals for further research in the field of information management, increasing its importance in the protection of the national information space, debunking the information and psychological manipulations of Russian propaganda and its agents in Ukraine.*

**Keywords:** information management, methodology, functions, principles, methods, Russian occupation-hybrid aggression, occupied territories, information warfare, consciousness, misinformation, manipulation.

*Постановка проблеми та її актуальність*

Восьмий рік окупаційно-гібридної агресії путінської Росії проти України переконливо засвідчив, що однією з пріоритетних її складових є інформаційна війна, спрямована на дезінтеграцію і знищення української державності шляхом дезінформації суспільства і світової громадськості, маніпуляції свідомістю населення та нав'язування парадигм «общей історії», «одного народу», «русского міра». До інформаційно-світоглядної та психологічної війни долучилися фінансовані Росією антиукраїнські сили всередині країни, формуючи п'яту колону зі своїми політичними об'єднаннями та засобами масової інформації, пресою, радіо- та телевізійними каналами, агентурою в онлайн-мережах, створюючи внутрішню загрозу безпеці держави. За словами президента України, особи, які вели бізнес на тимчасово окупованих територіях і фінансували канали Медведчука, сформували «дезоінформаційні батальйони, які атакували українців залпами брехні та маніпуляцій» з метою розколоти суспільство, деморалізувати і підірвати його з середини (Зеленський, 2021).

За таких умов на пріоритетне місце національної безпеки держави висувається протидія гібридній війні та інформаційної інтервенції Росії адекватними засобами і методами інформаційно-розвінчувальної контрпропаганди, підвищення ефективності усієї інформаційної діяльності, удосконалення форм координації та управління нею. У цьому зв'язку **особливої ваги і актуальності набуває інформаційний менеджмент як наука про управління інформаційними системами**, визначення стратегічних, оперативних і тактичних цілей, форм, методів і засобів інформаційної політики, її вироблення та реалізації, мобілізації кадрових, технологічних, фінансових та інших ресурсів для досягнення поставленої мети.

*Актуальність* означеної проблеми зумовлюється низкою наступних чинників.

**По-перше**, на зміну індустріальному суспільству приходять цифрове або інформаційне як принципово нова цивілізаційна модель, в якому володіння інформацією (а не лише матеріальними благами) є рушійною силою соціокультурних перетворень, а пріоритетом його розвитку виступає інтелектуальна творчість людини. Інформаційне суспільство спричинило появу нових форм воєн — гібридних та інформаційних, як способів інформаційного протистояння між різними суб'єктами (державами, народами, неурядовими, економічними та іншими структурами). Вони передбачають проведення комплексу заходів і дій для нанесення шкоди інформаційній сфері конкуруючої сторони і захисту власної інформаційної безпеки. Завдання інформаційної війни: створення атмосфери невпевненості, розгубленості, бездуховності, негативного ставлення до власних цінностей, що

в свою чергу диктує необхідність наукового осмислення цих процесів та їх упередження.

**По-друге**, російська окупаційно-гібридна війна продиктувала нагальну потребу створення єдиного інформаційного поля для адекватного протистояння і рішучої відсічі ворожій пропаганді, що в сучасних умовах не може бути успішно зреалізоване без опори на наукові студії та прогнози.

**По-третьє**, розвиток інформаційного суспільства передбачає цілеспрямовану і скоординовану діяльність усіх органів державної влади та місцевого самоврядування, громадянських інститутів, засобів масової комунікації, а також установ культури, освіти і науки, спрямовану на формування та реалізацію державної інформаційної політики, забезпечення інформаційної безпеки та інформаційного супроводу деокупації Криму, частини Донецької і Луганської областей, враховуючи, що тамтешні окупаційні та терористичні організації діють за сценаріями, інструкціями, фінансовою і технічною підтримкою Кремля.

**По-четверте**, не дивлячись на помітний пласт наукових студій із інформаційного менеджменту, його модернізації в умовах глобалізації та окупаційно-гібридної війни, питання методології управлінської діяльності в інформаційній сфері залишаються недостатньо дослідженими. З цією проблемою переплітається й необхідність оновлення освітніх програм підготовки нового покоління фахівців з інформаційної діяльності, включаючи й журналістів.

Не менш актуальною видається й *мета* пропонованого дискурсу, яка полягає в тому, щоб на основі загальної теорії менеджменту з'ясувати сутність і особливості його інформаційної складової, розкрити її методологічний інструментарій і значення в умовах російської окупаційно-гібридної агресії. Реалізуючи цю мету, автор опирався передусім на законодавчо-нормативну базу інформаційної діяльності та управління нею (Верховна Рада України, 2011; Верховна Рада України. (1992); Верховна Рада України, 1994; Верховна Рада України, 1998; Верховна Рада України, 2017), на доктрину інформаційної безпеки України (Президент України, 2017), на теоретико-методологічні засади менеджменту як наукової основи керування інформаційними процесами, на опубліковані наукові праці і навчально-методичну літературу з інформаційного менеджменту, на вже набутий досвід інформаційної діяльності в умовах війни.

#### *Стан розробки проблеми*

Оцінюючи стан дослідження теми, вважаємо доцільним наявну її історіографію класифікувати умовно за трьома напрямками:

а) наукові праці із загальної теорії і практики менеджменту (Кулицький, 2002; Сухарський, 2002; Мельник та ін., 2006; Гордієнко 2016; Калакура, 2018);

б) студії з теорії інформаційної діяльності та практики управління нею (Матвієнко, 2004; Бебик, 2005; Жежнич, 2010; Кресіна, 2019; Лизанчук, 2017; Тимошик, 2018; Палеха та ін., 2019);

в) дослідження, присвячені сутності окупаційно-гібридної війни та місця в ній інформаційного сегменту (Магда, 2015; Тымчук и др., 2016; Малик, 2015; Полянський, 2015; Дубов, 2016; Петрик, 2009; Штогрін, 2014; Я. Малик & І. Малик, 2016; Горбулін, 2017).

Особливо цінними є студії В. Бебика (2005), В. Горбуліна (2015; 2017), О. Матвієнко (2004), Д. Дубова (2016), О. Золотаря (2017), І. Кресіної (2019), В. Лизанчука (2017), Є. Магди (2015), Я. Малик (2015; 2016), Є. Мануйлова, Ю. Палехи (2019), М. Тимошика (2018) та ін., у яких органічно поєднані ключові питання теорії інформаційної діяльності з особливостями інформаційного менеджменту в умовах окупаційно-гібридної війни.

Появу терміна «інформаційний менеджмент» (Informatsiynnyu menedzhment) пов'язують з іменем видатного британського вченого Т. Бернерса-Лі, засновника всесвітнього Інтернету на межі 1970–1980-х рр. Під цим терміном, який в Україні почав поширюватись у середині 1990-х рр., розуміють широкий спектр діяльності, пов'язаної з управління інформаційними системами, ресурсами та інформаційним процесом у різних сферах суспільного життя. Майже три десятиріч триває формування національного комунікаційного простору, вироблення законодавчого поля державної інформаційної політики, її реалізації, а водночас й опрацювання основ інформаційного менеджменту, адже в умовах СРСР Україна була частиною советської інформаційної системи. Умовно можна виокремити щонайменше п'ять етапів цього процесу: перший (1991–1995) — формування засад інформаційного законодавства, розроблення доктрини інформаційної безпеки, визначення принципів, завдань, основних напрямів державної інформаційної політики, інституціоналізація її органів; другий (1996–2004) — конституційне унормування державної інформаційної політики і програми, становлення організаційної системи управління інформаційним полем, уніфікація нормативно-правової бази та інформаційних відносин; третій (2005–2013) — поступове згортання цінностей Євромайдану, зростання впливу російської пропаганди під виглядом лібералізації інформаційної сфери, надання публічності політичній діяльності через ЗМІ; четвертий (з 2014–2019) — оновлення змісту інформаційної системи під впливом Революції гідності, її модернізація з урахуванням умов окупаційно-гібридної війни РФ проти України, наближення до європейських стандартів. З 2020 р. почався сучасний етап, пов'язаний з поглибленням взаємодії інформаційної сфери із стратегічними завданнями національної безпеки, активізацією контрпропаганди та діяльністю новостворених Центрів

протидії дезінформації на тлі нової фази російської окупаційно-гібридної війни. На сьогодні вимальовується два таких центри боротьби з дезінформацією: Рада національної оборони і Міністерство культури та інформаційної політики.

Більшість дослідників, трактуючи інформаційний менеджмент як управління інформаційним впливом на суспільство, виокремлюють три його рівні в Україні: вищий (загальнодержавний), середній (у межах областей, міст, районів і територіальних громад); нижчий або базовий (місцеві громади, підприємства, установи, організації). Що ж до структури інформації, то вона включає такі сегменти як міжнародна, внутрішньо політична, соціокультурна, економічна, ідеологічна, релігійна на інші.

Управління інформаційною сферою в Україні покладено на два регуляторних органи: Національну раду з питань телебачення і радіомовлення та Національну комісію з питань зв'язку та інформації. Нині у сфері інформації функціонує п'ять органів виконавчої влади: Міністерство культури та інформаційної політики, Міністерство цифрової трансформації, Державний комітет з телебачення і радіо, Національне агентство з питань науки, інновацій та інформатизації, Державна служба спеціального зв'язку. Крім того, у складі Верховної Ради цією ділянкою опікуються два комітети: свободи слова та інформації і інформаційних технологій. З погляду менеджменту, така багатоаспектна та багатоступенева структура державних органів, пов'язаних з управлінням інформаційною діяльністю на загальнодержавному та місцевому рівнях, потребує більшої координації і взаємодії, особливо з урахуванням умов війни. Йдеться про необхідність більш системного підходу до стратегічного та оперативного планування інформаційної діяльності, своєчасне ухвалення управлінських рішень з питань задоволення інформаційних потреб держави, суспільства і людини, а також забезпечення доступності інформації, її правдивості, об'єктивності, своєчасності та захисту державної таємниці.

Методологічний інструментарій інформаційного менеджменту включає систему принципів (правил), методів і управлінських процедур, пов'язаних з обґрунтуванням цілей, плануванням і прогнозуванням очікуваних результатів, виділення необхідних ресурсів, стимулювання організації інформаційної діяльності, спрямованої на досягнення поставленої мети. При цьому корегування цілей інформаційного процесу, прийняття рішень щодо підвищення ефективності роботи системи інформаційно-комунікаційних засобів, оптимізації джерел отримання інформації, регулювання інформаційних потоків мають носити комплексний та безперервний характер і потребують постійної уваги на різних рівнях менеджменту (Калініна,

2009). Що ж стосується безпосереднього управління інформаційними ресурсами, то воно передбачає: оцінку конкретної ситуації, формулювання мети і постановку завдань; забезпечення інформаційного супроводу-виконання завдань; ухвалювання оперативних рішень відповідно до кожного етапу інформаційної діяльності; аналіз підсумків проведеної роботи.

Важливе місце в інформаційному менеджменті посідає безпека, тобто захищеність систем обробки і зберігання інформації, її конфіденційність. У новітній практиці інформаційної діяльності і відповідно у лексиці появились такі поняття як «інформаційний тероризм» — використання комп'ютерних та телекомунікаційних технологій, насамперед Інтернету в терористичних цілях, «кібербезпека», тобто захист від вірусів, які спроможні вивести з ладу комп'ютерні системи, знищити інформацію, від хакерських атак, від перехоплення інформації, від підробки веб-сайтів і даних тощо (Ліпкан, 2003). Принагідно нагадаємо, що в Україні діє комплексна система захисту інформації (КСЗІ), функціонує Державна служба спеціального зв'язку та захисту інформації, створений Національний центр кібербезпеки.

Одна з особливостей сучасного етапу інформаційного менеджменту полягає в тому, що відбувається антропологізація та інтелектуалізація усіх його систем і механізмів шляхом запровадження адаптивних архетипів, тобто своєрідних образів у свідомість і психіку людини. Саме людина залишається головним об'єктом морально-психологічного ураження, її світогляд, а також нервова система та психіка. З цієї метою використовується подвійна психобіологічна суть інформації, яка може бути «комфортна» з погляду психобіологічного сприйняття, завдаючи водночас шкоду на психосоціальному рівні або, навпаки, «цікава» і «захоплююча», але спроможна призвести до неусвідомлюваних психобіологічних змін, моральних зсувів, стимулюючи девіантну поведінку особи та руйнуючи позитивні соціальні тенденції в суспільстві. Мова йде фактично про наміри програмування суспільної свідомості і психіки з тим, щоб змінити особистість, індивідуальну або групову свідомість, її ідентичність, добитися очікуваної еволюції поведінки індивіда (Шевчук, 2014). Російська сторона, реалізуючи подібні наміри, якраз і посилює негативні інформаційно-психологічні та маніпулятивні впливи, спрямовані проти інтересів України на всіх рівнях — особи, суспільства і держави загалом.

З огляду означеної теми особливої уваги заслуговують погляди тих дослідників, які безпосередньо торкаються менеджменту забезпечення інформаційної діяльності та інформаційної безпеки на тлі окупаційно-гібридної війни Росії як інструменту нищення державності України. За визначенням Є. Магди (2015), в умовах гібридної

війни бойові дії певною мірою стають другорядними, а на перший план виходять інформаційні операції та інші важелі впливу (с. 3). Автор, як інші дослідники (Я. Малик & І. Малик, 2016; Курбан, 2017) наголошують, що підготовку до анексії АР Крим і вторгнення на Донбас Росія розпочала задовго до 2014 р. як частини спланованої військово-політичної спецоперації «Русская весна». Вона передбачала широкий спектр розвідувальної, агентурної та пропагандистської діяльності. Не випадково, що вже в перші дні агресії так звані «ополченці» та «зелені чоловічки» за вказівкою кремлівських наставників відключили українські радіо- та телеканали, заборонили видання газет на окупованих територіях, замінивши їх російськими.

Найбільш об'єктивну, цілком справедливую і прогностичну оцінку тогочасних дій Москви з приходом до влади Путіна дав В. Горбулін, назвавши їх довгонапрацьовуваним «геополітичним реваншем», проявом ностальгії за розпадом СРСР. Стратегія російської сторони стосовно України полягала в тому, щоб зберегти її в зоні своїх інтересів та впливу, ослабити центральну владу, посягти певне «безвладдя» на місцях, а на цьому тлі актуалізувати суперечності Центром і регіонами, провокувати незадовільний психологічний і матеріально-технічний стан українських безпекових структур і підігрівати антагонізм між різними силовими структурами. При цьому пріоритетна роль відводилась інформаційно-пропагандистській роботі (Горбулін, 2015). У зовнішньополітичній сфері головний акцент робився на перешкоджання євроінтеграції України, згортання її співпраці з НАТО, поширення упередженої, недостовірної та викривленої інформації про Революцію гідності з метою назування упередженого ставлення світової громадськості до українських патріотичних сил та їх лідерів (Петрик & Канарський, 2015).

Українська сторона не тільки не вживала асиметричних контрзаходів, але навпаки, протягом тривалого часу інформаційне поле України продовжувало залишатися залежним від російського або й підконтрольного. Пропагандистська машина РФ успадкувала інформаційний потенціал СРСР та його «інформаційну політику» в світі. В її інтересах працюють Інтернет-портал «Sputnik» як інтерактивний майданчик з можливістю підключення Інтернет-радіостанції «Sputnik», а також Інтернет-доступ до телеканалів RT, де мовлення здійснюється 45 мовами і використовується для пропагандистських цілей. До того ж упродовж 2010–2013 рр. за мовчазної згоди тодішнього президента В. Януковича та підтримки голови СБУ В. Хорошковського в Україні була допущена діяльність агентурних мереж ФСБ РФ та ГРУ ГШ ВС РФ («Діяльність СБУ», 2020).

Важливу роль в інформаційній війні противник відводить друкованої продукції. Наприклад, в Києві видавалася і безкоштовно по-



ширювалася газета «Вести», в окупованому Луганську було засновано новий ілюстрований дитячий пізнавально-розважальний журнал «Вежливые человечки», розрахований на дошкільнят та дітей молодшого шкільного віку. Головними героями розповідей тут виступають «героїчні дітлахи» в образах так званих «бійців Малоросії», а в негативних героях — керівники Української держави, командири та воїни ЗС України, а також добровольці.

Після окупації Криму і частини Донбасу, провалу операції щодо створення так званої «Харківської народної республіки», починаючи з весни 2015 р. стала активно поширюватись ідея «Югоросії» на півдні України. Зокрема, в межах Одеської області вона передбачала реалізацію проєкту міфічних «Народного Совета Бессарабии» та створення «Бессарабской народной республики». Інформаційний супровід цього проєкту забезпечували вже відомі на той час мережеві групи під брендами «Антимайдан», «Киберберкут», «Новороссия» й відповідні інтернет-портали. Можна згадати поширення таких медіавірусів, як «бандерівці», «фашисти в Києві», «звірства каральних батальйонів», «розіп'ятий хлопчик», «два раба», «іноземні найманці в ВСУ» та ін., що супроводжувалися відповідними тропами-хештегами. Залучивши додаткові матеріально-фінансові, технічні та людські ресурси, російська сторона забезпечила досить потужний інформаційний супровід спільних із найманцями воєнних дій шляхом поширення дезінформації; залякування місцевих жителів та здійснення психологічного тиску; нав'язування українській стороні своїх правил ведення переговорів та дій щодо обміну військовополоненими і заручниками.

Російська пропаганда постійно намагається ввести в оману світове співтовариство щодо реальних подій, ізолювати Україну інформаційно, створити викривлене бачення її позиції щодо виконання Мінських угод тощо. Вона спрямована на політику «керованого хаосу» в Україні, на розмивання української ідентичності, почуття нації та народу, на формування стереотипу меншовартості та вторинності українців, а відтак на домінування російської мови, культури та традицій. З цією метою широко використовується мережа Інтернет, програми «Skype», «Viber», російські сайти «Российский диалог», «Правда.Ру», створення фейкових сторінок у соціально-спрямованих ресурсах «Вконтакте», «Одноклассники», «Facebook» для розпалювання сепаратистських настроїв серед населення різних регіонів України, дестабілізації суспільно-політичної ситуації в Україні, формування протестних настроїв і сприяння діяльності терористичних організацій «ДНР», «ЛНР» (Семен, 2017).

При цьому варто зазначити, що в багатьох випадках із боку владних структур України не було дій на випередження, не давалась своєчасна і належна відповідь інформаційним атакам РФ. Це й спону-

кало громадськість взяти на себе частину інформаційних функцій держави. Так появилися волонтерські проекти («Миротворець», «Інформаційний спротив», «InformNapalm»), активізувалася діяльність блогерів. Суспільство стало свідком того, що поряд з професійною (традиційною) журналістикою сформувалася «народна», або «блогерна», діяльність якої, на жаль, досі не отримала правового захисту.

Виходячи з результатів та наслідків семирічної російської окупаційно-гібридної війни та інформаційної агресії на Сході України, критично осмислюючи набутий досвід, можна зазначити, що українські владні структури та інформаційні служби, хоч із запізненням, але зуміли зробити певні висновки з прорахунків і невдач на початку подій, зосередитись на ключових питаннях національної інформаційної безпеки. Було визначено пріоритетні напрями подальшого удосконалення державної політики у сфері національного інформаційного простору, управління ним та інформаційною безпекою. Йдеться, передусім, про ширше використання інформаційного потенціалу телекомунікацій та соціальних онлайнмереж, стимулювання участі в них патріотично налаштованих громадян, створення та підтримку незалежних аналітичних центрів та громадських рухів. Оскільки в умовах війни **єдиний інформаційний простір** держави порушений, інформаційна політика повинна враховувати специфіку як окупованих, так і вже звільнених територій. Можна погодитись з думкою деяких експертів про те, що для їх населення має проводитись дещо інша версія державної інформаційної політики, спрямована на деміфологізацію спотворюваного російською пропагандою та її агентурою на місцях образу України, враховувати специфіку різних цільових аудиторій.

#### *Висновки*

Підсумовуючи, можна зробити низку **висновків та сформулювати декілька рекомендацій**.

**По-перше**, в умовах окупаційно-гібридної війни РФ проти України на пріоритетне місце висунулись проблеми дійового менеджменту інформаційної діяльності, оскільки, за визначенням американського дослідника Г. Маклюєна, гібридну війну можна віднести до істинно тотальних, тобто воєн за допомогою інформації, яка також потребує стратегічного і оперативного управління.

**По-друге**, сучасний етап інформаційного менеджменту супроводжується оновленням як людських, технологічних та фінансових ресурсів, так і змісту інформаційної діяльності, її модернізацією з урахуванням нової фази окупаційно-гібридної війни РФ проти України та наближенням до європейських стандартів. На пріоритетне місце висунулись завдання поглиблення координації та взаємодії інформаційної сфери із стратегічними завданнями національної безпеки,

активізацією контрпропаганди та діяльністю новоствореного Центру протидії і боротьби з дезінформацією.

**По-третє**, потужна антиукраїнська пропагандистсько-підривна кампанія Росії висвітлила суттєві недоліки і прорахунки інформаційного менеджменту України, слабку скоординованість і відсутність належної взаємодії органів державної влади, громадянського суспільства, наукового, експертного середовищ та журналістів у протидії інформаційній агресії.

Уроки інформаційної війни засвідчили необхідність **подальшого удосконалення законодавства** країни з питань управління інформаційною системою і політикою, приведення його не лише до європейських стандартів, але й максимально адаптувати до умов затяжної окупаційно-гібридної війни. Як справедливо зазначають В. Тарасюк (2018) та І. Розкладай (2018), практика останніх років диктує необхідність переформатувати діючу модель функціонування медіапростору з тим, щоб вона повніше відповідала особливостям функціонування суспільства у стані війни.

Державна інформаційна діяльність покликана чіткіше проєктуватися на тимчасово окуповані території з метою морально-психологічної підготовки задурманеного ворожою пропагандою населення до його повернення в Україну. Особливої уваги заслуговує удосконалення формату і змісту інформаційного позиціонування України на міжнародній арені, надання їй більшої переконливості та ефективності, підвищення професіоналізму її організаторів (Тарасюк, 2018; Розкладай, 2018).

І найголовніше, державна інформаційна політика, вся її система і новітні комунікаційні технології мають відігравати роль «диригента» у створенні позитивного іміджу України на міжнародній арені, утвердженні морально-ціннісних орієнтацій суспільства, його консолідації, вихованні патріотизму, формуванні національної та цивілізаційної ідентичності українців.

## СПИСОК БІБЛІОГРАФІЧНИХ ПОСИЛАНЬ

- Бебик, В. М. (2005). *Інформаційно-комунікаційний менеджмент у глобальному суспільстві: психологія, технології, техніка паблік рилейшнз* [Монографія]. Міжрегіональна академія управління персоналом.
- Верховна Рада України. (1992). *Про інформацію*. Закон України (від 02.10.1992, № 2657–XII). <https://zakon.rada.gov.ua/laws/card/2657-12>
- Верховна Рада України. (1994). *Про захист інформації в інформаційно-телекомунікаційних системах*. Закон України (від 05.07.1994, № 80/94-ВР). <https://zakon.rada.gov.ua/laws/card/80/94-%D0%B2%D1%80>
- Верховна Рада України. (1998). *Про Національну програму інформатизації*. Закон України (від 4.02.1998, № 74/98-ВР). <https://zakon.rada.gov.ua/laws/card/74/98-%D0%B2%D1%80>

- Верховна Рада України. (2011). *Про доступ до публічної інформації*. Закон України (від 13.01.2011, № 2939–VI). <https://zakon.rada.gov.ua/laws/card/2939-17>
- Верховна Рада України. (2017). *Про основні засади забезпечення кібербезпеки України*. Закон України (від 05.10.2017, № 2163–VIII). <https://zakon.rada.gov.ua/laws/card/2163-19>
- Горбулін, В. (2015, 23 січня). «Гібридна війна» як ключовий інструмент російської геостратегії реваншу. *Дзеркало тижня. Україна, 2*.
- Горбулін, В. (Ред.). (2017). *Світова гібридна війна: український фронт* [Монографія]. Національний інститут стратегічних досліджень.
- Гордієнко, Л. Ю. (2016). *Адміністративний менеджмент*. Харківський національний економічний університет імені С. Кузнеця.
- Діяльність СБУ в період президентства Віктора Януковича. (2020, 5 серпня). В *Вікіпедія*. <https://uk.wikipedia.org/w/index.php?curid=1744503>
- Дубов, Д. В. (2016). Державна інформаційна політика України в умовах гібридного миру та війни. *Стратегічні пріоритети, 3*(40), 86–93.
- Жежнич, П. І. (2010). *Технології інформаційного менеджменту*. Видавництво Львівської політехніки.
- Зеленський, В. (2021, 13 квітня). *Зеленський: Ми заблокували дезінформаційні батальйони, які атакували українців залпами брехні*. Всеукраїнские вести. <https://vv.org.ua/poslednie-novosti/zelenskij-mi-zablokuvali-dezinformacijni-bataljoni-jaki-atakuvali-ukrainciv-zalpami-brehni/>
- Калакура, Я. С. (2018). *Менеджмент в архівній справі*. Видавничо-поліграфічний центр «Київський університет».
- Калініна, Л. М. (2009). Генезис інформаційного менеджменту як галузі наукового знання. *Стратегічні пріоритети, 4*(13), 71–76.
- Кресіна, І. О. (2019). Державна інформаційна політика: аксіологічний та правовий виміри. *Міжнародні відносини. Серія: Політичні науки, 21*. [http://journals.iir.kiev.ua/index.php/pol\\_n/article/view/3851/3511](http://journals.iir.kiev.ua/index.php/pol_n/article/view/3851/3511)
- Кулицький, С. П. (2002). *Основи організації діяльності у сфері управління*. Міжрегіональна академія управління персоналом.
- Курбан, О. В. (2017). Інформаційне супроводження російської гібридної агресії в Донбасі (2014–2016). *Бібліотекознавство. Документознавство. Інформологія, 2*, 66–73.
- Лизанчук, В. (2017). *Інформаційна безпека України*. Львівський національний університет імені Івана Франка.
- Ліпкан, В. А. (2003). *Національна безпека України: нормативно-правові аспекти забезпечення*. Текст.
- Магда, Є. (2015). *Гібридна війна: вижити і перемогти*. Віват.
- Малик, Я. (2015). Інформаційна війна і Україна. *Демократичне врядування, 15*. [http://www.lvivacademy.com/vidavnitstvo\\_1/visnyk15/fail/Malyk.pdf](http://www.lvivacademy.com/vidavnitstvo_1/visnyk15/fail/Malyk.pdf)
- Малик, Я., & Малик, І. (2016, 24 березня). Інформаційна безпека суспільства та інформаційні війни: співвідношення понять. В *Актуальні проблеми міжнародних відносин та зовнішньої політики*, матеріали III Регіональної науково-теоретичної конференції (с. 21–24). Національний університет «Львівська політехніка».

- Матвієнко, О. В. (2004). *Основи інформаційного менеджменту*. Центр навчальної літератури.
- Мельник, А. Ф., Васіна, А. Ю., & Кривокульська, Н. М. (2006). *Менеджмент державних установ і організацій*. Професіонал.
- Палеха, Ю. І., Палеха, О. Ю., & Комісаренко, О. С. (2019). *Інформаційна культура*. Ліра-К.
- Петрик, В. (2009). Сутність інформаційної безпеки держави, суспільства та особи. *Юридичний журнал*, 5(83), 122–132.
- Петрик, В., & Канарський, Ю. (2015). Методи гібридної війни Росії проти України. Напрями протидії. *Information Technology and Security*, 3(1), 30–37.
- Полянський, П. (2015, 23 квітня). *Освіта як об'єкт інформаційної війни Росії проти України і як ресурс протидії такій війні*. MAIDAN <https://maidan.org.ua/2015/03/osvita-yak-objekt-informatsijnoi-vijny-rosiji-protu-ukrajiny-i-yak-resurs-protydiji-takij-vijni/>
- Президент України. (2017). *Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України»* (від 25.02.2017, № 47/2017). <https://zakon.rada.gov.ua/laws/card/47/2017>
- Розкладай, І. (2018, 15 січня). *Як Україна протидіє інформаційній агресії Росії* (Ч. 2). Центр демократії та верховенства права. <https://cedem.org.ua/articles/yak-ukrayina-protydiye-informatsijnij-agresiyi-rosiyi-chastyna-2/>
- Семен, Н. Ф. (2017). Висвітлення інформації про події на Сході України російськими Інтернет-ресурсами (на прикладі матеріалів російських сайтів «Російський діалог» і «Правда.ру» за 2016 рік). *Теле- та радіожурналістика*, 16, 221–226.
- Сухарський, В. С. (2002). *Менеджмент: теорія, методологія, практика* [Монографія]. Астон.
- Тарасюк, В. М. (2018). Інформаційний простір в Україні: виклики і загрози. *Правова держава*, 29, 375–381.
- Тимошик, М. (2018, 18–24 січня). Українська книжка як виклик Москві, або Історія про те, як імперська влада через заборону книг знесилювала дух російських українців. *Слово Просвіти*, с. 2–3.
- Тымчук, Д., Карин, Ю., Машовец, К., & Гусаров, В. (2016). *Вторжение в Украину: хроника российской агрессии*. Брайт Стар Паблішинг.
- Шевчук, П. (2014). Інформаційно-психологічна війна Росії проти України: як їй протидіяти. *Демократичне врядування*, 13. [http://lvivacademy.com/vidavnitstvo\\_1/visnik13/fail/Shevchuk.pdf](http://lvivacademy.com/vidavnitstvo_1/visnik13/fail/Shevchuk.pdf)
- Штогрін, І. (2014, 11 березня). *Називай агресію «захистом»: принципи інформаційної війни проти України*. Радіо Свобода <https://www.radiosvoboda.org/a/25293307.html>

## REFERENCES

- Bebyk, V. M. (2005). *Informatsiino-komunikatsiyni menedzhment u hlobalnomu suspilstvi: psykhohiia, tekhnolohii, tekhnika pablik ryleishnz* [Information and Communication Management in Global Society: Psychology, Technology, Technique of Public Relations] [Monograph]. Interregional Academy of Personnel Management [in Ukrainian].

- Diialnist SBU v period prezidentstva Viktora Yanukovycha [Activities of the SBU During the Presidency of Viktor Yanukovich]. (2020, August 5). In *Wikipedia*. <https://uk.wikipedia.org/w/index.php?curid=1744503> [in Ukrainian].
- Dubov, D. V. (2016). Derzhavna informatsiina polityka Ukrainy v umovakh hibrydnoho myru ta viiny [State Information Policy in Ukraine in Terms Hybrid Peace and War]. *Strategic priorities*, 3(40), 86–93 [in Ukrainian].
- Horbulin, V. (2015, January 23). «Hibrydna viina» yak kluchovyi instrument rosiiskoi heostrategii revanshu [«Hybrid War» as a Key Tool of Russia's Geostrategy of Revenge]. *Dzerkalo tyzhnia. Ukraina*, 2 [in Ukrainian].
- Horbulin, V. (Ed.). (2017). *Svitova hibrydna viina: ukrainskyi front* [World Hybrid War: Ukrainian Front] [Monograph]. National Institute for Strategic Studies [in Ukrainian].
- Hordienko, L. Yu. (2016). *Administratyvnyi menedzhment* [Administrative Management]. Simon Kuznets Kharkiv National University of Economics [in Ukrainian].
- Kalakura, Ya. S. (2018). *Menedzhment v arkhivnii spravi* [Management in Archives]. Kyiv University Publishing and Printing Center [in Ukrainian].
- Kalinina, L. M. (2009). Henezys informatsiinoho menedzhmentu yak haluzi naukovoho znannia [Genesis of Information Management as a Branch of Scientific Knowledge]. *Strategic priorities*, 4(13), 71–76 [in Ukrainian].
- Kresina, I. O. (2019). Derzhavna informatsiina polityka: aksiolohichni ta pravovyi vymiry [State Information Policy: Axiological and Legal Dimensions]. *International Relations. Series: Political Science*, 21. [http://journals.iir.kiev.ua/index.php/pol\\_n/article/view/3851/3511](http://journals.iir.kiev.ua/index.php/pol_n/article/view/3851/3511) [in Ukrainian].
- Kulytskyi, S. P. (2002). *Osnovy orhanizatsii diialnosti u sferi upravlinnia* [Fundamentals of Organization of Activities in the Field of Management]. Interregional Academy of Personnel Management [in Ukrainian].
- Kurban, O. V. (2017). Informatsiine suprovodzhennia rosiiskoi hibrydnoi ahresii v Donbasi (2014–2016) [Information Support of the Russian Hybrid Aggression in Donbass (2014–2016)]. *Library science. Record studies. Informology*, 2, 66–73 [in Ukrainian].
- Lipkan, V. A. (2003). *Natsionalna bezpeka Ukrainy: normatyvno-pravovi aspekty zabezpechennia* [National Security of Ukraine: Regulatory and Legal Aspects of Security]. Tekst [in Ukrainian].
- Lyzanchuk, V. (2017). *Informatsiina bezpeka Ukrainy* [Information Security of Ukraine]. Ivan Franko National University of Lviv [in Ukrainian].
- Mahda, Ye. (2015). Hibrydna viina: vyzhyty i peremohty [Hybrid War: Survive and Win]. Vivat [in Ukrainian].
- Malyk, Ya. (2015). Informatsiina viina i Ukraina [Information War and Ukraine]. *Democratic Governance*, 15. [http://www.lvivacademy.com/vidavnitstvo\\_1/visnyk15/fail/Malyk.pdf](http://www.lvivacademy.com/vidavnitstvo_1/visnyk15/fail/Malyk.pdf) [in Ukrainian].
- Malyk, Ya., & Malyk, I. (2016, March 24). Informatsiina bezpeka suspilstva ta informatsiini viiny: spivvidnoshennia poniat [Information Security of Society and Information Wars: the Relationship Between Concepts]. In *Aktualni problemy mizhnarodnykh vidnosyn ta zovnishnoi polityky* [Current Issues of International Relations and Foreign Policy], Proceedings of the III Regional Scientific and Theoretical Conference (pp. 21–24). Lviv Polytechnic National University [in Ukrainian].

- Matviienko, O. V. (2004). *Osnovy informatsiinoho menedzhmentu* [Fundamentals of Information Management]. Tsentri navchalnoi literatury [in Ukrainian].
- Melnyk, A. F., Vasina, A. Yu., & Kryvokulska, N. M. (2006). *Menedzhment derzhavnykh ustanov i orhanizatsii* [Management of Government Agencies and Organizations]. Profesional [in Ukrainian].
- Palekha, Yu. I., Palekha, O. Yu., & Komisarenko, O. S. (2019). *Informatsiina kultura* [Information Culture]. Lira-K [in Ukrainian].
- Petryk, V. (2009). Sutnist informatsiinoi bezpeky derzhavy, suspilstva ta osoby [The Essence of Information Security of the State, Society and the Individual]. *Yurydychnyi zhurnal*, 5(83), 122–132 [in Ukrainian].
- Petryk, V., & Kanarskyi, Yu. (2015). Metody hibrydnoi viiny Rosii proty Ukrainy. Napriamy protydii [Methods Hybrid War of Russia Against Ukraine. Areas Counter]. *Information Technology and Security*, 3(1), 30–37 [in Ukrainian].
- Polianskyi, P. (2015, April 23). *Osvita yak ob'iekt informatsiinoi viiny Rosii proty Ukrainy i yak resurs protydii takii viini* [Education as an Object of Russia's Information War Against Ukraine and as a Resource for Counteracting Such a War]. MAIDAN <https://maidan.org.ua/2015/03/osvita-yak-objekt-informatsiinoji-vijny-rosiiji-proty-ukrajiny-i-yak-resurs-protydiji-takij-vijni/> [in Ukrainian].
- Prezydent Ukrainy. (2017). *Pro rishennia Rady natsionalnoi bezpeky i oborony Ukrainy vid 29 hrudnia 2016 roku «Pro Doktrynu informatsiinoi bezpeky Ukrainy»* [On the Decision of the National Security and Defense Council of Ukraine of December 29, 2016 «On the Doctrine of Information Security of Ukraine»] (February 25, 2017, № 47/2017). <https://zakon.rada.gov.ua/laws/card/47/2017> [in Ukrainian].
- Rozkladai, I. (2018, January 15). *Yak Ukraina protydiie informatsiinii ahresii Rosii* [How Ukraine Counteracts Russia's Information Aggression] (Pt. 2). Tsentri demokratii ta verkhovenstva prava. <https://cedem.org.ua/articles/yak-ukrayina-protydiye-informatsiijnij-agresiyi-rosiyyi-chastyna-2/> [in Ukrainian].
- Semen, N. F. (2017). Vysvitlennia informatsii pro podii na skhodi Ukrainy rosiiskymy Internet-resursamy (na prykladi materialiv rosiiskykh saitiv «Rossiiskii dialog» i «Pravda.ru» za 2016 rik) [Coverage of Information About Events in Eastern Ukraine by Russian Internet Resources (on the Example of Materials from the Russian Sites «Russian Dialogue» and «Pravda.ru» in 2016)]. *TV and Radio Journalism*, 16, 221–226 [in Ukrainian].
- Shevchuk, P. (2014). Informatsiino-psykholohichna viina Rosii proty Ukrainy: yak yii protydiaty [Information and Psychological War of Russia Against Ukraine: How to Counteract it]. *Democratic Governance*, 13. [http://lvivacademy.com/vidavnistvo\\_1/visnik13/fail/Shevchuk.pdf](http://lvivacademy.com/vidavnistvo_1/visnik13/fail/Shevchuk.pdf) [in Ukrainian].
- Shtohrin, I. (2014, March 11). *Nazyvai ahresiiu «zakhystom»: pryntsyypy informatsiinoi viiny proty Ukrainy* [Call Aggression «Protection»: Principles of Information War Against Ukraine]. Radio Svoboda <https://www.radiosvoboda.org/a/25293307.html> [in Ukrainian].
- Sukharskyi, V. S. (2002). *Menedzhment: teoriia, metodolohiia, praktyka* [Management: Theory, Methodology, Practice] [Monograph]. Aston [in Ukrainian].
- Tarasjuk, V. M. (2018). Informatsiinyi prostir v Ukraini: vyklyky i zahrozy [Information Space in Ukraine: Challenges and Threats]. *Pravova derzhava*, 29, 375–381 [in Ukrainian].
- Tymchuk, D., Karin, Yu., Mashovets, K., & Gusarov, V. (2016). *Vtorzhenie v Ukrainu: khronika rossiiskoi ahresii* [Invasion of Ukraine: A Chronicle of Russian Aggression]. Brait Star Publishing [in Russian].

Tymoshyk, M. (2018, January 18–24). *Ukrainska knyzhka yak vyklyk Moskvi, abo Istoriia pro te, yak imperska vlada cherez zaboronu knih znesyliuvala dukh rosiiskykh ukrainsiv* [The Ukrainian Book as a Challenge to Moscow, or the Story of How the Imperial Government Weakened the Spirit of Russian Ukrainians by Banning Books]. *Slovo Prosvity*, pp. 2–3 [in Ukrainian].

Verkhovna Rada Ukrainy. (1992). *Pro informatsiiu* [On Information]. Law of Ukraine (October 2, 1992, № 2657–XII). <https://zakon.rada.gov.ua/laws/card/2657-12> [in Ukrainian].

Verkhovna Rada Ukrainy. (1994). *Pro zakhyst informatsii v informatsiino-telekomunikatsiinykh systemakh* [On Protection of Information in Automated Systems]. Law of Ukraine (July 5, 1994, № 80/94–VR). <https://zakon.rada.gov.ua/laws/card/80/94-%D0%B2%D1%80> [in Ukrainian].

Verkhovna Rada Ukrainy. (1998). *Pro Natsionalnu prohramu informatyzatsii* [On the National Informatization Program]. Law of Ukraine (February 4, 1998, № 74/98–VR). <https://zakon.rada.gov.ua/laws/card/74/98-%D0%B2%D1%80> [in Ukrainian].

Verkhovna Rada Ukrainy. (2011). *Pro dostup do publichnoi informatsii* [On Access to Public Information]. Law of Ukraine (January 13, 2011, № 2939–VI). <https://zakon.rada.gov.ua/laws/card/2939-17> [in Ukrainian].

Verkhovna Rada Ukrainy. (2017). *Pro osnovni zasady zabezpechennia kiberbezpeky Ukrainy* [On the Basic Principles of Cybersecurity in Ukraine]. Law of Ukraine (October 5, 2017, № 2163–VIII). <https://zakon.rada.gov.ua/laws/card/2163-19> [in Ukrainian].

Zelenskyi, V. (2021, April 13). *Zelenskyi: My zablokuvaly dezinformatsiini bataliony, yakі atakovali ukrainsiv zalpamy brekhni* [Zelenskyi: We Blocked Disinformation Battalions that Attacked Ukrainians with Volleys of Lies]. *Vseukrainskye vesty*. <https://vv.org.ua/poslednie-novosti/zelenskij-mi-zablokuvali-dezinformacijni-bataljoni-jaki-atakuvali-ukrainciv-zalpami-brehni/> [in Ukrainian].

Zhezhnych, P. I. (2010). *Tekhnolohii informatsiinoho menedzhmentu* [Information Management Technologies]. Lviv Polytechnic Publishing House [in Ukrainian].