

УДК 339.138:005.57]:355.451

Н. О. Шуляк,
А. М. Шуляк

ІНФОРМАЦІЙНА ГІГІЄНА В ЕРУ ЦИФРОВИХ ЗАГРОЗ: ВІД ПРОПАГАНДИ ДО ГІБРИДНИХ АТАК

Актуальність теми пов'язуємо з тим, що формування інформаційного суспільства та впровадження передових технологій у сферах інформації, телекомунікацій і зв'язку сприяли розвитку глобальних мереж і створенню нових можливостей для обміну даними. У 1990-х роках ХХ століття цифрова конвергенція відкрила широкі перспективи для інформаційного прогресу, що призвело до економічного зростання та інновацій у ХХІ столітті. Розглянуто концепцію стратегічних комунікацій, яка включає інформаційну гігієну та спрямована на вплив на громадську думку через різноманітні інформаційні операції. Виявлено, що стратегічні комунікації є важливим інструментом управління складними соціальними системами, захищаючи суспільство від деструктивного впливу інформації. Стаття аналізує важливість інформаційної безпеки для держави, особливо в контексті війни. Інформація може одночасно підтримувати стабільність держави та сприяти її розвитку, але також нести загрозу національним інтересам. Україна повинна приділяти особливу увагу захисту національного інформаційного простору, враховуючи ризики, пов'язані з гібридною війною, яку веде Росія. Автори підкреслюють, що стратегічні комунікації є ключовим елементом забезпечення інформаційної безпеки, а дотримання інформаційної гігієни повинно бути інституціоналізовано. Важливо, щоб Україна зберігала незалежність у своїй інформаційній політиці, ефективно реагуючи на загрози та маніпуляції, особливо в умовах активних воєнних дій. Стаття також розглядає вплив російської гібридної війни, яка об'єднує різні види воєнних дій, включаючи кібер- та інформаційні атаки. У цьому контексті українська "віртуальна армія" відзначається як ефективний інструмент протидії, що перевершує російські спроби маніпуляції через ботів та пропаганду. Автори звертають увагу на важливість підготовки населення до можливих інформаційних атак через підвищення рівня медіаграмотності та критичного мислення. Крім того, вони описують роль України в міжнародних інформаційних процесах та наводять приклади успішних ініціатив, таких як проєкт "Stopfake", спрямованих на боротьбу з дезінформацією. Зроблено акцент на необхідності активного захисту національного інформаційного простору, посилення медіаграмотності та стратегічних комунікацій, що є критично важливими для забезпечення національної безпеки України в умовах гібридної війни.

Ключові слова: інформаційна безпека, гібридна війна, інформаційна гігієна, стратегічні комунікації, пропаганда, дезінформація, кібербезпека, інформаційні війни, психологічні операції (ПСО), російська агресія, віртуальна армія.

DOI 10.34079/2226-2830-2024-15-40-185-195

Тему інформаційної гігієни автори вважають актуальною та перспективною, оскільки усвідомлення важливості інфогігієни стає дедалі поширенішим серед користувачів масових медіа. Люди активно користуються різними медіаканалами для отримання новин та інформації про події з усього світу, проте часто забувають перевіряти їх на достовірність, повноту та ясність. Це робить інформаційну гігієну

надзвичайно актуальною. Інформаційну гігієну можна розглядати як систему знань, яка вивчає вплив інформації на психічне, фізичне та соціальне благополуччя як окремої людини, так і суспільства в цілому, а також розробляє заходи для покращення інформаційного середовища. Її мета полягає в запобіганні негативного впливу інформації на здоров'я і благополуччя, а також у профілактиці захворювань, пов'язаних з інформаційним впливом. Завдання інформаційної гігієни включають розробку основ гігієнічної інформаційної поведінки, наукове обґрунтування заходів щодо організації інформаційних мереж і процесів, а також створення науково обґрунтованих нормативів для інформації та її середовища.

Методологічною основою дослідження є сукупність підходів і методів, що широко застосовуються у філософському аналізі наукових проблем. У роботі використовуються методи аналізу, синтезу, дедукції, а також міждисциплінарний і концептуальний підходи. Цей підхід дозволив виявити тенденції в дотриманні інформаційної гігієни, передбачити наслідки та можливий розвиток інформаційного простору під впливом деструктивних чинників. Структурно-функціональний підхід допоміг розглянути інформаційну гігієну в контексті стратегічних комунікацій як систему зі структурними компонентами, кожен з яких виконує певні функції. Політико-системний аналіз дав змогу комплексно дослідити політичний простір як систему комунікацій. Метод систематизації дозволив упорядкувати концепт інформаційної гігієни, а SWOT-аналіз допоміг оцінити внутрішні проблеми й зовнішні чинники, пов'язані з її недотриманням. Для прогнозування розвитку стратегічних комунікацій з урахуванням правил інформаційної гігієни були використані методи прогнозування.

Метою статті є виокремити та схарактеризувати інфогігієну під час російсько-української війни.

Науковці вважають, що активізація досліджень у сфері стратегічних комунікацій та інформаційної гігієни в Україні суттєво пов'язана з гібридною війною, ініційованою Росією проти України та міжнародного співтовариства у 2014 році. Від моменту розпаду СРСР і до сьогодні триває цивілізаційне протистояння між Україною та Росією, що відображає прагнення України до незалежності та спроби Росії відновити свою колишню гегемонію. У стратегії Росії Україна має ключове значення: без її повного підпорядкування успішне продовження агресивної зовнішньої політики РФ є неможливим, за думкою багатьох політиків і науковців. За словами О. та С. Васюти, головна мета російської агресії проти України полягає у бажанні перетворити її на сателіт Росії, при цьому зберігаючи формальну політичну незалежність. З 2014 року Росія активно використовує спеціальні операції в інформаційному, політичному, духовному та економічному просторах для приховування своєї збройної агресії проти України, сприяння економічному колапсу в деяких галузях і вплив на політичні еліти на Заході, спрямовані на лояльність до Росії (Wasiuta, O. and Wasiuta, S., 2020).

Для досягнення своїх експансіоністських цілей Росія використовує широкий арсенал засобів стратегічних комунікацій, маніпуляцій та дезінформації. Це включає пропаганду міфу про "руський мир", формування образу "іншого/чужого" та "європейського ворога", підтримку проросійських партій в Україні, використання історичних наративів і релігійного фактору (зокрема, діяльність УПЦ МП як "п'ятої колони" РФ в Україні), маніпуляції мовним питанням, а також порушення інформаційної гігієни та поширення дезінформації в українському медіапросторі (Shuliak, Konstankevych and Kunytskyu, 2021).

Необхідність ефективної протидії агресії змусила Україну та інші держави, які зазнали впливу російського неоімперіалізму, вдосконалювати свої стратегії комунікації та підвищувати рівень інформаційної гігієни. Це включає нейтралізацію деструктивної

інформації з Росії, яка підриває міжнародні відносини та провокує конфлікти на міжнародному та внутрішньому рівнях. У такому контексті дослідження стратегічних комунікацій набуває особливої актуальності (Шуляк, 2024).

Наукові праці зарубіжних дослідників, таких як Д. Андерсон, Р. Брукс, С. Бьорд, Ф. Денс, К. Йорк, М. Лінч, К. Ларсон, Дж. Магоні, Д. Мерфі, С. Патерсон, Д. Псакі, К. Халлахан, Б. Гамільтон, С. Татхем, К. Пол та інших, значною мірою присвячені феномену стратегічних комунікацій. Стратегічні комунікації залишаються складним концептом, який набуває різних значень залежно від контексту. Наприклад, Г. Почепцов досліджує соціальні комунікації, А. Баровська аналізує сучасне розуміння стратегічних комунікацій, а В. Ліпкан визначає їх ключове завдання як гарантування національних інтересів. С. Соловійов сформулював характеристики та принципи стратегічних комунікацій, О. Кушнір досліджує їх роль у формуванні української державності, а Д. Дубов розглядає концептуалізацію стратегічних комунікацій. Є. Макаренко вивчає національну ідею як інструмент деструктивних стратегічних комунікацій, тоді як Н. Піпченко аналізує стратегічні комунікації України.

Серед українських дослідників варто відзначити В. Бебика, С. Даниленка, В. Копійку, Є. Макаренко, І. та Г. Мінгазутдінових, М. Ожевана, Є. Тихомирову, О. Шевченко та інших, які висвітлюють як загальні питання розвитку системи стратегічних комунікацій, так і специфічні аспекти цієї сфери. У рамках дослідження науковцями факультету міжнародних відносин ВНУ ім. Лесі Українки протягом 2022–2025 рр. проекту «Стратегічні комунікації Європейського Союзу: протидія деструктивним впливам» (ERASMUS+ JEAN MONNET MODULE № 101047033 – EUSCCDI – ERASMUS-JMO-2021-HEI-TCH-RSCH). “Strategic Communications of the European Union: Combating Destructive Influences” (ERASMUS + JEAN MONNET MODULE № 101047033 – EUSCCDI – ERASMUS-JMO-2021-HEI-TCH-RSCH) також досліджено питання інформаційної гігієни та стратегічних комунікацій (Шуляк, 2024).

Розвиток медіаграмотності та інформаційної гігієни в цифрову епоху є ключовим завданням, яке має значний вплив на індивідуальний рівень, громади та суспільство в цілому. Незважаючи на постійні зусилля щодо підвищення цих навичок, все ще існує потреба в подальших дослідженнях, розробках і співпраці для подолання складних викликів, що виникають у цифровому медіасередовищі. Основними цілями є підтримка освіти з медіаграмотності, підвищення її рівня серед населення та розвиток навичок створення медіаконтенту.

Інформація може одночасно бути інструментом для зміцнення стабільності держави та сприяти її соціально-економічному й політичному розвитку, але також становити загрозу національним інтересам. Україні слід бути особливо уважною та обережною щодо захисту свого інформаційного простору, приділяючи особливу увагу інформаційній гігієні. Стратегічні комунікації кожної суверенної, демократичної та стабільної держави мають бути спрямовані на забезпечення національної інформаційної безпеки всіх учасників інформаційного обігу. Важливо інституціоналізувати процес дотримання інформаційної гігієни. В умовах війни, яку Росія веде на території України, необхідні оперативні та ефективні рішення.

На момент вторгнення Росії в Україну у 2014 році питання членства України в НАТО не було на порядку денному, оскільки у 2010 році був ухвалений закон про засади внутрішньої та зовнішньої політики, який закріплював позаблоковий статус держави. Україна в цей час зосередилася на підписанні Угоди про асоціацію з ЄС, що поступово зменшувало вплив Росії в країні. Як зазначають Сидорук та Павлюк (2022), Путіна турбувало не НАТО, а прагнення українців до демократії та зближення з європейською спільнотою. Прем'єр-міністр Латвії Артурс Кріш'яніс Каріньш вдало підкреслив:

«Москва боїться не НАТО, а української демократії» (Edelman, Kramer, 2022). Кремль вважає, що демократія, навіть з певними недоліками, де нація може змінювати владу через вибори, є серйозною загрозою для авторитаризму Путіна. Після російського вторгнення підтримка членства України в НАТО різко зросла — з 25 % у 2014 році до 62 % у лютому 2022 року (Фахурдінова, 2022). Російська агресія тільки посилила бажання українців захищати незалежність і рухатися в бік Європи. З моменту анексії Криму та початку війни на сході України Росія стала основною зовнішньою загрозою безпеці та суверенітету країни. Думка, що Путін об'єднав Україну та прискорив її наближення до Заходу, має підґрунтя (Сидорук, Павлюк, 2022).

Найбільшою загрозою для інформаційної безпеки України є гібридна війна РФ, що поєднує різні способи ведення конфлікту і ігнорує загальнолюдські цінності для досягнення власних цілей. Українська віртуальна армія є перевагою над ворогом, оскільки Росія, хоч і запускає мільйони ботів для поширення пропаганди, не здатна мобілізувати мільйони живих людей, які б широко доносили правду про події та власний досвід (Шуляк, 2023).

На початку ХХІ століття формується новий рід військ – інформаційно-комунікаційні війська, потенціал яких є не менш руйнівним, ніж у традиційних військових формувань, таких як сухопутні, морські або повітряні сили, зазначає В. Бебик. Він підкреслює, що в умовах глобального інформаційного суспільства методи війни залишаються незмінними: відбувається руйнування державних і соціальних інститутів, економіки, інфраструктури, культури та моралі, а також системи виховання і людської психіки. Інформаційно-комунікаційні та гібридні війни, що виникли на межі ХХ і ХХІ століть, змінили базові поняття військової науки, зокрема поняття театру військових дій, яке раніше розглядалося лише в територіальному контексті, що визначало специфіку дій різних родів військ (Бебик, 2023).

Інформаційно-комунікаційна війна, як правило, розпочинається задовго до реального відкриття звичайних бойових дій. Це відбувається в глобальному інформаційно-комунікаційному просторі, а також в національному інформаційно-комунікаційному просторі країни-агресора та просторі його майбутнього ворога (Становлення і розвиток..., 2018). З одного боку, для підготовки власного населення до війни важливо створити через систему пропаганди та маніпуляцій медіа образ ворога, переконавши людей і збройні сили в неминучості війни. Це досягається ідеологічними, політичними та соціально-психологічними засобами. З іншого боку, проводиться ідеологічний, політичний та психологічний вплив на майбутнього супротивника, спрямований на дезорганізацію його суспільної свідомості та морально-психологічного стану. Паралельно здійснюються кібератаки на урядові структури, об'єкти критичної інфраструктури, а також диверсії проти військових складів і підприємств.

Водночас інформаційно-комунікаційна війна охоплює глобальний інформаційний простір. Її головна мета – дискредитація супротивника на міжнародній арені через медіа, соціальні мережі та міжнародні організації.

Як зауважує О. Дорош, Росія володіє значним потенціалом для гібридного впливу, використовуючи інструменти м'якої сили. Серед її переваг – російська мова, культурні досягнення та православні цінності. Такі організації, як «Росспівробітництво» та фонд «Русский мир», активно поширюють російську культуру, а міжнародні події, такі як Олімпіади та Чемпіонат світу з футболу, слугують для посилення впливу. Російські медіаресурси, такі як RT та «Россия сегодня», а також експертні майданчики, як Російська рада з міжнародних справ, клуб «Валдай» та Фонд Горчакова, сприяють зміцненню цього впливу. Однак, попри ці зусилля, російські медіа часто використовують пропаганду, що, у свою чергу, знижує ефективність і руйнує імідж. Крім того, через

агресивну та ізоляційну політику РФ м'який вплив Росії залишається обмеженим, і вона сприймається на Заході як авторитарна та корумпована держава (Дорош, 2020).

В. Бебик указує на те, що в контексті інформаційно-комунікаційних та гібридних воєн противники активно використовують різноманітні суспільні структури, які мають значний вплив на глобальну та національну суспільну свідомість країни або країн, що стали об'єктом атаки (Куйбіда, В. та Бебик, В. (ред.), 2019):

- Засоби масової комунікації, такі як телебачення, радіо, супутникові та кабельні мережі, а також інтернет-зв'язок через супутник, мобільний, мережевий відео та аудіо, а також соціальні медіа мережі, веб-сайти, паперові та електронні видання, журнали та книги.

- Різнноманітні суспільні організації, такі як релігійні, журналістські, правозахисні, профспілкові, культурологічні, екологічні та інші.

- Дипломатичні структури, включаючи Міністерство закордонних справ, посольства та представництва в міжнародних та міжурядових організаціях.

- Розвідувальні структури, які діють через таємних або легалізованих агентів у засобах масової інформації, міжнародних та суспільних організаціях.

Велика кількість чат-ботів, створених владними органами та структурами для захисту інформаційного простору, свідчить про значну підтримку з боку населення і скоординовані дії інституцій, які відповідають за безпеку інформаційного простору. Такі заходи сприяють ефективному досягненню цілей інформаційної гігієни під час війни. Вони включають здатність критично мислити, аналізувати та створювати інформацію, а також розуміння природи інформаційного впливу на суспільство.

«Stopfake Україна» - це платформа для перевірки фактів, запущена 2 березня 2014 року з ініціативи викладачів, випускників і студентів Могиллянської школи журналістики та програми Digital Future of Journalism. До проєкту приєдналися журналісти, редактори, програмісти та перекладачі, які хотіли захистити Україну від дезінформації під час окупації Криму і війни на Донбасі. Спочатку проєкт зосереджувався на спростуванні фейків у медіа про події в Україні, але з часом перетворився на інформаційний хаб, що аналізує кремлівську пропаганду в різних аспектах, включаючи її вплив на інші країни та регіони, як-от Європейський Союз і держави колишнього СРСР (Тихомирова, 2019b).

Команда «Stopfake» постійно зростає, залучаючи фахівців, які перевіряють, редагують, перекладають та поширюють інформацію 11 мовами, включаючи російську, англійську, іспанську, французьку та інші. Контент можна знайти на сайті, дивитися в інтернеті, слухати на радіо, читати в друкованих виданнях, а також у соцмережах. Важливо, що «Stopfake» є незалежним проєктом і не фінансується урядом України. Проєкт існував на волонтерських засадах, а згодом фінансувався через краудфандинг та підтримку міжнародних фондів. Його місія полягає у верифікації інформації, підвищенні медіаграмотності та боротьбі з пропагандою шляхом чіткого розмежування журналістики фактів і дезінформації (Stopfake.org, 2018).

У 2023 році інформаційна гігієна отримує нові виклики (InfoLightUA, 2023). У сучасному геополітичному контексті нові процеси та конфлікти, пов'язані з розширенням інтернет-простору та активним використанням інформаційних технологій, набувають якісно нового значення. Інформаційна революція привнесла цілу низку нових категорій у геополітичний аналіз, серед яких ключовими є поняття «інформаційна війна», «гібридна війна», «смысловая війна» та «інформаційна зброя». Однією з головних цілей сучасної інформаційної війни є створення сприятливих умов для реалізації геополітичних та гео економічних стратегій. Інформаційна війна розглядається як протистояння, де інформаційні технології, системи та медіа використовуються для впливу на управлінські системи противника, його політичне та військове керівництво,

суспільство загалом, а також для атаки на інформаційну інфраструктуру супротивника, одночасно захищаючи власний інформаційний простір (Інформаційна гігієна..., 2023).

Основні методи інформаційної війни включають блокування або спотворення інформаційних потоків та процесів ухвалення рішень супротивника. Це може включати збір тактичної інформації, захист власних інформаційних ресурсів, поширення пропаганди або дезінформації з метою деморалізації супротивника, а також підрив достовірності його інформаційних ресурсів. У таких війнах застосовуються різноманітні методи, такі як спеціальна пропаганда, психологічний тиск, дезінформація, розсіювання суспільної свідомості та поширення чуток. Інформаційна війна проводиться в комплексі з кібер- та психологічними операціями, а також використовує радіоелектронну боротьбу та мережеві технології. У контексті інформаційної революції цей тип війни часто називають техноцентричною або мережецентричною (Тихомирова, 2019а).

Під час військових конфліктів активно застосовуються інформаційно-психологічні операції (ІПСО) або Psychological Operations (PSYOP). Цей термін набув особливої актуальності останнім часом. Суть ІПСО полягає у систематичних заходах, спрямованих на вплив переважно на іноземні аудиторії для зміни їхніх емоцій, мотивів і поведінки урядів, організацій, груп чи індивідів. Основними об'єктами ІПСО є керівництво іноземних держав, їхні спецслужби та агентурні структури, медіа, неурядові організації та інтернет-ресурси.

Методи інформаційно-психологічних операцій включають дезінформацію, пропаганду, перебільшення або замовчування певної інформації, диверсії в тилу та кібератаки. Основна суть ІПСО полягає в тому, щоб змусити вас діяти в інтересах противника, при цьому створюючи враження, що це ваше власне рішення. Це типовий приклад ІПСО, але не завжди використовуються стандартні методи й підходи. Хоча дії українських спецслужб ще зарано обговорювати, слід розуміти, що такі операції тривають, і, зважаючи на загальний хід бойових дій, ми діємо не менш ефективно, ніж ворог.

Інформаційна війна завжди базується на маніпулюванні інформацією, якою об'єкт довіряє, з метою змусити його ухвалювати рішення, що суперечать його власним інтересам, але підтримують інтереси агресора. У професійно організованій кампанії ми не знатимемо, коли інформаційна війна почалася, наскільки вона потужна або руйнівна, і коли вона завершиться. Її наслідки можна побачити лише тоді, коли вона поєднується зі звичайною війною. Структурно це виглядає як маніпулювання масами, основною метою якого є:

- впровадження у суспільну та індивідуальну свідомість ворожих і шкідливих ідей;
- дезорієнтація та дезінформація громадськості;
- послаблення певних переконань і звичаїв для піднесення власних ідей як єдино правильних; – залякування населення образом ворога;
- підтримка або супровід звичайної війни;
- залякування супротивника демонстрацією своєї сили.

Інформаційна війна, яка передувала повномасштабному вторгненню в Україну, а також подіям 2014 року, має своє коріння ще з часів подій 2004 року. Навіть перед тим, як влада Януковича була повалена у 2014 році, почали циркулювати міфи про «бандерівців», які, за легендою, збиралися знищувати російськомовне населення. Росія активно розпочала інформаційну війну проти України вже після подій 2004 року, і вже в 2007 році Путін фактично оголосив війну тодішньому світовому порядку на Мюнхенській конференції, вчинивши це під час захоплення спочатку Грузії, а потім і України, і, ймовірно, не обмежившись лише цими державами.

Аналізуючи напад на Україну в лютому 2022 року, можна помітити його подібність до операції коаліції на чолі з США, відомої як "Шок і трепет". Ця доктрина, розроблена в 1996 році, передбачала блискавичний наступ із використанням усіх доступних засобів для досягнення миттєвої переваги. Основною метою було не лише знищення військових сил противника, а й вплив на психологію всього суспільства. Інформаційна війна в таких умовах спрямована на декілька аудиторій: свою, противника та міжнародну спільноту. Спершу всі ці аудиторії готуються до неминучих і "виправданих" бойових дій. США, наприклад, використовували звіти про зброю масового знищення в Іраку, тоді як Росія маніпулювала наративом про "нацистів" в Україні, нібито відповідальних за знищення "мирного Донбасу". Це лише один із прикладів дезінформації, яку розгорнули проти України під час цього періоду (Суспільство і право, 2019)..

Після створення переконання про неминучість війни відбувається швидка атака з масованим використанням озброєнь та інформаційних впливів, за винятком неконвенційних засобів. У військових операціях важливо адекватно оцінювати силу противника, його психологічні особливості та передбачати реакції як окремих людей, так і суспільства в цілому. За планами Кремля, українське керівництво мало б втекти, армія капітулювати, а населення – прийняти нейтральну чи навіть прихильну позицію. Однак у перші тижні вторгнення українці на окупованих територіях влаштовували масові протести, виступали проти російської техніки та активно висловлювали свою незгоду (Інформаційна гігієна...2023)..

Українці демонстрували стійкість перед ворогом і активно використовували гумор і абсурд для протидії. Це проявлялося в історіях про банку з огірками, яка нібито "збила" російський дрон, або чутках про циганів і фермерів, які "віджимали" російську техніку. Деякі з цих історій мали реальну основу, а інші були міфами, але вони піднімали бойовий дух. Наприклад, попри відсутність російських танків у Києві, історії про те, як "троєщинські пацани" захоплювали техніку ворога, поширювались і залишались в пам'яті народу. Ця контрпропаганда зображала ворога як комічного, незграбного та слабкого (наприклад, історія з банкою огірків, яка нібито «збила» дрон), через що його не сприймали як серйозну загрозу, що вимагала негайної відсічі. Українці майстерно реалізували цю стратегію.

Інформаційно-психологічні операції під час війни або для її підготовки спрямовуються на різні «аудиторії»:

- на власні війська, щоб зміцнити їх психологічну готовність та емоційну стійкість;
- на війська противника, щоб деморалізувати їх і знизити бойову ефективність;
- на мирне населення своєї країни та противника, з метою здобути підтримку або забезпечити нейтралітет;
- на керівництво та населення інших країн для досягнення міжнародної підтримки чи нейтралітету.

Під час активних бойових дій кожен з нас стає джерелом інформації, яке необхідно ретельно контролювати, адже за нами спостерігають як власні, так і ворожі сили. Тому важливо дотримуватися правил інформаційної гігієни, зокрема:

- отримувати інформацію виключно з офіційних джерел;
- звертати увагу на звіти ЗСУ, військово-цивільних адміністрацій та офіційних медіа;
- перевіряти інформацію в кількох джерелах;
- співпрацювати з фактчекінговими платформами, такими як «StopFake».

Метою ворога є створення страху, паніки та невпевненості. Тому важливо це усвідомлювати й бути обачними при отриманні та поширенні інформації. Якщо ви вмієте критично оцінювати інформацію і дотримуетесь цих принципів, діліться цими знаннями зі своїм оточенням, щоб захистити його від інформаційних атак ворога.

Найбільшу загрозу інформаційній безпеці України сьогодні становить гібридна війна з Росією, яка поєднує різні види бойових дій, ігноруючи загальнолюдські цінності та сучасні правила ведення воєн для досягнення своїх цілей. Однією з характерних рис російсько-української війни є функціонування інформаційних військ. Ці війська стали популярними завдяки розвитку інтернету та соціальних мереж, застосовуючи різні методи, такі як бот-мережі, фейки, спам і кібератаки.

Особливо важливою подією в 2022 році стало створення українських інформаційних військ, які об'єднали активних громадян для боротьби з російською інформаційною пропагандою, виявлення провокацій і поширення контрпропаганди. Ці війська активно співпрацюють з Національним координаційним центром кібербезпеки, відповідальним за захист критичної інфраструктури та інформаційну безпеку, а також з іншими структурами, такими як чат-боти державних органів та Центр протидії дезінформації при РНБО України.

Українська віртуальна армія надає перевагу над ворогом, який не має аналогічних ресурсів. Хоча Росія активно використовує мільйони ботів для розповсюдження пропаганди, вона не може мобілізувати таку ж кількість людей, які щиро діляться своїми переживаннями. Важливо розуміти, що інформаційні війська можуть використовуватися не лише військовими, але й державними структурами, політичними партіями та навіть злочинними угрупованнями. Це може бути як загрозою, так і засобом захисту національної безпеки, тому важливо бути обережними в інтернеті.

Висновки. У сучасному світі, перенасиченому інформацією та взаємозв'язками, деструктивні впливи становлять серйозну загрозу для суспільства та окремих людей. Одним із найшкідливіших явищ є воєнні конфлікти, що призводять до людських втрат, руйнування міст, інфраструктури та культурних цінностей, а також до фізичного та психологічного знищення. Поширення дезінформації та фейкових новин, маніпулювання громадською думкою, атаки на інформаційну інфраструктуру, розповсюдження ворожої риторики та ідеологічних конфліктів — усе це приклади деструктивних впливів, які можуть мати серйозні негативні наслідки для суспільства та індивідів. У світі, де деструктивні впливи є невід'ємною частиною, необхідно навчитися їх розпізнавати та протидіяти їм. Дотримання інформаційної гігієни є одним із ключових аспектів захисту від негативних наслідків. В умовах війни інформаційні виклики можуть поставити під сумнів навіть саму істину, тому збереження розумового здоров'я та фільтрація дезінформації стають надзвичайно важливими. Важливо розуміти, що воєнні конфлікти можуть бути платформою для поширення дезінформації та пропаганди, і тому необхідно критично оцінювати отриману інформацію, розвивати навички критичного мислення та використовувати надійні джерела інформації.

Бібліографічний список

- Бебик, В.М. 2023. Інформаційно-комунікаційні війни та інформаційно-комунікаційні війська. *Інформація і право*, 3(46), с. 86-97.
- Дорош, Л.О. 2020. Відповіді на гібридні загрози : особливості стратегії Європейського Союзу у боротьбі з дезінформацією. *Вісник Маріупольського державного університету. Серія: Історія. Політологія: збірник наукових праць*, 27. с. 106–116
- Суспільство і право, 2019. Інформаційна гігієна або як розпізнати неправдиві новини в інтернеті? Львів: Видавництво «Простір».

- Інформаційна гігієна в мережі (taslife.com.ua) [онлайн]. Доступно: <https://taslife.com.ua/blog/information-hygiene> (дата звернення 20.09.2023)
- InfoLightUA, 2023. Інформаційна гігієна у 2023 році. Нові виклики: частина перша. [онлайн]. Доступно: <https://infolight.in.ua/2023/02/16/informatsijna-hihiiena-u-2023-rotsi-novi-vyklyky-chastyna-persha/> (дата звернення 20.11.2023)
- Куйбіда, В. та Бебик, В. (ред.), 2019. Національна безпека в умовах інформаційних та гібридних війн : монографія. Київ : НАДУ, 384 с.
- Сидорук Т. В. та Павлюк В. В., 2022. Розширення НАТО як фальшивий привід для виправдання війни Росії проти України. Стратегічна панорама. Спецвипуск «Гібридна війна і демократичний мир: що означає нова фаза російського наступу для України і Європи та як з ним упоратися» [онлайн]. Доступно: <https://niss.gov.ua/news/novyny-nisd/hibrydna-viyna-i-demokratychnyy-myrt-shcho-oznachaye-nova-faza-rosiyskoho-nastup>
- Становлення і розвиток системи стратегічних комунікацій сектору безпеки і оборони України, 2018. / Пилипчук В.Г., Компанцева Л.Ф., Кудінов С.С., Доронін І.М., Дзьобань О.П., Акульшин О.В., Заруба О.Г. / за заг. ред. В.Г. Пилипчука: монографія. Київ: ТОВ “Видавничий дім “АртЕк”, 272 с.
- Тихомирова, Є.Б. 2019а. ЄС: проекти з протидії сфабрикованим новинам. *Міжнародні відносини, суспільні комунікації та регіональні студії*, 1 (5), с. 53-63.
- Тихомирова, Є. 2019b. Stopfake Україна. Боротьба з неправдивими відомостями. Глосарій: навчальний енциклопедичний словник-довідник із питань інформаційної безпеки / Ред. Шуляк А. Київ, 580 с.
- Фахурдінова, М., 2022. Переваги від НАТО: чим небезпечна для України відмова від курсу на вступ до Альянсу. Європейська правда [онлайн]. Доступно: <https://www.eurointegration.com.ua/articles/2022/04/15/7137884/> (дата звернення 15.04.2022)
- Stopfake.org, 2018. Фейки, спростовані проектом StopFake в 2014-2017 роках: наративи та джерела [онлайн]. Доступно: <https://www.stopfake.org/uk/fejky-sprostovani-proektom-stopfake-v-2014-2017-rokah-narratyvy-ta-dzherela/> (дата звернення 19.04.2023)
- Шуляк, Н. 2023. Функціонування інформаційних військ України під час російсько-української війни 2022-2023 рр. Мат. XVII Міжнар. наук.-практ. конф. студ., асп. та мол. вчених «Молода наука Волині: пріоритети та перспективи досліджень» (16–17 травня 2023 року). Луцьк: ВНУ ім. Лесі Українки, 1 електрон. опт. диск (CD-ROM). Об'єм даних 9,38 Мб. С. 704-707
- Шуляк, Н. О. 2024. Інформаційна гігієна в системі стратегічних комунікацій України: дис.. на здобуття наук. ст. док. Філ. за спеціальністю 291 Міжнародні відносини, суспільні комунікації та регіональні студії, Луцьк, 273 с.
- Edelman, E. S., Kramer, D. J., 2022. Keep NATO's Door Open to Ukraine. Washington Shouldn't Grant Putin the Sphere of Influence He Wants. Foreign Affairs [онлайн]. Доступно: <https://www.foreignaffairs.com/articles/ukraine/2022-01-31/keep-natos-door-open-ukraine> (дата звернення 31.01.2022)
- Shuliak, A., Konstankevych, I. and Kunytskyu, M., 2021. Use of "the other / alien" image in the strategic communications of the Russian Federation during the russian-ukrainian confrontation (2014-2021). *Przegląd Strategiczny*. Wydawnictwo Naukowe WNPiD UAM, Poznań, 14, p. 195-210. DOI: 10.14746/ps.2021.1.12
- Wasiuta, O. and Wasiuta, S., 2020. Kremłowska dezinformacja w Internecie i reakcja społeczeństw zachodnich, *Przegląd Geopolityczny*, tom 34, s. 136-147

References

- Edelman, E. S., Kramer, D. J., 2022. Keep NATO's Door Open to Ukraine. Washington Shouldn't Grant Putin the Sphere of Influence He Wants. *Foreign Affairs* [online]. Available at: <https://www.foreignaffairs.com/articles/ukraine/2022-01-31/keep-natos-door-open-ukraine> (accessed: 31 January 2022).
- Shuliak, A., Konstankevych, I., Kunytskyi, M., 2021. Use of "the other / alien" image in the strategic communications of the Russian Federation during the Russian-Ukrainian confrontation (2014-2021). *Przegląd Strategiczny*. Wydawnictwo Naukowe WNPiD UAM, Poznań, 14, pp. 195-210. DOI: 10.14746/ps.2021.1.12.
- Wasiuta, O., Wasiuta, S., 2020. Kremlowska dezinformacja w Internecie i reakcja społeczeństw zachodnich. *Przegląd Geopolityczny*, vol. 34, pp. 136-147.
- Bebyik, V.M., 2023. Information and Communication Wars and Information and Communication Forces. *Information and Law*, No. 3(46), pp. 86-97.
- Dorosh, L.O., 2020. Responses to Hybrid Threats: Features of the European Union's Strategy in Combating Disinformation. *Bulletin of Mariupol State University. Series: History. Political Science: Collection of Scientific Papers*, 27, pp. 106-116.
- Information Hygiene or How to Recognize False News on the Internet? *Prostir Publishing*, Lviv, 2019. 7 pp.
- Information Hygiene Online (taslife.com.ua) [online]. Available at: <https://taslife.com.ua/blog/information-hygiene> (accessed: 20 September 2023).
- Information Hygiene in 2023. New Challenges: Part One. *InfoLightUA* [online]. Available at: <https://infolight.in.ua/2023/02/16/informatsijna-hihiiena-u-2023-rotsi-novi-vyklyky-chastyna-persha/> (accessed: 20 November 2023).
- National Security in the Context of Information and Hybrid Wars / edited by V. Kuybida and V. Bebyik: Monograph. Kyiv: NADU, 2019. 384 pp.
- Sydooruk, T. V., Pavliuk, V. V., 2022. NATO Expansion as a False Pretext for Justifying Russia's War Against Ukraine. *Strategic Panorama*. Special Issue "Hybrid War and Democratic Peace: What the New Phase of Russian Aggression Means for Ukraine and Europe and How to Deal with It" [online]. Available at: <https://niss.gov.ua/news/novyny-nisd/hibrydna-viyna-i-demokratychnyy-myr-shcho-oznachaye-nova-faza-rosiyskoho-nastup>.
- Formation and Development of the Strategic Communications System in Ukraine's Security and Defense Sector, 2018 / Pylypchuk, V. H., Kompantseva, L. F., Kudynov, S. S., Doronin, I. M., Dzioban, O. P., Akulshyn, O. V., Zaruba, O. H. / edited by V. H. Pylypchuk: Monograph. Kyiv: Publishing House "ArtEk," 272 pp.
- Tykhomyrova, Y.B., EU Projects to Counter Fabricated News. *International Relations, Public Communications and Regional Studies*, 2019. No. 1 (5). pp. 53-63.
- Tykhomyrova, Y., 2019. Stopfake Ukraine. Combatting False Information. Glossary: Educational Encyclopedic Dictionary on Information Security / edited by Shuliak, A. Kyiv, 580 pp.
- Fakhurdivna, M. Benefits of NATO: How Refusal to Join the Alliance is Dangerous for Ukraine. *European Truth* [online]. Available at: <https://www.eurointegration.com.ua/articles/2022/04/15/7137884/> (accessed: 15 April 2022).
- Fake News Debunked by the StopFake Project in 2014-2017: Narratives and Sources [online]. Available at: <https://www.stopfake.org/uk/fejky-sprostovani-proektom-stopfake-v-2014-2017-rokah-narratyvy-ta-dzherela/> (accessed: 19 April 2023).
- Shuliak, N., 2023. Functioning of Ukraine's Information Troops During the Russo-Ukrainian War of 2022-2023. Materials from the XVII International Scientific-Practical

Conference of Students, Postgraduates, and Young Scientists "Young Science of Volyn: Priorities and Research Perspectives" (16-17 May 2023). Lutsk: Lesya Ukrainka Volyn National University, 1 electronic optical disk (CD-ROM). Data volume 9.38 MB. pp. 704-707.

Shuliak, N. O., 2024. Information Hygiene in the System of Strategic Communications of Ukraine: Dissertation, Doctor of Philosophy in International Relations, Public Communications, and Regional Studies. Lutsk, 273 p.

Стаття надійшла до редакції 03.09. 2024 р.

N. Shuliak,
A. Shuliak

INFORMATION HYGIENE IN THE ERA OF DIGITAL THREATS: FROM PROPAGANDA TO HYBRID ATTACKS

The relevance of the topic is connected with the fact that the formation of information society and implementation of advanced technologies in the fields of information, telecommunications, and communication have contributed to the development of global networks and new opportunities for data exchange. In the 1990s digital convergence opened great prospects for information progress, leading to economic growth and innovation in the 21st century. The concept of strategic communications, which includes information hygiene and aims to influence public opinion through various information operations, is examined. It is found that strategic communications are an important tool for managing complex social systems, protecting society from the destructive impact of information. The article analyzes the importance of information security for the state, especially in the context of war. Information can simultaneously support the stability of the state and contribute to its development, but it can also pose a threat to national interests. Ukraine must pay special attention to protecting the national information space, considering the risks associated with the hybrid war waged by Russia. The authors emphasize that strategic communications are a key element in ensuring information security, and adherence to information hygiene should be institutionalized. It is important for Ukraine to maintain independence in its information policy, effectively responding to threats and manipulations, especially in the context of active military operations. The article also examines the impact of Russian hybrid warfare, which combines various types of military actions, including cyber and information attacks. In this context, the Ukrainian "virtual army" is noted as an effective tool for countering, surpassing Russian attempts to manipulate through bots and propaganda. The authors highlight the importance of preparing the population for potential information attacks by increasing media literacy and critical thinking. Additionally, they describe Ukraine's role in international information processes and provide examples of successful initiatives, such as the "Stopfake" project, aimed at combating disinformation. The emphasis is placed on the need for active protection of the national information space, enhancing media literacy, and strategic communications, which are critically important for ensuring Ukraine's national security in the conditions of hybrid warfare.

Keywords: information security, hybrid warfare, information hygiene, strategic communications, propaganda, disinformation, cybersecurity, information wars, psychological operations (PsyOps), Russian aggression, virtual army