УДК 316.485.26:659.3:327.88]:355.48

Поправка М. О.
здобувач третього рівня освіти,
кафедра політології
Одеський національний університет імені І. І. Мечникова,
Французький бульв., 24/26, м. Одеса, 65058, Україна
E-mail: Anna.maria.1861y@gmail.com
ORCID ID: https://orcid.org/0009-0003-6151-8540
DOI https://doi.org/10.32782/2707-5206.2024.38.22

ІНФОРМАЦІЙНА ВІЙНА В КОНТЕКСТІ ГІБРИДНОГО КОНФЛІКТУ

Гібридні конфлікти, які стали невід'ємною частиною сучасної геополітичної реальності, суттєво змінюють правила ведення війни, роблячи інформаційний складник одним із найважливіших аспектів боротьби за перевагу. У сучасному світі інформаційні війни стали потужним інструментом геополітичного впливу та маніпулювання суспільною свідомістю і громадською думкою. Інформаційна війна відрізняється від традиційних форм війни тим, що вона не обмежується фізичним знищенням противника, а спрямована на підрив морального духу, зміну політичного курсу, дестабілізацію соціальної ситуації або зміну світогляду. Це робить її особливо ефективною в умовах гібридних конфліктів, де фізичне протистояння може бути мінімальним або взагалі відсутнім.

У статті розглядається роль інформаційної війни в умовах гібридних конфліктів, коли традиційні військові дії доповнюються комплексом нелінійних методів впливу, таких як економічні санкції, політичний тиск, кібератаки, дезінформаційні кампанії та пропаганда. Проаналізовано ключові стратегії та методи ведення інформаційних війн, їхній вплив на громадську думку, державні інститути та міжнародні відносини. Особливу увагу приділено вивченню прикладів із сучасної міжнародної практики, зокрема ролі інформаційних кампаній у конфліктах на пострадянському просторі. Розглянуто підходи до протидії інформаційним атакам у контексті захисту національної безпеки. Окрім того, проаналізовано методи виявлення та нейтралізації дезінформації, а також заходи з підвищення медіаграмотності населення як одного з важливих чинників протидії маніпулюванню громадською думкою. Розглянуто роль державних інституцій, медіа та громадянського суспільства у боротьбі з інформаційними атаками.

Досліджено як технічні, так і соціальні підходи, що використовуються для захисту суспільства від маніпуляцій та дезінформації. Аналізуються передові технології, зокрема штучний інтелект, блокчейн, а також методи кібербезпеки, для виявлення та запобігання інформаційним атакам. Обговорюються стратегічні підходи, що сприятимуть ефективному реагуванню на нові виклики інформаційних війн.

Ключові слова: інформаційна війна, гібридний конфлікт, дезінформація, пропаганда, кібероперація.

Гібридні конфлікти, що стали характерними для сучасного міжнародного середовища, являють собою складну та багаторівневу комбінацію різних форм впливу та протидії, включаючи військові, політичні, економічні, інформаційні та кібернетичні операції.

Одним з основних складників гібридного конфлікту є інформаційна війна, ключова мета якої – зміна поведінки цільової аудиторії шляхом маніпуляції інформацією, поширення дезінформації та пропаганди.

Актуальність дослідження зумовлена зростанням впливу засобів масової інформації на процеси всередині громадянського суспільства. Дослідження наукового підґрунтя та передумов виникнення інформаційної війни дає змогу визначити низку методів та засобів протидії більш глобальним викликам сучасного світу – гібридним конфліктам.

Актуальним питанням дослідження ролі засобів масової інформації та інших форм комунікації у розв'язанні та веденні інформаційних війн присвячено роботи таких українських та зарубіжних авторів, як: Е. Бернейс (Bernays, 1928), П. Прибутько (Prybutko & Luk'yanets, 2007), К. Водолазька (Vodolazka, 1999), Т.Ю. Ковалевська, Н.В. Кондратенко, Н.В. Кутуза, О.О. Порпуліт, А.В. Ковалевська (Kovalevska, Kondratenko, Kutuza, Porpulit & Kovalevska, 2009), І. Луб'янець, А. Мегель, М. Яремчук (Megel & Yaremchuk, 2023), В. Петрик, С. Гнатюк, О. Черненко та В. Гуреєв (Petryk, Hnatyuk, Chernenko & Gureev, 2021), М. Присяжнюк, Л. Компанцева, Є. Скулиш, О. Бойко, В. Остроухов (Petryk, Prysiazhnyuk, Kompantseva, Skulysh, Boyko & Ostroukhov, 2023), Л. Веселова (Veselova, 2021), Ю. Когут (Kohut, 2023) та ін.

В умовах глобалізації та розвитку цифрових технологій інформаційна війна набула нових форм та інструментів, що дає змогу агресорам впливати на суспільну думку, державні інститути та міжнародні відносини без застосування традиційних військових засобів. Інформаційна війна є процесом цілеспрямованого використання інформації як засобу впливу на свідомість та поведінку окремих груп населення, суспільств і навіть цілих держав. Її основними інструментами є пропаганда, дезінформація, медіаманіпуляції, психологічні операції, а також використання соціальних мереж для поширення впливу.

Ю. Когут зауважує, що інформаційна війна виникла як форма інформаційного протиборства, але надалі стала самостійним видом здійснення зовнішньої політики країн і необхідним доповненням до класичної війни (Kohut, 2023, p. 277). Термін «інформаційна війна» уперше опинився у фокусі уваги міжнародної спільноти у зв'язку з війною в Перській затоці в 1991 р. Раніше, у 1976 р., було введено в обіг подібний термін – information war, що його запропонував учений-фізик Т. Рейнер стосовно війн, основними об'єктами ураження в яких виступають інформаційні системи (Kohut, 2023, p. 278).

У гібридних конфліктах інформаційна війна відіграє роль не менш важливу, ніж фізичні бойові дії. Вона може використовуватися для підготовки населення до конфлікту, створення підґрунтя для військової агресії або, навпаки, для дискредитації дій супротивника. Наприклад, у випадку конфлікту в Україні російська федерація активно використовувала інформаційну війну для формування негативного іміджу українського уряду, поширення дезінформації про події у зоні бойових дій та створення ворожого образу Заходу.

Інформаційні кампанії також відіграють ключову роль у впливі на міжнародну думку, зокрема через дезінформаційні атаки на міжнародні організації, маніпуляції громадською думкою в інших державах, а також використання кібероперацій для підриву довіри до демократичних інститутів.

Однією з основних стратегій інформаційної війни є використання так званих «м'яких» інструментів впливу, що включають контроль за інформаційними потоками, створення та підтримку пропагандистських медіаструктур, використання соціальних мереж для поширення фейкових новин та формування певного дис-

курсу в інформаційному просторі. Ці стратегії часто підкріплюються кіберопераціями, які дають змогу отримати доступ до конфіденційної інформації, зламати інформаційні системи або провести інформаційно-психологічні операції.

Іншим важливим інструментом є пропаганда, яка спрямована на формування певного сприйняття подій і явищ у суспільстві. Пропагандистські кампанії можуть бути спрямовані як на внутрішню, так і на зовнішню аудиторію, з метою зміцнення патріотизму або ж дискредитації супротивника. У своїй праці «Пропаганда» Е. Бернейс визначає пропаганду як «послідовну, досить тривалу діяльність, спрямовану на створення або інформаційне оформлення різних подій із метою впливу на ставлення мас до підприємства, ідеї або групи» (Bernays, 1928, p. 17). На думку автора, сучасна пропаганда враховує не окрему особистість, а структуру суспільства, що складається з пересічних груп і зв'язків «лідер – послідовник». Людина розглядається не просто як клітина соціального організму, а як складник соціальної одиниці (Bernays, 1928, p. 19).

Інформаційна війна має серйозний вплив на міжнародні відносини, особливо в контексті гібридних конфліктів. Вона може використовуватися для зміни політичного курсу інших держав, створення коаліцій або ізоляції певних країн на міжнародній арені.

Після розпаду Радянського Союзу пострадянський простір став ареною численних конфліктів, що характеризуються як традиційними збройними зіткненнями, так і новими формами гібридних загроз, серед яких ключове місце посіли інформаційні кампанії. Одним із найяскравіших прикладів використання інформаційних кампаній є конфлікт в Україні, що розпочався у 2014 р. Росія використовувала широкий спектр інформаційних технологій для дезінформації, підбурювання конфліктів та створення вигідної для себе картини подій на міжнародній арені. Цілями інформаційної війни з боку країни-агресора стали, зокрема, вплив на емоції, думки, судження і в кінцевому підсумку – світогляд тих, ким маніпулюють; отримання переваги або деморалізація супротивника; легітимізація агресії та обґрунтування перемоги у збройному конфлікті; дискредитація противника тощо (Megel & Yaremchuk, 2023, p. 6). А. Мегель, зокрема, зазначає, що агресор досягає своїх цілей, використовуючи інформаційно-психологічні операції (ІПСО) різного масштабу впливу.

Інформаційно-психологічна операція – це спланований та поетапно реалізований вплив на думки, переконання, настрій та світоглядні позиції людей із метою досягнення власних цілей організатора. В основі всіх ІПСО лежить маніпуляція свідомістю. Вищезазначена тема вже вийшла за межі наукових досліджень і розширила рамки публічної дискусії, що, своєю чергою, вимагає чіткої визначеності суті феномену маніпуляції, технологій її організації та результатів впливу. Під маніпулюванням зазвичай розуміють специфічну форму духовного впливу, що виражається як приховане, анонімне панування, здійснюване «ненасильницьким» способом. Проте дослідник В. Петрик зазначає, що запропоноване визначення вочевидь недосконале та вказує лише на одну характерну рису маніпулювання – непомітний вплив – і не дає відповіді на питання: хто здійснює маніпулювання, на кого спрямована ця форма духовного впливу і яка його мета (Petryk, Prysiazhnyuk, Kompantseva, Skulysh, Boyko & Ostroukhov, 2023, p. 10).

До російської ІПСО відноситься операція, яку низка авторів та дослідників умовно позначає, як «Потворне обличчя українського націоналізму» (Megel

& Yaremchuk, 2023, p. 7). Так, спецоперація охопила багатомільйонну аудиторію і була реалізована в різних сферах: політичній, культурній, науковій тощо. Одним із прикладів формування культурного контексту є російський військово-фантастичний фільм 2010 р. «Ми з майбутнього – 2». Фільм було оцінено низкою критиків як пропагандистський та антиукраїнський, проте це не завадило йому зібрати близько 8 млн доларів у прокаті (Megel & Yaremchuk, 2023, p. 7).

Також варто зазначити конфлікт у Грузії у 2008 р., де інформаційні кампанії відіграли ключову роль у формуванні громадської думки щодо легітимності дій сторін конфлікту. Даний конфлікт має глибоке коріння в історичних та політичних суперечностях, які продовжилися та набули нових форм після розпаду Радянського Союзу. Головною передумовою війни 2008 р. стала боротьба за контроль над Південною Осетією та Абхазією – двома регіонами, які прагнули незалежності від Грузії за підтримки росії. Невирішеність цих конфліктів і напруга між Грузією та росією призвели до військового протистояння у серпні 2008 р. Під час конфлікту Грузія використовувала інформаційні кампанії для мобілізації підтримки з боку міжнародних організацій та західних країн (зокрема, США та ЄС), формування національної ідентичності та мобілізації внутрішнього населення. Серед головних цілей інформаційної стратегії Грузії була міжнародна дипломатія, адже за допомогою інформаційних кампаній країна прагнула привернути увагу світових лідерів та міжнародних організацій до конфлікту.

Російська сторона також проводила масштабні інформаційні кампанії, спрямовані на виправдання своїх дій та дискредитацію Грузії. Основні аспекти російської стратегії включали пропаганду через традиційні медіа, дезінформацію та контроль інформаційного простору. Російські державні медіа активно поширювали наративи, що виправдовували військові дії росії як «захист» мирного населення Південної Осетії від т. зв. «грузинської агресії». Росія також намагалася контролювати доступ до інформації у регіоні, блокуючи або обмежуючи грузинські медіа.

Інформаційні кампанії мали значний вплив на міжнародну реакцію на конфлікт. Грузинські зусилля у поширенні своєї версії подій сприяли отриманню підтримки з боку західних країн, що проявилося у дипломатичних заявах, санкціях та гуманітарній допомозі. Водночас російська інформаційна кампанія хоча й була менш успішною на Заході, змогла консолідувати підтримку серед внутрішньої аудиторії та деяких союзників росії.

Одним із найяскравіших прикладів сучасної інформаційної війни є дії росії у контексті конфліктів в Україні, Сирії, а також утручання у вибори в різних країнах. Російські інформаційні атаки включають поширення дезінформації через контрольовані медіа та соціальні мережі, пропаганду через російськомовні ЗМІ, такі як RT та Sputnik, які транслюють на міжнародну аудиторію, кібератаки на урядові та приватні установи для підриву довіри до інститутів влади.

Іншим важливим прикладом є втручання в демократичні процеси через інформаційні атаки, зокрема під час виборів у США та країнах Європи. Це, зокрема, масове поширення фейкових новин у соціальних медіа для дискредитації кандидатів, кібератаки на виборчу інфраструктуру з метою підриву довіри до виборчих результатів, підтримка радикальних груп через онлайн-платформи, що сприяє поляризації суспільства.

Ключову роль у протидії інформаційним загрозам відіграє використання передових технологій, таких як штучний інтелект (ШІ), блокчейн та сучасні методи

кібербезпеки, що стало критично важливим для виявлення та запобігання цим атакам.

Штучний інтелект, зокрема машинне навчання та обробка природної мови (NLP), широко використовується для виявлення дезінформації та фейкових новин.

Основні аспекти включають:

– аналіз тексту та контенту: ШІ здатний аналізувати великі обсяги текстової інформації для виявлення відхилень від нормального паттерну, які можуть указувати на фейкові новини або маніпуляції;

– класифікація джерел: використання алгоритмів для визначення надійності джерел інформації, зокрема шляхом аналізу історії публікацій та поведінки користувачів;

– виявлення ботів: ШІ може ідентифікувати автоматизовані акаунти, які поширюють дезінформацію, шляхом аналізу їхньої поведінки та взаємодії з іншими користувачами.

Штучний інтелект також відіграє важливу роль у прогнозуванні та виявленні кіберзагроз. Зокрема, алгоритми ШІ використовуються для моніторингу мережевого трафіку та виявлення аномальної поведінки, що може свідчити про наявність кібератаки. Окрім цього, системи, керовані ШІ, можуть автоматично реагувати на загрози в режимі реального часу, запобігаючи розповсюдженню атак та мінімізуючи їхні наслідки.

Унікальні можливості для забезпечення прозорості та незмінності даних, що є важливим у контексті боротьби з дезінформацією, пропонує технологія блокчейну. Так, блокчейн дає змогу зберігати дані на децентралізованих платформах, що робить їх менш уразливими до маніпуляцій та цензури. Важливо, що одноразово записана в блокчейні інформація не може бути змінена без згоди більшості учасників мережі, що гарантує її достовірність і збереження.

Блокчейн-технології можуть використовуватися для верифікації автентичності контенту. Йдеться, зокрема, про верифікацію джерел (блокчейн дає змогу підтверджувати справжність джерел інформації, забезпечуючи їх прозорість та надійність) та захист інтелектуальної власності: за допомогою смарт-контрактів блокчейн може забезпечувати авторські права та запобігати несанкціонованому використанню контенту.

Одним із ключових підходів до кібернетичної безпеки є використання мультирівневого захисту. Серед них важливу роль відіграють автентифікація та авторизація – упровадження двофакторної автентифікації, біометричних даних та інших сучасних методів захисту доступу до інформаційних систем. Інший підхід – шифрування даних. Так, використання сучасних методів шифрування для захисту даних під час їх передачі та зберігання суттєво ускладнює їх перехоплення та розшифрування.

Поєднання штучного інтелекту, блокчейну та сучасних методів кібербезпеки може значно підвищити ефективність виявлення та запобігання інформаційним атакам. Інтеграція цих технологій дає змогу створити комплексні системи захисту, що забезпечують надійну верифікацію даних, виявлення загроз та їх нейтралізацію. Своєю чергою, використання штучного інтелекту для аналізу даних, що зберігаються у блокчейні, може забезпечити швидку адаптацію до нових загроз та розроблення нових методів захисту.

Ще один не менш важливий метод протидії – підвищення рівня медіаграмотності серед населення, зокрема інтеграція курсів із медіаграмотності в шкільну

та університетську програми, державні та громадські ініціативи, що навчають населення критично сприймати інформацію та розпізнавати фейки.

Нарешті, ефективна протидія інформаційним атакам потребує тісної міжнародної співпраці: створення міжнародних платформ для обміну даними про кібератаки та дезінформаційні кампанії, координацію міждержавних зусиль для протидії дезінформації та пропаганді на глобальному рівні.

У сучасному світі інформаційна війна стала невід'ємним складником гібридних конфліктів, що вимагає комплексного підходу до протидії її впливам. Гібридні конфлікти, які включають поєднання військових, економічних, дипломатичних та інформаційних методів, є однією з найбільш загрозливих форм сучасних збройних конфліктів. Інформаційна війна як елемент гібридного протистояння спрямована на маніпуляцію свідомістю людей, формування негативних стереотипів, деморалізацію населення та послаблення здатності держави до опору.

Передові технології, такі як штучний інтелект, блокчейн та сучасні методи кібернетичної безпеки, відіграють критично важливу роль у виявленні та запобіганні інформаційним атакам. Хоча кожна із цих технологій має свої сильні боки, найбільш ефективним є їх комплексне використання, що забезпечує багаторівневий захист від загроз. Подальші дослідження та розробки у цій сфері повинні бути спрямовані на інтеграцію цих технологій та їх адаптацію до змінних умов сучасного інформаційного простору.

Одним із ключових підходів до протидії інформаційним атакам є розроблення та впровадження законодавчих і регуляторних заходів. Це, зокрема, закони про кібербезпеку та захист персональних даних, мета яких – забезпечення безпеки інформаційних систем та захист особистої інформації громадян від несанкціонованого доступу.

На думку Ю. Когута, ефективний кіберзахист держави значною мірою забезпечує створення спеціалізованих кібервійськ, здатних відбивати атаки злочинців. Високий ступінь автоматизації управління та глобалізації інформаційних систем через інформаційно-телекомунікаційну мережу загального користування сприяє створенню глобального інформаційного суспільства (Kohut, 2023, p. 255).

Важливу роль відіграє регулювання діяльності ЗМІ та соціальних мереж, що передбачає встановлення правил для онлайн-платформ щодо верифікації інформації, запобігання поширенню фейків та маніпулятивного контенту.

Не менш важливі технічні рішення, серед яких чільне місце посідає кібербезпека – упровадження сучасних засобів захисту від кібератак, включаючи антивірусні програми, системи виявлення вторгнень та шифрування даних, та аналіз даних і штучний інтелект, зокрема використання алгоритмів для виявлення дезінформації, фейкових новин та інших форм маніпуляції у реальному часі.

Особлива роль належить освіті та підвищенню обізнаності населення щодо орієнтування в інформаційному просторі. Цей напрям передбачає розроблення навчальних програм із медіаграмотності в освітні програми для школярів та студентів, а також проведення інформаційних кампаній, спрямованих на підвищення обізнаності громадян щодо ризиків дезінформації та методів її виявлення.

Також варто пам'ятати, що інформаційні атаки часто мають транснаціональний характер, що робить міжнародну співпрацю необхідною для ефективної протидії. Основні аспекти цієї співпраці включають обмін інформацією, зокрема створення міжнародних платформ для обміну інформацією про кіберзагрози та інформаційні атаки, а також спільні операції, що передбачають координацію зусиль правоохоронних органів різних країн для запобігання та розслідування інформаційних атак.

Протидія інформаційним війнам є ключовим елементом стратегії безпеки в умовах гібридних конфліктів. Важливо усвідомлювати, що інформаційна безпека має стати пріоритетом для держави, а розвиток медіаграмотності та кібернетичної безпеки – невід'ємними складниками цього процесу. Лише комплексний підхід, що поєднує зусилля державних структур, медіа, громадянського суспільства та міжнародної спільноти, дасть змогу ефективно протидіяти загрозам інформаційної війни та забезпечити стабільність і безпеку в умовах гібридних конфліктів.

References [Список використаної літератури]

Bernays E. L. (1928). Propaganda. California, N.-Y.: University of California. [in English]. [Бернейс Е. Пропаганда. Каліфорнія, Університет Каліфорнії, 1928. 166 p. URL: https://babel.hathitrust.org/cgi/pt?id=uc1.$b21229&seq=8 (дата звернення: 28.08.2024)

Veselova, L. (2021) *Cyber security in conditions of hybrid war: administrative and legal foundations:* monograph. Odesa: Helvetica. [in Ukrainian]. [Веселова Л. Ю. Кібербезпека в умовах гібридної війни: адміністративно-правові засади : монографія. Одеса : Гельветика, 2021. 488 с.]

Vodolazka, K. (1999) *Model of the structure of the information space of the individual as an object of verbal influence: scientific and technical collection*. Kyiv: NNDC of Ukraine. [in Ukrainian]. [Водолазька К. В. Модель структури інформаційного простору особистості як об'єкта вербального впливу : науково-технічний збірник. Київ : ННДЦ України, 1999. 180 с.]

Kovalevska, T., Kondratenko, N., Kutuza, N., Porpulit, O., Kovalevska, A. (2009) *Advertising and PR in mass information space*: monograph. Odesa: Astroprint. [in Ukrainian]. [Реклама та PR у масово-інформаційному просторі : монографія / Т. Ю. Ковалевська та ін. Одеса : Астропринт, 2009. 248 с.]

Kohut, Y. (2023) *Hybrid war of a new type as a threat to the national security of states*. Kyiv: Consulting Company «SIDCON». [in Ukrainian]. [Когут Ю. І. Гібридна війна нового типу як загроза національній безпеці держав. Київ : Консалтингова компанія «СІДКОН», 2023. 348 с.]

Megel, A., Yaremchuk, M. (2023) *Enemies of IPSO. How to identify and resist: a guide*. Kyiv: SKIF. [in Ukrainian]. [Мегель А., Яремчук М. Ворожі ІПСО. Як визначити та протистояти : посібник. Київ : СКІФ, 2023. 96 с.]

Petryk, V., Hnatyuk, S., Chernenko, O., Gureev, V. (2021) *Modern technologies of neurolinguistic programming*: a study guide. Kyiv: Center for Educational Literature. [in Ukrainian]. [Петрик В. М., Гнатюк С. О., Черненко О. Є., Гуреєв В. О. Сучасні технології нейролінгвістичного програмування : навчальний посібник. Київ : Центр учбової літератури, 2021. 200 с.]

Petryk, V., Prysiazhnyuk, L., Kompantseva, L., Skulysh, E., Boyko, O., Ostroukhov, V. (2023). *Suggestive technologies of manipulative influence*: a study guide. Kyiv: SKIF. [in Ukrainian]. [Сугестивні технології маніпулятивного впливу : навчальний посібник / В. М. Петрик та ін. Київ : СКІФ, 2023. 248 с.]

Prybutko, P., Luk'yanets, I. (2007) *Informational influences: role in society and modern military conflicts*. Kyiv: PALIVODA A. S [in Ukrainian]. [Прибутько П. С., Лук'янець І.Б. Інформаційні впливи: роль у суспільстві та сучасних воєнних конфліктах. Київ : Паливода А. С., 2007. 252 с.]

Стаття надійшла до редакції 28.08.2024.

Popravka M. O.
Department of Political Science
Odesa I. I. Mechnikov National University
French blv. 24/26, Odesa, 65058, Ukraine

INFORMATION WARFARE IN THE CONTEXT OF HYBRID CONFLICT

Summary
Hybrid conflicts, which have become an integral part of modern geopolitical reality, significantly change the rules of warfare, making the informational component one of the most important aspects of the struggle for superiority. In the modern world, information wars have become a powerful tool of geopolitical influence and manipulation of

public consciousness and public opinion. Information war differs from traditional forms of war in that it is not limited to the physical destruction of the enemy, but is aimed at undermining morale, changing the political course, destabilizing the social situation or changing worldview. This makes it particularly effective in the context of hybrid conflicts, where physical confrontation may be minimal or absent.

The article examines the role of information warfare in the context of hybrid conflicts, where traditional military actions are supplemented by a complex of non-linear methods of influence, such as economic sanctions, political pressure, cyber attacks, disinformation campaigns and propaganda. Key strategies and methods of conducting information wars, their influence on public opinion, state institutions and international relations are analyzed. Special attention is paid to the study of examples from modern international practice, in particular, the role of information campaigns in conflicts in the post-Soviet space. Approaches to countering information attacks in the context of national security protection are also considered. In addition, the methods of identifying and neutralizing disinformation are analyzed, as well as measures to increase media literacy of the population as one of the important factors in countering the manipulation of public opinion. The role of state institutions, media and civil society in the fight against information attacks is considered.

The article examines both technical and social approaches used to protect society from manipulation and misinformation. Advanced technologies are analyzed, including artificial intelligence, blockchain, as well as cyber security methods for detecting and preventing information attacks. Strategic approaches contributing to effective response to new challenges of information wars are discussed.

Key words: information war, hybrid conflict, disinformation, propaganda, cyber operation.