УДК 316.6:659.9:004.7

В. С. Васищев **Є. В. Денисенко**

ТЕОРЕТИКО-МЕТОДОЛОГІЧНИЙ АНАЛІЗ ІННОВАЦІЙНИХ ФОРМ І МЕТОДІВ ВЕДЕННЯ ІНФОРМАЦІЙНОЇ БОРОТЬБИ: ВИКЛИКИ ТА ЗАГРОЗИ КІБЕРБЕЗПЕЦІ

Проведено аналіз інноваційних форм та методів ведення інформаційної боротьби як складової гібридної війни у призмі кібербезпеки. Розглянуто етапи гібридного протистояння, зокрема детально досліджено етап інноваційної агресії. Розкрито ключові технологічні аспекти інформаційної онлайн-мережевої війни.

***Ключові слова**: інноваційна боротьба, гібридна війна, кібербезпека, кіберпростір, мережевий онлайн-простір, інформаційна онлайн-мережева війна.*

Постановка проблеми. Приклади інформаційного впливу на широку аудиторію значною мірою можна простежити протягом усієї історії суспільства, та у XX ст. він постає як один з основних видів протистояння разом із зміцненням засобів масової комунікації, їхнім розширенням та урізноманітненням. З початком повномасштабної та відкритої агресії з боку російської федерації актуальним питанням стало удосконалення системи забезпечення національної безпеки України. При цьому забезпечення кібербезпеки є одним із пріоритетів у системі національної безпеки. Реалізація зазначеного пріоритету має здійснюватися шляхом посилення спроможностей національної системи кібербезпеки для протидії кіберзагрозам у сучасному безпековому середовищі.

Стратегією кіберпезпеки України [9], затвердженою Указом Президента України від 26 серпня 2021 р. № 447/2021, зазначено, що питома вага кіберзагроз зростає, і ця тенденція в міру розвитку інформаційних технологій та їх конвергенції з технологіями штучного інтелекту в найближче десятиліття посилюватиметься. Зростання такого впливу на функціонування структур управління як національних, так і транснаціональних формує нову безпекову ситуацію. Між світовими центрами сили відбувається поділ сфер впливу в кіберпросторі, посилюється їх прагнення внаслідок цього забезпечити реалізацію власних геополітичних інтересів.

Аналіз останніх досліджень і публікацій. На теперішній час є достатньо наукових публікацій з проблематики інформаційно-психологічного протистояння, проведення інформаційно-психологічних операцій, становлення світового кіберпростору та забезпечення кібербезпеки держави. Ці питання досліджували такі науковці, як: О. Данильян, О. Дзьобань, І. Жаровська, О. Курбан, А. Шумка, Ю. Радковець, Л. Кобиляцький, А. Кожаринова, Г. Пєвцов та ін. Однак, на нашу думку, наразі у фаховій літературі ще недостатньо враховано потенціал сучасних інноваційних форм і методів інформаційної боротьби як засобів гібридної агресії проти України у кіберпросторі.

Метою статті є проведення теоретико-методологічного аналізу інноваційних форм та методів інформаційної боротьби та визначення їхніх спроможностей у сфері кібербезпеки України.

Виклад основного матеріалу. Людство перебуває на історичному роздоріжжі, за якого новітні технології можуть нести як позитивну, конструктивну тенденцію, так і деструктивну. «Індустріальна епоха висунула на перший план протиборство держав, а у XX ст. – ідеологічних і політичних систем. Складові перемоги стали формуватися з комплексу економічних, морально-політичних та технологічних факторів. Поява мікроелектроніки, котра відкрила можливості для масової комунікації, в поєднанні з інформаційними технологіями породила мережеві інформаційні структури, а разом з ними і концепцію інформаційно-мережевих війн» [10]. Особливістю є не тільки те, що вплив здійснюється з використанням новітніх засобів, а й те, що це непідконтрольний ресурс, який

дуже слабо піддається правовій регламентації, тому активно застосовує неправдиву, перекручену інформацію як засіб маніпуляції свідомістю [2].

Світ проходить через цифрову трансформацію — процес зміни бізнесу через технології. Проте змінюється не тільки бізнес. Змінюється те, що століттями залишалося незмінним — війна. Певна річ, замаскована пропаганда була в усі часи. Наприклад, у 40-х рр. XX ст. Сполучені Штати вигадали Капітана Америку, щоб підвищити репутацію армії та стимулювати молодь охочіше вступати до збройних сил. А ще раніше – під час Першої світової війни – Британія на повну використовувала підроблені сюжети про звірства німецьких солдатів, наприклад, про те, що вони переробляють трупи співвітчизників на корм свиням.

Проте у зв'язку з тим, що нині майже у кожного жителя планети є доступ до інтернету, можливостей впливати на наші думки та дії набагато більше. Інформаційні агресори тепер не просто розповідають казки про противника, вони формують інше бачення світу, підміняють реальність настільки продуманою містифікацією, що відрізнити її від правди майже неможливо [6].

Наприкінці XX – початку XXI ст. світ отримав нову форму ведення протистоянь – гібридну війну. Однією з провідних країн, яка активно застосовує сьогодні інструменти такої війни, є Росія. Базові складові російської стратегії і тактики сучасної гібридної війни були сформульовані в 2013 р. начальником Генерального штабу ЗС РФ В. Герасимовим [8].

Послідовними, типовими складовими етапами гібридної війни було визначено [5] такі:

– інноваційна агресія (кібервійна, економічний тиск, інформаційно-психологічні атаки та ін.);

– застосування нерегулярних збройних формувань або приватних армій (повстанський, партизанський рух, тероризм);

– офіційні військові дії або демонстрація сили (ідентифікована уніформа, зброя, офіційне визнання участі в конфлікті).

Відповідно до визначеної тематики, увагу авторів статті зосереджено на розкритті питання інноваційної агресії, а вірніше – кіберпростору.

Етап інноваційної агресії іноді може бути розтягненим на роки і десятиліття. Класичним прикладом цьому може бути й агресія росії проти України. Типовими ознаками її були газові і торговельні війни, намагання захопити стратегічні підприємства, поширити вплив власних ЗМІ, тиск на політичному рівні в питаннях захисту прав російськомовного населення, просуванні елементів російської культури (кіно, література, твори мистецтва тощо). Саме на цьому етапі відбувається закладання конкретних масових психологічних установок, які згодом, у моменти переходу конфлікту до відкритої фази, використовують для послаблення сторони, проти якої здійснюється агресія.

Аналіз подій, що відбуваються протягом останнього десятиріччя у протистоянні між росією та Україною, дає можливість стверджувати, що російська федерація активно застосовувала та продовжує застосовувати медіапростір з метою впливу на свідомість і підсвідомість наших громадян за такими основними напрямками [1]:

– забезпечення прийняття військово-політичним керівництвом України бажаних для росії рішень і спонукання до виконання нав'язуваних політичних, економічних і воєнних кроків;

– підрив легітимності української політичної влади;

– підрив міжнародного авторитету України, створення її негативного іміджу з метою недопущення широкомасштабної військової, економічної та фінансової допомоги європейських країн та США;

– дестабілізація ситуації в цілому в Україні, провокування політичних протестів, соціальних конфліктів, підрив морально-психологічного стану українського населення;

– підрив обороноздатності України та боєздатності її Збройних Сил;

– підтримка дій внутрішніх деструктивних сил і колаборантів, спрямованих на знищення чи завдання шкоди українській державі і суспільству, у тому числі шляхом корумпування влади й політичної еліти;

– створення негативного образу українця шляхом розповсюдження фейків про «неонацизм», «бандерівців», діаметрально протилежне істинним подіям висвітлення військових злочинів російської армії;

– заміна соціально-культурної ідентичності всього населення України або його частини, нав'язування сумнівів щодо національних цінностей та засад державотворення.

Також фахівцями згруповано ознаки, за якими на сьогодні проявляється така боротьба [10]:

– монополізація газет, журналів, радіо і телебачення, а також засобів зв'язку спеціалізованими корпораціями;

– пряме підпорядкування засобів інформації та зв'язку олігархічному капіталу;

– відкрите втручання державних органів у сферу ЗМІ, заборона або позазаконне обмеження свободи слова;

– панування порівняно невеликої кількості ЗМІ й інформаційних агентств на світовому ринку новин;

– монополізація інформаційного простору країни або регіону;

– поглиблення диспропорцій у забезпеченості засобами інформації та зв'язку між розвиненими державами і країнами, що розвиваються;

– використання друкованою пресою, радіо, телебаченням та інформаційними агентствами розвинених країн інформаційного забезпечення власної внутрішньої та зовнішньої політики на теренах інших країн;

– публікація низки матеріалів, спрямованих на дискредитування певної політичної сили, заходу, політики; створення негативного іміджу політичної сили, руху, державного діяча, значного заходу в країні – об'єкті інформаційної експансії.

Слід зауважити, що головним завданням мережевих онлайн-проєктів у межах гібридної війни є створення певної віртуальної реальності (симулякри), що формує необхідне для атакуючої сторони бачення ситуації конкретними цільовими групами, які є об'єктами інформаційно-психологічної агресії. При цьому головною метою такої діяльності є забезпечення сприятливих умов для реалізації атакуючих дій у режимі офлайн, на економічному, військовому, політичному полях або одночасно в усіх площинах. Вирішення зазначених питань можливе лише за умови інтегрованого підходу – поєднання сучасних технічних комунікацій та психотехнологій. При цьому тривалість дії та глибина ударного ефекту залежать від часу, впродовж якого здійснюється обробка свідомості цільових груп, та потужності тиску. Роль і значення в цих процесах соціальних онлайн-мереж важко переоцінити.

За аналогією, технології web 2.0 в цьому контексті можна визначити як високоточну зброю, що може поцілити не просто в певні цільові групи, але і в конкретних її представників, чітко визначених персоналій. Така адресність та, за необхідності, вибірковість дає можливість досягати максимального ефекту із оптимізацією витрат у плані часу, інтелектуальних та матеріально-технічних ресурсів [5].

Одним з базових напрямків роботи в межах інформаційної війни в соціальних онлайн-мережах є тематичні проєкти. Останні мають монотематичне спрямування, гнучку схему управління та принципи і схеми розбудови комунікацій із відповідними, чітко визначеними цільовими групами.

За теоретичним визначенням «проєкт» – це сукупність дій та завдань, що внаслідок їх унікальності й неповторності має такі відмінні ознаки [3]:

– чіткі цілі, що досягаються одночасним виконанням певних технічних, технологічних та інших вимог;

– внутрішні та зовнішні взаємозв'язки завдань, робіт, операцій і ресурсів, що потребують чіткої координації в процесі реалізації проєкту;

– визначені терміни початку й завершення проєкту та обмеженість ресурсів;

– визначений ступінь унікальності проєкту та умов його здійснення.

За складністю визначаються [3]:

– монопроєкти – окремі конкретні проєкти чітко визначеної орієнтації та масштабу; припускають певні спрощення щодо проєктування та реалізації, формування команди проєкту тощо;

– мультипроєкти – комплексні проєкти, які складаються з монопроєктів;

– мегапроєкти – комплексні проєкти, які охоплюють окремі регіони, сектори суспільства, економіки; складаються з моно- і мультипроєктів, об'єднаних однією метою.

У контексті функціонування мережевого онлайн-простору як засіб ведення інформаційної війни може використовуватися будь-який формат і тематика проєктів. Головна вимога до таких проєктів – наявність прямого доступу до конкретних цільових груп, а також можливість здійснення прямого або опосередкованого впливу та безперешкодного функціонування [5].

Будь-яка ефективна інформаційна атака починається з латентної фази – прихованого проникнення в інформаційне поле противника з метою дослідження середовища, апробації певних ідей та потенційного ефекту їх застосування, а також для створення і закріплення власних інформаційних майданчиків для подальшої агресії.

Найкращим інструментом для проникнення на вороже інформаційне поле є т. зв. медіавіруси – інформаційні носії (події, скандали, чутки, діяльність організацій та окремих осіб), що несуть у прихованому вигляді завуальовані ідеї та меседжі.

Зазвичай медіавіруси можуть поширюватися у вигляді мемів та лолів – окремих семіотичних фрагментів [4].

Найбільш вдалою формою камуфляжу для медіавірусів є події, винаходи, інноваційні технології, наукові теорії, філософські системи та культурологічні концепції. Саме за допомогою таких форматів простіше за все здійснювати проникнення в певне інформаційне середовище, не викликаючи особливих підозр [5].

Сучасний розвиток медіа та онлайн-середовища вносить певні корективи в наше життя. Поступово за норму сприймаються нові форми взаємин між об'єктами та суб'єктами соціуму в різних його сферах: економічних, політичних, соціальних тощо. Не винятком є й інформаційно-психологічне протистояння. Однією з форм такого протистояння є ***інформаційна онлайн-мережева війна***, під якою слід розуміти комплекс інформаційних впливів між соціальними системами (групами), що орієнтовані на отримання певних переваг у економічних, військових, політичних, культурних та громадських протистояннях.

У своїй основі інформаційна онлайн-мережева війна має три ключові технологічні аспекти: хай-тек, хай-х'юм та хай-сенсоро. Кожен з цих аспектів має власні технології, які формують профільні напрямки дослідження та практичної роботи [7].

Якщо коротко охарактеризувати ці технології, то хай-тек – сучасні високі технології цифрових комунікацій, що в основі мають системи телебачення, радіо, інтернету, месенджерів, стільникового, супутникового та інших видів сучасного зв'язку та наявні на таких гаджетах, як стаціонарні комп'ютерні пристрої, планшети, смартфони, пристрої індивідуального та групового зв'язку.

До цього аспекту відносять класичне телебачення в ефірному та цифровому форматах; радіо як класичне електронне ЗМІ розглядається у традиційному аналоговому (AM, FM) та цифровому форматах; інтернет — як всесвітня система об'єднаних комп'ютерних мереж для зберігання та транслювання інформації [5].

При цьому інтернет-телебачення визначається як телебачення міжмережевого протоколу (online TV) – система, що базується на двосторонньому цифровому передаванні телевізійного сигналу через інтернет-з'єднання за допомогою широкосмугового підключення.

Інтернет-радіо (або веб-радіо) визначають як групу технологій трансляції потокових аудіоданих через мережу Інтернет для здійснення широкої трансляції програм. Також терміном «інтернет-радіо» визначають радіостанцію, що використовує для трансляції технологію потокового віщання у глобальній мережі Інтернет.

Месенджери – мережі миттєвого з'єднання. Типовими прикладами таких технологій є WhatsApp, Facebook Chat, Hangouts (Google), Skype, LINE, WeChat, Viber, Kik, Snapchat, ICQ, Telegram.

Хай-х'юм в інформаційній онлайн-мережевій війні – це сучасні високі соціально-гуманітарні технології створення, зберігання, розповсюдження та пошуку інформації. До них належать такі технології, як:

1. SEO (Search Engine Optimization) – комплекс заходів із пошукової оптимізації, орієнтований на підвищення позиції веб-сайту в пошукових системах.
2. SMM (Social Media Marketing) – комплекс заходів із просування персонального акаунта або окремого контенту в соціальних мережах.
3. Таргетинг – рекламний механізм, що дає можливість виокремити з наявної аудиторії лише певну її частину, яка відповідає потрібним критеріям, і показати саме їй рекламне повідомлення.
4. Контекстна реклама – метод розміщення інформації, що орієнтована на зміст інтернет-ресурсу, представлена у вигляді банера чи текстового повідомлення.
5. Медіавіруси – інформаційні носії (події, скандали, чутки, діяльність організацій та окремих осіб), що несуть у прихованому вигляді завуальовані ідеї та меседжі.

Хай-сенсоро в інформаційній онлайн-мережевій війні – сучасні високі психотехнології, що дають можливість регулювати та керувати соціальними комунікаційними процесами на рівні соціальних груп та окремих індивідуумів. Типовими в цьому аспекті є соціальна психологія, прикладний психоаналіз та нейролінгвістичне програмування [5].

Висновки

На підставі проведеного дослідження можна дійти таких висновків. У системі сучасних економічних, політичних та військових протистоянь інформаційні війни в кіберпросторі посідають провідне місце як один з ключових супроводжувальних процесів. Головне призначення таких процесів – шляхом концентрації зусиль на певних ключових ланках забезпечувати суттєві переваги в межах комплексного протиборства сторін. Інформаційна зброя такого типу здатна знищувати чи, як мінімум, блокувати системи координації, поширення інформації та інші відповідні управлінські процеси, а також перешкоджати роботі відповідних центрів керування. Спектр інструментів при цьому доволі широкий – від кібератак до організації акцій протесту, терористичних актів та організованого збройного опору.

Автори вважають, що подальшим напрямом дослідження має бути застосування та впровадження інноваційних форм інформаційної боротьби в систему протидії негативному інформаційно-психологічному впливу на особовий склад сил безпеки України.

Перелік джерел посилання

1. Данильян О. Г., Дзьобань О. П. Інформаційна війна у медіапросторі сучасного суспільства. *Вісник НЮУ імені Ярослава Мудрого. Філософія, філософія права, політологія, соціологія*. Харків, 2022. № 3 (54). С. 11–29.

2. Жаровська І., Ортинська Н. Інформаційна війна як сучасне глобалізаційне явище. *Вісник Національного університету «Львівська політехніка». Юридичні науки*. Львів, 2020. Т. 7. № 2. С. 56–61.

3. Кобиляцький Л. С. Управління проектами : навч. посіб. Київ : МАУП, 2002. 200 с.

4. Курбан О. В. Медіавіруси та їх використання як інформаційної зброї. *Наукові записки [Української академії друкарства]*. 2016. № 1. С. 267–271. URL: http://nbuv.gov.ua/UJRN/Nz_2016_1_35 (дата звернення: 08.06.2023).

5. Курбан О. В. Сучасні інформаційні війни в мережевому он-лайн просторі : навч посіб. Київ : ВІКНУ, 2016. 286 с.

6. Найбільш вражаючі приклади інформаційних війн 21 століття // *BusinessViews*. URL: https://businessviews.com.ua/ru/studies/id/najbilsh-vrazhajuchi-prikladi-informacijnih-vijn-21-stolittja-2037/ (дата звернення: 12.06.2023).

7. Пєвцов Г. В., Залкін С. В., Сідченко С. О., Хударковський К. І. Інформаційно-психологічні операції Російської Федерації в Україні: моделі впливу та напрями протидії. URL: https://www.ukrmilitary.com/2015/12/ipo-rf-in-ukraine.html (дата звернення: 22.06.2022).

8. Радковець Ю. Гібридна політика сучасної Росії. *Урядовий кур'єр*. URL: http://ukurier.gov.ua/uk/articles/gibridna-politika-suchasnoyi-rosiyi/ (дата звернення: 12.06.2023).

9. Стратегія кібербезпеки України: безпечний кіберпростір – запорука успішного розвитку країни : Указ Президента України від 26.08.2021 р. № 447/2021. URL: https://zakon.rada.gov.ua/laws/show/447/2021#n12 (дата звернення: 09.06.2023).

10. Шумка А. В., Черник П. П. Інформаційно-мережева війна – нова форма міждержавного протиборства початку XXI ст. *Військово-науковий вісник*. Львів, 2013. Вип. 19. С. 243–255.

Стаття надійшла до редакції 30.06.2023 р.

UDC 316.6:659.9:004.7

V. Vasyshchev, Ye. Denysenko

THEORETICAL AND METHODOLOGICAL ANALYSIS OF INNOVATIVE FORMS AND METHODS OF INFORMATION WARFARE: CHALLENGES AND THREATS TO CYBER SECURITY

With the beginning of full-scale and open aggression on the part of the Russian Federation, improving the system of ensuring Ukraine's national security became an urgent issue. At the same time, ensuring cyber

security is one of the priorities in the national security system. The implementation of the specified priority should be carried out by strengthening the capabilities of the national cyber security system to counter cyber threats in the modern security environment.

Since now almost every inhabitant of the planet has access to the Internet, there are many more opportunities to influence our thoughts and actions. Information aggressors now do not just tell tales about the enemy, they form a different vision of the world, replace reality with such a well-thought-out hoax that it is almost impossible to distinguish it from the truth.

At the end of the 20th beginning of the 21st century. the world received a new form of confrontation – a hybrid war. One of the leading countries that actively uses the tools of hybrid warfare today is Russia. The basic components of the Russian strategy and tactics of modern hybrid warfare were formulated in 2013.

In the context of the functioning of the online network space, as a means of conducting information warfare, any format and topic of projects can be used.

The best tool for penetrating the enemy's information field is the so-called media viruses - information carriers (events, scandals, rumors, activities of organizations and individuals) that carry veiled ideas and messages in a hidden form.

The modern development of the media and online environment makes certain adjustments to our lives. Gradually, new forms of relations between objects and subjects of society in its various spheres: economic, political, social and other are perceived as the norm. Informational and psychological confrontation is no exception. One of the forms of such confrontation is informational online network war, which should be understood as a complex of informational influences between social systems (groups) aimed at obtaining certain advantages in economic, military, political, cultural and public confrontations.

Keywords: *innovative struggle, hybrid war, cyber security, cyberspace, online network space, informational online network war.*

Васищев Володимир Сергійович – кандидат педагогічних наук, доцент, начальник кафедри військово-соціального та психологічного забезпечення Національної академії Національної гвардії України
https://orcid.org/0000-0003-2630-6377

Денисенко Євген Володимирович – кандидат педагогічних наук, начальник відділу організації заочного та дистанційного навчання Національної академії Національної гвардії України
https://orcid.org/0000-0003-3776-0823