УДК 316.343.3
DOI https://doi.org/10.32689/maup.it.2024.1.12

Світлана ПЕТРЕНКО
науковий співробітник науково-організаційного центру
Національної академії Служби безпеки України
***ORCID:** 0000-0003-1219-2401*

Наталія НАЗАРЕНКО
старший викладач кафедри романо-германських мов
навчально-наукового гуманітарного інституту
Національної академії Служби безпеки України
***ORCID:** 0000-0001-6353-4761*

ПРАКТИЧНІ АСПЕКТИ ВЕДЕННЯ ІНФОРМАЦІЙНОЇ ВІЙНИ В ОН-ЛАЙН ПРОСТОРІ

***Анотація**. У статті розглядається інформаційна війна в он-лайн просторі як один з аспектів сучасного життя. Інформаційна війна, яка активно проводилася ворожою російською федерацією впродовж багатьох років в інформаційному просторі не лише України, а й багатьох країн світу, набула значних масштабів з повномасштабним вторгнення. Вивчення цієї проблеми є **актуальним**, і потребує нових підходів, що і визначає **новизну** представленої роботи.*

***Метою** роботи є аналіз способів, якими інформація може бути використана як зброя для досягнення різних цілей: політичних, економічних та соціальних. В статті акцентовано увагу на тому, що основна мета інформаційної війни – не фізичне знищення людей, а руйнування їх як соціальної групи.*

***Методологія.** Проаналізувавши численні медіа ресурси, в статті розглядаються ключові підходи до ведення інформаційної війни в он-лайн просторі, такі як створення та поширення дезінформації, використання соціальних медіа, кібератаки та пропаганда. Зокрема, підкреслено важливість критичного мислення та перевірки фактів, у боротьбі з дезінформацією. Стаття також описує способи використання інформації як зброї в он-лайн просторі, акцентуючи увагу на фабриках тролів, ботах, соціальних медіа та кібератаках. Обгунтовано, як ці елементи можуть бути використані для маніпулювання громадською думкою, формування соціальних рухів та впливу на політичні, соціальні та культурні відносини. Зокрема, розглядається вплив кібершпигунства та хакерських атак на різні об'єкти, включно з урядовими установами, корпоративними мережами та персональними комп'ютерами громадян. У контексті військового конфлікту між Україною та росією хакерські атаки та кібершпигунство стали ключовими інструментами ведення війни. Російські зловмисники активно використовують ці методи для атак на українські інформаційні системи, з метою викрадення або знищення конфіденційної інформації. Інформаційна війна переважно спрямована на порушення обміну достовірною інформацією та створення паніки серед українців. Російська пропаганда активно поширює маніпулятивні новини та використовує гіперболізацію, для негативного висвітлення діяльності українських військових та переселенців.*

***Висновки.** В статті наголошується на необхідності розробки, удосконалення ефективних стратегії захисту від кібератак, а саме: використання надійного програмного забезпечення, регулярне оновлення систем, резервне копіювання даних та підвищення обізнаності населення щодо безпеки і інформаційної гігієни. Автори статті наголошують на необхідності збалансованого підходу до захисту національної безпеки та дотримання основних прав людини, а також підкреслюють важливість створення ефективних засобів для боротьби з кіберзагрозами.*

***Ключові слова:** кібератака, онлайн простір, інформаційна війна, медіаманіпуляція, дезінформація, пропаганда.*

Svitlana PETRENKO, Natalia NAZARENKO. PRACTICAL ASPECTS OF INFORMATION WARFARE IN ONLINE DOMAIN

***Abstract.** The given article studies information warfare in the online domain as one of the aspects of contemporary life. Information warfare, which has been carried out by the hostile russian federation for a long time not only in the information space of Ukraine, but other countries all over the world, got a full swing with the full-scale invasion. Studying this problem from a new perspective is **crucial**, which defines the **novelty** of the given work*

***The aim** of the article is to analyse the ways of using information as a weapon to achieve diverse objectives, including political, economic and social. It emphases that the primary goal of information warfare is not the physical destruction of individuals, but the dismantling of their social cohesion.*

***Metodology.** Having analysed numerous media sources, there have been revealed the main approaches to conducting information warfare in the online domain, such as the creation and dissemination of disinformation, the use of social media, cyberattacks, and propaganda. The article emphasizes the significance of critical thinking and fact-checking in combating misinformation. It also describes the use of information as the information warfare weapon, focusing on troll factories, bots, social media, and cyberattacks, and how they can be used to manipulate public opinion, encourage social movements, and influence political, social and cultural relations in the society. The article considers the impact of cyber espionage and hacker attacks on various targets, particularly governmental institutions, corporate networks, and personal computers of ordinary users. In the context russian-Ukrainian war hacker attacks and cyber espionage have become pivotal tools of warfare. Russian malicious actors actively employ these methods to target Ukrainian information systems to steal or destroy confidential information. The main aim of information warfare predominantly is to disrupt the exchange of reliable information and induce*

panic among the Ukrainians. Russian propaganda actively disseminates manipulative news and employs hyperboles to show Ukrainian military personnel and displaced persons in a negative light.

Conclusions. *The article focuses on necessity to develop and improve efficient strategies for dealing with cyberattacks, such as the use of robust software, regular system updates, data backup and raise of public awareness about information security and hygiene. The authors of the article call for a balanced approach to ensuring national security and preserving fundamental human rights, as well as creating effective ways to resist various cyber threats.*

Key words: *cyberattack, online domain, information warfare, media manipulation, disinformation, propaganda.*

Постановка проблеми. У сучасному світі, де інформація є ключовим ресурсом, інформаційна війна стає все більш актуальною. Ця проблема набуває особливого значення в контексті повномасштабного вторгнення росії в Україну, де інформаційні війни в он-лайн-просторі стають важливим фронтом боротьби.

Інформаційна війна в он-лайн-просторі включає в себе різноманітні тактики та стратегії, які використовуються для маніпулювання громадською думкою, формування настрою та впливу на політичні процеси. Згадані тактики та стратегії можуть включати в себе все: від пропаганди та дезінформації до кібератак та використання соціальних медіа для поширення певних повідомлень або ідей.

Аналіз останніх досліджень і публікацій. Питання інформаційного впливу, інформаційних війн, їх стратегій та методів широко висвітлюються в наукових роботах як вітчизняних так і закордонних науковців, зокрема О. В. Курбана, В. І. Башманівського, Н. М. Шульської, Д. М. Солоденка та інших. Але, зважаючи на стрімкий розвиток інформаційних технологій та широке використання інформаційного простору, ця проблема не втрачає своєї актуальності, а набуває нових образів і характеристик, що і визначає **актуальність** цього дослідження.

Метою дослідження є аналіз практичних аспектів ведення інформаційної війни в он-лайн просторі.

Виклад основного матеріалу. Інформаційна війна в он-лайн просторі стала важливим аспектом сучасного життя. Це поле, де інформація використовується як зброя для досягнення політичних, економічних або соціальних цілей.

Он-лайн простір – це віртуальне середовище, у якому люди взаємодіють й обмінюються інформацією. Він включає в себе соціальні медіа, веб-сайти, електронну пошту та інші платформи.

Інформаційна війна – це сучасний спосіб беззбройного конфлікту, який набирає шалених обертів, і її наслідки є загрозливими та непередбачуваними . Її основна мета – не фізичне знищення людей, а руйнування їх як соціальної групи. Таким чином, людство почало використовувати переваги прогресу в зловмисних цілях – проведенням інформаційних воєн, тобто поширення інформації з метою формування потрібних думок, настроїв та системи поглядів щодо певних питань, подій або людей на користь організатора конкретної інформаційної або пропагандистської кампанії. Основне завдання такої діяльності – це маніпулювання масами, тобто внесення потрібних ідей та поглядів у свідомість ворога, дезорієнтація та дезінформація цільової аудиторії, залякування власного народу образом ворога та створення почуття страху у супротивника, пропагуючи своєю могутністю.

Швидкість проведення інформаційної кампанії – це запорука успіху інформаційної війни, оскільки вона впливає на здатність ворога швидко та оперативно приймати рішення, реагувати на ситуації та вести війну на реальному полі бою. Вдала інформаційна кампанія проти ворога призводить до прийняття ним помилкових рішень і забезпечує невиконання запланованих завдань [3, с. 70].

О. В. Курбан виділяє наступні аспекти ведення інформаційної війни в он-лайн просторі :

– створення та поширення дезінформації для введення в оману людей або для створення певного враження;

– використання соціальних медіа для маніпулювання громадською думкою або для створення соціального руху;

– кібератаки для збору інформації, пошкодження інфраструктури або зламу систем безпеки;

– пропаганда для формування певного враження або впливу на громадську думку або для підтримки певної політичної агенди або ідеології [7].

Генерування дезінформації відіграє центральну роль в контексті інформаційної війни. Дезінформація, як правило, використовується для маніпулювання публічною свідомістю та формування специфічного сприйняття. Після генерування дезінформації наступним етапом є її дисемінація (з англ. «*dissemination*» – розповсюдження), яка здійснюється через різні канали, такі як соціальні медіа, веб-сайти, блоги, форуми тощо. Її мета полягає в тому, щоб донести цю інформацію до якомога більшої аудиторії.

Дезінформація може мати значний вплив на громадську думку та поведінку людей. Вона може використовуватися для формування певного враження, маніпулювання громадською думкою або навіть впливу на різні соціально-політичні події, такі як результати соцопитувань, вибори тощо.

Важливо пам'ятати, що дезінформація – це потужний інструмент, який може бути використаний для маніпулювання громадською думкою та формування певного поглядів, настроїв в суспільстві. Тому важливо завжди бути насторожі та критично ставитися до отриманої інформації [5]. Боротьба з дезінформацією вимагає, в першу чергу, критичного мислення та ретельної перевірки фактів, достовірності джерел, порівняння інформації, що надається іншими джерелами, та пошук офіційних або незалежних джерел перевірки фактів.

Використання соціальних медіа в інформаційній війні відіграє вирішальну роль, оскільки ці платформи служать потужними каналами для дисемінації інформації. Вони можуть бути використані для маніпулювання громадською думкою, шляхом поширення дезінформації, пропаганди або інших форм маніпулятивного контенту за допомогою ботів, тролів або інших автоматизованих засобів для поширення інформації, які підтримують певну агенду або враження [9]. Фабрики тролів представляють собою організації, де працівники створюють коментарі в Інтернеті, відповідно до завдань замовника, використовуючи фальшиві профілі в соціальних мережах. Основними характеристиками таких тролінг-провокацій є конфіденційність, маскування, тіньова позиція та безкарність. По відношенню до цих провокацій практично немає ефективних методів протидії, крім блокування форумів та обмеження можливості коментувати і поширювати далі інформацію. Боти – це програми, які автоматично відправляють повідомлення, особливо відгуки на появу конкретного ключового слова. Однак проблема полягає в тому, що одна людина може управляти десятками ботів одночасно, і це ускладнює їх виявлення та заборону. Принцип роботи ботів можна описати так: спершу троль розміщує пост, велика кількість інших ботів починає виражати вподобання, коментувати та репостити його. Алгоритм соціальної мережі реєструє – це як зацікавленість реальних користувачів у даному пості. У результаті він потрапляє в стрічки вже не ботів, а справжніх людей. Якщо пост вдалий, його розповсюджують далі звичайні користувачі, а потім його можуть використати і журналісти [2, с. 116-117].

Соціальні медіа також можуть бути використані для створення або підтримки соціальних рухів. З допомогою хештегів, мемів або інших форм вірального контенту відбувається мобілізації аудиторії навколо певної проблеми або агенди. Використання певних алгоритмів для визначення інтересів, переглядів або поведінки користувачів дозволяє соціальним медіа точно визначити конкретні цільові групи, що забезпечує ефективне поширення інформації. Соціальні медіа також надають можливість моніторити та аналізувати реакцію аудиторії на поширену інформацію, шляхом відслідковування таких метрик, як кількість переглядів, вподобань, коментарів або репостів. Важливо пам'ятати, що використання соціальних медіа в інформаційній війні вимагає глибокого розуміння цих платформ та їх динаміки, що передбачає знання того, як інформація поширюється в цих мережах, як вона сприймається користувачами, та як вона може впливати на громадську думку та поведінку [9].

Одним з найдієвіших методів інформаційної війни є кібератаки, оскільки вони спрямовані на збір інформації, ураження інфраструктури або зламу систем безпеки. Кіберзлочинці використовують цілий арсенал засобів для досягнення своїх цілей, а саме фішинг, DDoS-атаки, віруси, трояни та інше, для несанкціонованого доступу до систем, крадіжки даних, знищення або зміни інформації, а також перешкоджання нормальному функціонуванню мереж. Ці атаки можуть мати значні наслідки, такі як порушення конфіденційності, втрату даних, фінансові втрати та підрив репутації [8]. У контексті війни України з росією, хакерські атаки та кібершпигунство стають ключовими інструментами ведення війни. Російські зловмисники активно використовують ці методи для атак на українські інформаційні системи, метою яких є викрадення або знищення конфіденційної інформації. Хакерські атаки переважно спрямовані на урядові установи, корпоративні мережі, а також персональні комп'ютери та мобільні пристрої громадян України. Кібершпигунство, з іншого боку, зосереджується на отриманні доступу до конфіденційних даних або слідкуванні за діями користувачів за допомогою шпигунського ПЗ, фішингу, соціальної інженерії та інших тактик для отримання доступу до приватної інформації або для слідкування за діями користувачів. Сучасна війна набула нових рис, оскільки агресор прагне не лише завдати конкретних втрат противнику на полі бою, але й, вдаючись до засобів інформаційної війни, суттєво вплинути на поширення достовірної інформації, на механізми прийняття важливих державних рішень, а також викликати паніку серед українців, створити у населення відчуття страху та дезорієнтації, спонукати його до швидкої капітуляції. Завдання полягає в тому, щоб громадяни думали про втечу, витрачаючи свій час на поширення фейкових повідомлень, замість надання реальної допомоги війську та своїй державі [1, с. 274].

Пропаганда в інформаційній війні є стратегічним інструментом, що використовується для формування специфічного сприйняття реальності та впливу на громадську думку через поширення інформації, яка підтримує певну політичну агенду або ідеологію. Пропаганда широко використовується для маніпулювання громадською свідомістю, формування соціальних настроїв і рухів, а також для зміни

або підтримки певних політичних, соціальних або культурних відносин. Це вимагає глибокого розуміння психології мас, медіа-ландшафту та динаміки соціальних медіа [7].

Російські засоби пропаганди дуже активно поширюють маніпулятивні новини на різні теми, але здебільшого вони стосуються українських військових та наших переселенців із територій, де ведуться активні бойові дії. Кремлівські ЗМІ у своїх текстах намагаються виставити Збройні сили України в негативному світлі та дискредитувати їх в очах громадськості. Якщо ж сприймати інформацію критично й перевіряти дані в офіційних джерелах, то абсолютно нескладно зрозуміти, що ці текстові матеріали неправдиві [3, с. 71].

Показовим засобом російської пропаганди слугує виразна гіперболізація, як-от у фейкових новинах про те, що на Херсонщині був дуже великий ажіотаж серед місцевих мешканців, які буцімто масово хотіли отримати документи про набуття російського громадянства. Такого типу новини характеризуються додатковими маркерами маніпуляції, а саме лексемами «*великий ажіотаж*» (підсилення контексту надає ненормативний плеоназм), «*дуже*», «*масово*» і т. і. Після окупації Маріуполя російська влада почала поширювати неправдиву інформацію, що України вже нібито «не існує», а російська армія просувається далі. Російські медіа поширювали хибні «вкиди» про те, що начебто в Запоріжжі формують списки добровольців, які прагнуть захищати місто від українських збройних сил. Зрозуміло, що подібного роду інформація видається цілком абсурдною [1, с. 277].

Ще один спосіб, який широко застосовується окупантами на тимчасово окупованих територіях, це блокування або обмеження доступу до Інтернету та інших джерел інформації, що має великий вплив на суспільство. Це дозволяє контролювати або маніпулювати інформацією, яка надходить до громадян, і є дієвим засобом безпеки для запобігання поширенню правдивої інформації. Беззаперечно, такі дії порушують право на свободу вираження думки та доступ до інформації, що є основними правами людини. Крім того, вони перешкоджають нормальному функціонуванню суспільства, оскільки багато сфер життя, включно з освітою, охороною здоров'я, бізнесом та урядовими службами, залежать від доступу до Інтернету та інших засобів комунікації.

З іншого боку, обмеження доступу до певних джерел інформації або неоприлюднення певної інформації є необхідністю для забезпечення певних аспектів національної безпеки під час війни. Однак, це питання створює певні суперечки і несприйняття в суспільстві. Тому важливо знайти баланс між потребою в захисті національної безпеки та захисті основних прав людини. Необхідно розробити і запровадити прозорі та обґрунтовані процедури для блокування або обмеження доступу до комунікаційних засобів, а також забезпечити можливість оскарження таких дій та відновлення доступу, коли це безпечно та доцільно. Крім того, важливо контролювати, щоб такі дії були тимчасовими та пропорційними, а не стали постійними або надмірними обмеженнями на свободу вираження думки та доступ до інформації [6].

Отже, зважаючи на те, що інформаційна війна може мати серйозні, а й подекуди катастрофічні наслідки для національної безпеки країни, особливо під час війни необхідно вживати невідкладні заходи і використовувати ефективні методи протидії, а саме:

– активно розвивати власні інформаційні технологій та систем, щоб забезпечити свою здатність до протидії інформаційним атакам;

– підвищувати обізнаність громадян щодо інформаційних війн та їх наслідків;

– застосовувати норми міжнародного та національного законодавства в боротьбі проти інформаційних війн, а також для притягнення до відповідальності тих, хто проводить інформаційні атаки. Створювати відповідні закони та норми, які регулюють інформаційний простір;

– співпрацювати з міжнародними партнерами для обміну інформацією, координації дій та спільної розробки стратегій протидії інформаційній агресії;

– розроблювати ефективні стратегій протидії інформаційним атакам, з урахуванням специфіки інформаційного простору та особливостей сучасних інформаційних війн;

– здійснювати постійний моніторинг інформаційного простору;

– використовувати асиметричні моделі інформаційної боротьби – непередбачувані, нестандартні методи протидії інформаційній агресії [10].

Особливої уваги потребує проблема кіберзахисту, яка вимагає системного підходу. Захист від кібератак та забезпечення цілісності та конфіденційності інформації – це безперервний процес, що вимагає постійного моніторингу, оновлення та адаптації до нових загроз [6]. В Україні розроблено Стратегію кібербезпеки, яка включає в себе ряд заходів для забезпечення кібербезпеки в країні. Ця стратегія передбачає розробку надійних систем безпеки, освіту користувачів та постійний моніторинг і оновлення заходів безпеки для відповіді на нові загрози. Крім того, Україна співпрацює з міжнародними партнерами, такими як USAID, для підвищення рівня кібербезпеки в країні.

Розвиток власних інформаційних технологій є важливим елементом стратегії України проти інформаційної війни, яку веде росія. Створення та впровадження власних програмних рішень та систем сприятимуть ефективному виявленню, блокуванню та попередженню можливих кіберзагроз. Ці технології допомагають Україні виявляти та відстежувати інформаційні атаки, а також розробляти стратегії для їх протидії. Вони також дозволяють забезпечити доступ до точної та актуальної інформації, що є важливим елементом протидії інформаційній війні. Однак, розвиток власних інформаційних технологій вимагає постійного аналізу потенційних загроз, оновлення та адаптації до нових. Тому Україна повинна продовжувати інвестувати в розвиток своїх інформаційних технологій та підвищувати свою здатність до протидії інформаційним атакам [4].

Висновки. Отже, інформаційна війна в он-лайн просторі визначається низкою складних та динамічних аспектів, що вимагають комплексного підходу до вивчення та контролю. Здійснення таких операцій стає неодмінною складовою стратегій впливу в сучасному геополітичному середовищі. В ході аналізу було виявлено, що практичні аспекти ведення інформаційної війни в он-лайн просторі визначаються широким спектром технічних, соціальних та політичних факторів.

У сучасному інформаційному полі кіберпростір відіграє головну роль у формуванні громадської думки, впливі на глобальну політику та формуванні образу країни в світі. Використання сучасних технологій, алгоритмів штучного інтелекту, а також вміння ефективно маніпулювати інформаційними потоками дозволяє надзвичайно швидко й ефективно досягати визначених стратегічних цілей: формувати погляди суспільства та його реакції на події, що відбуваються, зловживати психологічними та емоційними аспектами для впливу і маніпулювання масовим суспільством, поширювати неправдиву інформацію та багато іншого.

Загальним висновком є те, що інформаційна війна в он-лайн просторі визначається високою складністю та необхідністю вивчення та аналізу всіх її аспектів. Ефективна протидія цьому явищу вимагає поєднання технічних, правових, соціальних та політичних заходів для забезпечення цілісності та безпеки сучасного інформаційного простору.

Список використаних джерел:

1. Башманівський В. І., Шульська Н. М., Зінчук Р. С. Фейкоінструментарій ведення інформаційної війни в Україні: на матеріалі мови сучасних медіа. *Вчені записки Таврійського національного університету імені В. І. Вернадського.* 2023. №34(73). С. 274–280.

2. Солоденко Д. М. Методи ведення війни у віртуальному просторі. *Актуальні проблеми соціальних комунікацій :* матер. восьмої всеукр. студ. наук. конф. 2022. С. 116–120.

3. Шульська Н. М. Медіаманіпуляції в умовах російсько-української війни (на прикладі локальних ЗМІ). *Південний архів* (*філологічні науки*). Херсон, 2022. Вип. 90. С. 68–76.

4. Як українці створили мапу, яка розповідає про війни та протести в усьому світі. *Liveuamap*. URL: https://www.bbc.com/ukrainian/-news-55543745 (дата звернення: 27.01.2024).

5. У віртуальної війни – нове обличчя». *Детектор Медіа*. URL: https://detector.media/withoutsection/article/135987/2018-03-26-u- virtualnoi-viyny-nove-oblychchya/ (дата звернення: 27.01.2024).

6. Інформаційна війна проти України та методи її ведення. *PolUkr.* URL: https://www.polukr.net/uk/blog/2021/04/informacijna-vijna-proti-ukraini/ (дата звернення: 27.01.2024).

7. Курбан О. В. Сучасні інформаційні війни в мережевому он-лайн просторі. UKR: http://www.interinf.chnu.edu.ua/res//interinf/Inf%20vijny.pdf.

8. Невельська-Гордєєва О. Нечитайло В. Феномен «fake news» в контексті забезпечення інформаційної безпеки держави. *Вісник НЮУ імені Ярослава Мудрого. Сер. : Філософія, філософія права, політологія, соціологія*. 2022. №1(52). URL: https://doi.org/10.21564/2663-5704.52.250655 (дата звернення: 25.01.2024).

9. Федотенко К. «Інформаційна війна» та «інформаційний фронт»: наукове осмислення понять. *Вісник НЮУ імені Ярослава Мудрого. Сер. : Філософія, філософія права, політологія, соціологія*. 2023. №3(58): веб-сайт. URL: https://doi.org/10.21564/2663-5704.58.285787 (дата звернення: 24.01.2024).

10. Information Warfare and the Changing Face of War. URL: https://www.rand.org/pubs/monograph_reports/MR661.html (дата звернення: 26.01.2024).