УДК 004.9:555
DOI https://doi.org/10.32689/maup.it.2024.4.10

Денис ЄФІМОВ
старший науковий співробітник науково-дослідного відділу
перспектив розвитку та проблем супроводження моделей
операцій центру імітаційного моделювання,
Національний університет оборони України імені Івана Черняховського
***ORCID:** 0000-0002-8101-9699*

Роман ТИМОШЕНКО
кандидат технічних наук,
начальник науково-дослідного відділу перспектив розвитку
та проблем супроводження моделей операцій,
Національний університет оборони України імені Івана Черняховського
***ORCID:** 0000-0001-8069-023X*

Катерина ВОЙТЕХ
старший науковий співробітник науково-дослідної лабораторії розробки моделей видів забезпечення операцій та бойових дій науково-дослідного відділу розробки моделей операцій та бойових дій,
Національний університет оборони України імені Івана Черняховського
***ORCID:** 0000-0003-4290-1766*

ВПЛИВ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ НА СУЧАСНІ БОЙОВІ СТРАТЕГІЇ

Анотація. *У статті досліджено питання щодо впливу інформаційних технологій на сучасні бойові стратегії.*
У статті досліджено вплив інформаційних технологій на сучасні бойові стратегії.

Мета роботи *полягає у вивченні того, як новітні технологічні досягнення змінюють способи ведення бойових дій і формують нові стратегії, зокрема в контексті гібридної війни.*

Методологія *включає аналіз сучасних технологій, таких як комп'ютери, електроніка, інформаційні системи, штучний інтелект, а також їх вплив на тактику і стратегію ведення війни. Автори використовують порівняльний та історичний аналіз для оцінки трансформації військових методів за допомогою новітніх інновацій.*

Наголошено на тому, що війна, як явище, є динамічною за своєю суттю, враховуючи постійно змінювані тенденції. Сучасне геополітичне середовище та технологічний розвиток формують нові стратегії й наслідки ведення бойових дій. Сучасні методи, які активно впроваджуються, в поєднанні з традиційним розумінням війни, складають основу концепції гібридної війни. Елементи цієї концепції можна спостерігати на всіх етапах історії.

Сучасні технологічні досягнення, такі як комп'ютери, електроніка, інформаційні системи, засоби зв'язку, нові види зброї, підвищена швидкість, ефективні датчики, швидке розгортання, приховані технології, економія пального, смертоносність, космічні системи, біохімія та штучний інтелект, суттєво трансформують способи ведення війни. У цій новій системі противники використовують інформацію як засіб маніпуляції, що, в свою чергу, веде до виникнення нестабільних умов

Як висновок, сказано про те, що вплив інформаційних технологій на сучасні бойові стратегії є беззаперечним. Вони не лише трансформують традиційні підходи до ведення війни, але й відкривають нові можливості для збирання, аналізу та використання інформації. Кібербезпека, автоматизація, штучний інтелект – всі ці елементи формують нову реальність військових дій, де інформація стає не менш важливою, ніж зброя. У майбутньому, з огляду на постійний розвиток технологій, важливо буде враховувати ці зміни, аби адаптувати стратегії до нових умов ведення війни.

Наукова новизна *роботи полягає у виокремленні інформаційних технологій як ключового елемента, що визначає сучасні бойові стратегії, а також у визначенні ролі кібербезпеки та автоматизації у новій реальності військових дій.*

Висновки *свідчать, що інформаційні технології значно трансформують традиційні методи ведення війни, відкриваючи нові можливості для збирання, аналізу та використання інформації. Враховуючи швидкий розвиток технологій, майбутні стратегії повинні адаптуватися до нових умов, де інформація стає не менш важливою за зброю.*

Ключові слова: *війна, технології, штучний інтелект, прогрес, розвиток.*

Denis YEFIMOV, Roman TYMOSHENKO, Kateryna VOITEKH. THE INFLUENCE OF INFORMATION TECHNOLOGIES ON MODERN COMBAT STRATEGIES

Abstract. *The article examines the impact of information technologies on modern combat strategies.*
The article examines the influence of information technologies on modern combat strategies.

The purpose *of the work is to study how the latest technological advances change the ways of conducting military operations and form new strategies, in particular in the context of hybrid warfare.*

The methodology *includes the analysis of modern technologies, such as computers, electronics, information systems, artificial intelligence, as well as their impact on the tactics and strategy of warfare. The authors use comparative and historical analysis to assess the transformation of military methods through the latest innovations.*

It is emphasized that war, as a phenomenon, is dynamic in nature, taking into account constantly changing trends. The modern geopolitical environment and technological development shape new strategies and consequences of conducting hostilities. Modern methods, which are actively implemented, in combination with the traditional understanding of war, form the basis of the concept of hybrid war. Elements of this concept can be observed at all stages of history.

Modern technological advances such as computers, electronics, information systems, communications, new weapons, increased speed, effective sensors, rapid deployment, stealth technology, fuel economy, lethality, space systems, biochemistry, and artificial intelligence are essential transform the ways of waging war. In this new system, adversaries use information as a means of manipulation, which in turn leads to unstable conditions

As a conclusion, it is said that the influence of information technologies on modern combat strategies is undeniable. They not only transform traditional approaches to warfare, but also open new opportunities for gathering, analyzing and using information. Cyber security, automation, artificial intelligence – all these elements form a new reality of military operations, where information becomes no less important than weapons. In the future, given the constant development of technology, it will be important to take these changes into account in order to adapt strategies to the new conditions of warfare.

***The scientific novelty** of the work consists in identifying information technologies as a key element that determines modern combat strategies, as well as in determining the role of cyber security and automation in the new reality of military operations.*

***The conclusions** show that information technology significantly transforms traditional methods of warfare, opening up new opportunities for gathering, analyzing and using information. Given the rapid development of technology, future strategies must adapt to new conditions where information becomes as important as weapons.*

***Key words:** war, technology, artificial intelligence, progress, development.*

Вступ. Постановка проблеми. У наш час інформаційні технології (ІТ) стають не лише супутником, але й основою сучасних бойових стратегій. Військові конфлікти все більше переходять у цифрову площину, де інформація та її обробка відіграють ключову роль у прийнятті рішень. Від дронів до систем управління боєм, інформаційні технології змінюють саму суть війни, роблячи її більш комплексною, швидкою та ефективною.

Виклад основного матеріалу. Незважаючи на певні позитивні зміни у військово-політичній ситуації наприкінці ХХ – на початку ХХІ століття, що зменшили загрозу масштабної звичайної та ядерної війни, основний принцип політики щодо забезпечення національної безпеки й захисту національних інтересів залишається незмінним. Він полягає в активному використанні всіх можливостей держави: дипломатичних, інформаційних, військових та економічних.

З огляду на активне впровадження новітніх досягнень у сфері комунікації та інформатизації, військові фахівці надають особливого значення ролі інформаційного простору, визнаючи його важливість у розв'язанні міждержавних суперечностей і досягненні зовнішньополітичних цілей.

Враховуючи характер завдань та дій, заходи інформаційного менеджменту включають:

Залучення стратегічної комунікації – це комплекс заходів, які проводять військові сили для інформування іноземних аудиторій про позиції держави та для просування національних інтересів, впливу на інші сторони та схиляння їх до співпраці в інтересах держави. Ці заходи проводяться в координації з програмами публічної дипломатії.

Участь у засіданнях міжвідомчої групи – дорадчого органу, який створюється для забезпечення командувача всебічною ситуативною обізнаністю в зоні відповідальності. Учасники цієї групи, окрім військових, включають представників державних органів, уряду та регіональних організацій.

Забезпечення зв'язку з громадськістю – це скоординовані дії з підготовки та поширення інформації про діяльність держави, спрямовані на формування позитивного сприйняття громадянами.

Військово-цивільні операції – це заходи зі співпраці з урядовими та неурядовими організаціями й цивільним населенням для досягнення оперативних цілей. Вони можуть відбуватися до, під час або після бойових дій.

Операції в кіберпросторі – це комплекс заходів, спрямованих на вплив на об'єкти противника у кіберпросторі, які проводяться за єдиним планом для досягнення стратегічних цілей.

Війна, як явище, є динамічною за своєю суттю, враховуючи постійно змінювані тенденції. Сучасне геополітичне середовище та технологічний розвиток формують нові стратегії й наслідки ведення бойових дій.

Сучасні методи, які активно впроваджуються, в поєднанні з традиційним розумінням війни, складають основу концепції гібридної війни. Елементи цієї концепції можна спостерігати на всіх етапах історії [1, с. 52].

Термін «гібридна війна» є порівняно новим, тому немає єдиного загальноприйнятого визначення цього поняття. Суб'єктивність терміна призводить до появи різних трактувань у міжнародному контексті. Вперше цей термін ввів Вільям Дж. Немет у 2002 році, висунувши ідею про те, що гібридна війна є поєднанням синхронізованих невійськових і військово-стратегічних елементів [2, с. 73].

Еволюція війни тісно пов'язана з технологічним прогресом, який забезпечує створення вдосконаленої зброї та нових стратегій ведення бойових дій. Історично можна виділити кілька етапів цієї еволюції.

Війна першого покоління виникла після Вестфальського договору 1648 року, коли було сформульовано поняття територіального суверенітету, що заклало основи державної монополії на ведення війни.

Друге покоління війни, яке з'явилося за часів французької армії, завершилося після Першої світової війни. В цей час культурні норми порядку були збережені, а жива сила була замінена масовою вогневою потужністю, що дозволяло домінувати на полі бою. Третє покоління війни, розроблене Німеччиною під час Другої світової, ґрунтувалося на тактиці проникнення, яку Німеччина застосовувала в Першій світовій війні і яка призвела до появи танків у Другій світовій [3, с. 58].

Війна четвертого покоління, що розвивалася протягом останніх шістдесяти років, представила недержавних акторів як учасників конфлікту, чим завершила державну монополію на ведення бойових дій. Війна п'ятого покоління радикально змінила філософію ведення бойових дій, інтегруючи інструменти для сприйняття та обробки інформації. Ця ідея передбачає, що конкуренція між державами відбувається на основі маніпуляцій сприйняттям світу і політики, що призводить до нестабільності.

Інформаційні технології займають ключову роль у всіх аспектах життя сучасного суспільства. Процес інформатизації набуває все більшого поширення, впливаючи як на внутрішню, так і на зовнішню політику держав. Особливо важливу роль інформаційні технології відіграють у забезпеченні інформаційної безпеки.

Створення єдиного інформаційного простору сприяє розвитку та застосуванню інформаційної зброї, яка є важливим елементом національної безпеки. Рівень захисту держави значною мірою залежить від володіння інформаційною зброєю, її ефективності, методів використання та засобів захисту.

Нині існує безліч визначень поняття «інформаційна зброя», і жодне з них не можна вважати остаточно правильним чи неправильним. Більшість визначень базуються на переліку суб'єктів та об'єктів інформаційного впливу. Проте для кращого розуміння інформаційної зброї важливо спочатку визначити, що саме мається на увазі під терміном «зброя».

Зброя – це засоби та пристрої, які використовуються у збройних конфліктах для ураження та знищення противника. У контексті інформаційного протиборства цей термін набуває додаткового значення. За одним з визначень, інформаційна зброя – це спеціальні технології, засоби й інформація, здатні здійснювати вплив на інформаційний простір суспільства, завдаючи шкоди політичним, оборонним, економічним та іншим важливим інтересам держави.

Інформаційну зброю можна поділити на дві основні категорії: інформаційно-технічну та інформаційно-психологічну. Перший вид спрямований на вплив на технічні системи, тоді як другий має за мету вплив на людей. Інформаційна зброя може також включати технології, призначені для втручання в роботу управлінських систем противника, поширення дезінформації, а також психологічний вплив на керівництво та населення з метою отримання переваги в інформаційному протиборстві.

Інформаційна зброя має ряд особливих характеристик, що відрізняють її від інших видів зброї:

1. Керованість – здатність здійснювати вплив на об'єкти у конкретний момент і з заданою інтенсивністю.
2. Прихованість – важко визначити момент початку дії та джерело атаки.
3. Універсальність – здатність уражати різноманітні об'єкти в широкому спектрі.
4. Низька вартість створення в поєднанні з високою ефективністю застосування.
5. Доступність – легке поширення та можливість високого контролю за виконанням операцій.
6. Тривалість – можливість тривалого використання без втрати ефективності.
7. Використання в мирний час – раптове застосування можливе як під час конфліктів, так і в мирний період.

Принципова відмінність інформаційного протистояння від звичайної війни полягає в тому, що інформаційне протиборство певною мірою регулюється законодавством. Єдина мета інформаційної зброї – завдання інформаційних систем супротивника найбільшої шкоди. Досягнення цієї мети противники реалізують практично певні завдання. Інформаційна зброя відрізняється від звичайного озброєння керованістю, прихованістю, універсальністю, економічністю та тривалістю. Крім того, різні види інформаційної зброї впливають на людську психіку, управлінські та радіоелектронні системи, а також на програмно-технічне оснащення, використовуючи при цьому найбільш відповідні методи впливу. Що стосується сфери законодавства з проблеми, то можна зробити висновок, що у зв'язку із встановленням інформаційного простору та розвитком інформаційних технологій, структура українського законодавства включає в себе малу кількість нормативно-правових актів. З розвитком даного сектора база офіційних 37 документів буде поповнюватися, що допоможе покращити контроль за процесом регулювання проведення інформаційного протиборства.

Цілісність сучасного світу забезпечується в основному за рахунок інтенсивного інформаційного обміну. Інформаційна зброя здатна призупинити глобальні інформаційні потоки, що може призвести до

глобальної кризи. Для того, щоб розібратися в питанні застосування інформаційної зброї, необхідно виявити сферу її застосування. Найбільш широкодоступною областю є світові інформаційні мережі. Світові інформаційні мережі – це сукупність електронно-обчислювальних машин, що пов'язані між собою каналами телекомунікації. Такі інформаційні мережі дозволяють користувачам обмінюватися інформацією, спільно використовувати необхідні інформаційні ресурси [4].

Глобальна інформаційна мережа поділяється на загальнодоступну та спеціалізовану. Загальнодоступна мережа (Internet, електронна пошта) знаходиться у вільному та рівному доступі для звичайних користувачів. Спеціалізовані мережі є корпоративними або відомчими, тобто призначені для обмеженого кола осіб. Перша комутована мережа ARPANET розпочала своє існування у США у 1969 р. Тоді до неї було підключено лише 4 комп'ютери. На сьогоднішній день на Заході існує безліч глобальних мереж. Наприклад, BITNET – мережа, що об'єднує понад 800 колективних учасників, переважно серед університетів, коледжів і наукових центрів. Ця мережа охоплює 35 країн Європи, Азії та Америки.

Сучасні технологічні досягнення, такі як комп'ютери, електроніка, інформаційні системи, засоби зв'язку, нові види зброї, підвищена швидкість, ефективні датчики, швидке розгортання, приховані технології, економія пального, смертоносність, космічні системи, біохімія та штучний інтелект, суттєво трансформують способи ведення війни. У цій новій системі противники використовують інформацію як засіб маніпуляції, що, в свою чергу, веде до виникнення нестабільних умов.

Сучасні бойові дії характеризуються комплексною інтеграцією ІТ у різні аспекти військових операцій. У класичних війнах інформація часто була обмежена, і її збір вимагав значних зусиль.

Сьогодні ж завдяки безпілотним літальним апаратам (БПЛА), супутникам і розвідувальним системам дані про противника можна отримати в режимі реального часу. Ці технології дозволяють військовим командувачам здійснювати більш точні аналізи ситуації на полі бою, що впливає на прийняття стратегічних рішень.

Системи супутникового спостереження, наприклад, забезпечують можливість відстеження переміщень ворога, виявлення його позицій та ресурсів. Це дозволяє планувати атаки з максимальною ефективністю, скорочуючи час реакції на дії противника. У сучасній війні, де кожна секунда може стати вирішальною, швидкість обробки даних і їх аналізу є критично важливими.

Окрім фізичного ведення бойових дій, ІТ внесли значні зміни у ведення кібервійни. Кібернетичні атаки можуть призводити до збою в системах управління, знищення важливих даних або навіть до паралічу критично важливих інфраструктур. На відміну від традиційної війни, де противник вражається фізично, кібервійна діє на інформаційному рівні, що робить її менш передбачуваною [5].

Відомими прикладами є атаки на енергетичні системи та інформаційні мережі держав, що призводять до серйозних наслідків для національної безпеки.

Кіберзахист став невід'ємною частиною стратегій держав, адже втрата інформації або збої у системах можуть мати катастрофічні наслідки.

Штучний інтелект (ШІ) стає важливим інструментом у сучасних бойових стратегіях. Алгоритми машинного навчання здатні аналізувати величезні обсяги даних, виявляти патерни та робити прогнози. Це дозволяє військовим планувати операції з врахуванням ймовірних дій противника.

Крім того, ШІ застосовується у системах управління боєм, що дозволяє автоматизувати ряд завдань, зменшуючи навантаження на військовий персонал. Це також допомагає зменшити ймовірність помилок, адже рішення приймаються на основі об'єктивних даних та аналізу.

Конфлікти останніх років, такі як війна в Україні, продемонстрували важливість ІТ у бойових діях. Військові з різних країн активно використовують дрони для розвідки та нанесення ударів, а також для ведення інформаційної війни. Інформаційні технології стали важливим елементом у комунікації між підрозділами, що дозволяє забезпечити координацію дій у реальному часі [6].

Війна в Україні також показала, як соціальні медіа та інформаційні платформи можуть використовуватися для пропаганди та маніпуляції. З одного боку, технології допомагають поширювати правду про конфлікт, з іншого – можуть бути використані для дезінформації та створення паніки.

Висновки. Отже, вплив інформаційних технологій на сучасні бойові стратегії є беззаперечним. Вони не лише трансформують традиційні підходи до ведення війни, але й відкривають нові можливості для збирання, аналізу та використання інформації. Кібербезпека, автоматизація, штучний інтелект – всі ці елементи формують нову реальність військових дій, де інформація стає не менш важливою, ніж зброя. У майбутньому, з огляду на постійний розвиток технологій, важливо буде враховувати ці зміни, аби адаптувати стратегії до нових умов ведення війни.

В умовах російсько-української війни існує нагальна потреба в адекватній системній інформаційній протидії, яка повинна включати ефективні стратегії для виявлення та реагування на дезінформацію, а також сприяти розвитку інформаційної грамотності серед населення. Посилення кібербезпеки,

створення прозорих інформаційних каналів і активна комунікація є основними складовими цієї інформаційної стратегії.

Важливо вивчати міжнародний досвід, аналізувати законодавство та стратегії інших країн, які успішно протистоять інформаційним загрозам, а також впроваджувати відповідні нормативні акти та заходи в Україні. Крім того, корисним буде вивчення ефективних практично-організаційних методів виявлення та розкриття дезінформації, а також розробка механізмів співпраці з міжнародними партнерами для спільної боротьби з інформаційними загрозами.

Список використаних джерел:

1. Довгань Б. В., Мартинюк О. В. Становлення та розвиток поняття інформаційної війни. *Вісник студентського наукового товариства ДонНУ імені Василя Стуса*. 2020. № 12. С. 51–56.
2. Дунаєва Л. М. Дезінформаційні виклики під час російсько-української війни: політологічний аналіз. *Політикус* : наук. журнал. 2022. № 5. С. 73–78.
3. Жаровська І., Ортинська Н. Інформаційна війна як сучасне глобалізаційне явище. *Вісник Національного університету «Львівська політехніка»*. Серія : Юридичні науки. 2020. Т. 7, № 2. С. 56–61.
4. Hayat,R. A. B. B. I. A. Hybrid Warfare: A Challenge to National Security. *PCL Student Journal of Law*, 5(1). 2021. P. 102.
5. Solmaz, T. Hybrid warfare': one term, many meanings. Small Wars Journal, 25. 2022.
6. Steingartner W., Galinec D. Cyber threats and cyber deception in hybrid warfare. *Acta Polytechnica Hungarica*, 18(3). 2021. P. 25.